GUSTAVO TERRA BASTOS

COMPARAÇÃO DE TÉCNICAS PARA O CÁLCULO DE IDEMPOTENTES GERADORES DE CÓDIGOS ABELIANOS

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

VIÇOSA
MINAS GERAIS - BRASIL
2013

Ficha catalográfica preparada pela Seção de Catalogação e Classificação da Biblioteca Central da UFV

T
B327c
2013

Bastos, Gustavo Terra, 1986-
Comparação de técnicas para o cálculo de idempotentes geradores de códigos abelianos / Gustavo Terra Bastos. – Viçosa, MG, 2013.
vii, 82f. : il. ; 29cm.

Orientador: Marinês Guerreiro
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 81-82

1. Teoria dos grupos. 2. Álgebra.
I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática.
II. Título.

CDD 22. ed. 512.2

GUSTAVO TERRA BASTOS

COMPARAÇÃO DE TÉCNICAS PARA O CÁLCULO DE IDEMPOTENTES GERADORES DE CÓDIGOS ABELIANOS

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

APROVADA: 21 de fevereiro de 2013.

Cícero Fernandes de Carvalho	Rogério Carvalho Picanço
Allan de Oliveira Moura (Coorientador)	Raul Antonio Ferraz (Coorientador)

Marinês Guerreiro
(Orientadora)

Não há caminho errado. O aprendizado e a experiência estão em todos os caminhos.
Gasparetto

Agradecimentos

Em primeiro lugar, gostaria de agradecer a Deus pela oportunidade de ter uma vida maravilhosa, ao lado de pessoas que fazem valer a pena cada minuto vivido. Só Ele sabe o quanto eu desejei chegar aonde estou e sempre esteve ao meu lado em todos os momentos. Obrigado Pai por sempre me iluminar e me guiar.

Não existem palavras para expressar o quanto eu sou agradecido por ter os meus pais Arlindo e Luiza e os meus irmãos Felipe e André como base da minha vida. Obrigado por serem o meu maior orgulho. Este momento não seria possível se não fossem os inúmeros sacrifícios feitos desde os estudos iniciais. Esta é uma vitória nossa !

A minha namorada, amiga e psicóloga Mariela, obrigado por estar comigo sempre: na alegria, na tristeza e na insônia. Algumas vezes você acreditou mais em mim do que eu mesmo. Você é um grande exemplo para mim e me espelho sempre em você para me tornar uma pessoa melhor. Te amo!

Já dizia Machado de Assis: *"Benditos sejam todos os amigos de raízes, verdadeiros. Porque amigos são herdeiros da real sagacidade. Ter amigos é a melhor cumplicidade!"*. Sou muito grato por ter feito grandes amigos em Varginha, Campestre (PMMG), São João del Rei e Viçosa (os amigos do Mestrado, em especial, as Alanas, Anna Paula, Fernanda e Michely que nesta etapa dividiram momentos de diversão, de estudos e de insônia comigo). Obrigado pela palavra amiga e pelos bons momentos que dividimos!

A minha orientadora Marinês, obrigado por confiar em mim, pela paciência e pelos ensinamentos repassados. Aos co-orientadores Raul e Allan, agradeço as sugestões dadas para a melhoria do trabalho desenvolvido. Também gostaria de agradecer aos professores Cícero e Rogério pela participação na banca avaliadora e pelas contribuições dadas a este trabalho.

Obrigado aos mestres da graduação e do mestrado por todo conhecimento matemático repassado durante estes anos. Em especial, muito obrigado aos professores Anderson e Rogério por confiarem em mim e acreditarem no meu potencial.

Obrigado Paulo, Miriam e Sr. Jair por todo suporte burocrático/administrativo e, claro, pelo cafezinho!

Obrigado à CAPES pelo apoio financeiro.

Sumário

Resumo **vi**

Abstract **vii**

Introdução **1**

1 Preliminares Algébricos **5**

1.1 Tópicos de Teoria dos Números 5

1.2 Anéis de Grupo 6

1.2.1 Fatos Básicos 6

1.2.2 Semissimplicidade 12

1.2.3 Álgebras de Grupo de Grupos Abelianos 14

2 Introdução à Teoria dos Códigos **18**

2.1 Códigos Corretores de Erros 18

2.1.1 Métrica de Hamming 18

2.2 Códigos Lineares 19

2.2.1 Códigos Cíclicos 20

3 Códigos Abelianos Minimais **23**

3.1 O Número de Componentes Simples 24

3.2 Códigos Cíclicos Minimais 26

3.3 Códigos Abelianos Minimais 28
3.3.1 Subgrupos e Idempotentes 31

4 A λ-Aplicação e os Idempotentes Primitivos em Anéis Semissimples 33

4.1 A λ-aplicação e as classes ciclotômicas 33
4.2 Idempotentes Primitivos em $\mathcal{R}_m = \frac{\mathbb{F}_l[x]}{\langle x^m-1\rangle}$ 42

5 Códigos Abelianos Binários Minimais 48

5.1 Resultados Auxiliares 48
5.2 Códigos Abelianos Minimais Binários 50
5.2.1 Idempotentes Primitivos 51
5.2.2 Códigos em $\mathbb{F}_2\left(\mathcal{C}_p \times \mathcal{C}_q\right)$ 53
5.2.3 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p^m} \times \mathcal{C}_{q^n}\right)$, para $m \geq 2, n \geq 2$ 58
5.2.4 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}\right)$ 59
5.3 Idempotentes Primitivos de $\mathbb{F}_2\left(\mathcal{C}_{121} \times \mathcal{C}_{169}\right)$ 65

6 Comparação de técnicas para códigos de comprimento $p^n q$ 67

6.1 Exemplos Comparativos 67
6.1.1 Idempotentes Primitivos de $\mathcal{R}_{245} = \dfrac{\mathbb{F}_3[x]}{\langle x^{245}-1\rangle}$ 67
6.1.2 Idempotentes Primitivos de $\mathbb{F}_3\left(\mathcal{C}_{49} \times \mathcal{C}_5\right)$ 71
6.2 Idempotentes Primitivos em $\mathbb{F}_l\left(\mathcal{C}_{p^n} \times \mathcal{C}_q\right)$ 73
6.3 Considerações Finais 80

Referências Bibliográficas 81

Resumo

BASTOS, Gustavo Terra, M.Sc., Universidade Federal de Viçosa, Fevereiro de 2013. **Comparação de técnicas para o cálculo de idempotentes geradores de códigos abelianos**. Orientador: Marinês Guerreiro. Coorientadores: Allan de Oliveira Moura e Raul Antonio Ferraz.

Neste trabalho, desenvolvemos um estudo de técnicas polinomial e de álgebra de grupo de grupos abelianos para o cálculo de idempotentes primitivos em anéis semissimples, sob certas hipóteses. Estes idempotentes primitivos podem ser vistos como geradores de códigos abelianos minimais. Apresentamos resultados recentes para ambas as técnicas e, a partir de exemplos, realizamos um estudo comparativo das mesmas. Nesta comparação, identificamos possíveis erros na técnica polinomial abordada e propomos as devidas correções para o caso de códigos de comprimento $p^n q$, utilizando ambas as abordagens para a demonstração do resultado correto.

Abstract

BASTOS, Gustavo Terra, M.Sc., Universidade Federal de Viçosa, February, 2013. **Comparison of techniques for the computation of the generator idempotents of abelian codes**. Adviser: Marinês Guerreiro. Co-advisers: Allan de Oliveira Moura and Raul Antonio Ferraz.

In this work, under certain hypotheses, we study two techniques for the computation of primitive idempotents in semissimple rings, namely, the polynomial and the group algebra techniques, the latter for abelian groups. These primitive idempotents can be seen as generator idempotents of minimal abelian codes. We present recent results for both techniques and, with examples, we compare them. In this comparison, we identify possible errors in the polynomial technique and we propose the corrections for the case of codes of length $p^n q$, using the both approaches to prove the correct result.

Introdução

A transmissão de dados através dos meios de comunicação sofrem a interferência de fatores externos, como por exemplo, os campos magnéticos, o que pode ocasionar distorção nas mensagens transmitidas, sendo que em alguns casos, não é possível ou desejável que essa mensagem seja retransmitida. A Teoria de Códigos Corretores de Erros busca adicionar informação a essa mensagem, para que possíveis erros possam ser detectados e corrigidos. A teoria básica adotada neste trabalho pode ser vista em [13] e [19].

A utilização de teorias matemáticas mais avançadas permitiu desenvolver códigos com parâmetros melhores e mais elaborados. Uma classe especial de códigos corretores de erros, e que será usada constantemente neste trabalho, é a classe dos códigos lineares. Um código linear é um subespaço próprio do espaço vetorial $\mathbb{F}_q^n$, onde $\mathbb{F}_q$ é um corpo finito com q elementos e n é um número natural. Em particular, um código linear $\mathfrak{C}$ é dito cíclico se, para qualquer palavra $(v_0, v_1, \ldots, v_{n-1})$ em $\mathfrak{C}$, a palavra $(v_{n-1}, v_0, \ldots, v_{n-2})$ também está em $\mathfrak{C}$. Os códigos cíclicos são muito utilizados por formarem uma classe de códigos lineares que possui bons algoritmos de codificação e de decodificação.

É simples verificar que as estruturas algébricas $\mathbb{F}_q^n$ e $\mathcal{R}_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ são isomorfas e, em particular, qualquer código cíclico de $\mathbb{F}_q^n$ é isomorfo a um ideal não trivial de $\mathcal{R}_n$. Ainda, sob certas condições, o anel $\mathcal{R}_n$ é semissimples e pode ser decomposto como soma direta de ideais minimais, de acordo com o Teorema de Wedderburn-Artin [7]. Como qualquer ideal em $\mathcal{R}_n$ é escrito como soma de alguns ideais minimais e todo ideal minimal de um anel semissimples é gerado por um idempotente primitivo, então estudar códigos cíclicos é equivalente a estudar idempotentes primitivos geradores dos ideais minimais de $\mathcal{R}_n$.

Uma outra abordagem para o estudo de códigos corretores de erros é utilizar a estrutura algébrica chamada álgebra de grupo, cuja teoria básica pode ser encontrada em [7] e [22]. Observamos que o espaço vetorial $\mathbb{F}_q^n$ também pode ser construído a partir de um isomorfismo entre $\mathbb{F}_q^n$ e a álgebra de grupo $\mathbb{F}_q\mathcal{C}_n$, onde $\mathcal{C}_n$ é o grupo cíclico de ordem n. Este isomorfismo estabelece uma correspondência entre os códigos cíclicos de $\mathbb{F}_q^n$ e os ideais da álgebra de grupo $\mathbb{F}_q\mathcal{C}_n$. Desta maneira, os códigos cíclicos também serão vistos

como ideais de $\mathbb{F}_q\mathcal{C}_n$.

Seja $\mathbb{F}G$ a álgebra de grupo de um grupo G sobre um corpo $\mathbb{F}$. Estendendo os resultados sobre grupos cíclicos, S.D.Berman [3] e F.J MacWilliams [18] definiram **códigos abelianos** como ideais (próprios) na álgebra de grupo de um grupo abeliano sobre um corpo finito. Já para códigos sobre grupos não abelianos, podemos citar os trabalhos [8] e [25]. Por fim, de forma geral, em [5] os autores definem **códigos de grupo** sobre grupos finitos quaisquer.

Um elemento $e \in \mathbb{F}G$ é idempotente se $e^2 = e$. Observamos ainda que um elemento em $\mathbb{F}G$ é central se ele comuta com todos os outros elementos da álgebra. Um idempotente central não nulo e é chamado **primitivo** se ele não pode ser decomposto na forma $e = e' + e"$, onde e' e $e"$ são ambos idempotentes centrais não nulos tais que $e'e" = e"e' = 0$. Em uma álgebra de grupo $\mathbb{F}G$, quando $car(\mathbb{F}) \nmid |G|$, os idempotentes primitivos centrais são geradores dos ideais bilaterais minimais. Dois idempotentes e' e $e"$ são ortogonais se $e'e" = e"e' = 0$.

Em particular, o conjunto dos idempotentes primitivos de $\mathbb{F}G$ geram os ideais minimais de $\mathbb{F}G$, aos quais nos referimos como **códigos minimais**.

Os indianos Pruthi e Arora [23] e [1] desenvolveram técnicas para apresentar os idempotentes primitivos dos anéis $\mathcal{R}_m = \dfrac{\mathbb{F}_q[x]}{\langle x^m - 1\rangle}$, onde $m = p^n$ ou $m = 2p^n$, para p um primo ímpar, n um inteiro positivo e q é uma raiz primitiva módulo p^n. Em [11], Ferraz e Polcino Milies obtiveram, para o anel $\mathbb{F}_q\mathcal{C}_m$, os mesmos idempotentes primitivos e é notório que a linguagem e a expressão destes elementos se mostraram muito mais simples do que em [23] e [1]. O cálculo dos idempotentes é direto e depende essencialmente da estrutura dos subgrupos de $\mathcal{C}_m$.

Nos últimos anos estes resultados foram estendidos. Em [16], via a abordagem polinomial, é possível expressar os idempotentes primitivos para anéis do tipo $\mathcal{R}_m$, onde $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, com cada p_i um número primo positivo, $p_i \neq p_j$, para $1 \leq i \neq j \leq r$. Já em [6], a partir da abordagem de álgebras de grupo, são exibidos os idempotentes primitivos de $\mathbb{F}_2\left(G_p \times G_q\right)$, onde G_p e G_q são p e q-grupos abelianos, respectivamente. Em ambas as técnicas, existem restrições sobre a característica do corpo sobre o qual estão definidos os códigos. Dado G um grupo abeliano e H um subgrupo de G, dizemos que H é um **subgrupo co-cíclico** de G se o grupo quociente G/H é não trivial e cíclico. Em [10], os autores tratam de uma generalização das hipóteses sobre a ordem do grupo abeliano G e apresentam a expressão dos idempotentes primitivos que dependem dos subgrupos co-cíclicos de G.

Neste trabalho apresentamos as abordagens polinomial e de álgebra de grupo para o cálculo dos idempotentes geradores de códigos abelianos, a partir do estudo detalhado dos artigos [16], [11] e [6]. Além disso, exibimos exemplos para casos particulares, que nos apontam quais as vantagens e desvantagens de cada técnica. Por fim, explicitamos os

idempotentes primitivos da álgebra de grupo $\mathbb{F}_l\left(\mathcal{C}_{p^n} \times \mathcal{C}_q\right)$, onde $l \neq 2$, com o auxílio da técnica polinomial.

O Capítulo 1 desta Dissertação está divido em duas seções. Na primeira, definimos o que são resíduos quadráticos e não quadráticos módulo um inteiro m e apresentamos alguns resultados importantes da Teoria de Números utilizados, em especial, no Capítulo 4. Na segunda seção definimos o que é uma álgebra de grupo e exibimos alguns resultados da teoria importantes para este trabalho. Vale destacar o Teorema de Perlis-Walker sobre a decomposição da álgebra de grupo de grupos abelianos e a sua demonstração. Este resultado é fundamental para determinar o número de códigos minimais em uma álgebra de grupo de um grupo abeliano.

No Capítulo 2, apresentamos uma introdução à Teoria de Códigos Corretores de Erros (ou simplesmente Teoria de Códigos), definindo códigos lineares e códigos cíclicos, que são de interesse especial para este trabalho. Além disso, sob certas hipóteses, relacionamos códigos minimais via as abordagens polinomial e de álgebra de grupo.

O Capítulo 3 é dedicado ao estudo dos códigos abelianos minimais. Iniciamos com os resultados de Ferraz [9], onde é feito um paralelo entre o comportamento do número de componentes simples em uma álgebra de grupo racional, que mostra-se como um limitante inferior, via o Teorema de Perlis-Walker, para o número de componentes simples de uma álgebra de grupo semissimples sobre corpos finitos. Sob certas hipóteses, definimos álgebras de grupo que se comportam, com relação ao número de componentes simples, como uma álgebra de grupo racional e assim descrevemos todos os idempotentes primitivos para casos particulares do tipo p^n e $2p^n$, análogos aos trabalhos [23] e [1]. Estes resultados são fundamentais e sugerem a expansão desta técnica para casos mais gerais. Na última seção estendemos estes resultados para álgebras de grupo semissimples $\mathbb{F}G$, onde G é um grupo abeliano finito e $\mathbb{F}$ um corpo finito. Por fim, relacionamos os subgrupos co-cíclicos com os idempotentes primitivos da álgebra de grupo. Um exemplo particular desta técnica é apresentado no último capítulo para fins de comparação.

