Universidade Federal da Bahia - UFBA
Instituto de Matemática e Estatística - IME
Programa de Pós-Graduação em Matemática - PGMAT
Tese de Doutorado

Códigos corretores de erros sobre grupos com decomposição m-abeliana

Silvina Alejandra Alderete

Salvador-Bahia
Janeiro de 2018

Códigos corretores de erros sobre grupos com decomposição m-abeliana

Silvina Alejandra Alderete

Tese de Doutorado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do título de Doutor em Matemática.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Salvador-Bahia
Janeiro de 2018

Alderete, Silvina Alejandra.

Códigos corretores de erros sobre grupos com decomposição m-abeliana / Silvina Alejandra Alderete. – Salvador: UFBA, 2018.

62 f. : il.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Tese (Doutorado) – Universidade Federal da Bahia, Instituto de Matemática e Estatística, Programa de Pós-graduação em Matemática, 2018.

Referências bibliográficas.

1. Códigos. 2. Anéis de Grupo. 3. Códigos de Grupo. 4. Grupos com decomposição m-abeliana. I. Lobão, Thierry Corrêa Petit. II. Universidade Federal da Bahia, Instituto de Matemática e Estatística. III. Título.

"Códigos Corretores de Erros sobre Grupos com Decomposição m-Abeliana"

Silvina Alejandra Alderete

Tese apresentada ao Colegiado do Programa de Doutorado em Matemática em Associação UFBA/UFAL na Universidade Federal da Bahia, como requisito parcial para obtenção do Título de Doutora em Matemática.

Banca Examinadora

Prof. Dr. Thierry Côrrea Petit Lobão (Orientador)
Universidade Federal da Bahia - UFBA

Prof.ª Dr.ª Manuela da Silva Souza
Universidade Federal da Bahia - UFBA

Profª. Drª. Carmela Sica
Universidade Federal da Bahia - UFBA

Prof. Dr. Raul Antonio Ferraz
Universidade São Paulo - USP

Prof. Dr. Marinês Guerreiro
Universidade Federal de Viçosa - UFV

Aos meus pais, Cristina e Dante, e aos meus irmãos, Melisa e Carlos.

Agradecimentos

Eternamente agradeço a Deus por não ter me dado tudo, mas ter indicado o caminho certo para conquistar mais um sonho.

Traduzir em palavras toda gratidão às pessoas que passaram pela minha vida neste período é difícil.

Gostaría de agradecer a meu orientador Prof. Thierry Petit Lobão pela paciência, atenção e dedicação. Agradeço também ao Professor Raul Ferraz da USP pelas valiosas discussões e sugestões durante o desenvolvimento da tese. Ao pessoal do seminário de Álgerba agradeço pelas conversas e sugestões. Aos funcionários do IME, obrigada pela atenção e paciência.

À banca julgadora, professores Thierry Petit Lobão, Manuela da Silva Souza, Carmela Sica, Raul Ferraz e Marinês Guerreiro, agradeço pelas sugetões e pelo privilégio de tê-los como membros da comissão julgadora.

O desenvolvimento desta teses foi apoiado inicialmente pela FAPESB e, posteriormente pela CAPES, estas agências foram fundamentais para a realização do trabalho.

Agradeço o apoio incondicional de minha família. Especialmente a meus pais, Cristina e René, minha irmã Melisa e meu irmão Carlos, obrigada pela força, a confiança, o carinho e por estar sempre presentes em cada fases de minha vida apoiando minhas decisões. Obrigada às minhas sobrinhas Sofía e Emma, e meu sobrinho Teo, simplesmente por existir, tornando minha vida mais alegre e feliz.

Agradeço ao universo por ter conspirado ao meu favor, e ter colocado no meu caminho meus amigos e colegas Elen, Jacqueline e Edward.

A Elen obrigada pela grande amizade demonstrada a cada instante, pelo apoio, pela força que me deu durante todo o doutorado. Te agradeço por me animar nos momentos mais vulneráveis, pelos momentos de diversão e pelas profundas convesas sobre a vida. Obrigada por sua disposição para nossas discussões matemáticas. Você foi e ainda é como um anjo da guarda para mim. Te admiro muito.

Agradeço a Jacqueline e Edward pela amizade e companherismo. Jacqueline obrigada por estar sempre disposta a me ajudar, escutar e conversar sobre qualquer assunto. Edy agradeço por sua disponibilidade para discutir sobre matemática a qualquer hora do dia. Jacq e Edy muito obrigada por sua disposição a me ajuda em cada uma de minhas apresentações e seminários, pela sua preocupação e por me levar no médico nos momentos

que estive doente.

A Eliane e Oscar, duas pessoas muito especiais. Agradeço pelo apoio, as conversas e conselhos. Agradeço também à familia de Eliane por ter me acolhido.

Agradeço a Manuela pela amizade, os conselhos e por suas palavras nos meus momentos de desânimo.

Agradeço também a meus colegas e amigos de pós- graduação pelos conselhos, momentos de distração, pela força, pelas conversas e por ter me recebido de forma calorosa no instituto, especialmente a Elaine, Andressa e Roberto.

A todos que de alguma forma colaboraram para o desenvolvimento deste trabalho muito obrigada!!!

"Nossa maior fraqueza está em desistir. O caminho mais certo de vencer é tentar mais uma vez."

–Thomas Edison

Resumo

Os códigos lineares são subespaços vetoriais de $\mathbb{F}^n$, em que $\mathbb{F}$ é um corpo finito. Um código de grupo (esquerda) é um código linear que pode ser interpretado como um ideal (ou um ideal á esquerda) em uma álgebra de grupo $\mathbb{F}G$, para G um grupo finito. Neste caso, diremos que o código é um G-código (ou um G-código esquerda). Em [5], Bernal, del Río e Simón apresentam um procedimento geral que decide quando um código linear $\mathcal{C}$ é um código de grupo (ou código de grupo à esquerda) e, em tal caso, é possível determinar o grupo associado ao código. Este procedimento explora o fato de que a estrutura de código de grupo de um código linear $\mathcal{C}$ está determinada pelo grupo de automorfismos por permutação, $PAut(\mathcal{C})$, determinado pelo código. Sabin e Lomonaco, em [20], mostraram que, se $\mathcal{C}$ é um G-código para G um produto semidireto de grupos cíclicos, então $\mathcal{C}$ é um código abeliano. Como uma aplicação direta do método mencionado e estendendo o resultado de Sabin e Lomonaco, em [5] se exibem os G-códigos nos quais G é um grupo que tem decomposição abeliana, e estes são códigos abelianos. Neste trabalho mostramos uma condição necessária para que G-códigos à esquerda sejam códigos de grupo abelianos. Pillado, González, Martínez, Markov e Nechaev, em [9], mostraram algumas classes de grupos que satisfazem esta decomposição. Motivados por [8], em que se apresenta o menor grupo que não tem decomposição abeliana, e com a finalidade de estender o resultado de grupos com decomposição abeliana, estudamos grupos que se decompõem em uma quantidade mínima de três subgrupos abelianos. Encontramos condições sobre estes subgrupos para determinar códigos de grupo abelianos. Verificamos que o grupo S_4 satisfaz tais condições. Estendendo ainda mais os resultados, investigamos e obtivemos condições sobre uma classe $\mathcal{G}$ de grupos que podem ser escritos como produto de subgrupos abelianos, denominamos $\mathcal{G}$ como classe dos grupos com decomposição m-abeliana, tais que os G-códigos para $G \in \mathcal{G}$ sejam códigos de grupo abeliano.

Palavras-chave: Anéis de grupo; Códigos de grupo; Códigos de grupo abeliano; Decomposição abeliana; Decomposição m-abeliana.

Abstract

Linear codes are subspaces of $\mathbb{F}^n$, $\mathbb{F}$ being a finite field. A (left) group code is a linear code that can be interpreted as a (left) ideal of a group algebra $\mathbb{F}G$, G being a finite group. In this case, we will say that the code is a (left) G-code. In [5], Bernal, del Río, and Simón, present a general procedure that decides when a linear code $\mathcal{C}$ is a group code (left group code) and, in that case, it is possible to determine the group associated with the code. This procedure explores the fact that the group code structure of a linear code $\mathcal{C}$ is determined by the group of automorphisms by permutation, $\mathrm{PAut}(\mathcal{C})$, determined by the code. Sabin and Lomonaco, in [20], proved that, if $\mathcal{C}$ is a G-code, for G a semi-direct product of cyclic groups, then $\mathcal{C}$ is an abelian code. As a direct application of the mentioned method and extending the result of Sabin and Lomonaco, in [5], the G-codes in which G is a group having abelian composition are shown. Pillado, González, Martínez, Markov e Nechaev, in [9], exhibited some classes of groups which satisfy such a decomposition. Motivated by [8], where the smallest group which does not have abelian decomposition is shown, and in order to extend the result on groups with abelian decomposition, we have investigated and obtained conditions on the class of groups $\mathcal{G}$ that can be determined by the product of the abelian subgroups, such a class we shall call the class of groups with m-abelian decomposition, such that the G-codes for G in $\mathcal{G}$ are abelian group codes.

Keywords: Group Ring; Group code; Abelian decomposition; m-abelian decomposition.

Sumário

Introdução **1**

1 Códigos Corretores de Erros **6**

1.1 Conceitos Básicos 6

1.1.1 Códigos Lineares 8

1.1.2 Código Cíclico 9

2 Códigos de Grupo **11**

2.1 Anel de Grupo 11

2.2 Códigos de Grupo 14

2.3 Uma caracterização de códigos de grupo 15

3 Códigos de Grupo Abeliano **22**

3.1 Decomposição abeliana 22

3.1.1 Outros Exemplos 23

3.2 Decomposição 3-abeliana 29

3.3 Decomposição m-abeliana 32

3.4 Extensão de corpos 38

4 Exemplos **41**

4.1 Códigos sobre S_3 41

4.2 Códigos sobre S_4 47

5 Da aplicação dos resultados obtidos a grupos com decomposição m-abeliana **55**

Conclusão **58**

Bibliogrfía **60**

pag-final **62**

Introdução

A Teoria dos Códigos Detetores e Corretores de Erros se origina em 1948 com os trabalhos de Claude Shannon nos Laboratórios Bell [22]. Esta teoria apresenta várias aplicações, tanto científicas como tecnológicas nas quais uma mensagem é codificada, transmitida por um emissor através de um canal de comunicação, decodificada e entregue ao receptor. A ideia de codificar a informação antes de ser transmitida surge da necessidade de comprimir informações para diminuir o tempo e o espaço para executar uma comunicação, garantir a confiabilidade dos dados a serem transmitidos e finalmente recuperar a mensagem original, de modo tal que seja possível corrigir ou detectar os eventuais erros.
Em essência, um Código Detector e Corretor de Erros, também chamado Código de Erro, é um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar que permita, ao recuperar a informação, detectar e/ou corrigir erros [18], [16]. Esta última ideia é o que se conhece como teoria de códigos detectores e corretores de erros. Esta teoria se efetiva no ambiente da comunicação por intermédio de um canal o qual pode possuir interferências as quais chamamos de ruídos, que muitas vezes provocam os erros de transmisão.

Seja $\mathcal{A}$ um conjunto finito, o qual chamaremos de **alfabeto**. Um **código de erro** é um subconjunto próprio de $\mathcal{A}^n$, onde $\mathcal{A}^n$ representa o conjunto de todas as palavras de n letras, para algum natural n. Um código $\mathcal{C}$ sobre um alfabeto $\mathcal{A}$ possui três parâmetros fundamentais, $[n, M, d]$, que são respectivamente; o seu **comprimento**, o **número de elementos** de $\mathcal{C}$ e sua **distância mínima**, sendo que a distância entre duas palavras é o número de posições em que estas diferem. Se $\mathcal{C}$ é um código com distância mínima d, então $\mathcal{C}$ pode corrigir até $\left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d-1$ erros.

Para ter boas propriedades de decodificação, um código deve possuir uma distância mínima grande, mas também um número de palavras, M, suficientemente grande. Além disso, um código de comprimento, n, excessivo provoca gastos adicionais no canal e, portanto, menor eficiência na comunicação. Logo, os parâmetros (n, M, d) entram em conflito. Assim, consideraremos um bom código quando é obtido um equilíbrio entre n, M e d. Encontrar códigos com bons parâmetros não é suficiente; precisamos também que os processos de codificação e decodificação sejam rápidos. Por isso, é importante que os códigos possuam uma estrutura algébrica. Associamos o conjunto finito $\mathcal{A}$ com q elementos

com um corpo finito $\mathbb{F} = \mathbb{F}_q$ e, para cada número natural n, um $\mathbb{F}$-espaço vetorial $\mathbb{F}^n$ de dimensão finita n. Um código $\mathcal{C} \subset \mathbb{F}^n$ é dito **linear** se $\mathcal{C}$ for um subespaço vetorial de $\mathbb{F}^n$. Diremos que um código linear $\mathcal{C} \subset \mathbb{F}^n$ é **cíclico** se, para todo $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathcal{C}$, o vetor $(v_1, v_2, \ldots, v_{n-1}, v_0) \in \mathcal{C}$.

Diversas classes de códigos podem ser vistas como ideais em álgebras de grupos ou em várias classes de anéis, [3], [4], [12],[13].

A conexão entre códigos e anéis de grupo pode ser observada através da correspondência entre códigos cíclicos e ideais da álgebra de grupo $\mathbb{F}C_n$ de um corpo finito $\mathbb{F}$ sobre o grupo cíclico C_n de n elementos. Essa conexão permite estender a noção de código para um grupo finito G arbitrário. Um **código de grupo** é um ideal da álgebra de grupo $\mathbb{F}G$. Nesse caso, dizemos que o código é um G**-código**. Famílias clássicas de códigos foram identificadas com ideais de códigos de grupo. Por exemplo, os códigos de Reed-Solomon no sentido restringido, e seus estendidos por paridade [13], e os códigos de Golay e seus estendidos por paridade [14] são códigos de grupo.

A ação do grupo simétrico S_n sobre $\mathbb{F}^n$ é fundamental para definir o grupo $PAut(\mathcal{C})$ o qual é chamado **grupo de automorfismos por permutação do código linear** $\mathcal{C}$ em $\mathbb{F}^n$. Este grupo está formado por todas as permutações de S_n que fixam o código $\mathcal{C}$. O grupo $PAut(\mathcal{C})$ será uma ferramenta importante neste trabalho pois, apesar de oferecer informação interessante sobre o código, ele é difícil de ser determinado.

Neste trabalho, estudaremos códigos de grupo. Em [5], J.J. Bernal, A. del Río e J.J. Simón apresentaram um resultado que decide quando um código linear $\mathcal{C}$ é um código de grupo à esquerda, à direita ou simplesmente um código de grupo. Em qualquer um desses casos, é possível determinar o grupo G. Assim, $\mathcal{C}$ possuirá estrutura de G-código à esquerda ou G-código à direita e, no caso de ambos, simplesmente G-código. Sabin e Lomonaco, em [20], provaram que, se $\mathcal{C}$ é um G-código, sendo G um produto semidireto de grupos cíclicos, então $\mathcal{C}$ também será um K-código, onde K é um grupo abeliano. Em [5], este resultado é estendido para uma família de grupos, tal que cada código de grupo para um grupo desta família é um código de grupo abeliano. Esta família é formada pelos grupos $G = AB$, para A e B subgrupos abelianos.

Em [8], C. G. Pillado, S. Gonzáles, V. Markov, C. Martinez e A. Nechaev mostraram que os G-códigos sobre $\mathbb{F}$ são abelianos se $\mid G \mid < 24$. Nesse trabalho, é apresentado um exemplo de um grupo de ordem 24 tal que existe um G-código que não é abeliano. Também é provado que todo p-grupo de ordem p^3 ou p^4 pertence à família dos grupos no qual todo código de grupo é um código de grupo abeliano. Além disso, é demonstrado que, mudando o corpo base, os G-códigos abelianos continuam sendo abelianos.

Neste trabalho, primeiramente investigaremos sob quais condições os G-códigos à esquerda ou à direita, com $G = AB$, são códigos de grupo abelianos.

Provou-se, em [8], que os S_4-códigos não necessariamente são códigos abelianos. Mostraremos que o grupo simétrico S_4 se decompõe como um produto mínimo de três

subgrupos abelianos. Motivados pelo caso do grupo S_4, consideramos um grupo $H = ABD$, que se decompõe como uma quantidade mínima de três subgrupos abelianos. Nosso objetivo é encontrar condições sobre A, B e D para que os H-códigos sejam códigos de grupo abelianos. Verificaremos que o S_4 é um grupo que satisfaz tais condições. Ademais, estenderemos nosso estudo para grupos da forma $K = A_1 \dots A_n$, com A_i, $i = 1, \dots, n$, subgrupos abelianos de K . Mostraremos que K-códigos são L-códigos laterais, onde $L = B_1, \dots, B_t$, com $t < n$ e B_j subgrupo abeliano para $j = 1, \dots, t$. Apresentaremos uma família de grupos que se escreve como produto de uma quantidade mínima de subgrupos abelianos e que verificam as condições de nossos resultados. A partir desta família de grupos é possível deduzir uma família de grupos nilpotentes na qual é possível determinar os códigos de grupos abelianos aplicando um número finito de vezes os resultados obtidos.

Se $\mathbb{F}$ é um subcorpo de um corpo finito $\mathbb{E}$ e $G = AB$, um grupo com A e B subgrupos abelianos, então a partir de G-códigos à esquerda sobre $\mathbb{F}$ obtemos G-códigos abelianos sobre $\mathbb{E}$.

No primeiro capítulo apresentamos e introduzimos os fatos necessários sobre códigos corretores de erros.

No segundo capítulo, definimos anéis de grupo e, em seguida, exibimos a relação entre códigos e anéis de grupo, definindo assim os códigos de grupo. Encerramos este capítulo mostrando uma caracterização dos códigos lineares que tem estrutura de código de grupo.

No terceiro capítulo, começamos apresentando grupos com decomposição abeliana e estudamos os códigos de grupo para grupos correspondentes a esta classe. Mostramos que existem grupos de ordem 24, 48, 54, 60, 64, 72, 96, 108 e 120 e de ordem 64 que possuem decomposição abeliana e analisamos um grupo de ordem 48 que não possui decomposição abeliana. Definimos a classe de grupos que possuem uma decomposição mínima em três subgrupos abelianos, que chamaremos **grupos com decomposição 3-abeliana**, e analisamos os códigos de grupo. Logo, estendemos nossa pesquisa para **grupos com decomposição m-abeliana**, isto é, grupos que se decompõem como produto de uma quantidade mínima de m subgrupos abelianos. Exibimos uma familia de grupos com decomposição m-abeliana. Finalizando o capítulo exploramos a mudança de corpos para os códigos de grupos.

No quarto capítulo apresentamos alguns exemplos comprovando a aplicação de alguns resultados. Analisamos os S_3-códigos sobre $\mathbb{F}_5$, mostramos que todo código minimal é um código abeliano e apresentamos S_3-códigos à esquerda que são códigos de grupo abelianos abelianos. Também estudamos os S_4-códigos sobre $\mathbb{F}_5$, onde S_4 é um grupo com decomposição 3-abeliana. Mostramos que existem S_4-códigos que são K_1-códigos, para K_1 um grupo com decomposição abeliana e também mostramos a existência de S_4-códigos que são K_2-códigos, onde K_2 é um grupo abeliano.

Finalmente, no quinto e último capítulo apresentamos a proposta de analisar uma

família de grupos com decomposição m-abeliana com o objetivo de aplicar os resultados obtidos iteradamente para determinar se um G-código $\mathcal{C}$, onde G é um grupo nesta família, é ou não um código abeliano. Vale entretanto ressaltar que esta é uma proposta na qual ainda estamos trabalhando, ou seja, que ainda exige formalização todavia, tudo nos levar a afirmar que ela pode ser inteiramente desenvolvida.

Capítulo 1

Códigos Corretores de Erros

Neste capítulo, introduziremos os conceitos básicos sobre a Teoria de Códigos Detectores e Correstores de Erros que serão necessários ao longo do trabalho.

A ideia básica da Teoria de Códigos Detectores e Corretores de Erros é codificar uma informação inicial, adicionando informação redundante, de forma tal que, ao receber o sinal modificado pelo ruído, seja possível, de alguma forma, recuperar a mensagem original.

1.1 Conceitos Básicos

Seja $\mathcal{A}$ um conjunto finito com q elementos o qual chamaremos **alfabeto**. Os elementos de $\mathcal{A}$ são ditos **letras** ou **dígitos**. Uma **palavra** de comprimento n é uma sequência de n letras, $x = x_1x_2...x_n$. O conjunto de todas as palavras de comprimento n é denotado por $\mathcal{A}^n$.

Definição 1.1. *Um* **código** $\mathcal{C}$ *de comprimento* n *sobre* $\mathcal{A}$ *é um subconjunto próprio de* $\mathcal{A}^n$.

Um código no qual todas as palavras possuem o mesmo comprimento é chamado **código em bloco**. Todos os códigos que estudaremos serão deste tipo. Chamaremos um código $\mathcal{C}$ de um (n, M)-código sobre o alfabeto $\mathcal{A}$ se ele tem M elementos em $\mathcal{A}^n$. Em particular, se o cardinal de $\mathcal{A}$ é q, diremos que $\mathcal{C}$ é um **código q-ário**. Nos casos onde $q = 2, 3, 4$ o código chama-se binário, ternário e quaternário, respectivamente.

Um parâmetro importante de um código é a distância entre as palavras desse código. Dados dois elementos $x = x_1x_2...x_n$ e $y = y_1y_2...y_n$ de $\mathcal{A}^n$, define-se a **distância Hamming** de x a y como:

$$d(x, y) =| \{i|x_i \neq y_i, 1 \leq i \leq n\} | .$$

Se $\mathcal{C} \subset \mathcal{A}^n$ é um código, então **a distância mínima** de $\mathcal{C}$ é dada por:

$$d = min\{d(x,y)|x,y \in \mathcal{C}, x \neq y\}.$$

Diremos que um (n,M)-código com distância mínima d é um (n,M,d)**-código**.

A distância mínima é a menor distância entre as palavras de $\mathcal{C}$ e tem um papel muito importante no momento de determinar a capacidade de correção de erros do código. Existe um critério que nos permite medir a capacidade de detecção e correção de erros. Este nos permite verificar se a palavra recebida pertence ou não ao código $\mathcal{C}$. Uma vez detectado o erro, o critério de correção será substituir a palavra recebida pela palavra do código mais próxima. Para que a correção seja possível, é necessário que não tenhamos dúvida quanto à escolha do elemento do código.

Teorema 1.2. *Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir até $k = [\frac{d-1}{2}]$ erros ou detectar até $d-1$ erros.*

Demonstração. Ver [10], Teorema 1.9. □

Observe que fixado o comprimento e o número de palavras, o melhor código é aquele com maior distância mínima. Por outro lado, um código eficiente é aquele no qual podemos transmitir um número grande de palavras e que tenha uma distância mínima d relativamente grande para ter uma boa capacidade de correção de erros. No entanto, estes parâmetros entram em conflito, já que aumentar o número de palavras de um código naturalmente diminui a distância mínima. A ideia é encontrar um equilíbrio entre estes valores. Isto é o problema principal da teoria de códigos.