No Capítulo 4, apresentamos a **λ-técnica**, baseada em [16]. Para um número natural $r \geq 1$ e um inteiro $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, com cada p_i um número primo positivo, $p_i \neq p_j$, l uma raiz primitiva módulo $p_i^{\alpha_i}$, onde $mdc\left(\frac{\varphi\left(p_i^{\alpha_i}\right)}{2}, \frac{\varphi\left(p_j^{\alpha_j}\right)}{2}\right) = 1$ para cada $1 \leq i \neq j \leq r$ e l coprimo com m, definimos uma bijeção, conhecida por **λ-aplicação**, entre os conjuntos $A_1 \times A_2 \times \ldots \times A_r$ e A, onde $A_i = \{0, 1, 2, \ldots, p_i^{\alpha_i} - 1\}$, para cada $1 \leq i \leq r$ e $A = \{0, 1, 2, \ldots, m\}$, que nos permite definir e expressar todas as classes l ciclotômicas módulo m. Com estes resultados, a λ-técnica propõe a descrição dos idempotentes primitivos do anel $\mathcal{R}_m = \dfrac{\mathbb{F}_l[X]}{\langle X^m - 1\rangle}$ a partir das expressões dos idempotentes primitivos dos anéis $\mathcal{R}_{p_i^{\alpha_i}} = \dfrac{\mathbb{F}_{l^2}[X]}{\left\langle X^{p_i^{\alpha_i}} - 1\right\rangle}$, construídos a partir dos conjuntos de resíduos quadráticos e não

quadráticos módulo $p_i^{\alpha_i}$, para cada $1 \leq i \leq r$. Um exemplo é apresentado no último capítulo para fins de comparação entre as técnicas.

Como um caso particular do Capítulo 3, no Capítulo 5 descrevemos os códigos cíclicos binários minimais de $\mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2})$, $\mathbb{F}_2(\mathcal{C}_{p_1{}^m} \times \mathcal{C}_{p_2{}^n})$ e $\mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3})$, onde p_1, p_2 e p_3 são primos ímpares distintos dois a dois e m e n são inteiros positivos. Por fim, apresentamos um exemplo completo de um caso particular.

No Capítulo 6, exibimos todas as expressões dos idempotentes primitivos da álgebra de grupo $\mathbb{F}_3(\mathcal{C}_{49} \times \mathcal{C}_5)$ e do anel $\dfrac{\mathbb{F}_3[X]}{\langle x^{245}-1\rangle}$, onde observamos diferenças entre as expressões dadas, o que nos sugerem possíveis erros na λ-técnica, uma vez que, com o uso do software MAPLE, as expressões obtidas a partir da técnica de álgebra de grupo se mostraram ser de fato idempotentes. Ainda, na Seção 2 do Capítulo 6, apresentamos todas as expressões dos idempotentes primitivos da álgebra $\mathbb{F}_l(\mathcal{C}_{p^n} \times \mathcal{C}_q)$ (onde l é o mesmo primo positivo que satisfaz as hipóteses dadas no Capítulo 4), com o auxílio das expressões dadas em [2]. Com estas expressões, sugerimos correções para as expressões obtidas a partir da λ-técnica.

Capítulo 1

Preliminares Algébricos

1.1 Tópicos de Teoria dos Números

Nesta seção apresentamos a definição de resíduos quadráticos e não quadráticos módulo p, onde p é um número primo, e alguns resultados que são utilizados neste trabalho. Como referências para as demonstrações dos resultados indicamos [21] e [17].

Definição 1.1.1. *Seja m um número inteiro positivo. Para todo $a \in \mathbb{Z}$ tal que $mdc(a, m) = 1$, a é dito um **resíduo quadrático módulo** m se a congruência $x^2 \equiv a \,(mod\, m)$ possui pelo menos uma solução, caso contrário, dizemos que a é um **resíduo não quadrático módulo** m.*

Podemos considerar como resíduos quadráticos ou não quadráticos somente os elementos do sistema completo de resíduos módulo m $\{1, \ldots, m-1\}$. De fato, se a é resíduo quadrático módulo m (respectivamente resíduo não quadrático), então $a + m$ é resíduo quadrático módulo m (respectivamente resíduo não quadrático).

Definição 1.1.2. *Sejam p um primo ímpar e $a \in \mathbb{Z}$. O **símbolo de Legendre** $\left(\frac{a}{p}\right)$ é definido por:*

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático módulo } p; \\ -1, & \text{se } a \text{ é um resíduo não quadrático módulo } p; \\ 0, & \text{se } p|a. \end{cases}$$

Teorema 1.1.3 ([21], Teorema 3.1)**.** *Sejam p um primo ímpar e $a, b \in \mathbb{Z}$. Então:*

(i) $\left(\frac{a}{p}\right) \equiv a^{\left(\frac{p-1}{2}\right)} (mod\, p)$.

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(iii) *Se* $a \equiv b\,(mod\,p)$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(iv) *Se* $mdc(a,p) = 1$, *então* $\left(\frac{a^2}{p}\right) = 1$ *e* $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

(v) $\left(\frac{1}{p}\right) = 1$ *e* $\left(\frac{-1}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)}$.

Teorema 1.1.4. *(Lei da Reciprocidade Quadrática de Gauss) Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Observação 1.1.5. *Se p e q são primos ímpares distintos da forma* $4k+3$, *então uma das congruências* $x^2 \equiv p\,(mod\,q)$ *e* $x^2 \equiv q\,(mod\,p)$ *é solúvel e a outra não. Se pelo menos um dos primos é da forma* $4k+1$, *então ambas as congruências* $x^2 \equiv p\,(mod\,q)$ *e* $x^2 \equiv q\,(mod\,p)$ *são ou solúveis ou não solúveis.*

Observação 1.1.6. *De acordo com a Definição 1.1.1 e [17, Teorema 79], podemos escrever* $\mathbb{Z}_p = \{0\} \cup R \cup N$, *onde R denota o conjunto dos resíduos quadráticos módulo p, N o conjunto dos resíduos não quadráticos módulo p e* $|R| = |N| = \frac{p-1}{2}$.

Observação 1.1.7. *Da definição de resíduos quadráticos, para qualquer primo p, claramente* $\overline{1} \in R$. *Além disso, se* $\overline{2}$ *gera* $U(\mathbb{Z}_p)$, *então* $\overline{2} \in N$. *De fato, suponha* $\overline{2} \in R$. *Assim,* $\mathbb{Z}_p \setminus \{0\} = U(\mathbb{Z}_p) = \left\{\overline{2}^i, i = 1, ..., \varphi(p)\right\} = R$, *de acordo com o Teorema 1.1.3. Portanto,* $\mathbb{Z}_p = \{0\} \cup R$, *que é um absurdo.*

Lema 1.1.8 ([17], Teorema 83)**.** *Seja p um primo ímpar. O elemento* $\overline{-1}$ *é um resíduo quadrático em* $\mathbb{Z}_p$ *se, e somente se,* $p \equiv 1(mod\,4)$.

1.2 Anéis de Grupo

Nesta seção introduzimos a definição de anel de grupo e, em particular, de álgebra de grupo. Além disso, discutiremos condições sobre um grupo G e sobre um anel R para que o anel de grupo RG seja semissimples e demonstraremos o Teorema de Perlis-Walker. As demonstrações omitidas podem ser encontradas em [22].

1.2.1 Fatos Básicos

Seja G um grupo e R um anel com unidade. Denotemos por RG o conjunto de todas as combinações lineares da forma

$$\alpha = \sum_{g \in G} a_g g,$$

onde $a_g \in R$ e $a_g = 0$, para quase todos $g \in G$, isto é, somente um número finito de coeficientes são diferentes de 0 em cada soma.

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

$$supp(\alpha) = \{g \in G : a_g \neq 0\}.$$

Uma conseqüência imediata da definição é que, dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, temos $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Definimos a **soma** de dois elementos em RG componente a componente, isto é,

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g.$$

Agora, dados dois elementos $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, definimos o **produto** deles por

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh.$$

Reordenando os termos na fórmula acima, podemos escrever o produto $\alpha\beta$ como

$$\alpha\beta = \sum_{u \in G} d_u u,$$

onde

$$d_u = \sum_{gh=u} a_g b_h.$$

Com as operações acima, RG é um anel com unidade $1_{RG} = \sum_{g \in G} u_g g$, onde o coeficiente correspondente a unidade do grupo é igual a 1_G e $u_g = 0$, para todos os outros elementos de G.

Definimos também um produto de elementos em RG por elementos $\lambda \in R$ por

$$\lambda \left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} (\lambda a_g) g.$$

É fácil verificar que RG é um R-módulo. Na verdade, se R é comutativo, RG é uma álgebra sobre R.

Definição 1.2.1. *O conjunto RG, com as operações definidas acima, é chamado* ***anel de grupo de*** *G* ***sobre*** *R. No caso em que R é comutativo, RG é chamado* ***álgebra de grupo de*** *G* ***sobre*** *R.*

Definição 1.2.2. *Sejam V e W RG-módulos. Uma aplicação $\varphi : V \to W$ é dita ser um RG-homomorfismo se φ é um R-homomorfismo e*

$$\varphi(vg) = \varphi(v)\, g,$$

para todo $v \in V$ e $g \in G$.

Em [22, Página 134], os próximos dois resultados abaixo são dados como exercícios.

Teorema 1.2.3 (Exercício 4)**.** *Se R é um anel comutativo com unidade e G e H são grupos quaisquer, então*

$$(RG)H \cong R(G \times H) \cong RG \otimes_R RH.$$

Demonstração. Defina o homomorfismo $\overline{\varphi}$ do grupo $G \times H$ no grupo das unidades de $(RG)H$, dado por $\overline{\varphi}((g,h)) = gh$. É simples verificar que $\overline{\varphi}$ é um homomorfismo injetor.

Vamos estender $\overline{\varphi}$ linearmente da seguinte maneira:

$$\begin{array}{rccc} \varphi\ : & R(G\times H) & \longrightarrow & (RG)H \\ & \displaystyle\sum_{g\in G,\, h\in H} \alpha_{gh}(g,h) & \longmapsto & \displaystyle\sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h. \end{array} \tag{1.1}$$

Provemos que φ é um isomorfismo de álgebras de grupo. De fato, sejam $\alpha,\ \beta \in R(G\times H)$, onde $\alpha = \displaystyle\sum_{g\in G,\, h\in H} \alpha_{gh}(g,h)$ e $\beta = \displaystyle\sum_{j\in G,\, k\in H} \beta_{jk}(j,k)$. Assim

$$\varphi(\alpha\beta) = \varphi\left(\alpha_{gh}\beta_{jk}(gj,hk)\right) = \sum_{h,\,k\in H}\left(\sum_{g,\,j\in G}\alpha_{gh}\beta_{jk}gj\right)hk.$$

Por outro lado,

$$\varphi(\alpha)\cdot\varphi(\beta) \;=\; \sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h \cdot \sum_{k\in H}\left(\sum_{j\in G}\beta_{jk}j\right)k = \sum_{h,\,k\in H}\left(\sum_{g,\,j\in G}\alpha_{gh}\beta_{jk}gj\right)hk.$$

Logo $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. Além disso

$$\begin{aligned}\varphi(\alpha+\beta) &= \varphi\left(\sum_{g\in G,\, h\in H}(\alpha_{gh}+\beta_{gh})(g,h)\right) = \sum_{h\in H}\left(\sum_{g\in G}(\alpha_{gh}+\beta_{gh})\,g\right)h \\ &= \sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h + \sum_{h\in H}\left(\sum_{g\in G}\beta_{gh}g\right)h = \varphi(\alpha)+\varphi(\beta).\end{aligned}$$

Dado $r \in R$, temos

$$\varphi(r\alpha) = \varphi\left(\sum_{g\in G,\, h\in H} r\alpha_{gh}(g,h)\right) = \sum_{h\in H}\left(\sum_{g\in G} r\alpha_{gh}g\right)h = r\sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h = r\varphi(\alpha).$$

Por fim, vejamos que φ é injetora e sobrejetora. Dados α, $\beta \in R(G\times H)$, tais que $\varphi(\alpha) = \varphi(\beta)$, então

$$\begin{aligned}\varphi(\alpha)=\varphi(\beta) &\Rightarrow \sum_{h\in H}\left(\sum_{g\in G}\alpha_{gh}g\right)h - \sum_{h\in H}\left(\sum_{g\in G}\beta_{gh}g\right)h = 0 \\ &\Rightarrow \sum_{h\in H}\left(\sum_{g\in G}(\alpha_{gh}-\beta_{gh})\,g\right)h = 0 \\ &\Rightarrow \sum_{g\in G}(\alpha_{gh}-\beta_{gh})\,g = 0 \\ &\Rightarrow \alpha_{gh}=\beta_{gh}, \text{ para todos } g\in G \text{ e } h\in H.\end{aligned}$$

Verificamos as inclusões $GH \subset Im\overline{\varphi} \subset Im\varphi$. Sobre R, os elementos de $(RG)H$ são gerados por GH e considerando a extensão linear φ, $(RG)H \subset Im\varphi$, ou seja, φ é sobrejetora.

Vamos utilizar a *Propriedade Universal do Produto Tensorial* para mostrar que

$$\begin{array}{rccc}\zeta : & RG\otimes_R RH & \longrightarrow & R(G\times H) \\ & \sum_{i=0}^{n} r_i g_i \otimes \sum_{j=0}^{m} s_j h_j & \longmapsto & \sum_{i,\,j} r_i s_j\,(g_i,h_j)\end{array} \tag{1.2}$$

é um isomorfismo de álgebras de grupo.

Considere o seguinte diagrama:

$$\begin{array}{ccc} RG \times RH & \xrightarrow{\phi} & RG \otimes_R RH \\ & \searrow^{\psi} & \downarrow \zeta \\ & & R(G \times H) \end{array} \tag{1.3}$$

É simples verificar que a função $\psi : RG \times RH \to R(G \times H)$ dada por $\psi\left(\sum_i r_i g_i, \sum_j s_j h_j\right) = \sum_{i,j} r_i s_j (g_i, h_j)$ é uma aplicação balanceada.

Dados $\alpha \in RG$ e $\beta \in RH$ onde $\alpha = \sum_i r_i g_i$ e $\beta = \sum_j s_j h_j$, pela *Propriedade Universal do Produto Tensorial*, existe um único homomorfismo de álgebras $\zeta : RG \otimes_R RH \to R(G \times H)$ dado por

$$\zeta\left(\sum_i r_i g_i \otimes \sum_j s_j h_j\right) = \sum_{i,j} r_i s_j (g_i, h_j)$$

que faz o diagrama (1.3) comutar.