Existe uma relação entre o número de palavras e o comprimento do código denominada taxa de transmissão e é dada por $\frac{log_q M}{n}$. Note que o conflito aparece quando queremos achar uma taxa grande e uma **capacidade** k alta. Assim, a ideia é fixar o comprimento e a distâcia mínima e procurar o código com maior número de palavras.

Dado um alfabeto $\mathcal{A}$, $A_q(n,d)$ é o maior dos códigos de comprimento n e distância mínima d em $\mathcal{A}^n$. Em símbolos, temos

$$A_q(n,d) = max\{M \mid \text{ existe um } (n,M,d) - \text{código em } \mathcal{A}^n\}.$$

Definição 1.3. *Um (n,M,d)-código q-ário é chamado* **ótimo** *se $M = A_q(n,d)$.*

Desta maneira, um código $\mathcal{C} \subset \mathcal{A}^n$ é ótimo se seu tamanho é máximo dentre os códigos que têm distância mínima d.

Dentre as várias limitações para $A_q(n,d)$, há a Cota de Singleton apresentada no Teorema a seguir.

Teorema 1.4. *Seja $\mathcal{C}$ um (n,M,d)-código q-ário. Então $A_q(n,d) \leqslant q^{n-d+1}$.*

Demonstração. Ver [10], Teorema 10.17. □

Nos interessa também investigar quais são os códigos que têm os mesmos parâmetros. Para isto, introduziremos o conceito de códigos equivalentes por permutação.

Considere S_n o grupo simétrico de ordem n agindo sobre $\mathcal{A}^n$ de forma natural:

$$\sigma(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

para todo $\sigma \in S_n$ e $x = (x_1, \ldots, x_n) \in \mathcal{A}^n$. Aqui estamos identificando $x = x_1 \ldots x_n$ com a n-upla $(x_1, \ldots, x_n)$.

Para um código $\mathcal{C}$, de comprimento n e qualquer $\sigma \in S_n$, defina

$$\sigma(\mathcal{C}) = \{\sigma(x) \mid x \in \mathcal{C}\}.$$

Definição 1.5. *Dois códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ de comprimento n são* **equivalentes por permutação** *se existe $\sigma \in S_n$ tal que $\sigma(\mathcal{C}_1) = \mathcal{C}_2$.*

Note que se $\mathcal{C}_1$ é um (n, M, d)-código sobre o alfabeto $\mathcal{A}$, equivalente por permutação ao código $\mathcal{C}_2$, então $\mathcal{C}_2$ também é um (n, M, d)-código sobre $\mathcal{A}$. Na pespectiva da teoria de códigos, $\mathcal{C}_1$ e $\mathcal{C}_2$ são indistinguíveis.

Definição 1.6. *Seja $\mathcal{C}$ um código de comprimento n. O* **grupo de automorfismos por permutação** *de $\mathcal{C}$ é dado por :*

$$PAut(\mathcal{C}) = \{\sigma \in S_n \mid \sigma(\mathcal{C}) = \mathcal{C}\}.$$

O grupo de automorfismos por permutação de um código nos fornece informações sobre as propriedades específicas do código, mas não é simples de calcular. Este grupo será uma ferramenta muito importante em nosso trabalho.

1.1.1 Códigos Lineares

Para simplificar os processos de codificação/decodificação e facilitar o estudo dos parâmetros, surge a necessidade de introduzir uma estrutura algébrica nos códigos. Desta forma, nascem os códigos lineares e dentro deles temos uma outra classe muito especial de códigos: os códigos cíclicos.

Antes de enunciar uma definição formal, a partir de agora vamos considerar o alfabeto $\mathcal{A}$ como um corpo finito $\mathbb{F}_q = \mathbb{F}$, com q elementos, onde q é potência de um número primo. O conjunto $\mathcal{A}^n$ corresponderá a $\mathbb{F}^n = \{(x_1, x_2, ..., x_n) | \, x_i \in \mathbb{F}_q, 1 \leq i \leq n\}$, o qual tem estrutura de espaço vetorial sobre $\mathbb{F}$. Portanto, cada sequência de $\mathcal{A}^n$, $x_1 \ldots x_n$, será identificada com o vetor $(x_1, \ldots, x_n)$.

Definição 1.7. *Um* **código linear** $\mathcal{C}$ *de comprimento* n *é um subespaço vetorial de* $\mathbb{F}_q^n$, *de dimensão* m, *com* $m < n$.

Uma primeira vantagem que os códigos lineares oferecem é a facilidade no cálculo da sua distância mínima, pois um código linear $\mathcal{C}$ é um subespação vetorial e, claro, $0 \in \mathcal{C}$. Isto motiva a seguinte definição:

Definição 1.8. *Dado o elemento* $x \in \mathcal{C}$, *o* **peso de** x *é dado por:*

$$\omega(x) = d(x, 0) =| \{i \mid x_i \neq 0,\ 1 \leq i \leq n\} |$$

e o **peso de um código** $\mathcal{C}$ *é dado por:*

$$\omega(\mathcal{C}) = min\{\omega(x) \mid x \in \mathcal{C},\ x \neq 0\}.$$

Se $\mathcal{C}$ é um código linear, $d(\mathcal{C}) = \omega(\mathcal{C})$. O problema principal da teoria de códigos admite uma versão análoga para códigos lineares, isto é, dados n e d, o que se procura é um código linear eficiente que tenha o máximo de palavras. Se denota por $B_q(n, d)$ o número máximo de palavras que pode ter um código linear em $\mathbb{F}^n$ com distância mínima d. É evidente que $B_q(n, d) \leqslant A_q(n, d)$. A cota de Singleton para códigos lineares é dada pelo Corolário a seguir.

Corolário 1.9. *Se* $\mathcal{C} \subseteq \mathbb{F}^n$ *é um código linear com dimensão* m *e distância mínima* d, *então*

$$d \leqslant n - m + 1.$$

Demonstração. Ver [16], Corolario 4 do Teorema 14. □

Exemplo 1.10. *O código* $\mathcal{C} = \{(a, \ldots, a) \in \mathbb{F}^n \mid a \in \mathbb{F}\}$ *é chamado* **código de repetição** *de comprimento* n. *Neste caso note que* $PAut(\mathcal{C}) = S_n$.

Exemplo 1.11. *O conjunto* $\mathcal{C} = \{0000,\ 1011,\ 0110,\ 1101\}$ *é um subespaço vetorial de* $\mathbb{Z}_2^4$. *O conjunto* $\mathcal{B} = \{1011,\ 1101\}$ *é uma base de* $\mathcal{C}$. *Note que* $\omega(1011) = 3$, $\omega(0110) = 2$ *e* $\omega(1101) = 3$, *Portanto, a distância mínima de* $\mathcal{C}$ *é 2. Logo,* $\mathcal{C}$ *é um* $(2, 4, 2)$*-código*

1.1.2 Código Cíclico

Dentro da Teoria de Códigos, a família dos códigos cíclicos é uma das mais pesquisadas. Esta família possui propriedades algébricas que facilitam a codificação e decodificação. Este tipo de código é fundamental para a construção de outras famílias como os códigos não lineares e os códigos abelianos.

Definição 1.12. *Um código linear* $\mathcal{C}$ *é chamado* **código cíclico** *se, para toda palavra* $(x_0, x_1, ..., x_{n-1}) \in \mathcal{C}$, *o vetor* $(x_{n-1}, x_0, ..., x_{n-2}) \in \mathcal{C}$.

Observe que é possível identificar as palavras de um código cíclico de comprimento n sobre $\mathbb{F}$ com um polinômio de uma variável de grau menor que n em $\mathbb{F}[x]$. Para isto, definiremos um isomorfismo entre o anel quociente de polinômios $\dfrac{\mathbb{F}[x]}{\langle x^n - 1\rangle}$ e o espaço vetorial $\mathbb{F}^n$ e, a partir deste isomorrfismo, é possível identificar cada código cíclico com um ideal do anel quociente. De fato, note que dado o homomorfismo

$$\phi : \mathbb{F}^n \longrightarrow \frac{\mathbb{F}[x]}{\langle x^n - 1\rangle}$$

tal que $(a_0, a_1, ..., a_{n-1}) \mapsto [a_0 + a_1x + ... + a_{n-1}x^{n-1}]$ então

- ϕ é um isomorfismo de $\mathbb{F}$-espaços vetoriais.
- $\phi(a_{n-1}, a_0, ..., a_{n-2}) = \phi(a_0, a_1, ..., a_{n-1})[x]$.
- Dado $\mathcal{C}$ um código linear,
  $C \subset \mathbb{F}^n$ é cíclico se, e somente se, $\phi(\mathcal{C})$ é um ideal de $\dfrac{\mathbb{F}[x]}{\langle x^n - 1\rangle}$.

Portanto, estudar códigos cíclicos de comprimento n sobre $\mathbb{F}$ é equivalente a estudar ideais do anel quociente $\dfrac{\mathbb{F}[x]}{\langle x^n - 1\rangle}$.

Capítulo 2

Códigos de Grupo

Começaremos este capítulo apresentando a definição de um anel de grupo. O leitor interessado pode buscar informações adicionais em [17]. Consideramos neste trabalho somente anéis R associativos com unidade.

2.1 Anel de Grupo

Sejam R anel com unidade e G um grupo. Denotamos por RG o conjunto de todas as combinações lineares formais da forma:

$$\sum_{g \in G} \alpha_g g,$$

com $\alpha_g \in R$ e $\alpha_g = 0$, salvo para um número finito.

Daremos estrutura de anel com unidade a este conjunto definindo:

- soma de dois elementos em RG:

$$\left(\sum_{g \in G} \alpha_g g\right) + \left(\sum_{g \in G} \beta_g g\right) = \sum_{g \in G} (\alpha_g + \beta_g) g.$$

- produto de dois elementos em RG:

$$\left(\sum_{g \in G} \alpha_g g\right) \cdot \left(\sum_{h \in G} \beta_h h\right) = \sum_{g,\, h \in G} \alpha_g \beta_h \, gh.$$

- a unidade em RG:

$$1_{RG} = \sum_{g \in G} \alpha_g g,$$

  onde $\alpha_{1_G} = 1$ e $\alpha_g = 0$ se $g \neq 1_G$.

- O produto de um elemento de RG por um elemento $r \in R$

$$r\left(\sum_{g\in G}\alpha_g g\right) = \sum_{g\in G}(r\alpha_g)g.$$

Com as operações acima, RG é um R-módulo. Além disso, se R é comutativo então RG é uma álgebra sobre R.

Definição 2.1. *O conjunto RG com as operações definidas acima é chamado* **anel de grupo** *de G sobre R. No caso em que R seja comutativo, RG é uma álgebra com o produto chamado* **álgebra de grupo** *de G sobre R.*

Dado um elemento, $\alpha = \sum_{g\in G}\alpha_g g \in RG$, definimos o **suporte** *de α como o subconjunto de elementos de G que aparecem na expressão de α, isto é,*

$$supp(\alpha) = \{g \in G \mid \alpha_g \neq 0\}.$$

Recordamos que um elemento e no anel R é chamado **idempotente** se $e^2 = e$. Dois idempotentes e_1 e e_2 são chamados **ortogonais** se $e_1 \cdot e_2 = 0$. Um idempotente e é chamado **primitivo** se não existem idempotentes ortogonais e_1 e e_2 não nulos tais que $e = e_1 + e_2$. Um conjunto de idempotentes de um anel com unidade $\{e_1, \ldots, e_n\}$ é um **conjunto completo de idempotentes primitivos ortogonais** se $e_1 + \cdots + e_n = 1$, cada e_i é primitivo e $e_i \cdot e_j = 0$, se $i \neq j$, $1 \leq i, j \leq n$.

Um anel R é **simples** ou irredutível se R é não nulo e seus únicos ideais são o nulo e o anel todo. O anel R é dito **semissimples** se todo ideal de R é somando direto de R e, neste caso, cada ideal é gerado por um idempotente.

Podemos usar idempotentes para obter a clássica decomposição de Pierce, isto é, decompor o anel semissimples R como soma direta de ideis minimais à esquerda. Lembremos também que cada ideal bilateral minimal é uma componente simples de R e é obtido somando todos os ideais à esquerda minimais isomorfos entre si. Assim, a decomposição do anel semissimples R como soma direta de ideais bilaterais minimais é única. Dado que cada ideal bilateral é um ideal à esquerda, então cada componente simples também é gerada por um idempotente. Observe que não basta dizer que todo ideal é gerado por um idempotente. É importante saber se o número de idempotentes que geram as componentes simples do anel R é finito. O conjunto de idempotentes que geram os ideais minimais bilaterais é chamado **conjunto completo de idempotentes ortogonais centrais primitivos** de R.

O próximo resultado determina uma condição necessária e suficiente sobre R e G para que o anel de grupo RG seja semissimples.

Teorema 2.2. *(***Teorema de Maschke***) Se G é um grupo, então o anel de grupo RG é semissimples se, e somente se, as seguintes condições são satisfeitas:*

(i) R é um anel semissimples.

(ii) G é finito.

(iii) $|G|$ é invertível em R.

Demonstração. Ver [16], Teorema 3.4.7. □

O caso em que o anel é um corpo tem uma particular importância.

Corolário 2.3. *Sejam G um grupo finito e K um corpo. Então KG é semissimples se, e somente se, $char(K)$ não divide $|G|$.*

Demonstração. Ver [16], Corolario 3.4.8. □

Corolário 2.4. *Se G é um grupo abeliano finito e K é um corpo tal que $char(K)$ não divide $|G|$, então KG é soma direta de corpos.*

Demonstração. Ver [16], Corolario 3.5.6. □

Um ideal em RG é dito idecomponível se é diferente de 0 e se não pode ser escrito como soma direta de ideais não nulos.

Em termos de anéis de grupo temos:

Teorema 2.5. *Dados R um anel, G um grupo e e um idempotente de RG, são equivalentes:*

(i) e é primitivo.

(ii) RGe é indecomponível.

Assim, um anel de grupo RG é semissimples se existir um conjunto completo de idempotentes centrais primitivos ortogonais $\{e_1, \ldots, e_m\}$ tais que

$$RG = RGe_1 \oplus \cdots \oplus RGe_m.$$

Da mesma forma que para anéis, estudar a decomposição semissimples de um anel de grupo RG nos leva a estudar os idempotentes centrais primitivos de RG.

Apresentamos um interessante idempotente obtido a partir de um subgrupo do grupo G em RG.

Definição 2.6. *Dado H um subgrupo finito de um grupo G com $\mid H \mid$ invertível, definimos o elemento $\widehat{H}$ em RG por*

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h.$$

Proposição 2.7. *Sejam R um anel e H um subgrupo finito de um grupo G. Se $|H|$ é inversível em R, então $\widehat{H}$ é um idempotente de RG. Além disso, se H é um subgrupo normal em G, então $\widehat{H}$ é central.*

Demonstração. Ver [16], Lema 3.6.6. □

Observação 2.8. *Chamaremos* **idempotente principal** *de RG o elemento $\widehat{G}$.*

2.2 Códigos de Grupo

Vimos no capítulo anterior que um código linear $\mathcal{C}$ é cíclico se é fechado para permutações cíclicas. Além disso, se $\mathcal{C}$ possui comprimento n sobre $\mathbb{F}$, então $\mathcal{C}$ pode ser identificado com um ideal do anel $\dfrac{\mathbb{F}[x]}{< x^n - 1 >}$. Dada a álgebra de grupo $\mathbb{F}C_n$, com $C_n = \langle a \rangle$ um grupo cíclico de ordem n, é possível construirmos um isomorfismo de anéis entre $\mathbb{F}C_n$ e o anel de polinômio $\dfrac{\mathbb{F}[X]}{\langle x^n - 1 \rangle}$. Este isomorfismo é determinado pelo seguinte homomorfismo de anéis,

$$\begin{array}{rcl} \psi : \mathbb{F}[x] & \longrightarrow & \mathbb{F}C_n \\ f(x) & \mapsto & f(a) \end{array}$$

Por conseguinte, $\mathbb{F}^n$ é isomorfo como espaço vetorial a $\mathbb{F}C_n$. Assim, um código cíclico de $\mathbb{F}^n$ é associado a um ideal de $\mathbb{F}C_n$. Deste modo, o estudo de códigos cíclicos de comprimento n sobre $\mathbb{F}$ é equivalente ao estudo de ideais de $\mathbb{F}_qC_n$.

Em geral, códigos são identificados com ideais de álgebras de grupo onde o grupo não necessariamente é cíclico.

Sejam $\mathbb{F}$ um corpo finito com q elementos, $\mathcal{E}_n = \{e_1, e_2, \ldots, e_n\}$ a base canônica do espaço ambiente $\mathbb{F}^n$ e $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Dado $\mathcal{C} \subseteq \mathbb{F}^n$ um código linear, definimos:

Definição 2.9. *Dado um grupo G de ordem n, diremos que $\mathcal{C}$ é um* **G-código à esquerda (G-código à direita ou G-código)** *se existe uma bijeção $\phi : \mathcal{E}_n \to G$ cuja extensão linear a um isomorfismo de espaços vetoriais $\phi : \mathbb{F}^n \to \mathbb{F}G$ mapeia o código $\mathcal{C}$ em $\phi(\mathcal{C})$, um ideal à esquerda (ideal à direita ou ideal bilateral respectivamente) de $\mathbb{F}G$.*

O código linear $\mathcal{C}$ define um **código de grupo à esquerda (código de grupo à direita ou código de grupo)**, *se este é um G-código à esquerda (G-código à direita ou G-código) para algum grupo G.*

Esta definição fornece uma estrutura de código de grupo em famílias já existentes cujo objetivo é conhecer melhor o código através de propriedades algébricas da álgebra de grupo. Note também que os G-códigos à esquerda (ou G-códigos à direita ou G-código) são os códigos lineares de $\mathbb{F}^n$ equivalentes por permutação a algum código $\phi^{-1}(I)$, onde I é um ideal à esquerda (ideal à direita ou ideal bilateral) de $\mathbb{F}G$.

Observação 2.10. *Em particular, os códigos de grupo cíclicos são códigos lineares equivalentes por permutação a códigos cíclicos. Não obstante, nem todo C_n-código é um código cíclico. Se consideramos o código linear $\mathcal{C} = \{(a, a, b, b) : a, b \in \mathbb{F}\}$, ele não é cíclico mas é um C_4-código. De fato, a bijeção $\phi : \mathcal{E}_4 \to C_4$ dada por $\phi(e_1) = 1$, $\phi(e_2) = g^2$, $\phi(e_3) = g$, $\phi(e_4) = g^3$, induz um isomorfismo de $\mathbb{F}$-espaços vetoriais $\phi : \mathbb{F}^n \to \mathbb{F}C_4$ tal que $\phi(\mathcal{C})$ é um ideal de $\mathbb{F}C_4$.*

2.3 Uma caracterização de códigos de grupo

Os códigos cíclicos estão caracterizados em termos de certas permutações as quais nos permitem identificar estes códigos com ideais de um álgebra de um grupo cíclico. Em um contexto mais geral de códigos de grupo, J.J. Bernal, A. Del Río e J.J. Simón, em [5], caracterizaram os códigos lineares para que pudessem ser interpretados como ideais à esquerda ou ideais bilaterais em um álgebra de grupo, para um grupo não necessariamente cíclico, em termos do grupo de automorfismos por permutação.

Um subgrupo H do grupo simétrico S_n é **transitivo** se, para quaisquer $i,\ j \in \mathbb{N}_n$, existe $h \in H$ tal que $h(i) = j$. O subgrupo H é dito **regular** se, e somente se, este é transitivo e tem ordem n, ou equivalentemente, $\mid H \mid= n$ e $\sigma(x) \neq x$, para todo $\sigma \in H$ tal que $\sigma \neq id$.

Dado um grupo G, denotamos por $\mathcal{Z}(G)$ o centro de G, e por $C_G(H)$ o centralizador de H em G, para cada H subgrupo de G.

Antes de caracterizar os códigos lineares, segue um lema que foi de grande importância ao longo do trabalho.

Lema 2.11. *([5], Lema 1.1) Sejam H um subgrupo regular de S_n, $i_0 \in \mathbb{N}_n$ fixo e $\psi : H \to \mathbb{N}_n$ a bijeção dada por $\psi(h) = h(i_0)$, para qualquer $h \in H$. Então existe um anti-isomorfismo*
$\sigma : H \to C_{S_n}(H)$ tal que $\sigma(h) = \sigma_h$, definido por

$$\sigma_h(i) = \psi^{-1}(i)(h(i_0))\,,\ i \in \mathbb{N}.$$

Ademais, $\sigma_h = h$, para todo $h \in Z(H)$ e, portanto, $Z(H) = Z(C_{S_n}(H))$.

Demonstração. Dados $H \leq S_n$ regular e $i_0 \in \mathbb{N}_n$ é sempre possível obter a bijeção $\psi : H \to \mathbb{N}_n$. Observemos que:

(I) Para cada $i \in \mathbb{N}_n$, $\psi^{-1}(i)(i_o) = i$. De fato,

$$i = \psi\underbrace{(\psi^{-1}(i))}_{\in H} \underbrace{=}_{\text{def. de } \psi} \psi^{-1}(i)(i_0). \tag{2.1}$$

(II) Para cada $h \in H$, $\psi^{-1}(h(i_o)) = h$, pois,

$$h = \psi^{-1}(\psi(h)) \underbrace{=}_{\text{def. de } \psi} \psi^{-1}(h(i_0)). \tag{2.2}$$

Sejam $h, k \in H$ e $i \in \mathbb{N}_n$. Mostremos que σ está bem definida, isto é, $\sigma(H) \subset C_{S_n}(H)$.

$$\begin{aligned}
\sigma_h(k(i)) &\underbrace{=}_{(I)} \sigma_h(k(\psi^{-1}(i)(i_0))) \\
&\underbrace{=}_{\text{def. } \sigma} \psi^{-1}(\psi^{-1}(i)(i_0))(h(i_0)) \\
&= \psi^{-1}(\underbrace{[k(\psi^{-1}(i))]}_{\in H}(i_0))(h(i_0)) \\
&\underbrace{=}_{(II)} (k\psi^{-1}(i))(h(i_0)) \\
&= k(\psi^{-1}(i)(h(i_0))) = k\sigma_h(i),
\end{aligned} \tag{2.3}$$

para todo $i \in \mathbb{N}_n$ e, assim, $\sigma_h k = k\sigma_h$. A seguir, provaremos que σ é um anti-isomorfismo. De fato,

$$\begin{aligned}
\sigma_{hk}(i) = \underbrace{\psi^{-1}(i)}_{\in H}(hk(i_0)) &\underbrace{=}_{\text{assoc. em } H} (\psi^{-1}(i)h)(k(i_0)) \\
&\underbrace{=}_{(II)} \psi^{-1}(\psi^{-1}(i)h(i_0))(k(i_0)) = \\
&\underbrace{=}_{\text{def. } \sigma} \sigma_k(\psi^{-1}(i)h(i_0)) \\
&\underbrace{=}_{\text{def. } \sigma} \sigma_k\sigma_h(i),
\end{aligned} \tag{2.4}$$

Como isto acontece para todo $i \in \mathbb{N}_n$, tem-se $\sigma_{hk} = \sigma_k\sigma_h$. Para a injetividade, note que

se $\sigma_h = id$, então $\sigma_h(i) = i$, para todo $i \in \mathbb{N}_n$. Daí,

$$\begin{aligned}(\psi^{-1}(i)h)(i_0) &\underbrace{=}_{\text{assoc. em } H} \psi^{-1}(i)(h(i_0)) \\ &\underbrace{=}_{\text{def. } \sigma} \sigma_h(i) \\ &\underbrace{=}_{(I)} i \\ &= \psi^{-1}(i)(i_0), \quad \forall i \in \mathbb{N}_n.\end{aligned} \tag{2.5}$$

Logo, $\psi^{-1}(i)h = \psi^{-1}(i)$, para todo $i \in \mathbb{N}_n$. Como H é um subgrupo e $\psi^{-1}(i), h \in H$, segue $h = 1_H$ e assim fica demonstrada a injetividade de σ. Já mostramos que $\sigma(H) \subset C_{S_n}(H)$, assim, para mostrar a sobrejetividade, basta verificar a inclusão $C_{S_n}(H) \subset \sigma(H)$.

Para cada $x \in C_{S_n}(H)$, tome $h = \psi^{-1}(x(i_0)) \in H$. Daí

$$\begin{aligned}h(i_0) &= \psi^{-1}(\underbrace{x(i_0)}_{\in \mathbb{N}_n})(i_0) \\ &\underbrace{=}_{(I)} x(i_0) \\ &\underbrace{=}_{(I)} x([\psi^{-1}(i)]^{-1}(i)).\end{aligned} \tag{2.6}$$

De $x \in C_{S_n}(H)$ e $[\psi^{-1}(i)]^{-1} \in H$,

$$x([\psi^{-1}(i)]^{-1}) = [\psi^{-1}(i)]^{-1}(x).$$

Como consequência,

$$\begin{aligned}h(i_0) &= x([\psi^{-1}(i)]^{-1}(i)) \\ &= (x[\psi^{-1}(i)]^{-1})(i) \\ &= [\psi^{-1}(i)]^{-1}x(i).\end{aligned} \tag{2.7}$$

Isto implica que

$$x(i) = \psi^{-1}(i)h(i_0) = \sigma_h(i),$$

para todo $i \in \mathbb{N}_n$. Daí, $x = \sigma_h$. Se $x \in Z(H) = H \cap C_{S_n}(H)$, temos $h = x = \sigma_h$, o que prova a última afirmação.

□

Em [5], apresentou-se uma caracterização dos códigos lineares que têm estrutura de códigos de grupo. Essa caracterização depende puramente das propriedades do código como subespaço de $\mathbb{F}^n$ e é dada em termos do grupo dos automorfismos por permutação.

Teorema 2.12. *([5], Teorema 2.1) Sejam $\mathcal{C}$ um código linear de comprimento n sobre o corpo $\mathbb{F}$ e G um grupo finito de ordem n.*

(a) $\mathcal{C}$ é um G-código à esquerda se, e somente se, G é isomorfo a um subgrupo transitivo de S_n contido em $PAut(\mathcal{C})$.

(b) $\mathcal{C}$ é um G-código se, e somente se, G é isomorfo a um subgrupo transitivo H de S_n tal que $H \cup C_{S_n}(H) \subseteq PAut(\mathcal{C})$.

Demonstração. Sejam $\mathcal{E}_n$ a base canônica de $\mathbb{F}^n$ e $\phi : \mathcal{E}_n \to G$, defina $f = f_\phi : G \to S_n$ tal que

$$f(g)(i) = e_{f(g)(i)} = \phi^{-1}(g\phi(e_i)). \tag{2.8}$$

A ideia é mostrar que f é um homomorfismo de grupos injetor e tomar $H = f(G)$. Sejam $g,\ g_1,\ g_2 \in G$ e $e_i \in \mathcal{E}_n$,

$$\begin{aligned} f(g_1)f(g_2)(e_i) &= f(g_1)(f(g_2)e_i) \\ &= f(g_1)(\phi^{-1}(g_2\phi(e_i))) \\ &= \phi^{-1}(g_1\phi(\phi^{-1}(g_2\phi(e_i)))) \\ &= \phi^{-1}(g_1g_2\phi(e_i)) \\ &= f(g_1g_2)(e_i), \quad \forall i \in \mathbb{N}_n. \end{aligned} \tag{2.9}$$

Se $g \in Ker(f)$, então $f(g) = 1_{S_n}$. Logo, $e_i = f(g)(e_i) = e_{f(g)(i)} = \phi^{-1}(g\phi(e_i))$. Assim, $\phi(e_i) = g\phi(e_i)$. Como G é grupo e $\phi(e_i) \in G$, $g = 1_G$. e $G \cong f(G)$. Tomando $H = f(G)$, por definição, $H \leq S_n$ e $\mid H \mid= n$. Resta-nos verificar a transitividade. Suponha que existe $1_H \neq h \in H$ tal que $h(i) = i$ para algum $i \in \mathbb{N}_n$. Dado que $h \in H = f(G)$, existe $g \in G$ distinto de e com $f(g) = h$ e, como consequência, $f(g)(e_i) = e_{f(g)(i)} = e_i$. Mas, isto contradiz a injetividade de f implicando que H é regular.

Agora introduzimos outro resultado que precisaremos na demostração. Fixe $i_0 \in \mathbb{N}_n$ de tal forma que $\phi^{-1}(1_G) = e_{i_0}$. Nas condições do Lema 2.11, existe o anti-isomorfismo $\sigma : H \to C_{S_n}(H)$, sendo $\psi : H \to \mathbb{N}_n$ uma bijeção dada por $\psi(h) = h(i_0)$ e verifica-se que $\psi^{-1}(i)(i_0) = i$ para todo $i \in \mathbb{N}_n$.

Para cada $i \in \mathbb{N}_n$,

$$\begin{aligned} e_i &\underbrace{=}_{i=\psi^{-1}(i)(i_0)} e_{\underbrace{\psi^{-1}(i)}_{\in H}(i_0)} \\ &= e_{f(f^{-1}\circ\ \psi^{-1}(i))(i_0)} \\ &= \phi^{-1}(f^{-1}\circ\psi^{-1}(i).\underbrace{\phi(e_{i_0})}_{=1_G}) \\ &= \phi^{-1}\circ f^{-1}\circ\psi^{-1}(i) \end{aligned} \tag{2.10}$$

Por (2.10) e usando o fato que $f : G \to H$ é um isomorfismo para cada $h \in H$,

$$\begin{aligned}\sigma_h(e_i) = e_{\sigma_h(i)} &\underbrace{=}_{\text{def. } \sigma_h} e_{\psi^{-1}(i)(h(i_0))} \\ &= e_{\underbrace{(\psi^{-1}(i)h)}_{\in H}(i_0)} \\ &\underbrace{=}_{(2.10)} \phi^{-1} \circ f^{-1} \circ \psi^{-1}(\psi^{-1}(i)h)(i_0).\end{aligned} \tag{2.11}$$

Como $\psi^{-1}(i)h \in H$, por definição, $\psi(\psi^{-1}(i)h) = (\psi^{-1}(i)h)(i_0)$ e daí

$$\psi^{-1}(i)h = \psi^{-1}(\psi^{-1}(i)h(i_0)).$$

Voltando a (2.11) temos

$$\begin{aligned}\phi^{-1} \circ f^{-1} \circ \psi^{-1}(\psi^{-1}(i)h)(i_0) &= \phi^{-1} \circ f^{-1}(\psi^{-1}(i)h) \\ &\underbrace{=}_{f \text{ é homo}} \phi^{-1}(f^{-1}(\psi^{-1}(i))f^{-1}(h)) \\ &\underbrace{=}_{(2.10)} \phi^{-1}(\phi(e_i)f^{-1}(h)).\end{aligned}$$

Assim,

$$\sigma_h(e_i) = \phi^{-1}(\phi(e_i)f^{-1}(h)). \tag{2.12}$$

Estendendo por linearidade (2.12) para cada $y \in \mathbb{F}^n$, obtemos

$$\sigma_h(y) = \phi^{-1}(\phi(y)f^{-1}(h)), \tag{2.13}$$

para todo $h \in H$. Sem perda de generalidade denotamos por $\phi : \mathbb{F}^n \to \mathbb{F}G$ a extensão linear de $\mathcal{E}_n \to G$.

Suponha que $\mathcal{C} \leq \mathbb{F}^n$ seja um G-código à esquerda, mostremos que $\mathcal{C}$ é isomorfo a um grupo transitivo de S_n contido em $PAut(\mathcal{C})$. Pelo que visto acima, $H \cong G$ e $H \leq S_n$ é regular. Verifiquemos que $H \subset PAut(\mathcal{C})$. Sejam $h \in H = f(G)$ e $y \in \mathbb{F}^n$. Logo, podemos escrever $h = f(g)$, para algum $g \in G$ e $y = \sum_i^n y_i e_i$, para $y_i \in \mathbb{F}$. Assim,

$$\begin{aligned}h(y) = f(g)(\sum_i^n y_i e_i) &= \sum_i^n y_i e_{f(g)(i)} \\ &= \sum_i^n y_i \phi^{-1}(g\phi(e_i)) \\ &= \sum_i^n y_i \phi^{-1}(f^{-1}(h)\phi(e_i))\end{aligned} \tag{2.14}$$

$$= \phi^{-1}(f^{-1}(h)\phi(\sum_{i}^{n} y_i e_i))$$
$$= \phi^{-1}(f^{-1}(h)\phi(y)).$$

Em particular, se $y \in \mathcal{C}$, $\phi(y) \in \phi(\mathcal{C}) \lhd_l \mathbb{F}G$,

$$h(y) = \phi^{-1}(f^{-1}(h)\phi(y)) \ \in \mathcal{C}.$$

Logo, $h(\mathcal{C}) = \mathcal{C}$.
Considere agora $\mathcal{C}$ um G-código, provaremos que G é isomorfo a um subgrupo transitivo de S_n tal que $H \cup C_{S_n}(H) \subseteq PAut(\mathcal{C})$. Por (a), só falta verficar $C_{S_n}(H) \subset PAut(\mathcal{C})$. Dado $x \in C_{S_n}(H)$, pelo Lema 2.11, existe $h \in H$ tal que $x = \sigma_h$. Daí,

$$\begin{aligned} x(\mathcal{C}) &= \sigma_h(\mathcal{C}) \\ &\underbrace{=}_{(2.13)} \phi^{-1}(\underbrace{\phi(\mathcal{C})f^{-1}(h)}_{\in\phi(\mathcal{C})}) = \mathcal{C}. \end{aligned} \tag{2.15}$$

Agora suponha que G é isomorfo a um subgrupo regular de S_n. Sem perda de generalidade, tome $G = H$, o que implica que G é regular. Seja $\phi : \mathcal{E}_n \to G$ tal que $e_{g(1)} = \phi^{-1}(g)$. Provemos que $\phi(C)$ é ideal á esquerda de $\mathbb{F}G$. Observe que acontece, para todos h, $g \in G$,

$$\begin{aligned} h\phi(e_{g(1)}) &= hg \\ &= \phi(e_{hg(1)}) \underbrace{=}_{\text{ação de } S_n \text{ em } \mathcal{E}_n} \phi(he_{g(1)}). \end{aligned}$$

Logo, $h\phi(e_i) = \phi(h(e_i))$, para todo $i \in \mathbb{N}_n$, pois G é transitivo. Por hipótese, $G \subset PAut(\mathcal{C})$ e, assim,

$$h\phi(\mathcal{C}) = \phi\underbrace{(h(\mathcal{C}))}_{\in\mathcal{C}} \in \phi(\mathcal{C}).$$

Isto mostra (a).

Para mostrar a recíproca de (b) adicione $C_{S_n}(H) \subset PAut(\mathcal{C})$ à recíproca de (a), só faltará verificar que $\phi(\mathcal{C})$ é ideal à direita de $\mathbb{F}G$. Considere$f = f_\phi : G \to S_n$ definida no começo da demonstração. Se $g \in G$, então

$$\begin{aligned} f(g)e_i &\underbrace{=}_{\text{def.}} \phi^{-1}\underbrace{(g\phi(e_i))}_{\in G} \\ &= e_{(g\phi(e_i))(1)} \\ &\underbrace{=}_{\text{ação de } S_n} ge_{\phi(e_i)(1)} \\ &\underbrace{=}_{def.} g\phi^{-1}(\phi(e_i)) = ge_i, \ \forall i \in \mathbb{N}_n. \end{aligned}$$

Logo, $f(g) = g$, para todo $g \in G$. De (2.13) temos,

$$\phi(\sigma_h(y)) = \phi(y)f^{-1}(h),\ \forall y \in \mathbb{F}^n,\ h \in H. \tag{2.16}$$

Agora, observe

$$\begin{aligned} \phi(\mathcal{C})g &\underbrace{=}_{f(g)=g} \phi(\mathcal{C})f^{-1}(g) \\ &\underbrace{=}_{2.16} \phi(\sigma_h(\mathcal{C})) \underbrace{=}_{C_{S_n}(H)\subset PAut(\mathcal{C})} \phi(\mathcal{C}). \end{aligned} \tag{2.17}$$

Portanto, $\phi(\mathcal{C})$ é ideal bilateral. □

Este resultado foi aplicado para estudar as estruturas de duas famílias importantes: os códigos de Cauchy, em [5], e os códigos afim-invariantes, em [6].

A primeira família foi introduzida por Dür em 1987, [7]. Essa é a família dos códigos MDS que estendem os códigos Reed-Solomon. A segunda família de códigos foi introduzida por Kasami, Lin e Petersom, em 1968, como uma generalização dos códigos Reed-Muller, [11].

Os códigos Reed-Solomon foram introduzidos por Irving Reed e Gus Solomon, em 1960 [19]. Estes códigos possuem boas propriedades na correção de erros e são muito utilizados para codificar informação digital como discos compactos e discos de video digital. Também foram aplicados pela NASA em comunicações espacias junto com códigos de comprimento variável.

Os códigos Reed-Muller foram introduzidos em 1954, por D. E. Muller [15]. Eles têm a propriedade de possuir uma boa capacidade de correção de erro e ser facilmente decodificavéis. Os mesmos foram aplicados para transmitir fotografias de Marte à Terra através da espaçonave Mariner 9. Atualmente, são muito aplicados no mundo globalizado onde a troca de informações ocorre a todo momento. Com eles é possível enviar informacções por longas distâncias minimizando a perda de dados.

Capítulo 3

Códigos de Grupo Abeliano

Mostramos que um código cíclico pode ser visto como um ideal da álgebra de grupo de um grupo cíclico sobre um corpo. Assim, é natural definir, de forma mais geral, códigos como ideais de uma álgebra de grupo para um grupo não necessariamente cíclico. Uma classe de grupos de interesse particular, por causa de sua simplicidade, é a classe dos grupos abelianos. A estrutura desta classe de grupos é bem conhecida e representa uma extensão significativa dos grupos cíclicos.

3.1 Decomposição abeliana

Em [20], R.E. Sabin e S.J. Lomonaco mostraram que todo código de grupo de um grupo metacíclico que cinde é um código de grupo abeliano. Estendendo este resultado, J.J. Bernal, Á del Río e J.J. Simón, em [5], apresentam uma classe de grupos que contém estritamente a família dos grupos abelianos, na qual todo código de grupo, para um grupo nesta família, é um código de grupo abeliano, obtendo assim mais uma aplicação do Teorema 2.12

Dados A e B subgrupos de um grupo G, denote por $AB = \{ab \mid a \in A,\, b \in B\}$. Lembre-se que AB é um subgrupo de G se, e somente se, $AB = BA$ e, em tal caso, $AB = BA = \langle A, B\rangle$. Esta decomposição nos leva a introduzir a seguinte definição.

Definição 3.1. *Diremos que um grupo G tem* **decomposição abeliana** *se existem dois subgrupos abelianos A e B em G tais que $G = AB$.*

Teorema 3.2. *[5] Se G é grupo finito de ordem n que tem decomposição abeliana então todo G-código é um código de grupo abeliano.*

Uma pergunta natural que surge a partir deste teorema é: Quais são as famílias de grupos que têm decomposição abeliana? A seguir, apresentamos algumas famílias de grupos que têm tal decomposição.

(a) Um grupo G é **metacíclico** se existe $N \lhd G$ cíclico tal que G/N é cíclico. Diremos que G é **metacíclico cindido**, se G é produto semidireto de dois subgrupos cíclicos. Em [20], foi provado que todo código de um grupo metabeliano é um código de grupo abeliano. Como consequência direta do Teorema 3.2, este resultado foi estendido para grupos metacíclicos.

(b) Em [21], foram estudados códigos de grupo usando grupos extra especiais e verificou-se que todo código de grupo, para um grupo nesta familia, é um código de grupo abeliano. Dado G um p-grupo, com p um número primo, sejam $\mathcal{Z}(G)$ seu centro e $\Phi(G)$ o **subgrupo de Frattini**, subgrupo dado pela intersecção de todos os subgrupos próprios maximais de G. O grupo G chama-se **extraespecial**, se $\Phi(G) = \mathcal{Z}(G) = G'$ e $\mid \Phi(G) \mid = \mid \mathcal{Z}(G) \mid = \mid G' \mid = p$. Este grupo tem ordem p^{2n+1}, para algum inteiro positivo n, e verifica-se:

   i. cada subgrupo normal abeliano maximal possui ordem p^{n+1}.

   ii. para cada subgrupo normal abeliano maximal N, existe outro subgrupo normal abeliano maximal M com $G = NM$ e $N \cap M = \mathcal{Z}(G)$.

Em [8] e [9] foram analisadas as estruturas de grupos de ordens relativamente pequena.

(c) Grupos de ordem n, para $n \in \{1, \ldots, 23\}$.

(d) Grupos de ordem $p^i q^j$, com p e q primos para $1 < i, j < 3$.

(e) Grupos de ordem p^3 e p^4, para p um número primo.

(f) Grupos de ordem 2^5.

Encontram-se, obviamente, grupos que não admitem esta decomposição. Por exemplo:

(a) Para qualquer primo p ímpar existe um grupo de ordem p^5 que não possui decomposição abeliana.

(b) S_4 é o menor grupo que não admite decomposição abeliana.

3.1.1 Outros Exemplos

Utilizando o programa GAP (Groups, Algorithms and Programming), [23], Artur Schäfer, em [21] mostrou que grupos de ordem $n < 127$ para

$$n \notin \{24,\ 48,\ 54,\ 60,\ 64,\ 72,\ 96, 108,\ 120\}$$

possuem decomposição abeliana. Exibimos grupos de ordem 24, 48, 54, 60, 64, 72, 96, 108, 120 que possuem tal decomposição e apresentamos um grupo de ordem 48 que não

possui tal decomposição.

Começamos apresentando o grupo de ordem 48 que não possui decomposição abeliana. Utilizando o GAP para mostrar este fato. Definimos o grupo dado pelo produto semidireto entre o grupo dos quatérnio

$$\mathcal{Q}_8 = \langle i,\, j \mid i^4 = 1,\ i^2 = j^2 = -1,\ i.j = k \rangle$$

e o grupo simétrico

$$S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = (1), \sigma\tau = \tau\sigma^2 \rangle.$$

Consideramos S_3 agindo em $\mathcal{Q}_8$ segundo a ação definida a seguir. Logo faremos a representação regular $\mathcal{Q}_8 \rtimes S_3$ no grupo simétrico S_{48} mostrando que este é um grupo de ordem 48 que não possui decomposição abeliana. Esclarecendo que, escolhemos este caminho, pois é a forma mais acessível para manipular o programa GAP.

Definimos a ação de S_3 em $\mathcal{Q}_8$ da seguinte forma:

$$i^\sigma = j,\ \ j^\sigma = k,\ \ k^\sigma = i,\ \ i^\tau = -j,\ \ j^\tau = -i,\ \ k^\tau = -k.$$

Assim, os geradores de S_3 e $\mathcal{Q}_8$ no grupo simétrico S_{48} estão dados por:

$$\begin{aligned} i =&(1\ \ 2\ \ 3\ \ 4)(5\ \ 6\ \ 7\ \ 8)(9\ \ 10\ \ 11\ \ 12)(13\ \ 14\ \ 15\ \ 16)(17\ \ 18\ \ 19\ \ 20)(21\ \ 22\ \ 23\ \ 24)(25\ \ 26\ \ 27\ \ 28)\\ &(29\ \ 30\ \ 31\ \ 32)(33\ \ 34\ \ 35\ \ 36)(37\ \ 38\ \ 39\ \ 40)(41\ \ 42\ \ 43\ \ 44)(45\ \ 46\ \ 47\ \ 48), \end{aligned}$$

$$\begin{aligned} j =&(1\ \ 5\ \ 3\ \ 7)(2\ \ 8\ \ 4\ \ 6)(9\ \ 17\ \ 11\ \ 19)(10\ \ 20\ \ 12\ \ 18)(13\ \ 21\ \ 15\ \ 23)(14\ \ 24\ \ 16\ \ 22)(25\ \ 29\ \ 27\ \ 31)\\ &(26\ \ 32\ \ 28\ \ 30)(33\ \ 37\ \ 35\ \ 39)(34\ \ 40\ \ 36\ \ 38)(41\ \ 45\ \ 43\ \ 47)(42\ \ 48\ \ 44\ \ 46), \end{aligned}$$

$$\begin{aligned} \sigma =&(1\ \ 9\ \ 13)(25\ \ 33\ \ 41)(2\ \ 17\ \ 22)(5\ \ 18\ \ 14)(6\ \ 10\ \ 21)(4\ \ 19\ \ 24)(7\ \ 20\ \ 16)(8\ \ 12\ \ 23)(26\ \ 37\ \ 46)\\ &(29\ \ 38\ \ 42)(30\ \ 34\ \ 45)(28\ \ 39\ \ 48)(31\ \ 40\ \ 44)(32\ \ 36\ \ 47)(3\ \ 11\ \ 15)(27\ \ 35\ \ 43), \end{aligned}$$

$$\begin{aligned} \tau =&(1\ \ 25)(2\ \ 31)(3\ \ 27)(4\ \ 29)(5\ \ 28)(6\ \ 32)(7\ \ 26)(8\ \ 30)(9\ \ 41)(10\ \ 47)(11\ \ 43)(12\ \ 45)(13\ \ 33)\\ &(14\ \ 39)(15\ \ 35)(16\ \ 37)(17\ \ 44)(18\ \ 48)(19\ \ 42)(20\ \ 46)(21\ \ 36)(22\ \ 40)(23\ \ 34)(24\ \ 38), \end{aligned}$$

Fazendo os cálculos, é possível verificar que os subgrupos abelianos de $\mathcal{Q}_8 \rtimes S_3$ possuem ordens 2, 3, 4, 6 e 8. Assim, os candidatos prováveis para decompôr $\mathcal{Q}_8 \rtimes S_3$ como produto de dois subgrupos abelianos são os subgrupos de ordem 6 e os subgrupos de ordem 8. Mas a intersecção de qualquer subgrupo de ordem 6 com um subgrupo de

ordem 8 possui ordem 2. Portanto, $\mathcal{Q}_8 \rtimes S_3 \neq AB$, com A e B abelianos e $|A|= 6$ e $|B|= 8$.