Mostremos que ζ é um homomorfismo. De fato, dados $\gamma, \eta \in RG \otimes RH$ e $r \in R$, onde $\gamma = \sum_i r_i g_i \otimes \sum_j t_j h_j$ e $\eta = \sum_i s_i g_i \otimes \sum_j v_j h_j$, temos

$$\zeta(\gamma) + \zeta(\eta) = \sum_{i,j} (r_i t_j + s_i v_j)(g_i, h_j) = \zeta\left(\sum_{i,j} (r_i t_j + s_i v_j) g_i \otimes h_j\right) = \zeta(\gamma + \eta).$$

$$\zeta(\gamma\eta) = \zeta\left(\sum_i r_i s_i {g_i}^2 \otimes \sum_j t_j v_j {h_j}^2\right) = \sum_{i,j} r_i s_i t_j v_j \left({g_i}^2, {h_j}^2\right) = \zeta(\gamma)\zeta(\eta).$$

$$\begin{aligned} \zeta(r\gamma) &= \zeta\left(\sum_{i,j} r r_i g_i \otimes \sum_{i,j} t_j h_j\right) = \sum_{i,j} r r_i t_j (g_i, h_j) = r\left(\sum_{i,j} r_i t_j (g_i, h_j)\right) \\ &= r\zeta(\gamma). \end{aligned}$$

Seja $\widetilde{\zeta} : R(G \times H) \to RG \otimes RH$ a aplicação definida por

$$\widetilde{\zeta}\left(\sum_{i,j} r_{ij}\,(g_i, h_j)\right) = \sum_{i,j} r_{ij} g_i \otimes h_j.$$

Observe que

$$\zeta \circ \widetilde{\zeta}\left(\sum_{i,j} r_{ij}\,(g_i, h_j)\right) = \zeta\left(\sum_{i,j} r_{ij} g_i \otimes h_j\right) = \sum_{i,j} r_{ij}\,(g_i, h_j) = Id_{\widetilde{\zeta}}.$$

Por outro lado,

$$\begin{aligned}\widetilde{\zeta} \circ \zeta\left(\sum_i r_i g_i \otimes \sum_j s_j h_j\right) &= \widetilde{\zeta}\left(\sum_{i,j} r_i s_j\,(g_i, h_j)\right) = \sum_{i,j} r_i s_j g_i \otimes h_j \\ &= \sum_i r_i g_i \otimes \sum_j s_j h_j = Id_{\zeta}.\end{aligned}$$

Assim, $\widetilde{\zeta}$ e ζ são inversas uma da outra. Logo ζ é bijetora e, portanto, $RG \otimes_R RH$ e $R(G \times H)$ são isomorfos. ∎

Teorema 1.2.4 (Exercício 5)**.** *Dada uma família de anéis* $\{R_i\}_{i \in I}$*, se* $R = \bigoplus_{i \in I} R_i$*, então*

$$RG \cong \bigoplus_{i \in I} R_i G.$$

Demonstração. A aplicação

$$\begin{array}{rccc}\psi & : & RG & \longrightarrow & \displaystyle\bigoplus_{i \in I} R_i G \\ & & \displaystyle\sum_{g \in G} a_g g & \longmapsto & \displaystyle\sum_{i \in I} \sum_{g \in G} a_{gi} g.\end{array}$$

é um isomorfismo, onde $a_g = \sum_{i \in I} a_{gi}$, com $a_{gi} \in R_i$, para cada $i \in I$. De fato, vejamos que ψ é um homomorfismo de anéis de grupo. Dados $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$, temos

$$\begin{aligned}\psi(\alpha+\beta) &= \psi\left(\sum_{g\in G}(a_g+b_g)\,g\right)=\sum_{i\in I}\sum_{g\in G}(a_{gi}+b_{gi})\,g\\ &= \sum_{i\in I}\sum_{g\in G}a_{gi}g+\sum_{i\in I}\sum_{g\in G}b_{gi}g=\psi(\alpha)+\psi(\beta).\end{aligned}$$

Além diso, dado $\lambda \in R$, obtemos

$$\psi(\lambda\alpha) = \psi\left(\sum_{g\in G}\lambda a_g g\right)=\sum_{i\in I}\sum_{g\in G}\lambda a_{gi}g=\lambda\sum_{i\in I}\sum_{g\in G}\alpha_{gi}g=\lambda\psi(\alpha).$$

Por fim, dado $\alpha\beta=\sum_{u\in G}d_u u$, onde $d_u=\sum_{gh=u}a_g b_h$, temos

$$\begin{aligned}\psi(\alpha\beta) &= \psi\left(\sum_{u\in G}d_u u\right)=\sum_{i\in I}\sum_{u\in G}d_{ui}u=\sum_{i\in I}\sum_{h,k\in G}(a_{hi}b_{ki})\,gk\\ &= \left(\sum_{i\in I}\sum_{h\in G}a_{hi}h\right)\left(\sum_{i\in I}\sum_{k\in G}b_{ki}k\right)=\psi(\alpha)\psi(\beta).\end{aligned}$$

Assim, ψ é homomorfismo de anéis de grupo. Agora basta verificarmos que ψ é uma bijeção.

Suponha $\psi(\alpha)=0$. Então $\sum_{i\in I}a_{gi}=0$, para todo $g\in G$. Como $R_i\cap R_j=\varnothing$ para $i\neq j$, logo $a_{gi}=0$, para todo $g\in G$ e $i\in I$, ou seja, $a_g=0$. Assim $\alpha=0$ e ψ é injetiva.

A verificação de que ψ é sobrejetiva é direta, a partir da definição de a_g, para todo $g\in G$. ∎

1.2.2 Semissimplicidade

Um R-módulo M é dito semissimples se todo submódulo de M é um somando direto. Nesta seção enunciamos o Teorema de Maschke, que apresenta condições para que um anel de grupo seja semissimples, e alguns corolários deste resultado. Por fim, apresentamos uma descrição completa de uma álgebra de grupo para grupos abelianos com relação as suas componentes simples.

Vamos determinar condições necessárias e suficientes sobre R e G para que o anel de grupo RG seja semissimples. A demonstração para o próximo resultado pode ser vista

em [22, Teorema 3.4.7].

Teorema 1.2.5 (Teorema de Maschke)**.** *Seja G um grupo. O anel de grupo RG é semissimples se, e somente se, valem as seguintes condições:*

1. *R é um anel semissimples.*
2. *G é finito.*
3. *$|G|$ é invertível em R.*

O caso em que $R = \mathbb{F}$ é um corpo é de grande importância. Neste caso, $\mathbb{F}$ é sempre semissimples e $|G|$ é invertível em $\mathbb{F}$ se, e somente se, $|G| \neq 0$ em $\mathbb{F}$ e $car(\mathbb{F}) \nmid |G|$.

Corolário 1.2.6. *Sejam G um grupo finito e $\mathbb{F}$ um corpo. Então $\mathbb{F}G$ é semissimples se, e somente se, $car(\mathbb{F}) \nmid |G|$.*

Em Teoria de Anéis, um resultado importante que trata da estrutura de anéis semissimples é o Teorema de Wedderburn-Artin. Na Seção 2.6 de [22] é feita a demonstração completa deste teorema sob hipóteses mais gerais. Optamos por enunciar aqui uma adaptação do Teorema de Wedderburn-Artin que destaca as informações sobre a estrutura das álgebras de grupo, uma vez que este é um dos principais objetos de estudo nesta dissertação.

Teorema 1.2.7. *Sejam G um grupo finito e $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Então:*

1. *$\mathbb{F}G$ é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de $\mathbb{F}G$. Cada B_i é um anel simples.*
2. *Qualquer ideal bilateral de $\mathbb{F}G$ é uma soma direta de alguns dos membros da família $\{B_i\}_{1\leq i\leq r}$.*
3. *Cada componente simples B_i é isomorfa a um anel de matrizes completo da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia de $\mathbb{F}$ em seu centro, e o isomorfismo*
$$\mathbb{F}G \overset{\phi}{\simeq} \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$
é um isomorfismo de $\mathbb{F}$-álgebras.
4. *Em cada matriz $M_{n_i}(D_i)$, o conjunto*
$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} : x_1, x_2, \cdots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

é um ideal minimal à esquerda isomorfo ao D_i-módulo $D_i^{n_i}$.

Dado $x \in \mathbb{F}G$, consideramos $\phi(x) = (\alpha_1, \cdots, \alpha_r) \in \bigoplus_{i=1}^{r} M_{n_i}(D_i)$ e definimos o produto de x por um elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Com esta definição I_i torna-se um $\mathbb{F}G$-módulo simples.

5. *$I_i \not\simeq I_j$, se $i \neq j$.*
6. *Qualquer $\mathbb{F}G$-módulo simples é isomorfo a algum I_i, $1 \leq i \leq r$.*

A demonstração do próximo resultado pode ser vista em [7, 27.15].

Corolário 1.2.8. *Sejam G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado tal que $car(\mathbb{F}) \nmid |G|$. Então*

$$\mathbb{F}G \simeq \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{F})$$

e $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$.

1.2.3 Álgebras de Grupo de Grupos Abelianos

Apresentamos nesta seção uma descrição completa de uma álgebra de grupo para um grupo abeliano finito sobre um corpo $\mathbb{F}$ tal que $car(\mathbb{F}) \nmid |G|$.

Primeiro, consideremos $G = \langle a : a^n = 1 \rangle$ um grupo cíclico de ordem n e $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Considere a aplicação $\phi : \mathbb{F}[X] \to \mathbb{F}G$ dada por

$$\mathbb{F}[X] \ni f \mapsto f(a) \in \mathbb{F}G,$$

onde $\mathbb{F}[X]$ é o anel dos polinômios sobre $\mathbb{F}$ na indeterminada X.

É fácil verificar que ϕ é um epimorfismo de anéis. Logo, pelo Primeiro Teorema do Isomorfismo para Anéis,

$$\mathbb{F}G \simeq \frac{\mathbb{F}[X]}{Ker(\phi)},$$

onde $Ker(\phi) = \{f \in \mathbb{F}[X] : f(a) = 0\}$.

Já que $\mathbb{F}[X]$ é um domínio de ideais principais, $Ker(\phi)$ é o ideal gerado por um polinômio f_0, de menor grau, tal que $f_0(a) = 0$ em $\mathbb{F}G$.

Como $a^n = 1$, temos $X^n - 1 \in Ker(\phi)$. Agora se $f = \sum_{i=0}^{r} k_i X^i$ é um polinômio de grau $r \leq n$, então $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$, pois os elementos $\{1, a, a^2, \cdots, a^{n-1}\}$ são linearmente

independentes sobre $\mathbb{F}$. Logo $Ker(\phi) = \langle X^n - 1 \rangle$ e

$$\mathbb{F}G \simeq \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle}.$$

Seja $X^n - 1 = f_1 f_2 \cdots f_t$ a decomposição de $X^n - 1$ como um produto de polinômios irredutíveis em $\mathbb{F}[X]$. Como assumimos $car(\mathbb{F}) \nmid n$, este polinômio é separável sobre $\mathbb{F}$, e assim $f_i \neq f_j$, se $i \neq j$. Usando o Teorema Chinês do Resto, podemos escrever:

$$\mathbb{F}G \simeq \frac{\mathbb{F}[X]}{\langle f_1 \rangle} \oplus \frac{\mathbb{F}[X]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{\langle f_t \rangle}.$$

Sob este isomorfismo, o gerador a é aplicado no elemento

$$(X + (f_1), \cdots, X + (f_t)).$$

Se ζ_i denota uma raiz de $f_i, 1 \leq i \leq t$, então $\dfrac{\mathbb{F}[X]}{\langle f_i \rangle} \simeq \mathbb{F}(\zeta_i)$. Conseqüentemente,

$$\mathbb{F}G \simeq \mathbb{F}(\zeta_1) \oplus \mathbb{F}(\zeta_2) \oplus \cdots \oplus \mathbb{F}(\zeta_t).$$

Como todos os elementos ζ_i, $1 \leq i \leq t$, são raízes de $X^n - 1$, então $\mathbb{F}G$ é isomorfo a uma soma direta de extensões de $\mathbb{F}$. Sob este isomorfismo, o elemento a é levado no elemento $(\zeta_1, \zeta_2, \cdots, \zeta_t)$.

Dado um número inteiro d, o **polinômio ciclotômico** de ordem d, denotado por Φ_d, é o produto $\Phi_d = \prod_j (X - \zeta_j)$, onde ζ_j percorre todas as d-ésimas raízes primitivas da unidade. Também temos $X^n - 1 = \prod_{d|n} \Phi_d$, o produto de todos os polinômios ciclotômicos Φ_d em $\mathbb{Q}[X]$, onde d é um divisor de n. Para cada d, seja $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ a decomposição de Φ_d como um produto de polinômios irredutíveis em $\mathbb{F}[X]$. Logo a decomposição de $\mathbb{F}G$ pode ser reescrita na forma:

$$\mathbb{F}G \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{\mathbb{F}[X]}{\langle f_{d_i} \rangle} \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \mathbb{F}(\zeta_{d_i}),$$

onde ζ_{d_i} denota uma raiz de f_{d_i}, $1 \leq i \leq a_d$. Para um d fixo, todos os elementos ζ_{d_i} são raízes d-ésimas primitivas da unidade. Logo, todos os corpos da forma $\mathbb{F}(\zeta_{d_i})$, $1 \leq i \leq a_d$, são isomorfos uns aos outros e podemos assim escrever

$$\mathbb{F}G \simeq \bigoplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

onde ζ_d é uma raiz primitiva de ordem d e $a_d\mathbb{F}(\zeta_d)$ denota a soma direta de a_d corpos, todos eles isomorfos a $\mathbb{F}(\zeta_d)$.

Já que $\partial\left(f_{d_i}\right) = \left[\mathbb{F}\left(\zeta_d\right) : \mathbb{F}\right]$, os polinômios f_{d_i}, $1 \leq i \leq a_d$, possuem todos o mesmo grau. Logo, tomando os graus na decomposição de Φ_d, temos

$$\varphi(d) = \partial(\Phi_d) = a_d \left[\mathbb{F}\left(\zeta_d\right) : \mathbb{F}\right],$$

onde φ denota a função de Euler, a saber

$$\varphi(d) = \left|\{n \in \mathbb{Z} : 1 \leq n \leq d,\, mdc(n,d) = 1\}\right|.$$

Já que G é um grupo cíclico de ordem n, para cada divisor d de n, o número de elementos de ordem d em G, que denotamos por n_d, é precisamente $\varphi(d)$. Portanto, podemos escrever

$$a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}.$$

O próximo resultado nos dá a decomposição da álgebra de grupo $\mathbb{F}G$ para um grupo abeliano qualquer, utilizando o caso particular feito acima para grupos cíclicos.

Teorema 1.2.9 (Teorema de Perlis-Walker)**.** *Seja G um grupo abeliano finito de ordem n e seja $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid n$. Então*

$$\mathbb{F}G \simeq \bigoplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e $a_d = \dfrac{n_d}{\left[\mathbb{F}\left(\zeta_d\right) : \mathbb{F}\right]}$. Nesta fórmula, n_d denota o número de elementos de ordem d em G.

Demonstração. Vamos provar o resultado por indução sobre a ordem de G. Assumiremos que o resultado vale para todos os grupos abelianos de ordem menor do que n. Se G é cíclico, o resultado vale pelas considerações anteriores a este teorema. Do contrário, a partir do teorema relativo a estrutura dos grupos abelianos finitos, vamos escrever $G = G_1 \times H$, onde H é cíclico e $|G_1| = n_1 < n$. Pela hipótese de indução, podemos escrever $\mathbb{F}G_1 \cong \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})$, onde $a_{d_1} = \dfrac{n_{d_1}}{\left[\mathbb{F}\left(\zeta_{d_1}\right) : \mathbb{F}\right]}$ e n_{d_1} denota o número de elementos de ordem d_1 em G_1. Assim, de acordo com os Teoremas 1.2.3 e 1.2.4, obtemos

$$\mathbb{F}G = \mathbb{F}\left(G_1 \times H\right) \cong \left(\mathbb{F}G_1\right) H \cong \left(\bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})\right) H \cong \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})H. \tag{1.4}$$

Agora, pelas considerações anteriores obtidas no caso de grupos cíclicos, reescrevemos (1.4)

$$\mathbb{F}G \cong \bigoplus_{d_1|n_1} \left(\bigoplus_{d_2||H|} a_{d_1} a_{d_2} \mathbb{F}(\zeta_{d_1}\zeta_{d_2}) \right),$$

onde $a_{d_2} = \dfrac{n_{d_2}}{[\mathbb{F}(\zeta_{d_1}\zeta_{d_2}) : \mathbb{F}(\zeta_{d_1})]}$ e n_{d_2} denota o número de elementos de ordem d_2 em H.

Seja $d = mmc\,(d_1, d_2)$. Logo $\mathbb{F}\,(\zeta_{d_1}\zeta_{d_2}) = \mathbb{F}\,(\zeta_d)$ e assim

$$\mathbb{F}G \cong \bigoplus_{d|n} a_d \mathbb{F}\,(\zeta_d)\,,$$

com $a_d = \sum a_{d_1} a_{d_2}$, onde a soma é tomada sob todos os pares de divisores d_1, d_2 de $|G|$ tais que $mmc\,(d_1, d_2) = d$. Desde $[\mathbb{F}\,(\zeta_d) : \mathbb{F}] = [\mathbb{F}\,(\zeta_{d_1}\zeta_{d_2}) : \mathbb{F}\,(\zeta_{d_1})]\,[\mathbb{F}\,(\zeta_{d_1}) : \mathbb{F}]$, temos

$$a_d\,[\mathbb{F}\,(\zeta_d) : \mathbb{F}] = \sum_{d_1,d_2} a_{d_1}\,[\mathbb{F}\,(\zeta_{d_1}\zeta_{d_2}) : \mathbb{F}\,(\zeta_{d_1})]\,a_{d_2}\,[\mathbb{F}\,(\zeta_{d_1}) : \mathbb{F}] = \sum_{d_1,d_2} n_{d_1} n_{d_2}. \tag{1.5}$$

Finalmente, por hipótese, cada elemento $g \in G$ pode ser escrito na forma $g = g_1 h$, com $g_1 \in G_1$ e $h \in H$. É fácil verificar que $o(g) = mmc\,(o\,(g_1)\,, o(h))$. Assim, na soma $\sum_{d_1,d_2} n_{d_1} n_{d_2}$ cada somando representa o número de elementos de ordem $d = mmc(d_1, d_2)$ em G, para cada par d_1, d_2. Logo $\sum_{d_1,d_2} n_{d_1} n_{d_2} = n_d$ e por (1.5), concluímos

$$a_d = \frac{n_d}{[\mathbb{F}\,(\zeta_d) : \mathbb{F}]}$$

■

Corolário 1.2.10. *Seja G um grupo abeliano finito de ordem n. Então*

$$\mathbb{Q}G \simeq \bigoplus_{d|n} a_d \mathbb{Q}(\zeta_d),$$

onde ζ_d denota uma raiz primitiva da unidade de ordem d e a_d é o número de subgrupos cíclicos (ou fatores cíclicos) de G.

Capítulo 2

Introdução à Teoria dos Códigos

Neste capítulo apresentamos as definições e resultados básicos sobre Códigos Corretores de Erros. Vamos definir os códigos lineares e, em particular, os códigos cíclicos e abelianos, que são os objetos de estudo neste trabalho. As referências básicas para este capítulo são [13] e [19].

2.1 Códigos Corretores de Erros

Para definirmos um código corretor de erros precisamos de um conjunto finito qualquer $\mathcal{A}$ que será chamado **alfabeto**. A cardinalidade de $\mathcal{A}$ será denotada por $|\mathcal{A}| = q$ e os elementos deste conjunto serão chamados **letras** ou **dígitos**. Uma **palavra** é uma sequência de letras de $\mathcal{A}$ e o **comprimento** dessa palavra é o número de letras que a compõe.

Definição 2.1.1. *Dado um número natural n qualquer, um **código corretor de erros** (ou simplesmente um **código**) de comprimento n é um subconjunto próprio de $\mathcal{A}^n$.*

2.1.1 Métrica de Hamming

Definição 2.1.2. *Dados dois elementos $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathcal{A}^n$, a **distância de Hamming** entre u e v é dada por*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| .$$

*Seja $\mathfrak{C} \subset \mathcal{A}^n$ um código. A **distância mínima** de $\mathfrak{C}$ é o número*

$$d = min\{d(u, v) : u, v \in \mathfrak{C} \ e \ u \neq v\} .$$

Proposição 2.1.3. *A distância de Hamming determina uma métrica em $\mathcal{A}^n$, ou seja, dados u, v e $w \in \mathcal{A}^n$, valem as seguintes propriedades:*

- *Positividade: $d(u,v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.*
- *Simetria: $d(u,v) = d(v,u)$.*
- *Desigualdade Triangular: $d(u,v) \leq d(u,w) + d(w,v)$.*

Os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade. Quando uma informação é transmitida e o receptor recebe uma palavra diferente da esperada, é possível, com a utilização desta teoria, detectar os possíveis erros, corrigi-los e assim recuperar a informação original transmitida pela fonte.

Teorema 2.1.4. *Seja $\mathfrak{C}$ um código com distância mínima d. Então $\mathfrak{C}$ pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d-1$ erros.*

Do Teorema 2.1.4 podemos observar que quanto maior a distância mínima de um código, maior será a sua **capacidade de correção de erros** $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Os **três parâmetros fundamentais** de um código $\mathfrak{C} \subset \mathcal{A}^n$ são (n, M, d), onde n é o comprimento do código, M o número de elementos e d a distância mínima de $\mathfrak{C}$. Dados três inteiros positivos arbitrários n, M e d, nem sempre existe um código com esses parâmetros, uma vez que eles se relacionam, por exemplo, pela Cota de Singleton para o caso de códigos lineares (veja Seção 2.2)

2.2 Códigos Lineares

Nesta seção, a menos que mencionemos o contrário, vamos considerar como alfabeto um corpo finito $\mathbb{F}_q$ com q elementos e, dado o número natural n, consideremos o $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q^n$ de dimensão n.

Definição 2.2.1. *Um código $\mathfrak{C} \subset \mathbb{F}_q^n$ será chamado **código linear** se for um subespaço vetorial próprio de $\mathbb{F}_q^n$.*

*Se $\mathfrak{C}$ tem dimensão k sobre $\mathbb{F}_q$ dizemos que $\mathfrak{C}$ é um (n,k) **- código linear** e se $\mathfrak{C}$ tem distância mínima d, dizemos que $\mathfrak{C}$ é um (n,k,d) **- código linear**.*

Consideremos um código $\mathfrak{C}$ de dimensão k. Dada $\{v_1, v_2, \ldots, v_k\}$ uma de suas bases, todo elemento de $\mathfrak{C}$ se escreve de forma única como

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k,$$

onde $\lambda_i \in \mathbb{F}_q$, para todo $i = 1, ..., k$. Daí

$$M = |\mathfrak{C}| = q^k,$$

e, consequentemente,

$$dim_{\mathbb{F}_q}\mathfrak{C} = k = log_q q^k = log_q M.$$

Proposição 2.2.2 (Cota de Singleton)**.** *Os parâmetros (n, k, d) de um código linear satisfazem a desigualdade*

$$d \leq n - k + 1.$$

Definição 2.2.3. *Dado $x \in \mathbb{F}_q^n$, define-se o **peso** de x como sendo o número inteiro*

$$\omega(x) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, $\omega(x) = d(x, 0)$, onde d é a métrica de Hamming.

Definição 2.2.4. *O **peso** de um código linear $\mathfrak{C}$ é o inteiro*

$$\omega(\mathfrak{C}) := min\{\omega(x) : x \in \mathfrak{C}\backslash\{0\}\}.$$

Proposição 2.2.5. *Seja $\mathfrak{C} \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos*

(i) Para quaisquer $x, y \in \mathbb{F}_q^n$, $d(x, y) = \omega(x - y)$.

(ii) $d = \omega(\mathfrak{C})$.

Pelo item (ii) da Proposição 2.2.5, a distância mínima de um código $\mathfrak{C}$ é também chamada **peso do código**.

2.2.1 Códigos Cíclicos

Os códigos cíclicos são um caso particular de códigos lineares. Nesta seção apresentaremos os códigos cíclicos como ideais de um anel de polinômios e ideais em uma álgebra de grupo para um grupo cíclico. Estas duas abordagens serão usadas durante todo este trabalho.

Definimos a permutação cíclica de coordenadas em $\mathbb{F}_q^n$, tomadas módulo n, por

$$\begin{array}{rccc} T_\pi & : & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ & & c = (c_0, \ldots, c_{n-1}) & \mapsto & T_\pi(c) = (c_{n-1}, c_0, \ldots, c_{n-2}). \end{array} \tag{2.1}$$

Definição 2.2.6. *Um código linear $\mathfrak{C}$ é chamado **código cíclico** se, para toda palavra $u = (u_0, u_1, ..., u_{n-1})$ em $\mathfrak{C}$, o vetor $T_\pi(u) = (u_{n-1}, u_0, ..., u_{n-2})$ também está em $\mathfrak{C}$, ou seja, $T_\pi(\mathfrak{C}) \subset \mathfrak{C}$.*

Exemplo:

1) Dado $v \in \mathbb{F}_q^n$, o subespaço vetorial de $\mathbb{F}_q^n$

$$\langle v \rangle = \mathbb{F}_q v + \mathbb{F}_q T_\pi v + \cdots + \mathbb{F}_q T_\pi^{n-1} v$$

é um código cíclico.

De fato, temos

$$T_\pi(\mathbb{F}_q v + \mathbb{F}_q T_\pi v + \cdots \mathbb{F}_q T_\pi^{n-1} v) = \mathbb{F}_q T_\pi(v) + \mathbb{F}_q T_\pi^2(v) + \cdots + \mathbb{F}_q T_\pi^{n-1}(v) + \mathbb{F}_q v$$

e assim $T_\pi(\langle v \rangle) \subset \langle v \rangle$.

Considere $\mathcal{R}_n$ o anel das classes residuais em $\mathbb{F}_q[X]$ módulo $X^n - 1$, ou seja,

$$\mathcal{R}_n = \frac{\mathbb{F}_q[X]}{\langle X^n - 1 \rangle}.$$

Todo elemento de $\mathcal{R}_n$ pode ser representado unicamente por um polinômio

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}, \ a_i \in \mathbb{F}_q$$

de grau, no máximo, $n - 1$.

Os códigos cíclicos podem ser "realizados"de diferentes formas. É fácil verificar que

$$\begin{array}{rccc} \varphi: & \mathbb{F}_q^n & \longrightarrow & \mathcal{R}_n \\ & (b_0, ..., b_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i \overline{x}^i \end{array} \tag{2.2}$$

é um isomorfismo e que os códigos cíclicos em $\mathbb{F}_q^n$ correspondem aos ideais no anel quociente $\mathcal{R}_n$.

Teorema 2.2.7. *Um subespaço vetorial $\mathfrak{C} \subset \mathbb{F}_q^n$ é um código cíclico se, e somente se, $\varphi(\mathfrak{C})$ é um ideal de $\mathcal{R}_n$.*

Demonstração. Dada a palavra $c = (c_0, c_1, \ldots, c_{n-1})$, temos $T_\pi(c) \in \mathfrak{C}$ se, e somente se, $\varphi\left(T_\pi(c)\right) = x \displaystyle\sum_{i=0}^{n-1} c_i x^i \in \varphi(\mathfrak{C})$, isto é, $\varphi(\mathfrak{C})$ é um ideal em $\mathcal{R}_n$. ∎

Dado um ideal I de $\mathcal{R}_n$, existe um único polinômio mônico $\overline{g} \in \mathcal{R}_n$, o qual é um divisor de $X^n - 1$ e gera o ideal I. Este polinômio $\overline{g}$ é dito **polinômio gerador** de I. Se $mdc(q, n) = 1$, então $\mathcal{R}_n$ é semissimples e existe um idempotente $\varepsilon \in I$, que é o elemento

identidade em I tal que $I = \mathcal{R}_n\varepsilon$. Um polinômio $e \in \mathbb{F}_q[X]$ tal que $\overline{e} = \varepsilon$ será chamado um **idempotente gerador** de I.

Podemos também considerar os códigos cíclicos como ideais na álgebra de grupo de um grupo cíclico. De fato, dado $G = \langle a/a^n = 1\rangle$, definimos a aplicação

$$\begin{array}{rccc} \psi: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_qG \\ & (b_0,...,b_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i a^i, \end{array} \tag{2.3}$$

onde ψ é um isomorfismo de espaços vetoriais.

Teorema 2.2.8. *Um subespaço vetorial $\mathfrak{C}$ de $\mathbb{F}_q^n$ é um código cíclico se, e somente se, $\psi(\mathfrak{C})$ é um ideal de $\mathbb{F}_qG$.*

Demonstração. Dado o isomorfismo (2.3), é fácil ver que $\psi(\mathfrak{C})$ é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_qG$. Seja $\alpha \in \psi(\mathfrak{C})$. Logo existe $c \in \mathfrak{C}$ tal que $\psi(c) = \alpha$. Se $a \in G$, então

$$a\alpha = a\psi(c) = \psi(T_\pi(c)) \in \psi(\mathfrak{C}),$$

onde T_π é a permutação cíclica definida em (2.1). Assim, $\psi(\mathfrak{C})$ é um ideal de $\mathbb{F}_qG$.

Reciprocamente, seja $c \in \mathfrak{C}$. Como $\psi(\mathfrak{C})$ é um ideal da álgebra $\mathbb{F}_qG$, então $a\psi(c) = \psi(T_\pi(c)) \in \psi(\mathfrak{C})$, isto é, $T_\pi(c) \in \mathfrak{C}$, para qualquer $c \in \mathfrak{C}$. Portanto, $\mathfrak{C}$ é um código cíclico. ∎

Por (2.2) e (2.3), temos o isomorfismo $\psi\varphi^{-1}$ entre as $\mathbb{F}_q$-álgebras $\mathcal{R}_n$ e $\mathbb{F}_qG$:

$$\begin{array}{ccccccc} & & \varphi^{-1} & & & \psi & \\ \mathcal{R}_n & & \longrightarrow & & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_qG \\ \displaystyle\sum_{i=0}^{n-1} b_i\overline{x}^i & & \mapsto & & (b_0,b_1,...,b_{n-1}) & \mapsto & \displaystyle\sum_{i=0}^{n-1} b_i a^i \ , \end{array} \tag{2.4}$$

ou seja, podemos estudar códigos cíclicos a partir da abordagem polinomial ou via álgebras de grupo.

Dentre os objetivos do trabalho está descrever maneiras de se calcular esses idempotentes tanto do ponto de vista polinomial quanto do ponto de vista da álgebra de grupo e comparar essas técnicas.

Capítulo 3

Códigos Abelianos Minimais

Seja $\mathbb{F}G$ a álgebra de grupo de um grupo G sobre um corpo $\mathbb{F}$. Quando G é cíclico de ordem n e $\mathbb{F}$ é um corpo finito, vimos na Seção 2.2.1 que os ideais da álgebra de grupo $\mathbb{F}G$ correspondem aos códigos cíclicos de comprimento n. Estendendo estas idéias, S. D. Berman [3] e F.J.MacWilliams [18] definiram **códigos abelianos** como ideais (próprios) na álgebra de grupo de um grupo abeliano finito sobre um corpo finito. Em particular, o conjunto dos idempotentes primitivos de $\mathbb{F}G$ gera os ideais minimais de $\mathbb{F}G$, aos quais nos referimos como **códigos abelianos minimais**, quando G é abeliano.

Neste capítulo introduzimos a técnica de construção dos idempotentes primitivos geradores de códigos abelianos minimais, utilizando a estrutura do grupo adjacente para códigos de comprimento p^n e $2p^n$.

Na primeira seção, destacamos alguns resultados sobre o número de componentes simples de uma álgebra de grupo, que justificam as hipóteses exibidas para a maioria dos resultados importantes deste trabalho.

Na segunda e terceira seções, generalizamos as idéias de [23] e [1], apresentando os códigos abelianos minimais para os casos em que G tem expoente p^n ou $2p^n$.

Na última seção, estendemos os resultados das seções anteriores para álgebras de grupo semissimples $\mathbb{F}G$, onde G é um grupo abeliano finito e $\mathbb{F}$ um corpo finito, calculando os idempotentes primitivos da álgebra de grupo e relacionando-os com certos subgrupos de G.

A principal referência para este capítulo é [11].

3.1 O Número de Componentes Simples

Sejam $\mathbb{F}_q$ um corpo com q elementos e G um grupo abeliano finito tal que $mdc(q, |G|) = 1$. Logo $\mathbb{F}_qG$ é semissimples.

O Corolário 1.2.10 nos diz que o número de componentes simples da álgebra de grupo racional $\mathbb{Q}G$ de um grupo abeliano G é igual ao número de subgrupos (ou quocientes) cíclicos de G.

Nesta seção, exibimos condições para que o número de componentes simples de uma álgebra de grupo $\mathbb{F}_qG$ seja igual ao número de subgrupos cíclicos de G, ou seja, para que $\mathbb{F}_qG$ se "comporte"como a álgebra de grupo racional $\mathbb{Q}G$.

Pelo Teorema de Wedderburn-Artin 1.2.7, se $\{e_1, e_2, ..., e_r\}$ é o conjunto de idempotentes primitivos da álgebra de grupo $\mathbb{F}_qG$, temos

$$\mathbb{F}_qG = \bigoplus_{i=1}^{r} (\mathbb{F}_qG)e_i \simeq \bigoplus_{i=1}^{r} \mathbb{F}_i,$$

onde cada $\mathbb{F}_i \simeq (\mathbb{F}_qG)e_i$, para $1 \leq i \leq r$, é uma extensão finita de $\mathbb{F}_q$. Defina

$$\mathcal{A} = \bigoplus_{i=1}^{r} \mathbb{F}_q e_i \tag{3.1}$$

Observe que $\mathbb{F}_qe_i \cong \mathbb{F}_q$ como corpos e assim podemos considerar $\mathcal{A}$ como um $\mathbb{F}_q$-espaço vetorial de dimensão r.

Em [4] e [26], os autores apresentam um método para calcular o número de componentes simples de uma álgebra de grupo semissimples. Aqui apresentamos o resultado proposto por Ferraz em [9]. Sob algumas hipóteses para $\mathbb{F}_qG$, exibimos uma forma simples de determinar este número. Para isto, necessitamos de definições e resultados auxiliares que apresentamos a seguir

Lema 3.1.1. *Seja α um elemento de $\mathbb{F}_qG$. Então $\alpha \in \mathcal{A}$ se, e somente se, $\alpha^q = \alpha$.*

Seja $g \in G$. Definimos a **classe q-ciclotômica de** g como o conjunto

$$C_g = \left\{ g^{q^j} / 0 \leq j \leq t_g - 1 \right\}, \tag{3.2}$$

onde t_g é o menor inteiro positivo tal que

$$q^{t_g} \equiv 1 (mod\ o(g))$$

e $o(g)$ denota a ordem de g em G.

É simples verificar que as classes q-ciclotômicas também são classes de equivalência no grupo G sob a relação

$$g \sim h \Leftrightarrow g = h^{q^j},$$

onde $g, h \in G$ e $j \in \mathbb{Z}$. Seja $T = \{g_1, g_2, ..., g_s\}$ um conjunto de representantes das classes q-ciclotômicas de G.

Teorema 3.1.2. *Se $mdc\,(q, |G|) = 1$, então o número de componentes simples de $\mathbb{F}_q G$ é igual ao número de classes q-ciclotômicas de G.*

Demonstração. Conforme foi verificado em (3.1), o número de componentes simples de $\mathbb{F}_q G$ é igual a dimensão de $\mathcal{A}$ sobre $\mathbb{F}_q$. Vamos exibir uma base de $\mathcal{A}$ com s elementos, ou seja, o número de representantes das classes q-ciclotômicas de G.