Com o auxílio do GAP, além de conseguirmos mostrar que $\mathcal{Q}_8 \rtimes S_3$ não tem decomposição abeliana, demonstramos também que o mesmo pode ser escrito como um produto de três subgrupos abelianos, dados por :

$$A = \langle -\tau \rangle, \quad B = \langle \sigma \rangle \text{ e } D = \langle j\tau \rangle,$$

com $|A|= 2$, $|B|= 3$ e $|D|= 8$. Na seguinte seção, damos nome aos grupos que se decompõem como produto de três subgrupos abelianos mas que não se decompõem como produto de dois abelianos.

Avaliamos a ideia de construir grupos de ordem 48 com decomposição abeliana. Para isto, definimos o grupo $G = (C_3 \rtimes C_2) \times C_8$, onde C_2, C_3 e C_8 são subgrupos cíclicos de ordem 2, 3 e 8 respectivamente. Notando que C_8 é um subgrupo normal em G, temos que C_2C_8 ou C_3C_8 são subgrupos e, claramente, abelianos. Note que neste casso estamos identificando $C_2 = (\{0\} \rtimes C_2) \times \{0\}$, $C_3 = (C_3 \rtimes \{0\}) \times \{0\}$ e $C_8 = (\{0\} \rtimes \{0\}) \times C_8$.Portanto, concluímos que G possui decomposição abeliana.

Observação 3.3. *Também podemos construir grupos com decomposicção abeliana de ordens* 24, 54, 60, 72, 96, 108 *e* 120. *Basta definir o grupo* $G = (C_3 \rtimes C_2) \times A$ *no qual* A *seja um grupo abeliano com a ordem apropriada.*

Utilizamos a estratégia de $\mathcal{Q}_8 \rtimes S_3$ para apresentar um grupo de ordem 64 dado pelo produto direto do grupo diedral D_4 por si mesmo. Faremos a representação regular do grupo $D_4 \times D_4$ em S_{64} e daremos sua decomposição abeliana.

Consideramos duas cópias do grupo diedral D_4 dadas por:

$$D_4^{(1)} = \langle a_1, b_1 | a_1^4 = b_1^2 = 1,\ b_1 a_1 b_1^{-1} = a_1^{-1} \rangle$$
$$D_4^{(2)} = \langle a_2, b_2 | a_2^4 = b_2^2 = 1,\ b_2 a_2 b_2^{-1} = a_2^{-1} \rangle$$

Assim, os geradores de $D_4^{(1)}$ e $D_4^{(2)}$ no grupo simétrico S_{64} são:

$$\begin{aligned} a_1 =& (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)(9\ 10\ 11\ 12)(13\ 14\ 15\ 16)(17\ 18\ 19\ 20)(21\ 22\ 23\ 24) \\ & (25\ 26\ 27\ 28)(29\ 30\ 31\ 32)(33\ 34\ 35\ 36)(37\ 38\ 39\ 40)(41\ 42\ 43\ 44) \\ & (45\ 46\ 47\ 48)(49\ 50\ 51\ 52)(53\ 54\ 55\ 56)(57\ 58\ 59\ 60)(61\ 62\ 63\ 64); \end{aligned}$$

$$b_1 = (1\ 5)(2\ 8)(3\ 7)(4\ 6)(9\ 25)(10\ 28)(11\ 27)(12\ 26)(13\ 29)(14\ 32)(15\ 31)(16\ 30)$$
$$(17\ 33)(18\ 36)(19\ 35)(20\ 34)(21\ 49)(22\ 52)(23\ 51)(24\ 50)(37\ 53)(38\ 56)$$
$$(39\ 55)(40\ 54)(41\ 57)(42\ 60)(43\ 59)(44\ 58)(45\ 61)(46\ 64)(47\ 63)(48\ 62);$$

$$a_2 = (1\ 9\ 13\ 17)(2\ 10\ 14\ 18)(3\ 11\ 15\ 19)(4\ 12\ 16\ 20)(5\ 25\ 29\ 33)(6\ 26\ 30\ 34)$$
$$(7\ 27\ 31\ 35)(8\ 28\ 32\ 36)(21\ 53\ 57\ 61)(22\ 54\ 58\ 62)(23\ 55\ 59\ 63)$$
$$(24\ 56\ 60\ 64)(37\ 41\ 45\ 49)(38\ 42\ 46\ 50)(39\ 43\ 47\ 51)(40\ 44\ 48\ 52);$$

$$b_2 = (1\ 21)(2\ 22)(3\ 23)(4\ 24)(5\ 49)(6\ 50)(7\ 51)(8\ 52)(9\ 61)(10\ 62)(11\ 63)(12\ 64)$$
$$(13\ 57)(14\ 58)(15\ 59)(16\ 60)(17\ 53)(18\ 54)(19\ 55)(20\ 56)(25\ 45)(26\ 46)$$
$$(27\ 47)(28\ 48)(29\ 41)(30\ 42)(31\ 43)(32\ 44)(33\ 37)(34\ 38)(35\ 39)(36\ 40).$$

Em seguida, consideramos os subgrupos abelianos $A = \langle a_1, a_2 \rangle$ e $B = \langle b_1, b_2 \rangle$ em S_{64} de ordem 16 e 4, respectivamente. Note que $D_4 \times D_4 \cong AB$, o que confirma que o grupo possui decomposição abeliana.

Em [5], J.J. Bernal, Á del Río e J.J. Simón, também mostraram que se G é um grupo não abeliano e p é um número primo, sob determinadas condições existe um código de grupo à esquerda que não é abeliano:

Proposição 3.4. *([5], Proposição 3.3) Para todo grupo não abeliano G e todo primo p que não divide a ordem de G, existe um G-código à esquerda sobre algum corpo de característica p o qual não é um código de grupo abeliano.*

Tendo em conta este resultado, nos perguntamos quais são as condições necessárias para que um código à esquerda seja um código de grupo abeliano. Por conseguinte, nossa pesquisa está focada em estender o Teorema 3.2 para um G-código à esquerda e alcançamos o seguinte resultado.

Teorema 3.5. *Sejam G um grupo finito de ordem n tal que $G = AB$, onde A e B são subgrupos abelianos e $\mathcal{C}$ um G-código à esquerda tal que $\sigma(B) \subset PAut(\mathcal{C})$ (ou $\sigma(A) \subset PAut(\mathcal{C})$). Então $\mathcal{C}$ é um código abeliano em que σ é o anti-isomorfismo apresentado no Lema 2.11.*

Demonstração. Seja $\mathcal{C}$ um G-código à esquerda de comprimento n. Então, pelo Teorema 2.12,

$$G \cong H,$$

onde H é um subgrupo transitivo de S_n. Note que, em particular, H é regular e

$$H \subseteq PAut(\mathcal{C}).$$

Para mostrar que $\mathcal{C}$ é um código de grupo abeliano construiremos um grupo abeliano K a partir dos subgrupos A e B. Sem perda de generalidade, tome

$$G = AB = H.$$

Pelo Lema 2.11, existe o anti-isomorfismo

$$\sigma : G \to C_{S_n}(G)$$

tal que $\sigma(A)$ e $\sigma(B)$ são subgrupos abelianos de $C_{S_n}(H)$.

Definimos o grupo

$$K = \langle A, \sigma(B) \rangle \ \leq \langle G, \sigma(B) \rangle \leq PAut(\mathcal{C}).$$

Daí, $K \subset PAut(\mathcal{C})$. Como

$$A \subseteq G \text{ e } \sigma(B) \subseteq C_{S_n}(G)$$

são subgrupos abelianos, K é abeliano. Resta provar que K é regular, isto é, $\mid K \mid = n$ e o grupo K é transitivo. Verifiquemos que $\mid K \mid = n$. Para isto, observe que

$$\mid G \mid = \frac{\mid A \mid\mid B \mid}{\mid A \cap B \mid} \text{ e que } \mid K \mid = \frac{\mid A \mid\mid \sigma(B) \mid}{\mid A \cap \sigma(B) \mid}.$$

Como σ é um anti-isomorfismo $\mid \sigma(B) \mid = \mid B \mid$, assim basta mostrar que

$$\mid A \cap \sigma(B) \mid = \mid A \cap B \mid .$$

Visto que $A \cap B \subset \mathcal{Z}(G)$ pois $G = AB$ e A, B são abelianos, pelo Lema 2.11,

$$\begin{aligned} A \cap B &= \sigma(A \cap B) \\ &= \sigma(A) \cap \sigma(B) \\ &= A \cap B. \end{aligned}$$

Intersectando estas igualdades com $\sigma(B)$ temos:

$$\begin{aligned} A \cap B \cap \sigma(B) &= (A \cap \sigma(B)) \cap B \\ &= \sigma(A) \cap \sigma(B). \end{aligned}$$

Logo, $\sigma(A) \cap \sigma(B) \subset A \cap \sigma(B)$. Por outro lado, como $A \subset G$ e $\sigma(B) \subset C_{S_n}(G)$, tem-se

$$A \cap \sigma(B) \subset \mathcal{Z}(G).$$

Se tomarmos $z \in A \cap \sigma(B)$, então $\sigma(z) \in \sigma(A)$. Mas, $\sigma(z) = z$ pois z pertence ao centro

e, daí,

$$z \in A \cap \sigma(B) \cap \sigma(A).$$

Assim,

$$A \cap \sigma(B) \subset A \cap \sigma(B) \cap \sigma(A) = A \cap (\sigma(B) \cap \sigma(A)).$$

Disso, segue que

$$A \cap \sigma(B) \subset \sigma(A) \cap \sigma(B).$$

Logo,

$$\mid A \cap \sigma(B) \mid = \mid A \cap B \mid \text{ e } \mid K \mid = \mid G \mid .$$

Em seguida, mostraremos que K é transitivo. Para isto, veremos que o único elemento em K que estabiliza $\mathbb{N}_n$ é $k = id$. Considere $i \in \mathbb{N}_n$ e $k \in K$ tais que $k(i) = i$. Como

$$K = \langle A, \sigma(B) \rangle = A\sigma(B),$$

então, para cada $k \in K$, podemos escrever

$$k = a\beta, \text{ com } a \in A, \ \beta \in \sigma(B) \text{ e } \beta = \sigma(b), \text{ para algum } b \in B.$$

Por G ser regular, existe um único $g \in G$ tal que $g(i_0) = i$. Assim,

$$\begin{aligned} g(i_0) = i &= k(i) \\ &= a\beta(i) \\ &= a\beta(g(i_0)) \\ &= a\sigma_b(\psi(g)) \\ &= a\psi^{-1}(\psi(g))b(i_0) = agb(i_0), \end{aligned}$$

com ψ e σ definidas como no Lema 2.11. Como G é regular, $g = agb$. Para $g \in G = AB$, tome

$$g = a'b', \text{ com } a' \in A \text{ e } b' \in B.$$

Observe que

$$a'b' = g = agb = aa'b'b = a'abb'$$

que implica

$$ab = 1, \ \ b^{-1} = a \ \in \ A \cap B \subset Z(G) \text{ e } b \in Z(G).$$

Logo, $\beta = \sigma_b = b$. Assim,

$$k = a\beta = ab = 1 \text{ e } k = id.$$

□

Corolário 3.6. *Sejam $\mathcal{C}$ um código linear de comprimento n sobre um corpo e G um*

grupo como no Teorema 3.5. Se $\mathcal{C}$ é um G-código à esquerda, então $PAut(\mathcal{C})$ contém um subgrupo regular abeliano de S_n.

Demonstração. Se $\mathcal{C}$ é um G-código à esquerda, pelo Teorema 3.5, $\mathcal{C}$ é um K-código abeliano, com K um grupo abeliano. Logo, pelo Teorema 2.12, existe um subgrupo regular H de S_n tal que $K \cong H$ e $H \subset PAut(\mathcal{C})$. □

3.2 Decomposição 3-abeliana

Com a finalidade de estendermos tanto o Teorema 3.2 como o Teorema 3.5, consideramos grupos que não admitem decomposição abeliana, mas que podem ser escritos como um produto mínimo de três subgrupos abelianos. Chamaremos esta nova classe de grupos como grupos com decomposição 3-abeliana. Descobrimos condiçoẽs sobre os subgrupos que melhoram o estudo dos códigos de grupos referente a grupos com decomposição 3-abeliana. Estas condições se resumem no Teorema 3.8.

Definição 3.7. *Diremos que um grupo G tem* **decomposição 3-abeliana** *se existem três subgrupos abelianos não triviais, A, B e D em G, tais que $G = ABD$ e esta decomposiçcão é mínima, isto é, G não admite decomposiçcão como produto de dois subgrupos abelianos.*

Teorema 3.8. *Seja $G = ABD$ um grupo finito que tem decomposição 3-abeliana de ordem n com A, B e D subgrupos abelianos não triviais tais que $AB \leqslant G$ e $AB \cap D \subset \mathcal{Z}(G)$. Então todo G-código é um K-código à esquerda onde K é um grupo que tem decomposição abeliana.*

Demonstração. Seja $\mathcal{C}$ um G-código de comprimento n, $\mathcal{C} \leq \mathbb{F}^n$. Pelo Teorema 2.12, temos

$$G \cong H,$$

com H um subgrupo regular de S_n tal que

$$H \cup C_{S_n}(H) \subset PAut(\mathcal{C}).$$

Sem perda de generalidade, vamos supor

$$G = ABD = H.$$

Como G é um subgrupo regular de S_n, fixando i_0, pelo Lema 2.11, existe o anti-isomorfismo

$$\sigma : G \to C_{S_n}(G)$$

tal que $\sigma(A)$, $\sigma(B)$ e $\sigma(D)$ são subgrupos abelianos de $C_{S_n}(G)$.

Defina o grupo

$$K = \langle A, B, \sigma(D) \rangle \ \leq \langle G, C_{S_n}(G) \rangle \leq PAut(\mathcal{C}).$$

Note que podemos escrever

$$K = AB\sigma(D) \text{ ou } K = B(A\sigma(D)) \text{ ou } K = A(B\sigma(D)).$$

Em qualquer dos casos, K tem decomposição abeliana.

Para verificar a regularidade de K, provaremos que $\mid K \mid = n$ e que o mesmo é transitivo. De fato, visto que σ é um anti-isomorfismo,

$$\mid \sigma(D) \mid = \mid D \mid .$$

Por outro lado,

$$\mid AB \cap \sigma(D) \mid = \mid AB \cap D \mid .$$

De fato, como $AB \cap D \subset \mathcal{Z}(G)$, então

$$AB \cap D = \sigma(AB \cap D) = \sigma(AB) \cap \sigma(D).$$

Intersectando cada termo da igualdade anterior com $\sigma(D)$, obtemos

$$\sigma(AB) \cap \sigma(D) = AB \cap D \cap \sigma(D) = (AB \cap \sigma(D)) \cap D.$$

Por conseguinte,

$$AB \cap D \subset AB \cap \sigma(D).$$

Como $AB \subset G$ e $\sigma(D) \subset C_{S_n}(G)$ então

$$AB \cap \sigma(D) \subset \mathcal{Z}(G).$$

Se agora tomarmos $z \in AB \cap \sigma(D)$, $z \in AB$ e $z \in \sigma(D)$, teremos que $\sigma(z) = z$ também pertence a $\sigma(AB)$. Daí,

$$z \in AB \cap \sigma(AB) \cap \sigma(D) = AB \cap (\sigma(AB) \cap \sigma(D)).$$

Assim,

$$AB \cap \sigma(D) \subset \sigma(AB) \cap \sigma(D) = AB \cap D.$$

Como

$$\mid G \mid = \frac{\mid AB \mid\mid D \mid}{\mid AB \cap D \mid} \text{ e } \mid K \mid = \frac{\mid AB \mid\mid \sigma(D) \mid}{\mid AB \cap \sigma(D) \mid}$$

tem-se

$$\mid G \mid = \mid K \mid = n.$$

Com o mesmo argumento do teorema anterior, a transitividade de K será constatada comprovando que o único elemento em K que estabiliza $\mathbb{N}_n$ é $k = id$. Seja $k \in K$ tal que $k(i) = i$, para todo $i \in \mathbb{N}_n$. Como $K = AB\sigma(D)$, existem $a \in A$, $b \in B$ e $d \in D$ tais que

$$k = ab\sigma_d.$$

Uma vez que G é regular, existe um único $g \in G$ tal que para $i_0 \in \mathbb{N}_n$ fixo, $g(i_0) = i$. Lembrando que ψ e σ foram definidas no Lema 2.11, temos

$$\begin{aligned} g(i_0) = i &= k(i) \\ &= ab\sigma_d(g(i_0)) \\ &\underbrace{=}_{\text{def. } \psi} ab\sigma_d(\psi(g)) \\ &\underbrace{=}_{\text{def. } \sigma} ab(\psi^{-1}(\psi(g))d(i_0)) = abgd(i_0). \end{aligned}$$

Usando novamente a justificativa de que G é regular, temos

$$g = abgd.$$

Logo, existem $\widetilde{a} \in A$, $\widetilde{b} \in B$ e $\widetilde{d} \in D$ tais que

$$\begin{aligned} g &= a\,b\,g\,d \\ \widetilde{a}\,\widetilde{b}\,\widetilde{d} &= a\,b\widetilde{a}\,\widetilde{b}\,\widetilde{d}\,d \\ (\widetilde{a}\,\widetilde{b})^{-1}(ab)^{-1}(\widetilde{a}\,\widetilde{b}) &= \widetilde{d}d\widetilde{d}^{-1} \qquad \in AB \cap D \subset \mathcal{Z}(G) \\ (\widetilde{a}\,\widetilde{b})^{-1}(ab)^{-1}(\widetilde{a}\,\widetilde{b}) &= d \\ (\widetilde{a}\,\widetilde{b})^{-1}(ab)^{-1}(\widetilde{a}\,\widetilde{b})\,d^{-1} &= 1. \end{aligned} \tag{3.1}$$

Observe que se $x = (\widetilde{a}\,\widetilde{b})^{-1}(a\,b)^{-1}(\widetilde{a}\,\widetilde{b}) \in \mathcal{Z}(G)$, então

$$x^{(\widetilde{a}\widetilde{b})^{-1}} = (a\,b)^{-1} \in \mathcal{Z}(G).$$

Como consequência,

$$\begin{aligned} d &= (a\,b)^{-1} \qquad \in \mathcal{Z}(G) \\ 1 &= abd \end{aligned} \tag{3.2}$$

Dado que $d \in \mathcal{Z}(G)$ tem-se $\sigma_d = d$. Deste modo,

$$k = ab\sigma_d = abd = 1,$$

como queríamos. □

Corolário 3.9. *Sejam $\mathcal{C}$ um código linear de comprimento n sobre um corpo e G um grupo como no Teorema 3.8. Se $\mathcal{C}$ é um G-código, então $PAut(\mathcal{C})$ contém um subgrupo regular de S_n que tem decomposição abeliana .*

Demonstração. Se $\mathcal{C}$ é um G-código à esquerda, pelo Teorema 3.8, $\mathcal{C}$ é um K-código, com K é um grupo que tem decomposição abeliana. Logo, pelo Teorema 2.12, existe um subgrupo regular H de S_n tal que $K \cong H$ e $H \subset PAut(\mathcal{C})$. □

Como nosso interesse são os códigos de grupo abelianos, consideramos a família de grupos $\mathcal{L}$ que têm uma decomposição como no Teorema 3.8. Se $G \in \mathcal{L}$, estudamos as condições para que G-códigos determinem códigos de grupo abeliano. Reunimos essas condições no seguinte resultado:

Teorema 3.10. *Seja $G = ABD$ um grupo finito 3-abeliano de ordem n com A, B e D subgrupos abelianos não triviais tais que $AB \leqslant G$ e $AB \cap D \subset \mathcal{Z}(G)$. Então todo G-código que verifica as condições do Teorema 3.5 é código de grupo abeliano.*

3.3 Decomposição m-abeliana

Seja agora $G = A_1A_2 \dots A_m$ é um grupo finito, com A_i um subgrupo abeliano para cada $1 \leqslant i \leqslant m$, tal que a decomposição em m subgrupos abelianos é mínima, isto é, o grupo G não pode ser escrito como um produto de r subgrupos abelianos com $r < m$.

Definição 3.11. *Diremos que um grupo G possui* **decomposiçi̇ão m-abeliana** *se existem m subgrupos abelianos, A_1, A_2, ..., A_m em G, tais que $G = A_1A_2 \dots A_m$ e esta decomposiçi̇ão é mínima, isto é, G não admite decomposiçi̇ão como produto de r subgrupos abelianos com $r \leq m$.*

O resultado seguinte apresenta condições sobre os A_i's para que G-códigos sejam K-códigos à esquerda (ou à diereita), onde K é um grupo escrito como produto de t subgrupos abelianos com $t < m$.