Dada uma classe q-ciclotômica C_g, definimos $N_g = \sum_{h \in C_g} h$. Afirmamos que o conjunto $\mathcal{B} = \{N_{g_i} / 1 \leq i \leq s\}$ é uma $\mathbb{F}_q$-base de $\mathcal{A}$. Claramente $\mathcal{B}$ é um conjunto linearmente independente.

Vejamos que $\mathcal{B}$ gera $\mathcal{A}$. É fácil observar que $(N_{g_i})^q = N_{g_i}$ e, de acordo com o Lema 3.1.1, $\mathcal{B} \subset \mathcal{A}$. Seja $\alpha \in \mathcal{A} = \bigoplus_{i=1}^{r} \mathbb{F}_q e_i$. Novamente, pelo Lema 3.1.1, $\alpha^q = \alpha$. Assim, se $\alpha = \sum_{g \in G} \alpha_g g$, então

$$\sum_{g \in G} \alpha_g g = \alpha = \sum_{g \in G} \alpha_g^q g^q.$$

Logo, para cada $g \in G$, temos $\alpha_g = \alpha_{g^q} = \ldots = \alpha_{g^{q^{tg-1}}}$, e portanto

$$\alpha = \sum_{g \in T} \alpha_g N_g, \text{ onde } T = \{g_1, g_2, ..., g_s\}.$$

■

De acordo com o Corolário 1.2.10, o número de componentes simples de uma álgebra de grupo racional de um grupo abeliano finito G é igual ao número de subgrupos cíclicos de G e também igual ao número de seus quocientes cíclicos.

Observe que se $h \in C_g$, então $h = g^{q^j}$, para algum j. Como $mdc(q, o(g)) = 1$, temos $\langle g \rangle = \langle h \rangle$. Assim, cada classe q-ciclotômica C_g é um subconjunto do conjunto $\mathcal{G}_g$ de todos os geradores do grupo cíclico $\langle g \rangle$.

É claro que o número de subgrupos cíclicos de G é um limite inferior para o número de componentes simples da álgebra de grupo $\mathbb{F}_q G$ e este limite é atingindo se, e somente se, $C_g = \mathcal{G}_g$, para todo $g \in G$.

Para inteiros positivos r e m, indiquemos por $\overline{r} \in \mathbb{Z}_m$ a imagem de r nos anel dos inteiros módulo m. Assim:

$$\mathcal{G}_g = \{g^r | mdc\,(r, o\,(g)) = 1\} = \left\{g^r | \overline{r} \in U\left(\mathbb{Z}_{o(g)}\right)\right\}.$$

Teorema 3.1.3. *Sejam $\mathbb{F}_q$ um corpo com q elementos e G um grupo abeliano finito de expoente e tal que $mdc\,(q, |G|) = 1$. Então $C_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, $U(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\overline{q} \in \mathbb{Z}_e$.*

Demonstração. Seja $\overline{q}$ um gerador do grupo cíclico $U\,(\mathbb{Z}_e)$. Logo $mdc\,(q, e) = 1$, e assim verificamos que $mdc\,(q, o(g)) = 1$, ou seja, $\langle\overline{q}\rangle = U\left(\mathbb{Z}_{o(g)}\right)$, para todo $g \in G$.

Dado $h \in \mathcal{G}_g$, temos $h = g^r$, para algum $r \in \mathbb{N}$, onde $\overline{r} \in U\left(\mathbb{Z}_{o(g)}\right)$. Assim $\overline{r} = \overline{q}^j$, para algum $j \in \mathbb{N}$. Logo $h = g^{q^j} \in C_g$ e, portanto, $C_g = \mathcal{G}_g$.

Reciprocamente, suponha $\mathcal{G}_g = C_g$, para todo $g \in G$. Por hipótese, G é um grupo abeliano finito de expoente e, então garantimos a existência de um elemento $g_0 \in G$ tal que $o\,(g_0) = e$ e, em particular, $\mathcal{G}_{g_0} = C_{g_0}$. Assim, para cada $\overline{r} \in U\,(\mathbb{Z}_e)$, temos $g_0^r \in C_{g_0}$ e daí obtemos $j \in \mathbb{N}$ tal que $\overline{r} = \overline{q}^j$. Portanto, $\langle\overline{q}\rangle = U(\mathbb{Z}_e)$. ∎

Corolário 3.1.4 ([20], Teorema 7.10)**.** *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e G um grupo abeliano finito de expoente e tal que $mdc\,(q, |G|) = 1$. Então $C_g = \mathcal{G}_g$, para todo $g \in G$, se, e somente se, uma das seguintes condições vale:*

(i) $e = 2$ *e* q *é ímpar;*

(ii) $e = 4$ *e* $q \equiv 3 (mod\ 4)$*;*

(iii) $e = p^n$ *e* $o(q) = \varphi(p^n)$ *em* $U\,(\mathbb{Z}_{p^n})$*;*

(iv) $e = 2p^n$ *e* $o(q) = \varphi(p^n)$ *em* $U\,(\mathbb{Z}_{2p^n})$.

3.2 Códigos Cíclicos Minimais

Nesta seção vamos apresentar o método de construção de idempotentes primitivos nas álgebras de grupo $\mathbb{F}_qG$, onde G é um grupo cíclico de ordem p^n ou $2p^n$. As principais referências são [12], [11], [23] e [1].

Seja H um subgrupo finito de um grupo G. Se $mdc\,(q, |H|) = 1$, definimos

$$\widehat{H} = \frac{1}{|H|}\sum_{g\in H} g. \tag{3.3}$$

É fácil verificar que $\widehat{H}$ é um idempotente em $\mathbb{F}_qG$

Lema 3.2.1. *Sejam $\mathbb{F}_q$ um corpo com q elementos, p um primo e $G = \langle g \rangle$ um grupo cíclico de ordem $p^n, n \geq 1$. Seja*

$$G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$$

a cadeia descendente de todos os subgrupos de G. Então os elementos

$$e_0 = \widehat{G} \quad e \quad e_i = \widehat{G_i} - \widehat{G_{i-1}}, \qquad 1 \leq i \leq n$$

formam um conjunto de idempotentes ortogonais de $\mathbb{F}_q G$ tais que $e_0 + e_1 + ... + e_n = 1$.

Demonstração. É simples verificar que, dados $0 \leq i < j \leq n$, $\widehat{G_i}\widehat{G_j} = \widehat{G_i}$. Assim,

$$\begin{aligned} e_0 e_i &= \widehat{G}\left(\widehat{G_i} - \widehat{G_{i-1}}\right) = 0 \text{ e} \\ e_i e_j &= \left(\widehat{G_i} - \widehat{G_{i-1}}\right)\left(\widehat{G_j} - \widehat{G_{j-1}}\right) = G_i G_j - G_i G_{j-1} - G_{i-1} G_j + G_{i-1} G_{j-1} = 0, \end{aligned}$$

para $1 \leq i < j \leq n$. Logo os idempotentes são ortogonais.

Por fim, vejamos que a soma destes idempotentes é igual a 1.

$$\sum_{i=0}^{n} e_i = \widehat{G} + \widehat{G_1} - \widehat{G} + \widehat{G_2} - \widehat{G_1} + \ldots + \widehat{G_{n-1}} - \widehat{G_{n-2}} + \widehat{G_n} - \widehat{G_{n-1}} = \widehat{G_n} = 1.$$

■

Corolário 3.2.2. *Sejam $\mathbb{F}_q$ um corpo com q elementos e G um grupo cíclico de ordem p^n. Então o conjunto de idempotentes dado no Lema 3.2.1 é o conjunto de idempotentes primitivos de G se, e somente se, uma das seguintes condições vale:*

(i) $p = 2$ e tanto $n = 1$ e q é ímpar ou $n = 2$ e $q \equiv 3 \, (mod\ 4)$.

(ii) p é ímpar e $o\,(q) = \varphi\,(p^n)$ em $U\,(\mathbb{Z}_{p^n})$.

Agora estamos aptos a expressar todos os **Códigos Minimais Cíclicos** de comprimento p^n.

Teorema 3.2.3. *Sejam G um grupo cíclico de ordem p^n e $\mathbb{F}_q$ um corpo com q elementos onde $\overline{q}$ gera $U\,(\mathbb{Z}_{p^n})$. Seja*

$$G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$$

a cadeia descendente de todos os subgrupos de G. Então o conjunto de idempotentes primitivos de $\mathbb{F}_q G$ é dado por:

$$e_0 = \frac{1}{p^n} \sum_{g \in G} g \quad e \quad e_i = \widehat{G_i} - \widehat{G_{i-1}}, \text{ para } 1 \leq i \leq n.$$

Um cálculo direto mostra que estes idempotentes são os mesmos que os dados em [23], expressos polinomialmente em termos das classes ciclotômicas.

Os idempotentes geradores dos ideais minimais para álgebras de grupo de grupos cíclicos de ordem $2p^n$ agora seguem facilmente dos resultados acima e do Teorema 1.2.3, assim como foi feito em [1].

Teorema 3.2.4. *Sejam $\mathbb{F}_q$ um corpo com q elementos e G um grupo cíclico de ordem $2p^n$, onde p é um primo ímpar tal que $o(q) = \varphi(p^n)$ em $U(\mathbb{Z}_{p^n})$. Escreva $G = C \times A$, onde A é o p-subgrupo de Sylow de G e $C = \{1, t\}$ é o seu 2-subgrupo de Sylow. Se $\{e_i,\ 0 \leq i \leq n\}$ denota o conjunto dos idempotentes primitivos de $\mathbb{F}_q A$, então os idempotentes primitivos de $\mathbb{F}_q G$ são*

$$\frac{1+t}{2} \cdot e_i \quad e \quad \frac{1-t}{2} \cdot e_i, \text{ para } 0 \leq i \leq n.$$

3.3 Códigos Abelianos Minimais

Vamos estender os resultados da seção anterior para grupos abelianos finitos. Primeiro consideremos o caso de p-grupos.

Definição 3.3.1. *Seja G um grupo. Um subgrupo H de G é dito um **subgrupo co-cíclico** se o grupo quociente $\{1\} \neq G/H$ é cíclico.*

Observação 3.3.2. *Para G um p-grupo, se $\{1\} \neq G/H$ é cíclico, então garantimos a existência de um único subgrupo H^* de G tal que $H \subset H^*$ e $|H^*/H| = p$. Defina $e_H = \widehat{H} - \widehat{H^*}$.*

Lema 3.3.3. *Sejam G um p-grupo abeliano finito e $\mathbb{F}_q$ um corpo finito com q elementos, tal que $mdc(q, |G|) = 1$. O conjunto*

$$\left\{e_G = \widehat{G}\right\} \cup \{e_H :\ G/H \text{ é cíclico não trivial}\} \tag{3.4}$$

é formado por idempotentes ortogonais de $\mathbb{F}_q G$ cuja a soma é igual a 1.

Demonstração. É fácil verificar que o conjunto (3.4) é formado por elementos idempotentes. Vamos mostrar que estes elementos são ortogonais.

Sejam H e K subgrupos co-cíclicos distintos de G. Logo existem H^* e K^*, subgrupos de G tais que $[H^* : H] = [K^* : K] = p$. Se $H \subsetneq K$, logo $|K/H| = p^j$, com $j \geq 1$. Assim, existe $H_1 \leqslant G$, tal que $|H_1/H| = p$. Pela unicidade, $H^* = H_1$. Logo

$$e_H e_K = \left(\widehat{H} - \widehat{H^*}\right)\left(\widehat{K} - \widehat{K^*}\right) = \widehat{H}\widehat{K} - \widehat{H}\widehat{K^*} - \widehat{H^*}\widehat{K} + \widehat{H^*}\widehat{K^*} = \widehat{K} - \widehat{K^*} - \widehat{K} + \widehat{K^*} = 0$$

Se H e K não estão contidos um no outro, então $H \subsetneq HK$ e $K \subsetneq HK$. Pelo mesmo argumento usado quando $H \subset K$, temos $H^* \subsetneq HK$ e $K^* \subsetneq HK$, o que implica $H^*K^* \subset HK$. Por outro lado, da definição de subgrupo co-cíclico, temos $HK \subset H^*K^*$, ou seja, $HK = H^*K^*$. Além disso, $HK = H^*K = HK^*$. Assim, com $\widehat{HK} = \widehat{H}\widehat{K}$,

$$e_H e_K = \left(\widehat{H} - \widehat{H^*}\right)\left(\widehat{K} - \widehat{K^*}\right) = \widehat{H}\widehat{K} - \widehat{H}\widehat{K^*} - \widehat{H^*}\widehat{K} + \widehat{H^*}\widehat{K^*} = 0$$

Por fim, vamos mostar que a soma destes idempotentes é igual a 1.

Para cada subgrupo cíclico $\mathcal{C} = \langle c \rangle$ de G, denote por $G(\mathcal{C})$ o conjunto de todos os geradores de $\mathcal{C}$, ou seja, $G(\mathcal{C}) = \{c^j \in \mathcal{C} / \, mdc(j, |\mathcal{C}|) = 1\}$. Se $\mathbf{C}$ denota a família de todos os subgrupos cíclicos de G, então $|G| = \sum_{\mathcal{C} \in \mathbf{C}} |G(\mathcal{C})|$, e do fato de que G é um p-grupo,

$$|G(\mathcal{C})| = \varphi\left(p^i\right) = p^i - p^{i-1} = |\mathcal{C}| - \frac{|\mathcal{C}|}{p}.$$

Denote por $\mathcal{S}_{cc}(G)$ o conjunto de todos os subgrupos co-cíclicos de G. Seja $e = \sum_{H \in \mathcal{S}_{cc}} e_H$. Afirmamos que $e = 1$. De fato, vamos mostrar que $(\mathbb{F}_q G)e = \mathbb{F}_q G$.

Como os idempotentes são ortogonais, temos

$$(\mathbb{F}_q G)\, e = \bigoplus_{H \in \mathcal{S}_{cc}} (\mathbb{F}_q G)\, e_H.$$

Então

$$dim_{\mathbb{F}_q} (\mathbb{F}_q G)\, e = \sum_{H \in \mathcal{S}_{cc}} dim_{\mathbb{F}_q} (\mathbb{F}_q G)\, e_H.$$

Observe que $\widehat{H} = \widehat{H^*} + e_H$ implica $H^* e_H = 0$ e assim $(\mathbb{F}_q G)\, \widehat{H} = (\mathbb{F}_q G)\, \widehat{H^*} \oplus (\mathbb{F}_q G)\, e_H$.

Logo

$$\begin{aligned} dim_{\mathbb{F}_q} (\mathbb{F}_q G)\, e_H &= dim_{\mathbb{F}_q} (\mathbb{F}_q G)\, \widehat{H} - dim_{\mathbb{F}_q} (\mathbb{F}_q G)\, \widehat{H^*} \\ &= dim_{\mathbb{F}_q} \mathbb{F}_q (G/H) - dim_{\mathbb{F}_q} \mathbb{F}_q (G/H^*) \end{aligned}$$

Por [24, Teorema 10.57], garantimos a existência de uma bijeção $\phi : \mathbf{C} \to \mathcal{S}_{cc}(G)$ onde $|X| = |G/\phi(X)|$, para todo $X \in \mathbf{C}$. Se denotarmos por $\mathcal{C} \in \mathbf{C}$ o subgrupo de G tal que $\phi(\mathcal{C}) = H$, temos

$$dim_{\mathbb{F}_q} \mathbb{F}_q (G/H) = |\mathcal{C}| \text{ e } dim_{\mathbb{F}_q} \mathbb{F}_q (G/H^*) = \left| \frac{G/H}{H^*/H} \right| = \frac{|\mathcal{C}|}{p},$$

logo

$$dim_{\mathbb{F}_q}(\mathbb{F}_qG)e_H = |\mathcal{C}| - \frac{|\mathcal{C}|}{p} = |G(\mathcal{C})|.$$

Portanto

$$dim_{\mathbb{F}_q}(\mathbb{F}_qG)e = \sum_{H\in\mathcal{S}_{cc}} dim_{\mathbb{F}_q}(\mathbb{F}_qG)e_H = \sum_{\mathcal{C}\in\mathbf{C}} |G(\mathcal{C})| = |G| = dim_{\mathbb{F}_q}(\mathbb{F}_qG).$$

■

O próximo resultado é uma consequência imediata do Lema 3.3.3 e do Corolário 3.1.4.

Teorema 3.3.4. *Sejam p um primo, G um p-grupo abeliano de expoente p^r e $\mathbb{F}_q$ um corpo com q elementos tal que $mdc(p,q) = 1$. Então o conjunto de idempotentes (3.4) é o conjunto de idempotentes primitivos de $\mathbb{F}_qG$ se, e somente se, uma das seguintes condições é satisfeita:*

(i) $p^r = 2$ *e* q *é ímpar;*

(ii) $p^r = 4$ *e* $q \equiv 3\,(mod\ 4)$*;*

(iii) p *é um primo ímpar e* $o(q) = \varphi(p^n)$ *em* $U(\mathbb{Z}_{p^n})$*.*

Teorema 3.3.5. *Sejam p um primo ímpar e G um grupo abeliano de expoente $2p^r$. Escreva $G = E \times B$, onde E é um 2-grupo abeliano elementar e B um p-grupo de expoente p^r. Então os idempotentes primitivos de $\mathbb{F}_qG$ são produtos da forma $e \cdot f$, onde e é um idempotente primitivo de $\mathbb{F}_qE$ e f é um idempotente primitivo de $\mathbb{F}_qB$.*

Demonstração. Considere $E = \langle a_1\rangle \times \langle a_2\rangle \times \ldots \times \langle a_t\rangle$ a decomposição do 2-grupo E como produto de grupos cíclicos de ordem 2. Os idempotentes primitivos de $\mathbb{F}_qE$ são produtos da forma $e = \overline{e}_1\overline{e}_2\ldots\overline{e}_t$, onde $\overline{e}_i = \frac{1+a_i}{2}$ ou $\overline{e}_i = \frac{1-a_i}{2}$, para cada $1 \le i \le t$. Assim, para os inteiros positivos $r \le s$, sejam $\mathcal{U} = \{e_i / 1 \le i \le r\}$ e $\mathcal{V} = \{f_j / 1 \le j \le s\}$ os conjuntos dos idempontentes primitivos das álgebras de grupo $\mathbb{F}_qE$ e $\mathbb{F}_qB$, respectivamente. Pelo Teorema 1.2.3, temos $\mathbb{F}_qG = \mathbb{F}_q(E \times B) \cong \mathbb{F}_qE \otimes \mathbb{F}_qB$. Logo

$$\begin{aligned} \mathbb{F}_qG &\cong \mathbb{F}_qE \otimes \mathbb{F}_qB \cong (\mathbb{F}_qEe_1 \oplus \ldots \oplus \mathbb{F}_qEe_r) \otimes (\mathbb{F}_qBf_1 \oplus \ldots \oplus \mathbb{F}_qBf_s) \\ &\cong \mathbb{F}_q(E\times B)(e_1\otimes f_1) \oplus \ldots \oplus \mathbb{F}_q(E\times B)(e_i\otimes f_j) \oplus \ldots \oplus \mathbb{F}_q(E\times B)(e_r\otimes f_s) \end{aligned} \tag{3.5}$$

Afirmamos que a decomposição (3.5) é a decomposição de $\mathbb{F}_qG$ em ideais minimais, ou seja, os idempotentes da forma e_if_j são os idempotentes primitivos de $\mathbb{F}_qG$, para todos $1 \le i \le j \le s$. De fato, é fácil verificar $\mathbb{F}_qEe_i \cong \mathbb{F}_q$, para todo $1 \le i \le r$. Basta escrever $\mathbb{F}_qEe_i = \mathbb{F}_qE\overline{e}_1\overline{e}_2\ldots\overline{e}_t$ e, indutivamente, verificamos $\mathbb{F}_qEe_i \cong \mathbb{F}_q$. Analogamente, $\mathbb{F}_qBf_j \cong \mathbb{F}_{q^k}$ para todo $1 \le j \le s$ e $k \ge 1$. Assim, pelo Lema 5.1.1, temos

$$(\mathbb{F}_qEe_i \otimes \mathbb{F}_qBf_j) \cong \left(\mathbb{F}_q \otimes \mathbb{F}_{q^k}\right) \cong \mathbb{F}_{q^k}. \tag{3.6}$$

■

3.3.1 Subgrupos e Idempotentes

Nesta seção vamos estender os resultados obtidos na Seção 3.3. Exibiremos o comportamento dos idempotentes primitivos de uma álgebra de grupo para um grupo G abeliano qualquer, sob algumas hipóteses sobre o tamanho do corpo $\mathbb{F}_q$, relacionando-os com os subgrupos co-cíclicos de G.

Para um grupo abeliano finito G, escreveremos $G = G_{p_1} \times G_{p_2} \times \ldots \times G_{p_t}$, onde G_{p_i} denota o p_i-subgrupo de Sylow de G, para cada $1 \leq i \leq t$. Além disso, conforme a Definição 3.3.1, consideremos

$$\mathcal{S}_{cc}(G) = \{H/\ H \text{ é um subgrupo co-cíclico de } G\ \}. \tag{3.7}$$

Lema 3.3.6. *Sejam $G = G_{p_1} \times G_{p_2} \times \ldots \times G_{p_t}$ um grupo abeliano finito e $H \in \mathcal{S}_{cc}(G)$. Escreva $H = H_{p_1} \times H_{p_2} \times \ldots \times H_{p_t}$, onde H_{p_i} é o p_i-subgrupo de Sylow de H. Então H_{p_i} é co-cíclico em G_{p_i}, para cada $1 \leq i \leq t$.*

Demonstração. Dado $H \in \mathcal{S}_{cc}(G)$, G/H é cíclico e $G/H \cong \frac{G_{p_1} \times G_{p_2} \times \ldots \times G_{p_t}}{H_{p_1} \times H_{p_2} \times \ldots \times H_{p_t}} \geq G_{p_i}/H_{p_i}$. Portanto $H_{p_i} \in \mathcal{S}_{cc}(G_{p_i})$, para cada $1 \leq i \leq t$. ■

Dado $H \in \mathcal{S}_{cc}(G)$, seja e_H um idempotente de $\mathbb{F}_q G$. De acordo com a decomposição de H dada no Lema 3.3.6, para cada $1 \leq i \leq t$, ou $H_{p_i} = G_{p_i}$, ou existe um único subgrupo $H^*_{p_i}$ tal que $\left[H^*_{p_i} : H_{p_i}\right] = p_i$. Então, defina $e_{H_{p_i}} = \widehat{G_{p_i}}$ ou $e_{H_{p_i}} = \widehat{H_{p_i}} - \widehat{H^*_{p_i}}$, respectivamente. Assim

$$e_H = e_{H_{p_1}} e_{H_{p_2}} \ldots e_{H_{p_t}} \tag{3.8}$$

Para qualquer outro $K \in \mathcal{S}_{cc}(G)$, com $K \neq H$, temos $K_{p_i} \neq H_{p_i}$, para algum $1 \leq i \leq t$. Logo $e_{H_{p_i}} e_{K_{p_i}} = 0$ e, consequentemente, $e_H e_K = 0$. Portanto demonstramos o seguinte resultado

Proposição 3.3.7. *Sejam G um grupo abeliano finito e $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Então*

$$\mathcal{B} = \{e_H/H \in \mathcal{S}_{cc}(G)\} \tag{3.9}$$

é um conjunto de idempotentes ortogonais de $\mathbb{F}G$.

Observação 3.3.8. *Para $\mathbb{F} = \mathbb{Q}$, os idempotentes acima são primitivos, conforme [12]. Já para corpos finitos, este resultado nem sempre é verdadeiro. Como contra-exemplo, considere a álgebra de grupo $\mathbb{F}_3\mathcal{C}_{11}$ do grupo cíclico $\mathcal{C}_{11} = \{g/g^{11} = 1\}$. Esta álgebra é semissimples, mas como 3 não gera $U(\mathbb{Z}_{11})$, então existem mais do que $2 = |\mathcal{S}_{cc}(\mathcal{C}_{11})|$ idempotentes primitivos em $\mathbb{F}_3\mathcal{C}_{11}$.*

Observamos que a Proposição 3.3.7 nos garante a ortogonalidade deste conjunto de idempotentes, no entanto, não garante que esses idempotentes sejam primitivos. Realizar a decomposição de cada um desses idempotentes como soma de idempotentes primitivos não é uma tarefa simples, mesmo para grupos de ordem pequena, como veremos mais adiante no Capítulo 5, Seção 5.2.

Capítulo 4

A λ-Aplicação e os Idempotentes Primitivos em Anéis Semissimples

Vamos expor neste capítulo um método para obter códigos cíclicos minimais a partir de uma abordagem polinomial. Chamamos este método de **λ-técnica** e ela é definida a partir de uma **λ-aplicação** e um **λ-produto** de polinômios, que são definidos a seguir. A principal referência para este capítulo é [16].

4.1 A λ-aplicação e as classes ciclotômicas

Neste capítulo consideramos a seguinte **hipótese geral**:

$$\begin{aligned} &r \geqslant 2 \text{ e } \alpha_i \geqslant 1 \text{ são números inteiros,} \\ &m = \prod_{i=1}^{r} p_i^{\alpha_i}, \text{ com } p_i \text{ primos ímpares distintos, para } 1 \leq i \leq r, \\ &mdc\left(\frac{\varphi(p_i^{\alpha_i})}{2}, \frac{\varphi(p_j^{\alpha_j})}{2}\right) = 1, \text{ para } 1 \leq i \neq j \leq r, \\ &l \neq 2 \text{ é uma raiz primitiva } mod\, p_i^{\alpha_i}, \text{ para cada } 1 \leq i \leq r. \end{aligned} \tag{4.1}$$

Considere o conjunto $A = \{0, 1, ..., (m-1)\}$. Para $a, b \in A$, definimos

$$a \sim b \text{ se, e somente se, } a \equiv bl^i (mod\, m), \text{ para algum inteiro } i \geq 0. \tag{4.2}$$

Esta é uma relação de equivalência no conjunto A cujas classes de equivalência são chamadas **classes l-ciclotômicas de** A.

Se t é o menor inteiro positivo tal que $s \equiv sl^t (mod\, m)$, então a classe l-ciclotômica de s é definida por $C_s = \{s, sl, ..., sl^{t-1}\}$.

Usaremos aqui a mesma nomeclatura "classe l-ciclotômica"que foi usada anteriormente na definição de classe q-ciclotômica de elementos do grupo, dada na Página 24. O uso dessas definições ficará claro no contexto em que forem utilizadas.

Vamos definir e discutir os métodos chamados λ-aplicação e λ-produto para a obtenção, respectivamente, das classes l-ciclotômicas módulo m e das expressões explícitas dos idempotentes primitivos do anel semissimples $\mathcal{R}_m = \dfrac{\mathbb{F}_l[x]}{\langle x^m - 1\rangle}$. Provaremos que as classes l-ciclotômicas módulo m podem ser vistas como λ-imagem do produto cartesiano das r classes l^2-ciclotômicas módulo $p_i^{\alpha_i}$. Além disso, as expressões dos idempotentes primitivos em $\mathcal{R}_m$ são dadas como imagens do λ-produto de polinômios, onde cada um destes polinômios é um idempotente primitivo em $\mathcal{R}_{p_i^{\alpha_i}} = \dfrac{\mathbb{F}_{l^2}[x]}{\left\langle x^{p_i^{\alpha_i}} - 1\right\rangle}$, para $1 \leq i \leq r$.

Notações 4.1.1. *Sob a hipótese geral* (4.1)*, estabelecemos as seguintes notações e definições:*

(i) $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ *e, para* $1 \leq i \leq r$, $\overline{m}_i = \dfrac{m}{p_i^{\alpha_i}}$.

(ii) $A_i = \{0, 1, 2, ..., p_i^{\alpha_i} - 1\}$ *e* $A = \{0, 1, ..., (m-1)\}$.

(iii) R_i *e* N_i *são os conjuntos de resíduos quadráticos e não quadráticos módulo* $p_i^{\alpha_i}$.

(iv) $R_{p_i^{\beta_i}} = \left\{ rp_i^{\beta_i} / r \in R_i \right\}$ *e* $N_{p_i^{\beta_i}} = \left\{ sp_i^{\beta_i} / s \in N_i \right\}$.

(v) $\mathcal{R}_m = \dfrac{\mathbb{F}_l[x]}{\langle x^m - 1\rangle}$ *e* $\mathcal{R}_{p_i^{\alpha_i}} = \dfrac{\mathbb{F}_{l^2}[x]}{\left\langle x^{p_i^{\alpha_i}} - 1\right\rangle}$.

(vi) δ *é uma raiz* m*-ésima primitiva da unidade em alguma extensão do corpo* $\mathbb{F}_{l^2}$.

(vii) Para qualquer m*, sempre denotamos a classe ciclotômica* C_0 *módulo* m *por* $\{0\}$.

Definição 4.1.2. *Dado o produto cartesiano* $A_1 \times A_2 \times ... \times A_r$*, definimos a* λ***-aplicação*** *por*

$$\begin{array}{rccc} \lambda: & A_1 \times A_2 \times ... \times A_r & \longrightarrow & A \\ & (a_1, ..., a_r) & \mapsto & \displaystyle\sum_{k=1}^{r} a_k \overline{m}_k (mod\, m) \end{array}$$

Lema 4.1.3. *A* λ*-aplicação é uma bijeção. (A* λ*-aplicação é um isomorfismo de grupos abelianos.)*

Demonstração. De fato, a λ-aplicação *está bem definida* pois, dados $(a_1, ..., a_r)$ e $(b_1, ..., b_r)$ em $A_1 \times A_2 \times ... \times A_r$ tais que $a_i \equiv b_i \,(mod\, p_i^{\alpha_i})$, para cada $1 \leq i \leq r$, temos $a_i - b_i = t_i p_i^{\alpha_i}$, para $t_i \in \mathbb{Z}$. Assim

$$\begin{aligned}
\lambda(a_1, ..., a_r) &= \sum_{k=1}^{r} a_k \overline{m}_k \,(mod\, m) = \sum_{k=1}^{r} \left(b_k + t_k p_k^{\alpha_k}\right) \overline{m}_k \,(mod\, m) \\
&= \sum_{k=1}^{r} b_k \overline{m}_k + \sum_{k=1}^{r} t_k p_k^{\alpha_k} \overline{m}_k \,(mod\, m) \\
&\equiv \sum_{k=1}^{r} b_k \overline{m}_k (mod\, m) \\
&= \lambda(b_1, ..., b_r).
\end{aligned}$$

A λ-aplicação é *injetora*, pois se $\lambda(a_1, ..., a_r) \equiv \lambda(b_1, ..., b_r) \,(mod\, m)$, então

$$\sum_{k=1}^{r} (a_k - b_k) \overline{m}_k \equiv 0 \,(mod\, m).$$

Tomando essa igualdade $(mod\, p_i^{\alpha_i})$, para cada $1 \leq i \leq r$, temos

$$(a_i - b_i) \overline{m}_i = 0 \,(mod\, p_i^{\alpha_i}) \Leftrightarrow a_i \equiv b_i \,(mod\, p_i^{\alpha_i}),$$

uma vez que $mdc\,(p_i^{\alpha_i}, \overline{m}_i) = 1$.

Para verificar que a λ-aplicação é *sobrejetora*, basta observar que a λ-aplicação é injetora e $|A| = |A_1 \times A_2 \times ... \times A_r|$. Assim, λ-aplicação é uma bijeção.

Se tomarmos $A = \mathbb{Z}_m$ e $A_i = \mathbb{Z}_{p_i^{\alpha_i}}$, para cada $1 \leq i \leq r$, como grupos aditivos, então a λ-aplicação é um isomorfismo. ∎

Teorema 4.1.4. *Seja p um número primo positivo. Se l é uma raiz primitiva módulo p^n, então ela é também uma raiz primitiva módulo p^{n-j}, para todo $0 \leq j \leq n-1$.*

Demonstração. Seja l uma raiz primitiva módulo p^n. Logo l gera as unidades de $\mathbb{Z}_{p^n}$, isto é, dado $a \in U\,(\mathbb{Z}_{p^n})$, então $a \equiv l^t \;(mod\, p^n)$, para algum $0 \leq t \leq \varphi(p^n) - 1$ e daí, para algum $k \in \mathbb{Z}$ e para todo $1 \leq j \leq n-1$,

$$a - l^t = kp^n \Leftrightarrow a - l^t = \left(kp^j\right) p^{n-j} \Rightarrow a \equiv l^t \,(mod\, p^{n-j}) \Rightarrow \left\langle \bar{l} \right\rangle = U\left(\mathbb{Z}_{p^{n-j}}\right),$$

uma vez que se $mdc\,(a, p^n) = 1$, então $mdc\,(a, p^{n-j}) = 1$, isto é, $a \in U\left(\mathbb{Z}_{p^{n-j}}\right)$. Assim, podemos ver $U\left(\mathbb{Z}_{p^{n-j}}\right)$ isomorfo a um subgrupo de $U\,(\mathbb{Z}_{p^n})$, para todo $1 \leq j \leq n-1$. ∎

Teorema 4.1.5. *Sob a hipótese geral* (4.1), $\dfrac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}$ *é a ordem de l módulo* $\prod_{i=1}^{r} p_i^{\beta_i}$,

para $1 \leq \beta_i \leq \alpha_i$.