Teorema 3.12. *Sejam $G = A_1A_2 \dots A_m$ um grupo com decomposiçi̇ão m-abeliana finito, com A_i subgrupo abeliano para $1 \leqslant i \leqslant m$ e t um inteiro tal que $1 \leqslant t < m$. Se $(A_1 \dots A_t)$ e $(A_{t+1} \dots A_m)$ são subgrupos de G e $(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \subset \mathcal{Z}(G)$, então todo G-código é um K-código à esquerda para $K = B_1 \dots B_r$ um grupo com decomposição r-abeliana, onde B_i é subgrupo abeliano para $1 \leqslant i \leqslant r < t$.*

Demonstração. Seja $\mathcal{C}$ um G-código de comprimento n. Pelo Teorema 2.12, temos

$$G \cong H,$$

com $H \leqslant S_n$ transitivo tal que

$$H \cup C_{S_n}(H) \subseteq PAut(\mathcal{C}).$$

Sem perda de generalidade, suponhamos

$$G = A_1 A_2 \dots A_m = H,$$

logo G é regular e, pelo Lema 2.11, existe o anti-isomorfismo

$$\sigma : G \to C_{S_n}(G).$$

O objetivo é construir um grupo K nas condições do Teorema 2.12 para que $\mathcal{C}$ seja um $K-$código à esquerda . Sem perda de generalidade, vamos supor $t = \lceil \frac{m}{2} \rceil$, o menor inteiro imediato a $\frac{m}{2}$, e t ímpar, definamos K da seguinte forma:

$$K = \langle A_1 \dots A_t, \sigma(A_{t+1} \dots A_m) \rangle \leqslant \langle G, C_{S_n}(G) \rangle \subseteq PAut(\mathcal{C})$$

Pelo fato de $\sigma(A_i) \subseteq C_{S_n}(G)$, para cada $1 \leqslant i \leqslant m$, observe que também podemos escrever:

$$K = A_1(A_2\sigma(A_{t+1}))(A_3\sigma(A_{t+2})) \dots (A_t\sigma(A_m)), \tag{3.3}$$

com cada $A_i\sigma(A_j)$ é abeliano para cada $1 \leqslant i \leqslant t$ e cada $t+1 \leqslant j \leqslant m$. A seguir, mostraremos que $\mid K \mid = \mid G \mid$. Como σ é anti-isomorfismo,

$$\mid \sigma(A_{t+1} \dots A_m) \mid = \mid A_{t+1} \dots A_m \mid .$$

Por outro lado, como $(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \subset \mathcal{Z}(G)$, então

$$(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) = \sigma((A_1 \dots A_t) \cap (A_{t+1} \dots A_m)).$$

Se intersectamos cada lado com $\sigma(A_{t+1} \dots A_m)$, obtemos

$$\sigma((A_1 \dots A_t) \cap (A_{t+1} \dots A_m)) = ((A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m)) \cap (A_{t+1} \dots A_m).$$

Logo,

$$(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \subset (A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m).$$

Sabendo que $(A_1 \dots A_t) \subset G$ e $\sigma(A_{t+1} \dots A_m) \subset C_{S_n}(G)$ tem-se

$$(A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m) \subset \mathcal{Z}(G).$$

Se $z \in (A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m)$, então

$$\sigma(z) = z \in (A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m) \cap \sigma(A_1 \dots A_t).$$

Portanto,

$$(A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m) \subset \sigma(A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m) = (A_1 \dots A_t) \cap (A_{t+1} \dots A_m).$$

Disto decorre

$$(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) = (A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m),$$

e daí

$$\mid G \mid = \frac{\mid A_1 \dots A_t \mid\mid A_{t+1} \dots A_m \mid}{\mid (A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \mid} = \frac{\mid A_1 \dots A_t \mid\mid \sigma(A_{t+1} \dots A_m) \mid}{\mid (A_1 \dots A_t) \cap \sigma(A_{t+1} \dots A_m) \mid} = \mid K \mid .$$

Para mostrar que K é transitivo mostraremos que o único elemento que estabiliza $\mathbb{N}_n$ é a identidade. Seja $k \in K$ tal que $k(i) = i$, para todo $i \in \mathbb{N}_n$. Como $K = A_1 \dots A_t \sigma(A_{t+1} \dots A_m)$, existem $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_m \in A_m$ tais que

$$k = a_1 \dots a_t \sigma(a_{t+1} \dots a_m).$$

Usando o fato de G ser regular, existe um único $g \in G$ tal que para $i_0 \in \mathbb{N}_n$ fixo, $g(i_0) = i$.

$$\begin{aligned} g(i_0) =& i = k(i) = k(g(i_0)) = k(\psi(g)) = a_1 \dots a_t \sigma(a_{t+1} \dots a_m)(\psi(g)) = \\ =& a_1 \dots a_t \psi^{-1}(\psi(g))(a_{t+1} \dots a_m)(i_0) = a_1 \dots a_t g(a_{t+1} \dots a_m)(i_0). \end{aligned} \tag{3.4}$$

Por G ser regular,

$$g = a_1 \dots a_t g(a_{t+1} \dots a_m).$$

Tome $g = b_1 \dots b_t b_{t+1} \dots b_m$, com cada $b_i \in A_i$ para $1 \leqslant i \leqslant m$. Assim,

$$\begin{aligned} g &= a_1 \dots a_t \, g \, a_{t+1} \dots a_m \\ b_1 \dots b_m &= a_1 \dots a_t \, b_1 \dots\dots b_m \, a_{t+1} \dots a_m \\ \underbrace{(b_1 \dots b_t)^{-1}(a_1 \dots a_t)^{-1}(b_1 \dots b_t)}_{\in A_1 \dots A_t} &= \underbrace{(b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1}}_{\in A_{t+1} \dots A_m} \\ &\in A_1 \dots A_t \cap A_{t+1} \dots A_m \subset \mathcal{Z}(G). \end{aligned} \tag{3.5}$$

Então,

$$\begin{aligned}
b_1 \dots b_t =& (a_1 \dots a_t)(b_1 \dots b_t) \underbrace{(b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1}}_{\in \mathcal{Z}(G)} \\
b_1 \dots b_t =& (b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1}(a_1 \dots a_t)(b_1 \dots b_t) \\
1 =& (b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1}(a_1 \dots a_t) \qquad (3.6) \\
\underbrace{(a_1 \dots a_t)^{-1}}_{\in A_1 \dots A_t} =& \underbrace{(b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1}}_{\in A_{t+1} \dots A_m} \\
& \in A_1 \dots A_t \cap A_{t+1} \dots A_m \subset \mathcal{Z}(G).
\end{aligned}$$

Logo $a_1 \dots a_t \in \mathcal{Z}(G)$. Ainda, se

$$x = (b_{t+1} \dots b_m)(a_{t+1} \dots a_m)(b_{t+1} \dots b_m)^{-1} \in \mathcal{Z}(G)$$

então qualquer conjugado de x também pertence ao $\mathcal{Z}(G)$. Se tomarmos $y = (b_{t+1} \dots b_m)$ teremos $x^y = a_{t+1} \dots a_m \in \mathcal{Z}(G)$. Como consequência de 3.6 obtemos,

$$1 = (a_1 \dots a_t)(a_{t+1} \dots a_m).$$

Assim, $k = (a_1 \dots a_t)\sigma(\underbrace{a_{t+1} \dots a_m}_{\in \mathcal{Z}(G)}) = (a_1 \dots a_t)(a_{t+1} \dots a_m) = 1$. Desta forma, todas as condições do Teorema 2.12 se verificam e então podemos afirmar que $\mathcal{C}$ é um K-código à esquerda . Para t par, a demostração segue da mesma forma. □

Note que se, no teorema que acabamos de mostrar, trocamos G-código por G-código à esquerda ou G-código à direita, as hipóteses do teorema se enfraquesem. Assim, para compensar a perda da bilateralidade do G-código precisamos acrescentar uma condição que dependerá do grupo de automorfismos por permutação do código. Em consequência obtivemos:

Teorema 3.13. *Sejam $G = A_1 A_2 \dots A_m$ um grupo finito m-abeliano com A_i subgrupos abelianos para $1 \leqslant i \leqslant m$ e t um inteiro, com $1 \leqslant t < m$, tais que $(A_1 \dots A_t)$ e $(A_{t+1} \dots A_m)$ são subgrupos de G e $(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \subset \mathcal{Z}(G)$. Se $\mathcal{C}$ é um G-código à esquerda tal que $\sigma(A_{t+1} \dots A_m) \subset PAut(\mathcal{C})$, então $\mathcal{C}$ é um K-código à esquerda para $K = B_1 \dots B_r$ um grupo r-abeliano, onde B_i é um subgrupo abeliano, para $1 \leqslant i \leqslant r$. com σ o anti-isomorfismo apresentado no Lema 2.11.*

Demonstração. Seja $\mathcal{C}$ um G-código à esquerda de comprimento n. Pelo Teorema 2.12, sabemos que $G \cong H$, com

$$H \leqslant S_n$$

transitivo tal que $H \subseteq PAut(\mathcal{C})$. Sem perda de generalidade, suponhamos

$$G = A_1 A_2 \dots A_m = H;$$

logo G é regular e, pelo Lema 2.11, existe o anti-isomorfismo

$$\sigma : G \to C_{S_n}(G).$$

Sem perda de generalidade, vamos supor $t = \lceil \frac{m}{2} \rceil$, o menor inteiro imediato a $\frac{m}{2}$, e t ímpar. Definamos K da seguinte forma:

$$K = \langle A_1 \dots A_t, \sigma(A_{t+1} \dots A_m) \rangle \subseteq PAut(\mathcal{C}).$$

A demonstração segue da mesma maneira que a do Teorema 3.12 □

Para um grupo G e um G-código (ou um G-código à esquerda) nas condições dos teoremas anteriores, é possivel determinar se o G-código (ou G-código à esquerda) é um código de grupo abeliano aplicando repetidas vezes o Teorema 3.12 e\ou o Teorema 3.13 caso se verifiquem as hipóteses em cada passo.

Agora queremos apresentar grupos que se decompõem como produto de uma quantidade mínima de subgrupos abelianos para aplicar nossos teoremas.

Em 1965, R. Bercov e L. Moser, em [2], mostraram que o maior subgrupo abeliano de S_n tem ordem $f(n)$ onde:

(a) $f(n) = 3^m$, se $n = 3m$.

(b) $f(n) = 4 \cdot 3^{m-1}$, se $n = 3m + 1$.

(c) $f(n) = 2 \cdot 3^m$, se $n = 3m + 2$.

Em [1], M. Abért obteve limitantes para o mínimo número k tal que o grupo simétrico S_n seja o produto de k subgrupos abelianos. Ele provou que se $2^i \leqslant n \leqslant 2^{i+1}$, para algum $i \in \mathbb{N}$, então $k \leqslant 3\,i \leqslant 3(log_2\, n)$.

Agora podemos afirmar que existem grupos que se decompõem como um produto mínimo de subgrupos abelianos, mas não sabemos se eles verificam as condicões de nossos teoremas . Então consideramos a ideia de construir grupos que possuam decomposição n-abeliana. Utilizamos produto orlado (ou produto wreath) para construir grupos que verificam as hipóteses dos teoremas anteriores.

Lembremos primeiro como é definido um produto orlado. Para grupos X e Y, com $\mid Y \mid = n$, se define o **produto orlado** entre X e Y, denotado por $X\, wr\, Y$, como o produto semidireto $(\underbrace{X \times \cdots \times X}_{\text{n cópias}}) \rtimes_{\varphi} Y$, em que φ é a ação de Y em $(X \times \cdots \times X)$ dada da seguinte forma: Seja $Y = \{y_1, y_2, \dots, y_n\}$ e escrevendo $x \in X^n$ como $x = (x_{y_1}, x_{y_2}, \dots, x_{y_n}), temos$:

$$y^{-1}(x_{y_1}, x_{y_2}, \ldots, x_{y_n})y = (x_{y_1y^{-1}}, x_{y_2y^{-1}}, \ldots, x_{y_ny^{-1}}).$$

Uma aplicação importante do produto orlado é que podemos determinar os p-subgrupos de Sylow do grupo simétrico S_{p^r}, com r um inteiro positivo não nulo e p um número primo. Assim, pode-se também construir os p-subgrupos de Sylow de S_n, como o produto orlado iterado do grupo cíclico C_p de ordem p.

A título de exemplo, observemos primeiro como se comporta o produto orlado de três grupos cíclicos:

$$\begin{aligned} W = (C_p \, wr \, C_p) \, wr \, C_p &= [(\underbrace{C_p \times \cdots \times C_p}_{\text{p vezes}}) \rtimes C_p] \, wr \, C_p \\ &= \{[(C_p \times \cdots \times C_p) \rtimes C_p] \times \cdots \times [(C_p \times \cdots \times C_p) \rtimes C_p]\} \rtimes C_p \\ &= \{[\underbrace{(C_p \times \cdots \times C_p)^{\bullet_1} \times \cdots \times (C_p \times \cdots \times C_p)^{\bullet_p}}_{=A}] \rtimes (\underbrace{{C_p}^{\bullet_1} \times \cdots \times {C_p}^{\bullet_p}}_{=B})\} \rtimes \underbrace{C_p}_{=D}, \end{aligned}$$

onde as notações ${C_p}^{\bullet_i}$ e $(C_p \times \cdots \times C_p)^{\bullet_i}$ indicam que o grupo cíclico C_p na posição i age sobre $C_p \times \cdots \times C_p$, na posição i, para cada $i = 1, \ldots, n$. Por consequência, W é um produto de três grupos abelianos. Observe que AB é um subgrupo de W e $AB \cap D = \{id\} \subseteq \mathcal{Z}(W)$.

Podemos estender esta noção para um número finito de produtos orlados entre grupos cíclicos C_p de ordem p. Mostraremos que se $W = C_p \, wr \, \ldots \, wr \, C_p$, o produto orlado de n grupos C_p, então W pode ser escrito como um produto de n subgrupos abelianos e esta decomposição é mínima.

Proposição 3.14. *Seja $W = C_p \, wr \, \ldots \, wr \, C_p$, o produto orlado de n grupos C_p, então W possui decomposição n-abeliana.*

Demonstração. Provaremos por indução sobre o número de grupos $n \geqslant 2$.
Se $n = 2$,

$$W = C_p \, wr \, C_p = (Cp \times \cdots \times Cp) \rtimes Cp$$

é o produto de dois grupos abelianos. Suponha que a propriedade seja verdadeira para k grupos quaisquer, com $k < n$. Provemos que vale para n. Seja $t = \lceil \frac{n}{2} \rceil$ tal que $n = t + m$ com $m = t$, se n é par, e $m = t - 1$, se n é ímpar. Logo

$$W = C_p \, wr \ldots wr \, C_p \cong (\underbrace{C_p \, wr \ldots wr \, C_p}_{t}) wr \, (\underbrace{C_p \, wr \ldots wr \, C_p}_{m}).$$

Como m e t são menores que n, pela hipótese de indução, temos

$$\underbrace{(C_p\, wr \ldots wr\, C_p)}_{t} \cong \{[(A_1 \rtimes A_2) \rtimes A_3] \rtimes \cdots \rtimes A_{t-1}\} \rtimes A_t = H_t,$$

$$\underbrace{(C_p\, wr \ldots wr\, C_p)}_{m} \cong \{[(B_1 \rtimes B_2) \rtimes B_3] \rtimes \cdots \rtimes B_{m-1}\} \rtimes B_m = K_m,$$

com A_i e B_j subgrupos abelianos. Logo,

$$W = H_t\, wr\, K_m = (\underbrace{H_t \times \cdots \times H_t}_{|K_m|}) \rtimes K_m.$$

Denote por

$$H_i = \{[(A_1 \rtimes A_2) \rtimes A_3] \rtimes \cdots \rtimes A_{i-1}\} \rtimes A_i.$$

Se $\mid K_m \mid = s$, então

$$(\underbrace{H_i \times \cdots \times H_i}_{s}) = (H_{i-1}^{\bullet_1} \times \cdots \times H_{i-1}^{\bullet_s}) \rtimes (A_i^{\bullet_1} \times \cdots \times A_i^{\bullet_s}),$$

onde a notação $A_i^{\bullet_j}$ e $H_{i-1}^{\bullet_j}$, para $2 \leq i \leqslant t$, é definida como no caso anterior. Como consequência

$$\begin{aligned}&(H_t \times \cdots \times H_t) = \\ &=((((A_1 \times \cdots \times A_1) \rtimes (A_2 \times \cdots \times A_2)) \rtimes (A_3 \times \cdots \times A_3)) \rtimes \ldots) \rtimes (A_t \times \cdots \times A_t).\end{aligned}$$

Deste modo, W é um produto de $t + m = n$ subgrupos abelianos. □

Da forma que o grupo W foi construído, verifica-se que $(\underbrace{H_t \times \cdots \times H_t}_{s})$ e K_m são subgrupos de W tais que $(H_t \times \cdots \times H_t) \cap K_m = \{0\} \subset \mathcal{Z}(\mathcal{W})$.

Notemos que os p-subgrupos de Sylow do grupo simétrico S_{p^r} possuem ordem $N_r = p^r + p^{r-1} + \cdots + 1$. Como todo p-grupo é nilpotente, segue que os p-subgrupos de Sylow fazem parte desta classe de grupos. De acordo com nossa pesquisa, podemos analisar os G-códigos de um grupo G dado por $C_p\ wr\ C_p\ wr \ldots wr\ C_p$ para determinar os códigos de grupos abelianos.

3.4 Extensão de corpos

Sejam G um grupo e $\mathbb{F}$ é um subcorpo de um corpo finito $\mathbb{E}$. Poderíamos nos perguntar se existe alguma relação entre os G-códigos sobre $\mathbb{F}$ e os G-códigos sobre $\mathbb{E}$. Uma resposta a esta pergunta foi dada por C. García Pillado, S. González, C. Martínez,

V. Markov e A. Nechaev, em [8]. Nesta seção, nós estudamos algumas relações entre os G-códigos à esquerda que são abelianos sobre $\mathbb{F}$ e os G-códigos sobre $\mathbb{E}$. Mostraremos que nossos resultados permanecem válidos quando estendemos ás algebras de grupos.

O lema seguinte afirma que certos ideais dos anéis de grupo $\mathbb{E}G$ e $\mathbb{F}G$ possuem os mesmos grupos de automorfismos por permutação.

Lema 3.15. *([8], Lema 5.1) Sejam $\mathbb{F}$ um subcorpo de um corpo finito $\mathbb{E}$ e I um ideal do anel de grupo $\mathbb{F}G$. Então $\mathbb{E}I$ é um ideal em $\mathbb{E}G$ e $PAut(I) = PAut(\mathbb{E}I)$.*

O seguinte resultado assegura que G-códigos abelianos sobre $\mathbb{E}$ são códigos abelianos sobre $\mathbb{F}$.

Teorema 3.16. *([8], Teorema 5.1) Sejam $\mathbb{F}$ um subcorpo de um corpo finito $\mathbb{E}$ e G um grupo. Se todo G-código sobre $\mathbb{E}$ é abeliano, então todo G-código sobre $\mathbb{F}$ é abeliano.*

Se todo G-código à esquerda sobre $\mathbb{F}$ é abeliano não necessariamente todo G-códigos à esquerda sobre $\mathbb{E}$ também o é. C. García Pillado, S. González, C. Martínez, Victor Markov e A. Nechaev, em [8], mostraram isto para $\mathbb{F} = GF_2$, $\mathbb{E} = GF_4$ e $G = Q_8$.

Com o objetivo de achar G-códigos à esquerda sobre $\mathbb{E}$ que sejam códigos abelianos a partir de G-códigos à esquerda sobre $\mathbb{F}$, estabelecemos condições sobre estes, onde G é um grupo que têm decomposição abeliana. Afirmamos que se $\mathcal{C}$ é um código de grupo à esquerda sobre o corpo $\mathbb{F}$ que verifica as condições do Teorema 3.5, então existe um código de grupo abeliano sobre $\mathbb{E}$.

Teorema 3.17. *Sejam $\mathbb{F}$ um subcorpo de um corpo finito $\mathbb{E}$ e G um grupo que tem decomposição abeliana, $G = AB$. Se $\mathcal{C}$ é um G-código à esquerda sobre $\mathbb{F}$ tal que $\sigma(B) \subset PAut(\mathcal{C})$, então existe um G-código à esquerda sobre $\mathbb{E}$ que é abeliano e que possui o mesmo grupo de automorfismo por permutação que o código $\mathcal{C}$.*

Demonstração. Se $\mathcal{C}$ é um G-código à esquerda sobre $\mathbb{F}$ tal que

$$\sigma(B) \subset PAut(\mathcal{C}),$$

então, pelo Teorema 3.5, existe um grupo K abeliano tal que $\mathcal{C}$ é um K-código. Agora, se I é um ideal à esquerda de $\mathbb{F}G$ que corresponde ao código $\mathcal{C}$ de $\mathbb{F}^n$, então $PAut(I)$ contém um subgrupo regular abeliano. Por outro lado, $\mathbb{E}I$ é um ideal à esquerda de $\mathbb{E}G$ e como

$$PAut(I) = PAut(\mathbb{E}I)$$

contém um subgrupo regular abeliano, segue o teorema. □

Se

$$G = A_1 A_2 \dots A_n,$$

com A_i abeliano, para $1 \leq i \leq n$ e $\mathbb{F}$ é um subcorpo de $\mathbb{E}$, a situação é um pouco diferente. Dado um G-código sobre $\mathbb{F}$ nem sempre podemos achar G-códigos abelianos sobre $\mathbb{E}$. O que podemos afirmar é que um G-código sobre $\mathbb{F}$ com determinadas condições, apresentadas no teorema a seguir, é um K-código à esquerda sobre $\mathbb{E}$, para

$$K = B_1.B_2 \dots B_s$$

com $s < n$ e B_i abeliano, para $1 \leq i \leq s$.

Teorema 3.18. *Sejam $\mathbb{F}$ é um subcorpo de $\mathbb{E}$, $G = A_1A_2 \dots A_m$ um grupo finito, com A_i subgrupo abeliano, para $1 \leqslant i \leqslant m$ e t um inteiro tal que $(A_1 \dots A_t)$ e $(A_{t+1} \dots A_m)$ são subgrupos de G e $(A_1 \dots A_t) \cap (A_{t+1} \dots A_m) \subset \mathcal{Z}(G)$. Então se $\mathcal{C}$ é um G-código sobre $\mathbb{F}$, existe um G-código sobre $\mathbb{E}$ que é um K-código à esquerda para $K = B_1 \dots B_r$, com B_i subgrupo abeliano, para $1 \leqslant i \leqslant r < m$ e, ademais, possui o mesmo grupo de automorfismos por permutação que $\mathcal{C}$.*

Demonstração. Seja G um grupo. Para cada G-código $\mathcal{C}$ sobre $\mathbb{F}$, seja I o ideal de $\mathbb{F}G$ correspondente a este código. Logo $\mathbb{E}I$ é um ideal de $\mathbb{E}G$ tal que

$$PAut(I) = PAut(\mathbb{E}I).$$

Se o grupo G verifica as condições do teorema e $\mathcal{C}'$ é o G-código que corresponde ao ideal $\mathbb{E}I$, então pelo Teorema 3.12, $\mathcal{C}'$ é um K-código à esquerda para

$$K = B_1 \dots B_r,$$

com B_i subgrupo abeliano, para $1 \leqslant i \leqslant r$. $\square$

Capítulo 4

Exemplos

Neste capítulo mostraremos alguns exemplos nos quais aplicaremos os teoremas apresentados no capítulo anterior.

4.1 Códigos sobre S_3

Neste exemplo, primeiramete aplicaremos o Teorema 3.2 num grupo que possui decomposição abeliana. Mostraremos que os ideais minimais são códigos abelianos.

Consideremos o corpo $\mathbb{F}_5$ e o grupo simétrico

$$S_3 = \{id; (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}.$$

A álgebra de grupo $\mathbb{F}_5 S_3$ tem três ideais minimais dos quais um é de dimensão 4 e dois são de dimensão 1 sobre $\mathbb{F}_5$. Logo,

$$\mathbb{F}_5 S_3 \cong \mathbb{F}_5 S_3 f_1 \oplus \mathbb{F}_5 S_3 f_2 \oplus \mathbb{F}_5 S_3 f_3,$$

onde f_1, f_2 e f_3 são os idempotentes centrais primitivos dados por:

- $f_1 = (1) + (1\ \ 2\ \ 3) + (1\ \ 3\ \ 2) + (1\ \ 2) + (1\ \ 3) + (2\ \ 3)$.
- $f_2 = (1) + (1\ \ 2\ \ 3) + (1\ \ 3\ \ 2) - (1\ \ 2) - (1\ \ 3) - (2\ \ 3)$.
- $f_3 = 4(1) + 3(1\ \ 2\ \ 3) + 3(1\ \ 3\ \ 2)$.

O grupo S_3 tem decomposição abeliana, pois

$$S_3 = \langle (1\ \ 2) \rangle \langle (1\ \ 2\ \ 3) \rangle.$$

Daí, pelo Teorema 3.2, todo G-código é um código de grupo abeliano. Mostraremos que os códigos minimais de comprimento 6 que correspondem aos ideais minimais de $\mathbb{F}_5 S_3$

também correspondem a ideais de uma álgebra de grupo $\mathbb{F}_5 A$, para A um grupo abeliano.