Demonstração. Seja h_β a ordem de l módulo $\prod_{i=1}^{r} p_i^{\beta_i}$. Assim

$$l^{h_\beta} \equiv 1 \left(mod \prod_{i=1}^{r} p_i^{\beta_i} \right) \Rightarrow l^{h_\beta} \equiv 1 \left(mod\, p_i^{\beta_i} \right),$$

para todo $1 \leq i \leq r$.

Da hipótese geral (4.1), l é uma raiz primitiva módulo $p_i^{\alpha_i}$, para todo $1 \leq i \leq r$, logo, pelo Teorema 4.1.4, $\varphi\left(p_i^{\beta_i}\right) | h_\beta$, o que implica

$$mmc\Big(\varphi\left(p_1^{\beta_1}\right), \varphi\left(p_2^{\beta_2}\right), ..., \varphi\left(p_r^{\beta_r}\right)\Big) | h_\beta. \tag{4.3}$$

Cada p_i é um primo positivo ímpar, logo $p_i - 1 = 2^{k_i} l_i$, onde l_i é um número ímpar e $mdc(l_i, l_j) = 1$, para todo $1 \leq i \neq j \leq r$. Afirmamos que pode existir no máximo um $k_i \geq 2$. De fato, se existissem k_i e k_j, com $i \neq j$, ambos maiores ou iguais a 2, isto contrariaria a hipótese geral (4.1). Sem perda de generalidade, vamos assumir $k_i = 1$, para $1 \leq i \leq r-1$ e $k_r \geq 1$. Então, da definição de mmc, obtemos

$$\begin{aligned} mmc\left(\varphi\left(p_1^{\beta_1}\right), \varphi\left(p_2^{\beta_2}\right), \ldots, \varphi\left(p_r^{\beta_r}\right)\right) &= \prod_{i=1}^{r} p_i^{\beta_i - 1} \cdot mmc(p_1 - 1, p_2 - 1, \ldots, p_r - 1) \\ &= \prod_{i=1}^{r} p_i^{\beta_i - 1} \cdot \frac{2l_1 \cdot 2l_2 \ldots 2^{k_r} l_r}{2^{r-1}} \\ &= \frac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}. \end{aligned}$$

Substituindo em (4.3), obtemos

$$\frac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}} \mid h_\beta \tag{4.4}$$

Para cada $1 \leq i \leq r$, tem-se $l^{\varphi\left(p_i^{\beta_i}\right)} \equiv 1 \left(mod\, p_i^{\beta_i} \right)$. Logo

$$l^{\frac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}} \equiv 1 \left(mod\, p_i^{\beta_i} \right) \Rightarrow l^{\frac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}} \equiv 1 \left(mod \prod_{i=1}^{r} p_i^{\beta_i} \right).$$

A última implicação é válida pelo fato de $mdc(p_i, p_j) = 1$, para $i \neq j$. Logo $h_\beta | \frac{\varphi(\prod_{i=1}^{r} p_i^{\beta_i})}{2^{r-1}}$ e, portanto,

$$h_\beta = \frac{\varphi\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)}{2^{r-1}}.$$

■

Corolário 4.1.6. *Sob a hipótese geral* (4.1)*, seja* $\{i_1, i_2, ..., i_k\} \subseteq \{1, 2, ..., r\}$*. Então, para* $1 \leq \beta_{i_j} \leq \alpha_{i_j}$ *e* $1 \leq k \leq r$*, a ordem de* l *módulo* $\prod_{i=1}^{k} p_{i_j}^{\beta_{i_j}}$ *é* $\frac{\varphi\left(\prod_{i=1}^{k} p_{i_j}^{\beta_{i_j}}\right)}{2^{k-1}}$

Lema 4.1.7. *O número primo* l *é um resíduo não quadrático módulo* $p_i^{\alpha_i}$*, para todo* $1 \leq i \leq r$*.*

Demonstração. De fato, suponha que l seja um resíduo quadrático módulo $p_i^{\alpha_i}$. Em particular, l é um resíduo quadrático módulo p_i e, do fato de que $mdc(l, m) = 1$, de acordo com o Teorema 1.1.3, temos

$$1 \equiv \left(\frac{l}{p_i}\right) \equiv l^{\frac{(p_i-1)}{2}} \, (mod\, p_i)$$

Como l é uma raiz primitiva módulo $p_i^{\alpha_i}$, pelo Teorema 4.1.4, l também é uma raiz primitiva módulo p_i, assim

$$\varphi(p_i) | \tfrac{p_i-1}{2} \Rightarrow p_i - 1 | \tfrac{p_i-1}{2}, \text{ o que é um absurdo.}$$

Logo l é resíduo não quadrático módulo $p_i^{\alpha_i}$, para todo $1 \leq i \leq r$. ■

Lema 4.1.8. *Sob a hipótese geral* (4.1)*, para cada* $1 \leq i \leq r$ *e* $1 \leq \beta_i \leq \alpha_i - 1$*, os conjuntos* $R_i, N_i, R_{p_i^{\beta_i}}$ *e* $N_{p_i^{\beta_i}}$ *são as classes* l^2*-ciclotômicas módulo* $p_i^{\alpha_i}$*.*

Demonstração. Denote por $M_{p_i} = \{x \in A_i / \, x = tp_i, t \in \mathbb{Z}\}$ o conjunto de todos os múltiplos de p_i em A_i. Assim, da Definição 1.1.1, $A_i = R_i \cup N_i \cup M_{p_i}$.

Considere $\widetilde{C}_1$ a classe l-ciclotômica de 1 $(mod\, p_i^{\alpha_i})$. Como l é raiz primitiva $(mod\, p_i^{\alpha_i})$, logo $o\left(l^2\right) = \frac{\left|\widetilde{C}_1\right|}{2} = \frac{\varphi\left(p_i^{\alpha_i}\right)}{2}$ $(mod\, p_i^{\alpha_i})$. Além disso, pelo Lema 4.1.7, l é um resíduo não quadrático $(mod\, p_i^{\alpha_i})$ e assim

$$\widetilde{C}_1 = \widetilde{C}_1^{l^2} \cup \widetilde{C}_l^{l^2} \subset A_i \setminus M_{p_i},$$

onde $\widetilde{C}_1^{l^2}$ é a classe l^2-ciclotômica de 1 $(mod\, p_i^{\alpha_i})$ e $\widetilde{C}_l^{l^2}$ é a classe l^2-ciclotômica de l $(mod\, p_i^{\alpha_i})$.

Como $\left|\widetilde{C}_1\right| = \varphi\left(p_i^{\alpha_i}\right)$ e $|A_i \setminus M_{p_i}| = p_i^{\alpha_i} - \left\lfloor \frac{p_i^{\alpha_i}}{p_i} \right\rfloor = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$, então

$$|A_i \setminus M_{p_i}| = \left|\widetilde{C}_1\right| \text{ e daí } \widetilde{C}_1 = \widetilde{C}_1^{l^2} \cup \widetilde{C}_l^{l^2} = R_i \cup N_i = A_i \setminus M_{p_i}.$$

Novamente, como l é um elemento não quadrático $(mod\, p_i^{\alpha_i})$, então $\widetilde{C}_1^{l^2} \subset R_i$ e $\widetilde{C}_l^{l^2} \subset N_i$, logo $\widetilde{C}_1^{l^2} = R_i$ e $\widetilde{C}_l^{l^2} = N_i$. ∎

Proposição 4.1.9. *Sob a hipótese geral* (4.1)*, as classes l-ciclotômicas de A são dos seguintes tipos:*

$$\begin{aligned}
C_0 &= \{0\},\\
C_1 &= \left\{1, l, l^2, ..., l^{\frac{\varphi(m)}{2^{r-1}}-1}\right\},\\
C_b &= \left\{b, bl, bl^2, ..., bl^{\frac{\varphi(m)}{2^{r-1}}-1}\right\},\\
C_{p_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r}} &= \left\{p_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r}, p_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r} l, ..., p_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r} l^{\frac{\varphi\left(\prod_{i=1}^r p_i^{\alpha_i-\beta_i}\right)}{2^{r-1}}-1}\right\}\\
C_{bp_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r}} &= \left\{bp_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r}, bp_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r} l, ..., bp_1^{\beta_1}\cdot ...\cdot p_r^{\beta_r} l^{\frac{\varphi\left(\prod_{i=1}^r p_i^{\alpha_i-\beta_i}\right)}{2^{r-1}}-1}\right\},
\end{aligned}$$

onde $b \in A$ *é tal que* $mdc\left(b, \prod_{i=1}^r p_i\right) = 1$, $b \not\equiv l^t (mod\ m)$ *e* $0 \leq \beta_i \leq \alpha_i - 1$.

Sejam $D = \{1, 2, \ldots, r\}$ *e* $B = \{i_1, i_2, \ldots, i_s\}$ *um subconjunto próprio de* D. *Defina* $a = \prod_{j\in B} p_j^{\alpha_j} \cdot \prod_{t\in D\setminus B} p_t^{\beta_t}$. *Assim, as demais classes l-ciclotômicas de A são dos tipos:*

$$\begin{aligned}
C_a &= \left\{a, al, ..., al^{\frac{\varphi\left(\prod_{i=|B|+1}^r p_i^{\alpha_i-\beta_i}\right)}{2^{r-|B|-1}}-1}\right\},\\
C_{ba} &= \left\{ba, bal, ..., bal^{\frac{\varphi\left(\prod_{i=|B|+1}^r p_i^{\alpha_i-\beta_i}\right)}{2^{r-|B|-1}}-1}\right\},
\end{aligned}$$

desde que $C_b \cap C_1 = \varnothing$, *onde esta interseção é vista módulo* $\prod_{j\in D\setminus B} p_j^{\alpha_j-\beta_j}$.

Demonstração. Como λ é sobrejetora, existem $a_i \in A_i$, para cada $1 \leq i \leq r$, tais que

$$\lambda(a_1, a_2, ..., a_r) = 1 \tag{4.5}$$

Afirmação: $a_i \in R_i$ ou $a_i \in N_i$, ou seja, $a_i \not\equiv 0\ (mod\, p_i^{\alpha_i})$, para todo $1 \leq i \leq r$.

De fato, suponha sem perda de generalidade, que $a_r = 0$. Pela definição da λ-aplicação, temos:

$$1(mod\, m) \equiv \sum_{i=1}^{r-1} a_i\overline{m}_i(mod\, m) \Leftrightarrow 1 + t_0\prod_{i=1}^{r} p_i^{\alpha_i} = p_r^{\alpha_r}\left(\sum_{i=1}^{r-1} a_i\overline{n}_i\right) + t_1\prod_{i=1}^{r} p_i^{\alpha_i},$$

onde $\overline{n}_i = \dfrac{\overline{m}_i}{p_r^{\alpha_r}}$, para todo $1 \leq i \leq r-1$ e $t_0, t_1 \in \mathbb{Z}$. Logo

$$1 = p_r^{\alpha_r}\left(-t_0\prod_{i=1}^{r-1} p_i^{\alpha_i} + \sum_{i=1}^{r-1} a_i\overline{n}_i + t_1\prod_{i=1}^{r-1} p_i^{\alpha_i}\right) \Rightarrow p_r|1,$$

o que é um absurdo. Portanto $a_i \in R_i$ ou $a_i \in N_i$ para todo $1 \leq i \leq r$.

Considere agora duas classes l-ciclotômicas $C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}}$ e $C_{p_1^{\gamma_1}\cdot\ldots\cdot p_r^{\gamma_r}}$, onde $0 \leq \beta_i \leq \gamma_i \leq \alpha_i$, para $1 \leq i \leq r$, $1 \neq b \in A$ tal que $mdc\left(b, \prod_{i=1}^{r} p_i\right) = 1$ e $b \not\equiv l^t(mod\ m)$.

Afirmação: $C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}} \bigcap C_{p_1^{\gamma_1}\cdot\ldots\cdot p_r^{\gamma_r}} = \emptyset$.

Sob as mesmas hipóteses, basta verificarmos $C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}} \bigcap C_1 = \emptyset$ e daí o resultado da afirmação será uma consequência direta.

Seja $a \in C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}} \bigcap C_1$. Da definição de classe l-ciclotômica, temos a existência de inteiros positivos $j \leq i$ tais que

$$bp_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r} l^i \equiv l^j(mod\, m).$$

Assim

$$l^j\left(bl^{i-j}\prod_{i}^{r} p_i^{\beta_i} - 1\right) = k\prod_{i}^{r} p_i^{\alpha_i},$$

para algum $k \in \mathbb{Z}$. Como $\prod_{i}^{r} p_i^{\alpha_i}$ não divide l^j, então $\prod_{i}^{r} p_i^{\alpha_i} | \left(bl^{i-j}\prod_{i}^{r} p_i^{\beta_i} - 1\right)$. Logo

$$k_1\prod_{i}^{r} p_i^{\alpha_i} = bl^{i-j}\prod_{i}^{r} p_i^{\beta_i} - 1, \Rightarrow \prod_{i}^{r} p_i^{\beta_i}\left(k_1\prod_{i}^{r} p_i^{\alpha_i-\beta_i} - bl^{i-j}\right) = -1 \Rightarrow \prod_{i}^{r} p_i^{\beta_i}| - 1,$$

para algum $k_1 \in \mathbb{Z}$, o que é um absurdo.

Assim $C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}} \bigcap C_1 = \emptyset$ e portanto $C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}} \bigcap C_{p_1^{\gamma_1}\cdot\ldots\cdot p_r^{\gamma_r}} = \emptyset$.

Dado $b \in A$, onde $mdc\left(b, \prod_{i=1}^{r} p_i^{\alpha_i}\right) = 1$ e $b \not\equiv l^t (mod\ m)$, se multiplicarmos o lado direito de (4.5) por $b, bl, bl^2, ..., bl^{\frac{\varphi(m)}{2^{r-1}}-1}$, obtemos todos os elementos de C_b, de acordo com o Teorema 4.1.5. Como λ é injetiva e $mdc(l, m) = 1$, esses elementos são as λ-imagens de $(ba_1l^j, ba_2l^j, ..., ba_rl^j)$, para $0 \leq j \leq \dfrac{\varphi(m)}{2^{r-1}} - 1$.

Da Definição 1.1.1 (resíduos quadráticos) e do Lema 4.1.7, para j par, l^j é um resíduo quadrático módulo $p_i^{\alpha_i}$, para todo $1 \leq i \leq r$. De forma análoga, para j ímpar, l^j é um resíduo não quadrático módulo $p_i^{\alpha_i}$. Assim,

$$\begin{aligned} ba_i \in R_i\,(N_i) \ &\Rightarrow\ ba_il^j \in R_i\,(N_i)\,, \text{ para } j \text{ par.} \\ ba_i \in R_i\,(N_i) \ &\Rightarrow\ ba_il^j \in N_i\,(R_i)\,, \text{ para } j \text{ ímpar.} \end{aligned}$$

Defina $X_i = R_i(\text{ou } N_i)$, $Y_i = N_i(\text{ou } R_i)$, $X_{p_i^{\beta_i}} = R_{p_i^{\beta_i}}\left(\text{ou } N_{p_i^{\beta_i}}\right)$ e $Y_{p_i^{\beta_i}} = N_{p_i^{\beta_i}}\left(\text{ou } R_{p_i^{\beta_i}}\right)$. Logo

$$\lambda(X_1 \times ... \times X_r \cup Y_1 \times ... \times Y_r) = C_b \tag{4.6}$$

Multiplicando 1 em (4.5) por $bp_1^{\beta_1}p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}l^j\ (mod\, m)$, para algum $0 \leq \beta_i \leq \alpha_i - 1$, $1 \leq i \leq r$ e $0 \leq j \leq \dfrac{\varphi(\prod_{i=1}^{r} p_i^{\alpha_i-\beta_i})}{2^{r-1}} - 1$, obtemos

$$\lambda\left(X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}\right) = C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot ... \cdot p_r^{\beta_r}}. \tag{4.7}$$

De fato,

$$1 \equiv \sum_{i=1}^{r} a_i\overline{m}_i\,(mod\ m) \Rightarrow \sum_{i=1}^{r} d_ip_i^{\beta_i}\overline{m}_i = bp_1^{\beta_1}p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}l^j (mod\, m),$$

onde $d_i = ba_ip_1^{\beta_1} \cdot ... \cdot p_{i-1}^{\beta_{i-1}} \cdot p_{i+1}^{\beta_{i+1}} \cdot ... \cdot p_r^{\beta_r}l^j$. Logo $d_ip_i^{\beta_i} \in X_{p_i^{\beta_i}}$.