O idempotente f_3 gera o ideal minimal

$$I_3 = \mathbb{F}_5 S_3 f_3$$

de dimensão 4 sobre $\mathbb{F}_5$. Afirmamos que

$$\mathcal{B}_3 = \{f_3, (1\ \ 2)f_3, (1\ \ 3)f_3, (1\ \ 2\ \ 3)f_3\}$$

é uma base de I_3. Consideremos

$$\mathcal{E}_6 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$$

a base canônica de $\mathbb{F}_5^6$. Agora, a ideia é definir a bijeção

$$\phi : \mathcal{E}_6 \to S_3$$

para achar o código $\mathcal{C}_3 \leq \mathbb{F}_5^6$ que corresponde ao ideal I_3 através do isomorfismo de espaços vetoriais

$$\phi : \mathbb{F}_5^6 \to \mathbb{F}_5 S_3.$$

Sejam

$$\begin{aligned} H = \{h_1 &= (1),\ h_2 = (1\ \ 2)(3\ \ 6)(4\ \ 5),\ h_3 = (1\ \ 3\ \ 5)(2\ \ 4\ \ 6), \\ h_4 &= (1\ \ 4)(2\ \ 3)(5\ \ 6),\ h_5 = (1\ \ 5\ \ 3)(2\ \ 6\ \ 4),\ h_6 = (1\ \ 6)(2\ \ 5)(3\ \ 4)\} \end{aligned}$$

um subgrupo regular de S_6 isomorfo a S_3 e $1 = i_0 \in \mathbb{N}_6$. Pelo Lema 2.11, existe o anti-isomorfismo

$$\sigma : H \to C_{S_6}(H)$$

tal que $\sigma_h(i) = \psi^{-1}(i)(h(i_0))$, para cada $i \in \mathbb{N}_6$ e $h \in H$, com $\psi : H \to \mathbb{N}_6$ uma bijeção dada por $\psi(h) = h(1)$, para cada $h \in H$ que verifica $\psi^{-1}(i)(1) = i$, para cada $i \in \mathbb{N}_6$ e $\psi^{-1}(h(1)) = h$, para cada $h \in H$. Com a escolha $i_0 = 1$ temos:

- $\psi(h_1) = 1$, $\psi(h_2) = 2$, $\psi(h_3) = 3$, $\psi(h_4)) = 4$, $\psi(h_5) = 5$, $\psi(h_6) = 6$.
- $C_{S_6}(H) = \{(1), (1\ \ 2)(3\ \ 4)(5\ \ 6), (1\ \ 3\ \ 5)(2\ \ 6\ \ 4), (1\ \ 4)(2\ \ 5)(3\ \ 6), (1\ \ 5\ \ 3)(2\ \ 4\ \ 6), (1\ \ 6)(2\ \ 3)(4\ \ 5)\}$.

Definimos agora $f : S_3 \to S_6$ e os e_i's, lembrando que $\{e_1, \ldots, e_6\}$ é a base canônica de $\mathbb{F}_5^6$, tais que $Img(f) \cong H$ e $e_i = \phi^{-1} f^{-1} \psi^{-1}(i)$, ($f$ e os e_i's são dados na demonstração do

Teorema 2.12). Assim, a correspondência é

$$\begin{aligned}
(1) &\longmapsto h_1\\
(1\ \ 2\ \ 3) &\longmapsto h_3\\
(1\ \ 2) &\longmapsto h_2\\
(1\ \ 3) &\longmapsto h_4\\
(2\ \ 3) &\longmapsto h_6\\
(1\ \ 3\ \ 2) &\longmapsto h_5
\end{aligned}$$

Portanto,

$\phi(e_1) = (1)$, $\phi(e_2) = (1\ \ 2)$, $\phi(e_3) = (1\ \ 2\ \ 3)$, $\phi(e_4) = (1\ \ 3)$, $\phi(e_5) = (1\ \ 3\ \ 2)$, $\phi(e_6) = (2\ \ 3)$.

Observemos que, se $\gamma \in I_3$, então podemos escrever:

$$\begin{aligned}\gamma = \phi(e_1)(4\alpha_1 + 3\alpha_4) + \phi(e_2)(4\alpha_2 + 3\alpha_3) + \phi(e_3)(3\alpha_1 + 4\alpha_4) + \phi(e_4)(3\alpha_2 + 4\alpha_3) +\\ + \phi(e_5)(3\alpha_1 + 3\alpha_4) + \phi(e_6)(3\alpha_2 + 3\alpha_3).\end{aligned} \tag{4.1}$$

Logo, o elemento c pertencente ao código $\mathcal{C}_3 \leqslant \mathbb{F}_5^6$ é da forma:

$$c = (4\alpha_1 + 3\alpha_4,\ 4\alpha_2 + 3\alpha_3,\ 3\alpha_1 + 4\alpha_4,\ 3\alpha_2 + 4\alpha_3,\ 3\alpha_1 + 3\alpha_4,\ 3\alpha_2 + 3\alpha_3). \tag{4.2}$$

A seguir, construíremos o grupo abeliano K definido na demostração do Teorema 3.2. Consideremos $S_3 = \langle(1\ \ 2)\rangle\langle(1\ \ 2\ \ 3)\rangle$, o elemento $(1\ \ 2) \in S_3$ corresponde a $(1\ \ 2)(3\ \ 6)(4\ \ 5) \in S_6$ através do homomorfismo f e $(1\ \ 2\ \ 3)$ com $(1\ \ 3\ \ 5)(2\ \ 6\ \ 4) \in C_{S_6}(H)$, pelo anti-isomorfismo σ, definimos

$$K = \langle(1\ \ 2), \sigma((1\ \ 2\ \ 3))\rangle = \langle(1\ \ 6\ \ 5\ \ 2\ \ 3\ \ 4)\rangle,$$

como

$$\begin{aligned}K = \{k_1 = (1),\ k = (1\ \ 6\ \ 5\ \ 2\ \ 3\ \ 4),\ k^2 = (1\ \ 5\ \ 3)(2\ \ 4\ \ 6),\ k^3 = (1\ \ 2)(3\ \ 6)(4\ \ 5),\\ k^4 = (1\ \ 3\ \ 5)(2\ \ 6\ \ 4),\ k^5 = (1\ \ 4\ \ 3\ \ 2\ \ 5\ \ 6)\}.\end{aligned}$$

Observe que K é um subgrupo regular em S_6. Agora, vamos construir a bijeção

$$\phi' : \mathcal{E}_6 \to K$$

e, para isto, precisaremos de uma função $f' : K \to S_6$ tal que $Imf' \cong K$ e da bijeção $\psi' : K \to \mathbb{N}_6$, definida no Lema 2.11, tal que para cada $k \in K$, $\psi'(k) = k(i_0)$. Basta

tomar $f' = Id_K$, e daí, para $i_0 = 1$, temos

$$\begin{aligned} k^6 = id &\Rightarrow \psi'^{-1}(1) = id. \\ k = (1\ \ 6\ \ 5\ \ 2\ \ 3\ \ 4) &\Rightarrow \psi'^{-1}(6) = k. \\ k^2 = (1\ \ 5\ \ 3)(2\ \ 4\ \ 6) &\Rightarrow \psi'^{-1}(5) = k^2. \\ k^3 = (1\ \ 2)(3\ \ 6)(4\ \ 5) &\Rightarrow \psi'^{-1}(2) = k^3. \\ k^4 = (1\ \ 3\ \ 5)(2\ \ 6\ \ 4) &\Rightarrow \psi'^{-1}(3) = k^4. \\ k^5 = (1\ \ 4\ \ 3\ \ 2\ \ 5\ \ 6) &\Rightarrow \psi'^{-1}(4) = k^5. \end{aligned} \tag{4.3}$$

Como $e_i = \phi'^{-1} f'^{-1} \psi'^{-1}(i)$, obtemos $\phi'(e_i)$, para cada $i \in \mathbb{N}_6$, e ainda

$$\phi'(e_1) = id,\ \phi'(e_2) = k^3,\ \phi'(e_3) = k^4,\ \phi'(e_4) = k^5,\ \phi'(e_5) = k^2,\ \phi'(e_6) = k. \tag{4.4}$$

Aplicando ϕ' ao elemento $c \in \mathcal{C}_3$ obtém-se um elemento de $\mathbb{F}_5 K$, a saber,

$$\phi'(c) = \alpha_1(4id + 3k^4 + 3k^2) + \alpha_2(4k^3 + 3k^5 + 3k) + \alpha_3(3k^3 + 4k^5 + 3k) + \alpha_4(3id + 4k^4 + 3k^2).$$

Para finalizar, é possível mostrar, fazendo cálculos, que $\phi'(\mathcal{C}_3)$ é um ideal de $\mathbb{F}_5 K$ o que nos permite concluir que $\mathcal{C}_3$ é um código abeliano, mais ainda, é um código cíclico, a menos de permutacção.

O idempotente f_1 gera o ideal

$$I_1 = \mathbb{F}_5 S_3 f_1.$$

Tem-se, para cada $\alpha \in S_3$, $\alpha f_1 = f_1$. Um elemento $\gamma \in I_1$ é da forma:

$$\gamma = a(1) + a(1\ \ 2\ \ 3) + a(1\ \ 3\ \ 2) + a(1\ \ 2) + a(1\ \ 3) + a(2\ \ 3), \quad \text{com} \ \ a \in \mathbb{F}_5.$$

Logo, o código $\mathcal{C}_1$ de $\mathbb{F}_5^6$, que corresponde ao ideal I_1 pelo isomorfismo de espaços vetorias ϕ', é dado por

$$\{(a, a, a, a, a, a) \mid a \in \mathbb{F}_5\}.$$

Afirmamos que $\phi'(\mathcal{C}_1)$ é um ideal bilateral de $\mathbb{F}_5 K$ e assim $\mathcal{C}_1$ é um código abeliano.

Sejam

$$I_2 = \mathbb{F}_5 S_3 f_2$$

o ideal gerado por f_2 e $\gamma \in \mathbb{F}_5 S_3$. Disso, tem-se

$$\gamma = \gamma_1(id) + \gamma_2(1\ \ 2\ \ 3) + \gamma_3(1\ \ 3\ \ 2) + \gamma_4(1\ \ 3) + \gamma_5(1\ \ 2) + \gamma_6(2\ \ 3)$$

com $\gamma_i \in \mathbb{F}_5$. Tomando

$$a = \gamma_1 + \gamma_2 + \gamma_3 + 4\gamma_4 + 4\gamma_5 + 4\gamma_6,$$

obtemos

$$\gamma f_2 = a(1) + a(1\ \ 2\ \ 3) + a(1\ \ 3\ \ 2) + 4a(1\ \ 3) + 4a(1\ \ 2) + 4a(2\ \ 3).$$

Consequentemente, o código $\mathcal{C}_2$ de $\mathbb{F}_5^6$ que corresponde ao ideal I_2 através de ϕ' é dado pelo conjunto

$$\{(a, 4a, a, 4a, a, 4a) \mid a \in \mathbb{F}_5\}.$$

É possível verificar que $\phi'(\mathcal{C}_2)$ é um ideal de $\mathbb{F}_5 K$ e, portanto, $\mathcal{C}_2$ é um código abeliano.

Utilizaremos o mesmo anel de grupo para aplicar o Teorema 3.5. Apresentamos ideais laterais de $\mathbb{F}_5 S_3$ que verificam as condições do teorema e logo são códigos abelianos.

O elemento

$$e = 2(1) + (2\ \ 3) + 2(1\ \ 2) + 2(1\ \ 2\ \ 3) + (1\ \ 3\ \ 2) + 2(1\ \ 3)$$

de $\mathbb{F}_5 S_3$ é um idempotente que gera o ideal à esquerda

$$I = (\mathbb{F}_5 S_3)e$$

de dimensão 2 sobre $\mathbb{F}_5$. Uma base para este ideal é dada por

$$\mathcal{B} = \{e, (2\ \ 3)e\}.$$

Um elemento $\gamma \in I$, é da forma:

$$\begin{aligned}\gamma &= a_1 e + a_2(2\ \ 3)e \\ &= (1)(2a_1 + a_2) + (2\ \ 3)(a_1 + 2a_2) + (1\ \ 2)(2a_1 + a_2) + (1\ \ 2\ \ 3)(2a_1 + 2a_2) + \\ &\quad + (1\ \ 3\ \ 2)(a_1 + a_2) + (1\ \ 3)(2a_1 + 2a_2).\end{aligned}$$

Sejam H o subgrupo regular do grupo simétrico S_6 isomorfo a S_3, a bijeção $\psi : H \to \mathbb{N}_6$, o anti-isomorfismo $\sigma : H \to C_{S_6}(H)$, o homomorfismo $f : S_3 \to S_6$ e a bijeção $\psi : H \to \mathbb{N}_6$, como definidos acima. Obtemos o código $\mathcal{C}$ em $\mathbb{F}_5^6$ que correspode ao ideal à esquerda I de $\mathbb{F}_5 S_3$ tal que a extensão da bijeção ϕ ao isomorfismo de espaços vetoriais $\mathbb{F}_5^6 \to \mathbb{F}_5 S_3$ leva o código $\mathcal{C}$ no ideal à esquerda I.

Observe que o elemento $c \in \mathcal{C}$ que se identifica com o elemento γ de I é da forma

:

$$c = (2a_1 + a_2,\ 2a_1 + a_2,\ 2a_1 + 2a_2,\ 2a_1 + 2a_2,\ a_1 + 2a_2,\ a_1 + 2a_2)$$

Logo, o código $\mathcal{C}$ é gerado por

$$\{(2,2,2,2,1,1),\ (1,1,2,2,2,2)\}.$$

Temos que $S_3 = \langle(1\ \ 2)\rangle\langle(1\ \ 2\ \ 3)\rangle$. Como mostramos anteriormente, o elemento $(1,2)$ de S_3 se identifica com o elemento $h_2 = (1\ \ 2)(3\ \ 6)(4\ \ 5)$ de H. Daí,

$$\sigma(h_2) = (1\ \ 2)(3\ \ 4)(5\ \ 6).$$

Observe ainda

$$\sigma(\langle h_2\rangle) \subseteq PAut(\mathcal{C}) \text{ e } \sigma(\langle h_3\rangle) \nsubseteq PAut(\mathcal{C}),$$

consequentemente, pelo Teorema 3.5, $\mathcal{C}$ é um código de grupo abeliano. De fato, definimos o grupo $\widetilde{K}$ obtido a partir de S_3, por

$$\widetilde{K} = \langle h_5, \sigma(h_2)\rangle = \langle(1\ \ 4\ \ 5\ \ 2\ \ 3\ \ 6)\rangle,$$

com

$$\begin{aligned}\widetilde{K} = \{&\tilde{k}^6 = (1),\ \tilde{k} = (1\ \ 4\ \ 5\ \ 2\ \ 3\ \ 6),\ \tilde{k}^2 = (1\ \ 5\ \ 3)(2\ \ 6\ \ 4),\\ &\tilde{k}^3 = (1\ \ 2)(3\ \ 4)(5\ \ 6), \tilde{k}^4 = (1\ \ 3\ \ 5)(2\ \ 4\ \ 6),\ \tilde{k}^5 = (1\ \ 6\ \ 3\ \ 2\ \ 5\ \ 4)\}.\end{aligned}$$

Mostramos agora que $\mathcal{C}$ é um $\widetilde{K}$-código. Apresentamos o ideal de $\mathbb{F}_5\widetilde{K}$ que corresponde a $\mathcal{C}$.

Note que $\widetilde{K}$ é um subgrupo regular de S_6. Com a mesma ideia que utilizamos anteriormente construímos a bijeção

$$\phi' : \mathcal{E}_6 \to \widetilde{K};$$

para esta construção precisamos do homomorfismo $f' : \widetilde{K} \to S_6$ tal que $Imf' \cong \widetilde{K}$. Neste caso, consideramos $f' = id$ e a bijeção $\psi' : \widetilde{K} \to \mathbb{N}_6$, definida no Lema 2.11, tal que, para cada $\tilde{k} \in \widetilde{K}$, $\psi'(k) = k(i_0)$, com i_0 fixo. Tomando $i_0 = 1$, temos:

$$\begin{aligned}\tilde{k}^6 = (1) &\ \Rightarrow\ \psi'^{-1}(1) = (1).\\ \tilde{k} = (1\ \ 4\ \ 5\ \ 2\ \ 3\ \ 6) &\ \Rightarrow\ \psi'^{-1}(4) = \tilde{k}.\\ \tilde{k}^2 = (1\ \ 5\ \ 3)(2\ \ 6\ \ 4) &\ \Rightarrow\ \psi'^{-1}(5) = \tilde{k}^2.\\ \tilde{k}^3 = (1\ \ 2)(3\ \ 4)(5\ \ 6) &\ \Rightarrow\ \psi'^{-1}(2) = \tilde{k}^3.\end{aligned} \tag{4.5}$$

$$\tilde{k}^4 = (1\ \ 3\ \ 5)(2\ \ 4\ \ 6) \ \Rightarrow\ \psi'^{-1}(3) = \tilde{k}^4.$$
$$\tilde{k}^5 = (1\ \ 6\ \ 3\ \ 2\ \ 5\ \ 4) \ \Rightarrow\ \psi'^{-1}(6) = \tilde{k}^5.$$

Dado $e_i = \phi'^{-1} f'^{-1} \psi'^{-1}(i)$, para cada $i \in \mathbb{N}_6$,

$$\phi'(e_1) = (1),\ \phi'(e_2) = \tilde{k}^3,\ \phi'(e_3) = \tilde{k}^4,\ \phi'(e_4) = \tilde{k},\ \phi'(e_5) = \tilde{k}^2,\ \phi'(e_6) = \tilde{k}^5. \tag{4.6}$$

Logo, os elementos de $\phi'(\mathcal{C})$ são da forma:

$$\phi'(c) = a_1(2(1) + 2\tilde{k}^3 + 2\tilde{k}^4 + 2\tilde{k} + \tilde{k}^2 + \tilde{k}^5) + a_2((1) + \tilde{k}^3 + 2\tilde{k}^4 + 2\tilde{k} + 2\tilde{k}^2 + 2\tilde{k}^5),$$

com $a_1, a_2 \in \mathbb{F}$. Consequentemente $\phi'(\mathcal{C})$ é um ideal de $\mathbb{F}\widetilde{K}$.

Existem outros idempotentes como

$$f_1 = 2(1) + 2(2\ \ 3) + 2(1\ \ 2) + (1\ \ 2\ \ 3) + 2(1\ \ 3\ \ 2) + (1\ \ 3)$$

e

$$f_2 = 2(1) + 4(2\ \ 3) + 2(1\ \ 2) + 4(1\ \ 2\ \ 3) + 4(1\ \ 3\ \ 2) + 4(1\ \ 3),$$

geradores de ideais à esquerda de $\mathbb{F}S_3$. Os códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ em $\mathbb{F}^6$ que correspondem aos ideais $I_1 = (\mathbb{F}S_3)f_1$ e $I_2 = (\mathbb{F}S_3)f_2$ são S_3-códigos à esquerda e também são códigos abelianos.

4.2 Códigos sobre S_4

Aplicamos o Teorema 3.8 e o Teorema 3.5 num grupo G que se decompõe como um produto mínimo de três abelianos e encontramos G-códigos que são códigos de grupo abeliano.

Considere o grupo simétrico

$$S_4 = \langle (1\ \ 2),\ (1\ \ 2\ \ 3\ \ 4) \rangle.$$

A álgebra de grupo $\mathbb{F}_5 S_4$ possui 5 ideais minimais, dois de dimensão 1, dois de dimensão 9 e um de dimenão 4 gerados pelos idempotentes centrais primitivos f_1, f_2, f_3, f_4, f_5 respectivamente:

- $f_1 = \sum_{g \in S_4} g$, $f_2 = \sum_{g \in S_4} (-1)^{o(g)} g$ são os idempotentes que geram os ideais I_1 e I_2 de dimensão 1, em que $o(g)$ é a ordem do elemento $g \in S_4$

- $f_3 = 2(3(1) + 4(1\ \ 2)(3\ \ 4) + 4(1\ \ 3)(2\ \ 4) + 4(1\ \ 4)(2\ \ 3) + (1\ \ 2) + (1\ \ 3) + (1\ \ 4) + (2\ \ 3) + (2\ \ 4) + (3\ \ 4) + 4(1\ \ 2\ \ 3\ \ 4) + 4(1\ \ 3\ \ 2\ \ 4) + 4(1\ \ 3\ \ 4\ \ 2) + 4(1\ \ 4\ \ 3\ \ 2) +$

$4(1\ \ 4\ \ 2\ \ 3) + 4(1\ \ 2\ \ 4\ \ 3))$,
$f_4 = 2(3(1) + 4(1\ \ 2)(3\ \ 4) + 4(1\ \ 3)(2\ \ 4) + (1\ \ 4)(2\ \ 3) + 4(1\ \ 2) + 4(1\ \ 3) + 4(1\ \ 4) + 4(2\ \ 3) + 4(2\ \ 4) + 4(3\ \ 4) + (1\ \ 2\ \ 3\ \ 4) + (1\ \ 3\ \ 2\ \ 4) + (1\ \ 3\ \ 4\ \ 2) + (1\ \ 4\ \ 3\ \ 2) + (1\ \ 4\ \ 2\ \ 3) + (1\ \ 2\ \ 4\ \ 3))$ são os idempotentes geradores dos ideais I_3 e I_4 de dimensão 9.

- $f_5 = (1) + (1\ \ 2)(3\ \ 4) + (1\ \ 3)(2\ \ 4) + (1\ \ 4)(2\ \ 3) + 2(1\ \ 2\ \ 3) + 2(1\ \ 2\ \ 4) + 2(1\ \ 3\ \ 4) + 2(2\ \ 3\ \ 4) + 2(1\ \ 3\ \ 2) + 2(1\ \ 4\ \ 2) + 2(1\ \ 4\ \ 3) + 2(2\ \ 4\ \ 3)$ é o idempotente que gera o ideal I_5 de dimenão 4.

Note que S_4 não tem decomposição abeliana, mas ele pode ser escrito como um produto de 3 subgrupos abelianos

$$S_4 = (V \rtimes C_3) \rtimes C_2,$$

com $V = \langle (1\ \ 4)(2\ \ 3), (1\ \ 3)(2\ \ 4) \rangle$ é o subgrupo de Klein, $C_3 = \langle (1\ \ 2\ \ 3) \rangle$ o subgrupo cíclico de ordem 3 e $C_2 = \langle (1\ \ 2) \rangle$ o subgrupo cíclico de ordem 2.

Com a finalidade de aplicar os teoremas 3.5 e 3.8, verificaremos que $\mathcal{C}_5$ é um código de grupo abeliano. Primeiro vamos achar uma expresão para o código minimal $\mathcal{C}_5$ de comprimento 24 e dimensão 4 sobre $\mathbb{F}_5$ que correspode ao ideal I_5 de $\mathbb{F}_5 S_4$.

Seja

$$H = \langle h_{15},\ h_{18} \rangle$$

um subgrupo regular de S_{24} isomorfo a S_4, com

$$h_{15} = (1\ \ 15)(2\ \ 16)(3\ \ 13)(4\ \ 14)(5\ \ 18)(6\ \ 17)(7\ \ 9)(8\ \ 10)(11\ \ 12)(19\ \ 24)(20\ \ 23)(21\ \ 22)$$

e

$$h_{18} = (1\ \ 18\ \ 8\ \ 23)(2\ \ 17\ \ 7\ \ 24)(3\ \ 16\ \ 11\ \ 20)(4\ \ 15\ \ 12\ \ 19)(5\ \ 14\ \ 9\ \ 22)(6\ \ 13\ \ 10\ \ 21).$$

Denotaremos os elementos de H por h_i tais que $h_i(1) = i$, para cada $1 \leqslant i \leqslant 24$. Seguindo, definimos $f : S_4 \to S_{24}$ tal que $f(S_4) \cong H$. Basta definir f sobre os geradores:

$$\begin{aligned} (1\ \ 2) &\ \to\ h_{15} \\ (1\ \ 2\ \ 3\ \ 4) &\ \to\ h_{18} \end{aligned}$$

Para $1 = i_0 \in \mathbb{N}_{24}$, tem-se $\psi : H \to \mathbb{N}_{24}$ dado por $\psi(h_i) = i$ tal que $\psi^{-1}(i) = h_i$ e $\psi^{-1}(i)(1) = i$ para todo $i \in \mathbb{N}_{24}$.

Agora estamos em condições de apresentar a correspondência entre $\{e_i \mid 1 \leq i \leq 24\}$ e os elementos de S_4. Lembre-se que, para cada $i \in \mathbb{N}_{24}$,

$$e_i = \phi^{-1} f^{-1} \psi^{-1}(i).$$

Logo,

$\phi^{-1}(1) = e_1,\ \phi^{-1}((2\ \ 4)) = e_2,\ \phi^{-1}((2\ \ 3)) = e_3,\ \phi^{-1}((2\ \ 4\ \ 3)) = e_4,\ \phi^{-1}((2\ \ 3\ \ 4)) = e_5,$
$\phi^{-1}((3\ \ 4)) = e_6,\ \phi^{-1}((1\ \ 3)) = e_7,\ \phi^{-1}((1\ \ 3)(2\ \ 4)) = e_8,\ \phi^{-1}((1\ \ 3\ \ 2)) = e_9,$
$\phi^{-1}((1\ \ 3\ \ 2\ \ 4)) = e_{10},\ \phi^{-1}((1\ \ 3\ \ 4\ \ 2)) = e_{11},\ \phi^{-1}((1\ \ 3\ \ 4)) = e_{12},\ \phi^{-1}((1\ \ 2\ \ 3)) = e_{13},$
$\phi^{-1}((1\ \ 2\ \ 4\ \ 3)) = e_{14}\phi^{-1}((1\ \ 2)) = e_{15},\ \phi^{-1}((1\ \ 2\ \ 4)) = e_{16},\ \phi^{-1}((1\ \ 2)(3\ \ 4)) = e_{17},$
$\phi^{-1}((1\ \ 2\ \ 3\ \ 4)) = e_{18},\ \phi^{-1}((1\ \ 4\ \ 2\ \ 3)) = e_{19},\ \phi^{-1}((1\ \ 4\ \ 3)) = e_{20},\ \phi^{-1}((1\ \ 4\ \ 2)) = e_{21},$
$\phi^{-1}((1\ \ 4)) = e_{22},\ \phi^{-1}((1\ \ 4\ \ 3\ \ 2)) = e_{23},\ \phi^{-1}((1\ \ 4)(2\ \ 3)) = e_{24}$

Seja

$$\mathcal{B} = \{(1\ \ 3)f_5,\ (1\ \ 3\ \ 2)f_5,\ (2\ \ 3)f_5,\ (1\ \ 2\ \ 3)f_5\}$$

uma base de I_5. Um elemento $\gamma \in I_5$ é da forma:

$$\begin{aligned}
\gamma = {} & (1)(2\alpha_3 + 2\alpha_4) + (2\ \ 4)(\alpha_1 + 2\alpha_2) + (2\ \ 3)(2\alpha_1 + \alpha_2) + (2\ \ 4\ \ 3)(\alpha_3 + 2\alpha_4) + \\
& + (2\ \ 3\ \ 4)(2\alpha_3 + \alpha_4) + (3\ \ 4)(2\alpha_1 + 2\alpha_2) + (1\ \ 3)(\alpha_1 + 2\alpha_2) + (1\ \ 3)(2\ \ 4)(2\alpha_3 + 2\alpha_4) + \\
& + (1\ \ 3\ \ 2)(2\alpha_3 + \alpha_4) + (1\ \ 3\ \ 2\ \ 4)(2\alpha_1 + 2\alpha_2) + (1\ \ 3\ \ 4\ \ 2)(2\alpha_1 + \alpha_2) + (1\ \ 3\ \ 4)(\alpha_3 + \\
& + 2\alpha_4) + +(1\ \ 2\ \ 3)(\alpha_3 + 2\alpha_4) + (1\ \ 2\ \ 4\ \ 3)(2\alpha_1 + \alpha_2) + (1\ \ 2)(2\alpha_1 + 2\alpha_2) + (1\ \ 2\ \ 4)(2\alpha_3 + \\
& + \alpha_4) + +(1\ \ 2)(3\ \ 4)(2\alpha_3 + 2\alpha_4) + (1\ \ 2\ \ 3\ \ 4)(\alpha_1 + 2\alpha_2) + (1\ \ 4\ \ 2\ \ 3)(2\alpha_1 + 2\alpha_2) + \\
& + (1\ \ 4\ \ 3)(2\alpha_3 + \alpha_4) + (1\ \ 4\ \ 2)(\alpha_3 + 2\alpha_4) + (1\ \ 4)(2\alpha_1 + \alpha_2) + (1\ \ 4\ \ 3\ \ 2)(\alpha_1 + 2\alpha_2) + \\
& + (1\ \ 4)(2\ \ 3)(2\alpha_3 + 2\alpha_4).
\end{aligned}$$

com $\alpha_i \in \mathbb{F}_5$. O elemento $c \in \mathcal{C}_5 \leqslant \mathbb{F}_5^{24}$ correspondente a γ é:

$$\begin{aligned}
c = {} & (2\alpha_3 + 2\alpha_4)e_1 + (\alpha_1 + 2\alpha_2)e_2 + (2\alpha_1 + \alpha_2)e_3 + (\alpha_3 + 2\alpha_4)e_4 + \\
& + (2\alpha_3 + \alpha_4)e_5 + (2\alpha_1 + 2\alpha_2)e_6 + (\alpha_1 + 2\alpha_2)e_7 + (2\alpha_3 + 2\alpha_4)e_8 + \\
& + (2\alpha_3 + \alpha_4)e_9 + (2\alpha_1 + 2\alpha_2)e_{10} + (2\alpha_1 + \alpha_2)e_{11} + (\alpha_3 + 2\alpha_4)e_{12} + \\
& + (\alpha_3 + 2\alpha_4)e_{13} + (2\alpha_1 + \alpha_2)e_{14} + (2\alpha_1 + 2\alpha_2)e_{15} + (2\alpha_3 + \alpha_4)e_{16} + \\
& + (2\alpha_3 + 2\alpha_4)e_{17} + (\alpha_1 + 2\alpha_2)e_{18} + (2\alpha_1 + 2\alpha_2)e_{19} + (2\alpha_3 + \alpha_4)e_{20} + \\
& + (\alpha_3 + 2\alpha_4)e_{21} + (2\alpha_1 + \alpha_2)e_{22} + (\alpha_1 + 2\alpha_2)e_{23} + (2\alpha_3 + 2\alpha_4)e_{24}.
\end{aligned}$$

Por conseguinte, se pode mostrar que uma base para o código $\mathcal{C}_5$ é:

$$\begin{aligned}\mathcal{D} = \{&(0,1,2,0,0,2,1,0,0,2,2,0,0,2,2,0,0,1,2,0,0,2,1,0)\\ &(0,2,1,0,0,2,2,0,0,2,2,0,0,1,2,0,0,2,2,0,0,1,2,0)\\ &(2,0,0,1,2,0,0,2,2,0,0,1,1,0,0,2,2,0,0,2,1,0,0,2)\\ &(2,0,0,2,1,0,0,2,1,0,0,2,2,0,0,1,2,0,0,1,2,0,0,2)\}\end{aligned}$$

Como VC_2 é um subgrupo de S_4 e $VC_2 \cap C_3 = \{(1)\} \subset \mathcal{Z}(G)$, o seguinte passo é aplicar o Teorema 3.8 e achar o grupo K que tem decomposição abeliana. Fixemos $1 = i_0 \in \mathbb{N}_{24}$ e calculemos o grupo $\sigma(C_3) = \langle \sigma(1\ \ 2\ \ 3)\rangle$. O elemento $(1\ \ 2\ \ 3) \in S_4$ corresponde com $h_9 \in H$, logo

$\sigma_{h_9}(1) = 9$, $\sigma_{h_9}(9) = 13$, $\sigma_{h_9}(13) = 1$, $\sigma_{h_9}(2) = 11$, $\sigma_{h_9}(11) = 19$, $\sigma_{h_9}(19) = 2$, $\sigma_{h_9}(3) = 15$, $\sigma_{h_9}(15) = 7$, $\sigma_{h_9}(7) = 3$, $\sigma_{h_9}(4) = 17$, $\sigma_{h_9}(17) = 20$, $\sigma_{h_9}(20) = 4$, $\sigma_{h_9}(5) = 21$, $\sigma_{h_9}(21) = 8$, $\sigma_{h_9}(8) = 5$, $\sigma_{h_9}(6) = 23$, $\sigma_{h_9}(23) = 14$, $\sigma_{h_9}(14) = 6$, $\sigma_{h_9}(10) = 18$, $\sigma_{h_9}(18) = 22$, $\sigma_{h_9}(22) = 10$, $\sigma_{h_9}(12) = 24$, $\sigma_{h_9}(24) = 16$, $\sigma_{h_9}(16) = 12$.

Logo,

$$\sigma_{h_9} = (9\ \ 13\ \ 1)(2\ \ 11\ \ 19)(3\ \ 15\ \ 7)(4\ \ 17\ \ 20)(5\ \ 21\ \ 8)(6\ \ 23\ \ 14)(10\ \ 18\ \ 22)(12\ \ 24\ \ 16).$$

O subgrupo $V = \langle (1\ \ 4)(2\ \ 3), (1\ \ 3)(2\ \ 4)\rangle$ de S_4 é isomorfo ao subgrupo

$$\langle h_8, h_{24}\rangle \text{ de } S_{24},$$

e o grupo $C_2 = \langle (1\ \ 2)\rangle$ de S_4 é isomorfo ao subgrupo

$$\langle h_{15}\rangle \text{ de } S_{24}.$$

Portanto, definimos o grupo

$$K = \langle h_8, h_{24}\rangle \cdot (\langle \sigma(C_3)\rangle \cdot \langle h_{15}\rangle) = \langle k_8, k_{24}, k_7\rangle$$

o qual é um grupo que tem decomposição abeliana com:

$$k_7 = (1\ \ 7\ \ 13\ \ 15\ \ 9\ \ 3)(2\ \ 12\ \ 19\ \ 16\ \ 11\ \ 24)(4\ \ 6\ \ 20\ \ 14\ \ 17\ \ 23)(5\ \ 22\ \ 8\ \ 18\ \ 21\ \ 10),$$

$$k_8 = (1\ \ 8)(2\ \ 7)(3\ \ 11)(4\ \ 12)(5\ \ 9)(6\ \ 10)(13\ \ 21)(14\ \ 22)(15\ \ 19)(16\ \ 20)(17\ \ 24)(18\ \ 23),$$

$$k_{24} = (1\ \ 24)(2\ \ 23)(3\ \ 22)(4\ \ 21)(5\ \ 20)(6\ \ 19)(7\ \ 18)(8\ \ 17)(9\ \ 16)(10\ \ 15)(11\ \ 14)(12\ \ 13).$$

Denotamos o grupo

$$K = \{k_i \mid k_i(1) = i,\ 1 \leqslant i \leqslant 24\}.$$

Agora, nosso propósito é encontrar $\phi' : \mathcal{E}_{24} \to K$ tal que a extensão

$$\phi' : \mathbb{F}_5^{24} \to \mathbb{F}_5 K$$

leve o código $\mathcal{C}_5$ em um ideal de $\mathbb{F}_5 K$. Tomemos $f' : K \to S_{24}$ tal que $f' = Id$. Para $i_0 = 1$, $\psi' : K \to \mathbb{N}_{24}$ é definido por $\psi'(k_j) = j$ para $1 \leqslant j \leqslant 24$.
Continuando, encontramos $e_i = \phi'^{-1}\psi'^{-1}(i)$, para cada $1 \leq i \leq 24$.

$\phi'^{-1}(k_1) = e_1,\ \phi'^{-1}(k_2) = e_2,\ \phi'^{-1}(k_3) = e_3,\ \phi'^{-1}(k_4) = e_4,\ \phi'^{-1}(k_5) = e_5,\ \phi'^{-1}(k_6) = e_6,$
$\phi'^{-1}(k_7) = e_7,\ \phi'^{-1}(k_8) = e_8,\ \phi'^{-1}(k_9) = e_9,\ \phi'^{-1}(k_{10}) = e_{10},\ \phi'^{-1}(k_{11}) = e_{11},$
$\phi'^{-1}(k_{12}) = e_{12},\ \phi'^{-1}(k_{13}) = e_{13},\ \phi'^{-1}(k_{14}) = e_{14},\ \phi'^{-1}(k_{15}) = e_{15},\ \phi'^{-1}(k_{16}) = e_{16},$
$\phi'^{-1}(k_{17}) = e_{17},\ \phi'^{-1}(k_{18}) = e_{18},\ \phi'^{-1}(k_{19}) = e_{19},\ \phi'^{-1}(k_{20}) = e_{20},\ \phi'^{-1}(k_{21}) = e_{21},$
$\phi'^{-1}(k_{22}) = e_{22},\ \phi'^{-1}(k_{23}) = e_{23},\ \phi'^{-1}(k_{24}) = e_{24}$

É possível provar que $\phi'(\mathcal{C}_5)$ é um ideal à esquerda de $\mathbb{F}_5 K$. Logo, o isomorfismo de espaços vetoriais ϕ' leva o código $\mathcal{C}_5$ num ideal à esquerda de $\mathbb{F}_5 K$.

A seguir, aplicaremos o Teorema 3.5 para mostrar que $\mathcal{C}_5$ é um código de grupo abeliano. Fixado $1 = i_0 \in \mathbb{N}_{24}$, para o subgrupo abeliano

$$\langle k_8,\ k_{24} \rangle = \{k_1,\ k_8,\ k_{24},\ k_{17}\}$$

de K, calculamos $\sigma'(\langle k_8,\ k_{24} \rangle)$, com $\sigma' : K \to C_{S_{24}}(K)$ tal que $\sigma'_k(i) = \psi'^{-1}(i)(k(i_0))$, para todo $k \in K$ e para todo $i \in \mathbb{N}_{24}$. Assim,

- $\sigma'_{k_1} = k_1$,

- $\sigma'_{k_8}(1) = 8,\ \sigma'_{k_8}(8) = 1,\ \sigma'_{k_8}(2) = 23,\ \sigma'_{k_8}(23) = 2,\ \sigma'_{k_8}(13) = 21,\ \sigma'_{k_8}(21) = 13,$
  $\sigma'_{k_8}(3) = 22,\ \sigma'_{k_8}(22) = 3,\ \sigma'_{k_8}(4) = 12,\ \sigma'_{k_8}(12) = 4,\ \sigma'_{k_8}(5) = 9;\ \sigma'_{k_8}(9) = 5;$
  $\sigma'_{k_8}(6) = 19,\ \sigma'_{k_8}(19) = 6,\ \sigma'_{k_8}(7) = 18,\ \sigma'_{k_8}(10) = 15,\ \sigma'_{k_8}(15) = 10,\ \sigma'_{k_8}(11) = 14,$
  $\sigma'_{k_8}(14) = 11,\ \sigma'_{k_8}(16) = 20,\ \sigma'_{k_8}(20) = 16,\ \sigma'_{k_8}(17) = 24,\ \sigma'_{k_8}(24) = 17$, então,

  $$\sigma'_{k_8} = (1\ 8)(2\ 23)(3\ 22)(4\ 12)(5\ 9)(6\ 19)(7\ 18)(10\ 15)(11\ 14)(13\ 21)(16\ 20)(17\ 24).$$

- $\sigma'_{k_{17}}(1) = 17,\ \sigma'_{k_{17}}(17) = 1,\ \sigma'_{k_{17}}(2) = 18,\ \sigma'_{k_{17}}(18) = 2,\ \sigma'_{k_{17}}(3) = 14,\ \sigma'_{k_{17}}(14) = 3,$
  $\sigma'_{k_{17}}(4) = 13,\ \sigma'_{k_{17}}(13) = 4,\ \sigma'_{k_{17}}(5) = 16,\ \sigma'_{k_{17}}(16) = 5,\ \sigma'_{k_{17}}(6) = 15,\ \sigma'_{k_{17}}(15) = 6,$
  $\sigma'_{k_{17}}(7) = 23,\ \sigma'_{k_{17}}(23) = 7,\ \sigma'_{k_{17}}(8) = 24,\ \sigma'_{k_{17}}(24) = 8,\ \sigma'_{k_{17}}(9) = 20,\ \sigma'_{k_{17}}(20) = 9,$
  $\sigma'_{k_{17}}(10) = 19,\ \sigma'_{k_{17}}(19) = 10,\ \sigma'_{k_{17}}(11) = 22,\ \sigma'_{k_{17}}(22) = 11,\ \sigma'_{k_{17}}(12) = 21,$
  $\sigma'_{k_{17}}(21) = 12,$

daí

$$\sigma'_{k_{17}} = (1\ 17)(2\ 18)(3\ 14)(4\ 13)(5\ 16)(6\ 15)(7\ 23)(8\ 24)(9\ 20)(10\ 19)(11\ 22)(12\ 21).$$

- $\sigma'_{k_{24}}(1) = 24,\ \sigma'_{k_{24}}(24) = 1,\ \sigma'_{k_{24}}(2) = 7,\ \sigma'_{k_{24}}(7) = 2,\ \sigma'_{k_{24}}(3) = 11,\ \sigma'_{k_{24}}(11) = 3,$
  $\sigma'_{k_{24}}(4) = 21,\ \sigma'_{k_{24}}(21) = 4,\ \sigma'_{k_{24}}(5) = 20,\ \sigma'_{k_{24}}(20) = 5,\ \sigma'_{k_{24}}(6) = 10,\ \sigma'_{k_{24}}(10) = 6,$
  $\sigma'_{k_{24}}(8) = 17,\ \sigma'_{k_{24}}(17) = 8,\ \sigma'_{k_{24}}(9) = 16,\ \sigma'_{k_{24}}(16) = 9,\ \sigma'_{k_{24}}(12) = 13,$
  $\sigma'_{k_{24}}(13) = 12,\ \sigma'_{k_{24}}(14) = 22,\ \sigma'_{k_{24}}(22) = 14,\ \sigma'_{k_{24}}(15) = 19,\ \sigma'_{k_{24}}(19) = 15,$
  $\sigma'_{k_{24}}(18) = 23,\ \sigma'_{k_{24}}(23) = 18,$

  assim,

$$\sigma'_{k24} = (1\ 24)(2\ 7)(3\ 11)(4\ 21)(5\ 20)(6\ 10)(8\ 17)(9\ 16)(12\ 13)(14\ 22)(15\ 19)(18\ 23).$$

Logo,

$$\sigma'_{k_1}(\mathcal{C}_5) = \sigma'_{k_8}(\mathcal{C}_5) = \sigma'_{k_{17}}(\mathcal{C}_5) = \sigma'_{k_{24}}(\mathcal{C}_5) = \mathcal{C}_5.$$

Isto mostra a inclusão

$$\sigma'(\langle k_8, k_{24}\rangle) \subset PAut(\mathcal{C}_5).$$

e daí o Teorema 3.5 afirma que $\mathcal{C}_5$ é um código de grupo abeliano. Vejamos quem é este grupo abeliano que denotaremos por L. Tomemos

$$L = \sigma'(\langle k_8, k_{24}\rangle)\langle k_7\rangle = \{l_i \mid l_i(1) = i,\ 1 \leqslant i \leqslant 24\}.$$

Se conhecermos o morfismo $\widehat{f} : L \to S_{24}$ e a bijeção $\widehat{\psi} : L \to \mathbb{N}_{24}$, podemos encontrar $\widehat{\phi}(e_i)$, para cada $1 \leqslant i \leqslant 24$, pois $\phi(e_i) = \widehat{f}^{-1}\widehat{\psi}^{-1}(i)$.

Por definição, $Im\widehat{f}$ deve ser isomorfo a um subgrupo regular de S_{24}. Como o grupo L é regular, tomemos $\widehat{f} = Id$. Se $1 = i_0 \in \mathbb{N}_{24}$, então $\widehat{\psi}(l_i) = i$. Logo

$$\widehat{\phi}(e_i) = l_i, \qquad \text{para todo } i \in \mathbb{N}_{24}.$$

Fazendo os cálculos necessários é possível mostrar que $\widehat{\phi}(\mathcal{C}_5)$ é um ideal bilateral de $\mathbb{F}_5 L$.

Seja I_3 o ideal gerado por f_3 em $\mathbb{F}_5 S_4$. Pode ser demonstrado que

$$\mathcal{B}_3 = \{\ (1\ \ 4)f_3,\ (2\ \ 4)f_3,\ (3\ \ 4)f_3,\ (1\ \ 2\ \ 3\ \ 4)f_3,\ (1\ \ 4\ \ 3\ \ 2)f_3,\ (1\ \ 2\ \ 4\ \ 3)f_3,\ (1\ \ 3\ \ 4\ \ 2)f_3,\ (1\ \ 3\ \ 2\ \ 4)f_3,\ (1\ \ 4\ \ 2\ \ 3)f_3\ \}$$

uma base de I_3. Cada $\gamma \in I_3$ é da forma

$$\begin{aligned}\gamma = {} & (1)(2\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 3\alpha_5 + 3\alpha_6 + 3\alpha_7 + 3\alpha_8 + 3\alpha_9) + (2\ \ 4)(\alpha_3 + 3\alpha_4 + 3\alpha_5) \\ & + (2\ \ 3)(3\alpha_1 + 3\alpha_6 + 3\alpha_7) + (2\ \ 4\ \ 3)(3\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + 2\alpha_6 + 3\alpha_7 + 2\alpha_8 + \\ & + 3\alpha_9) + (2\ \ 3\ \ 4)(3\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4 + 3\alpha_5 + 3\alpha_6 + 2\alpha_7 + 3\alpha_8 + 2\alpha_9) + (3\ \ 4)(\alpha_2 + \\ & + 3\alpha_8 + 3\alpha_9)(1\ \ 3)(3\alpha_3 + 3\alpha_4 + 3\alpha_5) + (1\ \ 3)(2\ \ 4)(3\alpha_1 + 3\alpha_2 + 2\alpha_3 + 3\alpha_4 + 3\alpha_5 + 2\alpha_6 + \\ & + 2\alpha_7 + 2\alpha_8 + 2\alpha_9) + (1\ \ 3\ \ 2)(3\alpha_1 + 3\alpha_2 + 3\alpha_3 + 3\alpha_4 + 2\alpha_5 + 3\alpha_6 + 2\alpha_7 + 2\alpha_8 + 3\alpha_9) + \\ & + (1\ \ 3\ \ 2\ \ 4)(3\alpha_2 + \alpha_8 + 3\alpha_9) + (1\ \ 3\ \ 4\ \ 2)(3\alpha_1 + 3\alpha_6 + \alpha_7) + (1\ \ 3\ \ 4)(2\alpha_1 + 2\alpha_2 + 3\alpha_3 + \\ & + 2\alpha_4 + 3\alpha_5 + 3\alpha_6 + 2\alpha_7 + 2\alpha_8 + 3\alpha_9) + (1\ \ 2\ \ 3)(3\alpha_1 + 3\alpha_2 + 3\alpha_3 + 2\alpha_4 + 3\alpha_5 + 2\alpha_6 + \\ & + 3\alpha_7 + 3\alpha_8 + 2\alpha_9) + (1\ \ 2\ \ 4\ \ 3)(3\alpha_1 + \alpha_6 + 3\alpha_7) + (1\ \ 2)(3\alpha_2 + 3\alpha_8 + 3\alpha_9) + (1\ \ 2\ \ 4) \\ & (2\alpha_1 + 3\alpha_2 + 2\alpha_3 + 2\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7 + 2\alpha_8 + 3\alpha_9) + (1\ \ 2)(3\ \ 4)(3\alpha_1 + 2\alpha_2 + 3\alpha_3 \\ & + 2\alpha_4 + 2\alpha_5 + 2\alpha_6 + 2\alpha_7 + 3\alpha_8 + 3\alpha_9) + (1\ \ 2\ \ 3\ \ 4)(3\alpha_3 + \alpha_4 + 3\alpha_5) + (1\ \ 4\ \ 2\ \ 3)(3\alpha_2 + \\ & + 3\alpha_8 + \alpha_9) + (1\ \ 4\ \ 3)(2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 3\alpha_4 + 2\alpha_5 + 2\alpha_6 + 3\alpha_7 + 3\alpha_8 + 2\alpha_9) + (1\ \ 4\ \ 2) \\ & (2\alpha_1 + 3\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + 3\alpha_6 + 2\alpha_7 + 3\alpha_8 + 2\alpha_9) + (1\ \ 4)(\alpha_1 + 3\alpha_6 + 3\alpha_7) + \\ & + (1\ \ 4\ \ 3\ \ 2)(3\alpha_3 + 3\alpha_4 + \alpha_5) + (1\ \ 4)(2\ \ 3)(2\alpha_1 + 3\alpha_2 + 3\alpha_3 + 2\alpha_4 + 2\alpha_5 + 3\alpha_6 + 3\alpha_7 + \\ & + 2\alpha_8 + 2\alpha_9),\end{aligned}$$

onde $\alpha_i \in \mathbb{F}_5$, para todo $1 \leqslant i \leqslant 9$. Logo, o elemento c que pertence ao código $\mathcal{C}_3 \leqslant \mathbb{F}_5^{24}$ e corresponde a γ através de $\phi : \mathbb{F}_5^{24} \to \mathbb{F}_5 S_4$ é:

$$\begin{aligned}c = {} & (2\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 3\alpha_5 + 3\alpha_6 + 3\alpha_7 + 3\alpha_8 + 3\alpha_9)e_1 + (\alpha_3 + 3\alpha_4 + 3\alpha_5)e_2 + \\ & + (3\alpha_1 + 3\alpha_6 + 3\alpha_7)e_3 + (3\alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + 2\alpha_6 + 3\alpha_7 + 2\alpha_8 + 3\alpha_9)e_4 + \\ & + (3\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4 + 3\alpha_5 + 3\alpha_6 + 2\alpha_7 + 3\alpha_8 + 2\alpha_9)e_5 + (\alpha_2 + 3\alpha_8 + 3\alpha_9)e_6 + \\ & + (3\alpha_3 + 3\alpha_4 + 3\alpha_5)e_7 + (3\alpha_1 + 3\alpha_2 + 2\alpha_3 + 3\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7 + 2\alpha_8 + 2\alpha_9)e_8 + \\ & + (3\alpha_1 + 3\alpha_2 + 3\alpha_3 + 3\alpha_4 + 2\alpha_5 + 3\alpha_6 + 2\alpha_7 + 2\alpha_8 + 3\alpha_9)e_9 + (3\alpha_2 + \alpha_8 + 3\alpha_9)e_{10} + \\ & + (3\alpha_1 + 3\alpha_6 + \alpha_7)e_{11} + (2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + 3\alpha_5 + 3\alpha_6 + 2\alpha_7 + 2\alpha_8 + 3\alpha_9)e_{12} + \\ & + (3\alpha_1 + 3\alpha_2 + 3\alpha_3 + 2\alpha_4 + 3\alpha_5 + 2\alpha_6 + 3\alpha_7 + 3\alpha_8 + 2\alpha_9)e_{13} + (3\alpha_1 + \alpha_6 + 3\alpha_7)e_{14} + \\ & + (3\alpha_2 + 3\alpha_8 + 3\alpha_9)e_{15} + (2\alpha_1 + 3\alpha_2 + 2\alpha_3 + 2\alpha_4 + 3\alpha_5 + 2\alpha_6 + 3\alpha_7 + 2\alpha_8 + 3\alpha_9)e_{16} + \\ & + (3\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + 2\alpha_5 + 2\alpha_6 + 2\alpha_7 + 3\alpha_8 + 3\alpha_9)e_{17} + (3\alpha_3 + \alpha_4 + 3\alpha_5)e_{18} + \\ & + (3\alpha_2 + 3\alpha_8 + \alpha_9)e_{19} + (2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 3\alpha_4 + 2\alpha_5 + 2\alpha_6 + 3\alpha_7 + 3\alpha_8 + 2\alpha_9)e_{20} + \\ & + (2\alpha_1 + 3\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + 3\alpha_6 + 2\alpha_7 + 3\alpha_8 + 2\alpha_9)e_{21} + (\alpha_1 + 3\alpha_6 + 3\alpha_7)e_{22} + \\ & + (3\alpha_3 + 3\alpha_4 + \alpha_5)e_{23} + (2\alpha_1 + 3\alpha_2 + 3\alpha_3 + 2\alpha_4 + 2\alpha_5 + 3\alpha_6 + 3\alpha_7 + 2\alpha_8 + 2\alpha_9)e_{24}.\end{aligned}$$

É possível provar que:

- $\phi'(\mathcal{C}_3)$ é um ideal à esquerda de $\mathbb{F}_5K$,
- ${\sigma'}_{k_8}(\mathcal{C}_3) \neq \mathcal{C}_3$, e
- ${\sigma'}_{k_7}(\mathcal{C}_3) \neq \mathcal{C}_3$ para

$$ {\sigma'}_{k_7} = (1\ 7\ 13\ 15\ 9\ 3)(2\ 21\ 19\ 5\ 11\ 8)(4\ 6\ 20\ 14\ 17\ 23)(10\ 16\ 22\ 24\ 18\ 12) $$

Como

$$ \sigma'(\langle k_8, k_{24}\rangle) \nsubseteq PAut(\mathcal{C}_3) \text{ e } \sigma'(\langle k_7\rangle) \nsubseteq PAut(\mathcal{C}_3) $$

não podemos afirmar que $\mathcal{C}_3$ é um código de grupo abeliano, pois não atende às condições de nosso teorema. Portanto, note que no Teorema 3.5 a condição para $\sigma(A)$ ou $\sigma(B)$ é necessária para afirmar que um código à esquerda (ou à direita) é um código abeliano.

Capítulo 5

Da aplicação dos resultados obtidos a grupos com decomposição m-abeliana

A aplicação dos resultados que obtivemos para o grupo S_4 demonstra que as nossas técnicas têm validade quando aplicadas a alguns códigos cujos grupos associados atendem às exigências estabelecidas nos Teoremas 3.5 e 3.8, ou seja, a extensão do resultado inicial de J.J. Bernal, Á. del Río e J.J. Simón é efetiva. Contudo, considerando que existem famílias de grupos que, independentemente dos códigos determinados sobre estes grupos, atendem ao resultado mais restrito de J.J. Bernal, Á. del Río e J.J. Simón, a exemplo dos grupos com ordem inferior a 127, resta-nos a questão acerca de se algo semelhante poderá ocorrer com a extensão que obtivemos, ou seja: existem famílias de grupos, com decomposição m-abeliana, para os quais a aplicação repetida, isto é, a aplicação iterada para cada passo na redução do número de componentes abelianas, possa determinar, ao final do processo, códigos abelianos?

Neste capítulo apresentamos a proposta de analisar uma família de grupos com decomposição m-abeliana com o objetivo de aplicar os teoremas 3.12 e 3.13 iteradamente para determinar se um G-código $\mathcal{C}$, onde G é um grupo nesta familia, é ou não, um código abeliano. Vale entretanto ressaltar que esta é uma proposta na qual ainda estamos trabalhando, ou seja, que ainda exige formalização, todavia, tudo nos levar a afirmar que ela pode ser inteiramente desenvolvida. Para tal fim, exploramos a família $\mathcal{G}$ de grupos, tal que cada $W \in \mathcal{G}$ é um produto orlado de um número finito de grupos cíclicos C_p, de ordem p. Já vimos que esta família de grupos satisfaz às condições dos resultados mencionados anteriormente.

A fim de simplificar nossa análise, utilizaremos o grupo

$$W = C_2 \, wr \, C_2 \, wr \, C_2 \, wr \, C_2 \in \mathcal{G},$$

que pode ser generalizado usando ideias semelhantes, para um número finito de produtos orlados e para qualquer grupo cíclico C_p de ordem p.

Lembremos que dado G um grupo e $G_1,$, $G_1,$, $\ldots$, G_m subgrupos tais que

$$G = G_1 \times G_2 \times \cdots \times G_m$$

e $\mathbb{F}$ um corpo finito tal que $car(\mathbb{F}) \nmid | G |$, então

$$\mathbb{F}G \cong \mathbb{F}G_1 \otimes \mathbb{F}G_2 \otimes \cdots \otimes \mathbb{F}G_m = \bigotimes_{i=1}^{m} \mathbb{F}G_i.$$

Mostraremos que se I é um ideal de $\mathbb{F}G$, existem ideais I_i em $\mathbb{F}G_i$, para $1 \leqslant i \leqslant m$, tais que

$$I \cong I_1 \otimes \cdots \otimes I_m.$$

De fato, considere o isomorfismo de álgebras

$$\varphi : \mathbb{F}G \to \mathbb{F}G_1 \otimes \mathbb{F}G_2 \otimes \cdots \otimes \mathbb{F}G_m.$$

Dado que φ leva bases em bases, se I é ideal de $\mathbb{F}G$, então $\varphi(I)$ é ideal de $\bigotimes_{i=1}^{m} \mathbb{F}G_i$. Pois, dado que se $\{l_1, \ldots, l_r\}$ é base de I,

$$\begin{aligned} \varphi(l_i) &= \varphi(\sum_{i=1}^{r} a(x_{i_1}, \ldots, x_{i_m})) \\ &= \sum_{i=1}^{r} a(x_{i_1} \otimes \cdots \otimes x_{i_m}). \end{aligned} \tag{5.1}$$

Logo, temos que $\{ \ x_{i_1} \otimes \cdots \otimes, x_{i_m} \ \}_{i=1}^{r}$ define uma base para $\varphi(I)$. Agora, basta definir cada ideal I_i de $\mathbb{F}G_i$ como

$$I_i = \langle x_{1_i}, x_{2_i}, \ldots x_{r_i} \rangle, \text{ com } 1 \leqslant i \leqslant m.$$

Por construção, é simples verificar que $I_1 \otimes \cdots \otimes I_m$ é um ideal de $\bigotimes_{i=1}^{m} \mathbb{F}G_i$ e que $\varphi(I) = I_1 \otimes \cdots \otimes I_m$. Portanto, $I \cong I_1 \otimes \cdots \otimes I_m$.

Retomando o grupo W lembremos que este é um grupo com decomposição 4-abeliana e, neste caso, de acordo com o visto na Proposição 3.14, $W = A_1 \rtimes A_2 \rtimes A_3 \rtimes C_2$, com A_i abelianos, para $1 \leqslant i \leqslant 3$. Por outra parte, da definição de produto orlado, e denotando por $H_1 = C_2 \, wr \, C_2 \, wr \, C_2$, é possível reescrever o grupo W como

$$W = (H_1 \times H_1) \rtimes C_2.$$

Dado $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid | W |$, tome $\mathcal{C}$ um W-código sobre $\mathbb{F}$, aplicando o Teorema 3.12, temos que $\mathcal{C}$ também pode ser interpretado como um K_1-código à esquerda (ou à direita), para K_1 o grupo definido por:

$$K_1 = H_1 \times H_1 \times \sigma(C_2),$$

onde σ é o anti-isomorfismo apresentado no Lema 2.11. Pelo visto acima, note que, se I é o ideal à esquerda de $\mathbb{F}K_1$ correspondente ao código $\mathcal{C}$, então existem ideais bilaterais ou laterais I_1, I_2, I_3 tais que I_1 e I_2 são ideais de $\mathbb{F}H$ e I_3 é ideal de $\mathbb{F}\sigma(C_2) \cong \mathbb{F}C_2$. Em consequência, existem subcódigos $\mathcal{C}_1$, $\mathcal{C}_2$ e $\mathcal{C}_3$ sobre $\mathbb{F}$ correspondentes aos ideais I_1, I_2 e I_3, respectivamente, tais que

$$\mathcal{C} \cong \mathcal{C}_1 \otimes \mathcal{C}_2 \otimes \mathcal{C}_3.$$

Observe que o subcódigo $\mathcal{C}_3$ é um código de grupo abeliano, pois I_3 é um ideal de uma álgebra de grupo de um grupo abeliano. Como $\mathcal{C}_1$ e $\mathcal{C}_2$ são H_1-códigos ou H_1-códigos à esquerda (ou à direita) e supondo que eles verificam as hipóteses dos Teoremas 3.12 ou 3.13, logo o problema se reduz a estudar os H_1-códigos.

Suponha agora que $\mathcal{C}'$ é um H_1-código ou um H_1-código à esquerda (ou à direita), denote por $H_2 = C_2 \, wr \, C_2$, assim $H_1 = (H_2 \times H_2) \rtimes C_2$ e reproduzindo o processo anterior obteremos um grupo $K_2 = H_2 \times H_2 \times C_2$ e subcódigos $\mathcal{C}'_1$, $\mathcal{C}'_2$ e $\mathcal{C}'_3$ tais que, $\mathcal{C}' \cong \mathcal{C}'_1 \otimes \mathcal{C}'_2 \otimes \mathcal{C}'_3$. Com o mesmo raciocínio anterior, temos que $\mathcal{C}'_1$ e $\mathcal{C}'_2$ são H_2-códigos ou H_2-códigos à esquerda (ou à direita), caso $\mathcal{C}'_1$ e $\mathcal{C}'_2$ atendam às hipóteses dos Teoremas 3.12 ou 3.13, logo o problema se reduz a estudar os H_2-códigos.

Se $\mathcal{C}''$ é um H_2-código repetimos o procedimento anterior e obtemos um grupo $K_3 = C_2 \times C_2 \times C_2$, o que afirmaria que $\mathcal{C}''$ é um código abeliano. Assim, o K-código abeliano obtido é da forma

$$\mathcal{C} \cong \mathcal{C}_{11} \otimes \mathcal{C}_{12} \otimes \mathcal{C}_{13} \otimes \mathcal{C}_{21} \otimes \mathcal{C}_{22} \otimes \mathcal{C}_{23} \otimes \mathcal{C}_3,$$

com

$$\mathcal{C}_1 \cong \mathcal{C}_{11} \otimes \mathcal{C}_{12} \otimes \mathcal{C}_{13},$$

$$\mathcal{C}_2 \cong \mathcal{C}_{21} \otimes \mathcal{C}_{22} \otimes \mathcal{C}_{23},$$

com $\mathcal{C}_{11}$, $\mathcal{C}_{12}$, $\mathcal{C}_{21}$ e $\mathcal{C}_{22}$ K_3-códigos e $\mathcal{C}_{13}$, $\mathcal{C}_{23}$ e $\mathcal{C}_3$ códigos abelianos, onde claramente $K = K_3 \times K_3 \times C_2 \times K_3 \times K_3 \times C_2 \times C_2$ é abeliano.

No primeiro passo da iteração, para obter K_1 precisamos do anti-isomorfismo $\sigma : W \to C_{S_{|W|}}(W)$, definido no Lema 2.11. Também queremos que o H_1-código ou H_1-

código à esquerda (ou à direita) $\mathcal{C}_1$, reelembrando que $H_1 = C_2 \, wr \, C_2 \, wr \, C_2$, verifica as condições do Teorema 3.12 ou 3.13; caso $\mathcal{C}_1$ seja um H_1-código podemos aplicar novamente o Teorema 3.12. Caso contrário, $\mathcal{C}_1$ é um H_1-código à esquerda (ou à direita) e aqui gostaríamos que o H_1-código à esquerda (ou à direita) $\mathcal{C}_1$ verificasse as hipóteses do Teorema 3.13, isto é, $\sigma_1(C_2) \subseteq PAut(\mathcal{C}_1)$, com $\sigma_1 : H_1 \to C_{S_{|H_1|}}(H_1)$ o anti-isomorfismo do Lema 2.11. O mesmo raciocínio aplicamos para o H_1-código ou H_1-código à esquerda (ou à direita) $\mathcal{C}_2$.

Aplicando em cada iteração este argumento, observamos que aparacem novos subgrupos H_i e K_i, novos subćodigos $\mathcal{C}_i$ associados ao código anterior, um novo anti-isomorfismo σ_i que deve verificar $\sigma_i(C_2) \subseteq PAut(\mathcal{C}_i)$.
Embora ainda não tenhamos conseguido formalizar concretamente, podemos conjeturar o seguinte:

- existe uma relação entre o anti-isomorfismo σ_{i-1}, obtido na iteração i, e o anti-isomorfismo σ_i dada pela restrição de σ_{i-1} ao grupo H_i.

- se $\mathcal{C}_{i-1}$ é um H_{i-1}-código e $\mathcal{C}_i$ é um subcódigo de $\mathcal{C}_{i-1}$, existe uma relação entre o $PAut(\mathcal{C}_{i-1})$ e o $PAut(\mathcal{C}_i)$, tal que $PAut(\mathcal{C}_i)$ será um subgrupo de $PAut(\mathcal{C}_{i-1})$.

Conclusão

Neste trabalho, analisamos e estendemos principalmente o resultado de J.J. Bernal, Á del Río e J.J. Simón, [5], que apresenta uma classe de grupos que contém estritamente a família dos grupos abelianos, na qual todo código de grupo, para um grupo nesta família, é um código de grupo abeliano.

Estudamos, para os códigos de grupo, sob quais condições os G-código à esquerda ou à direita, com $G = AB$, são códigos de grupo abelianos. Exibimos S_3-códigos à esquerda que são códigos de grupo abeliano.

Mostramos que o grupo simétrico S_4 tem decomposição 3-abeliana. Motivados pelo grupo S_4, dado um grupo $H = ABD$, que tem decomposição 3-abeliana, apresentamos condições sobre A, B e D para que os H-códigos ou H-códigos laterais sejam K-códigos laterais, para K um grupo com decomposição abeliana. Comprovamos que é possível determinar se um S_4-código é um código de grupo abeliano aplicando os resultados obtidos.

Consideramos grupos $G = A_1A_2 \dots A_m$ com decomposição m-abeliana. Provamos que G-códigos ou G-códigos laterais, sobre determinadas condições, são K-códigos laterais onde K é um grupo com decomposição t-abeliana com $t < m$, com o fim de determinar códigos abelianos. Apresentamos uma família de grupos que verificam as exigências de nossos resultados.

Após o desenvolvimento deste trabalho concluímos que temos mais recursos para estudar G-códigos e G-códigos laterais, com G é um grupo com decomposição m-abeliana e determinar se eles podem ser ou não códigos abelianos. Vimos também que os resultados obtidos ainda são válidos se estendemos o corpo.

Como perspectiva de continuidade deste tema poderíamos aprofundar o estudos com a finalidade de melhorar as condições para determinar códigos abelianos. Também podemos pensar em determinar mais famílias que verificam as condições dos resultados obtidos nos capítulos anteriores para estudar os G-códigos e assim poder determinar, se

possível, códigos abelianos. Outra opção é explorar os parâmetros dos G-códigos para obter os processos de codificação e decodificação .

Referências Bibliográficas

[1] A. Abért, *Symmetric group as products of abelian subgroups*, Bull. London Math Soc., 34 (2002), 451-456.

[2] R. Bercov and L. Moser, *On abelian permutation groups* , Canad. Math., Bull 8(5) (1965), 627-630.

[3] S. Berman, *On the theory of group codes*, Kibernetika, 3(1) (1967), 31-39.

[4] S. Berman, *Semisimple cyclic and abelian codes II*, Kibernetika, 3(3) (1967), 21-30.

[5] J.J. Bernal, Á del Río and J.J. Simón, *An intrinsecal description of group codes*, Des. Codes Cryptogr., 51(3) (2009), 289-300.

[6] J.J. Bernal, Á del Río and J.J. Simón, *Group codes structures of affine-invariant codes*, Journal of Algebra, 325 (2011), 269-281.

[7] A. Dür, *The automorphism groups of Reed- Solomon codes*, J. Combin. Theory, Serie A 44 (1987), 69-82.

[8] C. García Pillado, S. González, C. Martínez, V. Markov and A. Nechaev, *Group code over non-abelian groups* , J. Algebra Appl., 12(7) (2013).

[9] C. García Pillado, S. González, C. Martínez, V. Markov and A. Nechaev, *When are all group codes of non comutative group abelian?* , J. Math. Sci., 186(5) (2012), 578-585.

[10] R. Hill, *A first course in coding theory*, Oxford University Press Inc, United States, 1986.

[11] T. Kasami, S. Lin and W. W. Peterson, *New generalizations of the Reed- Muller codes part I: primitive codes*, IEEE Trans. Inform. Theory, IT-14 (1968), 189-199.

[12] A. V. Kelarev and P. Solé, *Error correcting codes as ideals in group rings*, Des. Codes Chryptogr., 273 (2001), 11-18.

[13] P. Landrock and O. Manz, *Classical codes as ideals in group algebras*, Des. Codes Chryptogr., 2 (1992), 273-285.

[14] P. Landrock and O. Manz, *The extended Golay codes considered as ideals*, J. Combin. Theory, Series A 55 (1990), 235-246.

[15] D. E. Muller, *Application of boolean algebra to switching circuit design and to error detection*, IEEE Trans. Comput., 3 (1954), 6-12.

[16] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, 3rd ed., John Wiley & Sons, Inc (1998).

[17] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002.

[18] C. Polcino Milies, *Introdução à Teoria dos Códigos*, Colóquio de Matemática UFMS,(2009).

[19] I. S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, J. Siam 8 (1960), 300-304.

[20] R.E. Sabin, and S.J. Lomonaco, *Metacyclic error-correctting codes*, AAECC 6 (1995), 191-210.

[21] A. Schäfer, *Two Sided and Abelian Group Ring Codes*, Masters Thesis, (2012).

[22] C.E. Shannon, *A mathematical theory of communication*, Bell Systems Technical Journal, 27:379-423 (1948); 623-656.

[23] http://www.gap-system.org/.

Universidade Federal da Bahia - UFBA
Instituto de Matemática / Colegiado da Pós-Graduação em Matemática

Av. Adhemar de Barros, s/n, Campus Universitário de Ondina, Salvador - BA
CEP: 40170 -110
<http://www.pgmat.ufba.br>