Seja t o menor inteiro tal que $bp_1^{\beta_1} \cdot ... \cdot p_r^{\beta_r}l^t \equiv bp_1^{\beta_1} \cdot ... \cdot p_r^{\beta_r} (mod\, m)$. Logo

$$bp_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}l^t \equiv bp_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r} (mod\, m) \Leftrightarrow bl^t \equiv b\left(mod\, p_1^{\alpha_1-\beta_1} \cdot \ldots \cdot p_r^{\alpha_r-\beta_r}\right),$$

onde, pelo Teorema 4.1.5, $t = \dfrac{\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i-\beta_i}\right)}{2^{r-1}}$.

Sem perda de generalidade, consideremos agora elementos em A da forma $bp_1^{\alpha_1}p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}$, com uma escolha de β_i fixo, para $0 \leq \beta_i \leq \alpha_i - 1$ e $2 \leq i \leq r$.

Os casos mais gerais seguem o mesmo raciocínio. Pela λ-aplicação e por (4.5) obtemos

$$bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r} = \lambda(0, a_2 bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}, \ldots, a_r bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}) = \lambda(0, \widetilde{a}_2, \ldots, \widetilde{a}_r),$$

onde cada $a_i bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r} = \widetilde{a}_i \in R_{p_i^{\beta_i}}\left(N_{p_i^{\beta_i}}\right)$, para cada $2 \leq i \leq r$. Vamos calcular a cardinalidade da classe l-ciclotômica $C_{bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}}$.

Seja t o menor inteiro positivo tal que $bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}l^t \equiv bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}(mod\, m)$. Então

$$bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}l^t \equiv bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}(mod\, m) \Leftrightarrow bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}(l^t-1) = k\prod_{i=1}^{r}p_i^{\alpha_i}, \tag{4.8}$$

para $k \in \mathbb{Z}$. Assim

$$\prod_{i=1}^{r}p_i^{\alpha_i} | bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}(l^t-1) \Leftrightarrow bl^t \equiv b\left(mod\prod_{i=2}^{r}p_i^{\alpha_i-\beta_i}\right).$$

Logo, pelo Teorema 4.1.5, $t = \dfrac{\prod_{i=2}^{r}p_i^{\alpha_i-\beta_i}}{2^{r-2}}$ e

$$C_{bp_1^{\alpha_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}} = \lambda\left(C_0 \times X_{p_2^{\beta_2}} \times \ldots \times X_{p_r^{\beta_r}} \cup C_0 \times Y_{p_2^{\beta_2}} \times \ldots \times Y_{p_r^{\beta_r}}\right).$$

■

Observação 4.1.10. *De* (4.7) *e do Lema 4.1.8, a λ-aplicação faz corresponder a cada classe l-ciclotômica de A a união de dois produtos cartesianos de classes l^2-ciclotômicas módulo $p_i^{\alpha_i}$, para cada $1 \leq i \leq r$, a saber, $X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}$ e vice-versa.*

Teorema 4.1.11. *Sob a hipótese geral* (4.1)*, o número de classes l-ciclotômicas módulo m é*

$$\frac{(2\alpha_1+1)\ldots(2\alpha_r+1)+1}{2}. \tag{4.9}$$

Demonstração. De acordo com o Lema 4.1.8, os conjuntos (grupos aditivos abelianos) A_i podem ser particionados com relação as suas classes l^2-ciclotômicas $X_{p_i^{\beta_i}}$, onde $0 \leq \beta_i \leq \alpha_i - 1$ e $1 \leq i \leq r$, além das classes do tipo C_0 módulo $p_i^{\alpha_i}$. Ainda, conforme foi afirmado na Observação 4.1.10, qualquer classe l-ciclotômica pode ser vista como λ-imagem de uma combinação arbitrária de classes l^2-ciclotômicas. Por hora desconsideremos a classe C_0 módulo m, gerada de forma única pelos zeros dos A_i, para todo $1 \leq i \leq r$. Logo existem $(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_r+1)-1$ combinações possíveis. Neste cálculo devemos descartar um dos dois tipos de combinações abaixo:

$$\lambda\left(X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}}\right) \text{ ou } \lambda\left(Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}} \cup X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}}\right),$$

pois de acordo com a Proposição 4.1.9, estas λ-imagens geram a mesma classe l-ciclotômica. Assim existem $\dfrac{(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_r+1)-1}{2}$ classes l ciclotômicas. Adicionando mais uma classe, a saber, a classe C_0 módulo m, obtemos o resultado.

A expressão (4.9) é igual a proposta em [16, Teorema 2.6]. ∎

4.2 Idempotentes Primitivos em $\mathcal{R}_m = \frac{\mathbb{F}_l[x]}{\langle x^m-1\rangle}$

Aqui desenvolvemos um método para explicitar os idempotentes primitivos de $\mathcal{R}_m$ descrevendo-os como λ-**produto** de idempotentes primitivos de $\mathcal{R}_{p_i^{\alpha_i}}$, para cada $1 \leq i \leq r$.

Definição 4.2.1. *Para $1 \leq i \leq r$, seja $f_i(x) = \sum_{j_i=0}^{p_i^{\alpha_i}-1} a_{j_i}x^{j_i} \in \mathbb{F}_{l^2}[x]$. Definimos*

$$\lambda(f_1(x) \otimes \ldots \otimes f_r(x)) = \sum_{\lambda(j_1,\ldots,j_r)\in\lambda(A_1\times\ldots\times A_r)} a_{j_1}\cdot\ldots\cdot a_{j_r}x^{\lambda(j_1,\ldots,j_r)}. \tag{4.10}$$

*Chamamos este produto de λ-**produto** dos polinômios $f_i(x) = \sum_{j_i=0}^{p_i^{\alpha_i}-1} a_{j_i}x^{j_i}$.*

Definição 4.2.2. *A expressão $\theta_s = \dfrac{1}{m}\left(\sum_{i=0}^{m-1}\varepsilon_i x^i\right)$, onde $\varepsilon_i = \varepsilon_i^{C_s} = \sum_{s\in C_s}\delta^{-is}$, é um idempotente primitivo no anel $\mathcal{R}_m$. Esta técnica é chamada ε-**método** para obtenção da expressão explícita de θ_s. Para maiores informações, ver [19, Capítulo 8, Teorema 6].*

Observação 4.2.3.

(i) Para $1 \leq i \leq r$ e $0 \leq \beta_i \leq \alpha_i - 1$, denotemos por $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}}$ o idempotente primitivo correspondente a classe l-ciclotômica $C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}}$ no anel semissimples $\mathcal{R}_m$, onde $l^t \not\equiv b \in A$ e $mdc\left(b, \prod_{i=1}^{r} p_i\right) = 1$.

(ii) Denotemos por $\theta^*_{p_i^{\beta_i}}$ e $\theta^{**}_{p_i^{\beta_i}}$ os idempotentes primitivos básicos correspondentes as classes l^2-ciclotômicas $X_{p_i^{\beta_i}}$ e $Y_{p_i^{\beta_i}}$, respectivamente no anel $\mathcal{R}_{p_i^{\alpha_i}}$. Além disso, dado $s \in A$, defina $\sigma_s(x) = \sigma_{C_s}(x) = \sum_{t\in C_s} x^t$.

(iii) Sejam $X_1 \times \ldots \times X_r$, $X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}}$ e $\theta^*_{p_1^{\beta_1}} \otimes \ldots \otimes \theta^*_{p_r^{\beta_r}}$ as primeiras partes das expressões $\lambda(X_1 \times \ldots \times X_r \cup Y_1 \times \ldots \times Y_r)$, $\lambda\left(X_{p_1^{\beta_1}} \times \ldots \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times \ldots \times Y_{p_r^{\beta_r}}\right)$

e $\lambda\left(\theta^*_{p_1^{\beta_1}} \otimes ... \otimes \theta^*_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{**}_{p_r^{\beta_r}}\right)$, respectivamente. Ainda, X_i, $X_{p_i^{\beta_i}}$ e $\theta^*_{p_i^{\beta_i}}$ são as i-ésimas entradas de $X_1 \times ... \times X_r$, $X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}}$ e $\theta^*_{p_1^{\beta_1}} \otimes ... \otimes \theta^*_{p_r^{\beta_r}}$, respectivamente.

Teorema 4.2.4. *Se, para cada $0 \leq \beta_i \leq \alpha_i$, as i-ésimas entradas da primeira parte de*

$$C_1 = \lambda(X_1 \times ... \times X_r \cup Y_1 \times ... \times Y_r) \text{ e}$$

$$C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}\right),$$

são R_i e $R_{p_i^{\beta_i}}\left(\text{ou } N_{p_i^{\beta_i}}\right)$, então $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(\theta^*_{p_1^{\beta_1}} \otimes ... \otimes \theta^*_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{**}_{p_r^{\beta_r}}\right)$, onde, para $1 \leq i \leq r$, $\theta^*_{p_i^{\beta_i}}$ e $\theta^{**}_{p_i^{\beta_i}}$ são os idempotentes primitivos correspondentes as classes l^2-ciclotômicas $R_{p_i^{\beta_i}}\left(\text{ou } N_{p_i^{\beta_i}}\right)$ e $N_{p_i^{\beta_i}}\left(\text{ou } R_{p_i^{\beta_i}}\right)$, respectivamente.

Demonstração. Para $X_i = R_i$ e $X_{p_i^{\beta_i}} = R_{p_i^{\beta_i}}$, afirmamos que os idempotentes primitivos básicos $\theta^*_{p_i^{\beta_i}}$ e $\theta^{**}_{p_i^{\beta_i}}$ são definidos por

$$\theta^*_{p_i^{\beta_i}} = \frac{1}{p_i^{\alpha_i}}\left\{\varepsilon_0^{X_{p_i^{\beta_i}}}\sigma_{C_0}(x) + \sum_{j_i=0}^{\alpha_i-1}\left(\varepsilon_{p_i^{j_i}}^{X_{p_i^{\beta_i}}}\sigma_{R_{p_i^{j_i}}}(x) + \varepsilon_{\partial p_i^{j_i}}^{X_{p_i^{\beta_i}}}\sigma_{N_{p_i^{j_i}}}(x)\right)\right\} \text{ e} \tag{4.11}$$

$$\theta^{**}_{p_i^{\beta_i}} = \frac{1}{p_i^{\alpha_i}}\left\{\varepsilon_0^{Y_{p_i^{\beta_i}}}\sigma_{C_0}(x) + \sum_{j_i=0}^{\alpha_i-1}\left(\varepsilon_{p_i^{j_i}}^{Y_{p_i^{\beta_i}}}\sigma_{R_{p_i^{j_i}}}(x) + \varepsilon_{\partial p_i^{j_i}}^{Y_{p_i^{\beta_i}}}\sigma_{N_{p_i^{j_i}}}(x)\right)\right\}, \tag{4.12}$$

onde $\partial \in N_i$, $\varepsilon_{p_i^{j_i}}^{X_{p_i^{\beta_i}}\left(Y_{p_i^{\beta_i}}\right)} = \sum_{s_i \in X_{p_i^{\beta_i}}\left(Y_{p_i^{\beta_i}}\right)} \delta_i^{-p_i^{j_i}s_i}$, $\varepsilon_{\partial p_i^{j_i}}^{X_{p_i^{\beta_i}}\left(Y_{p_i^{\beta_i}}\right)} = \sum_{s_i \in X_{p_i^{\beta_i}}\left(Y_{p_i^{\beta_i}}\right)} \delta_i^{-\partial p_i^{j_i}s_i}$, $p_i^{j_i} \in R_{p_i^{j_i}}$, $\partial p_i^{j_i} \in N_{p_i^{j_i}}$ e δ_i é uma raiz $p_i^{\alpha_i}$-ésima primitiva da unidade, para cada $1 \leq i \leq r$, em alguma extensão de $\mathbb{F}_{l^2}$ que contenha uma raiz m-ésima primitiva da unidade.

De fato, o idempotente primitivo $\theta^*_{p_i^{\beta_i}}$ correspondente a classe l^2-ciclotômica $X_{p_i^{\beta_i}}$, de acordo com a Definição 4.2.2, é dado por

$$\theta^*_{p_i^{\beta_i}} = \frac{1}{p_i^{\alpha_i}}\left\{\varepsilon_0^{X_{p_i^{\beta_i}}} + \varepsilon_1^{X_{p_i^{\beta_i}}}x + ... + \varepsilon_{p_i-1}^{X_{p_i^{\beta_i}}}x^{p_i-1} + ... + \varepsilon_{p_i^{\alpha_i}-1}^{X_{p_i^{\beta_i}}}x^{p_i^{\alpha_i}-1}\right\} \tag{4.13}$$

O conjunto A_i pode ser escrito como união disjunta das suas classes l^2-ciclotômicas. Além disso, sejam $1 \leq t_1 < t_2 \leq p_i^{\alpha_i} - 1$, onde $t_1, t_2 \in R_{p_i^{\gamma_i}}$, para $0 \leq \gamma_i \leq \alpha_i - 1$ e $1 \leq i \leq r$. De acordo com o Teorema 1.1.3, o produto de resíduos quadráticos módulo

um primo p é um resíduo quadrático módulo p. Logo

$$\varepsilon_{t_1}^{X_{p_i^{\beta_i}}} = \sum_{s_i \in X_{p_i^{\beta_i}}} \delta_i^{-t_1 s_i} = \sum_{s_i \in X_{p_i^{\beta_i}}} \delta_i^{-t_2 s_i} = \varepsilon_{t_2}^{X_{p_i^{\beta_i}}}. \tag{4.14}$$

Assim $\varepsilon_{t_1}^{X_{p_i^{\beta_i}}} = \varepsilon_{p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}}$, para todo $t_1 \in R_{p_i^{\gamma_i}}$ e daí

$$\varepsilon_{p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}} \left(\sum_{t \in R_{p_i^{\gamma_i}}} x^t \right) = \varepsilon_{p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}} \sigma_{R_{p_i^{\gamma_i}}}(x) \tag{4.15}$$

De forma análoga ao raciocínio desenvolvido em (4.14), para todo $w_1 \in N_{p_i^{\gamma_i}}$, com $0 \leq \gamma_i \leq \alpha_i - 1$ e $1 \leq i \leq r$, obtemos $\varepsilon_{w_1}^{X_{p_i^{\beta_i}}} = \varepsilon_{\partial p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}}$ e daí

$$\varepsilon_{\partial p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}} \left(\sum_{w \in N_{p_i^{\gamma_i}}} x^w \right) = \varepsilon_{\partial p_i^{\gamma_i}}^{X_{p_i^{\beta_i}}} \sigma_{N_{p_i^{\gamma_i}}}(x) \tag{4.16}$$

Logo é possível reescrever a expressão (4.13) como (4.11). Para $\theta^{**}_{p_i^{\beta_i}}$ o racíocinio é análogo.

De posse das expressões de $\theta^{*}_{p_i^{\beta_i}}$ e $\theta^{**}_{p_i^{\beta_i}}$, vamos calcular a soma

$$\lambda\left(\theta^{*}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{*}_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{**}_{p_r^{\beta_r}}\right). \tag{4.17}$$

O coeficiente de $\sigma_{\lambda(Z_1 \times ... \times Z_i \times ... \times Z_r)}(x)$ em (4.17) é

$$\begin{aligned} \varepsilon_{\lambda(Z_1 \times ... \times Z_i \times ... \times Z_r)} &= \frac{1}{m}\left(\varepsilon_{z_1}^{X_{p_1^{\beta_1}}} \cdot \varepsilon_{z_2}^{X_{p_2^{\beta_2}}} \cdot ... \cdot \varepsilon_{z_r}^{X_{p_r^{\beta_r}}} + \varepsilon_{z_1}^{Y_{p_1^{\beta_1}}} \cdot \varepsilon_{z_2}^{Y_{p_2^{\beta_2}}} \cdot ... \cdot \varepsilon_{z_r}^{Y_{p_r^{\beta_r}}} \right) \\ &= \frac{1}{m}\left(\sum_{(s_1,...,s_r) \in (X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}})} \delta_1^{-z_1 s_1} \cdot ... \cdot \delta_r^{-z_r s_r} \right) \end{aligned} \tag{4.18}$$

onde Z_i está variando ao longo do conjunto $\{0\} \cup R_{p_i^{\beta_i}} \cup N_{p_i^{\beta_i}}$, $0 \leq \beta_i \leq \alpha_i - 1$, $z_i \in Z_i$ e

$1 \leq i \leq r$. Escolha Z_i^* tal que $Z_i^* = \partial Z_i$. Então o coeficiente de $\sigma_{\lambda\left(Z_1^*\times\ldots\times Z_i^*\times\ldots\times Z_r^*\right)}(x)$ é

$$\begin{aligned}\varepsilon_{\lambda\left(Z_1^*\times\ldots\times Z_i^*\times\ldots\times Z_r^*\right)} &= \frac{1}{m}\left(\varepsilon_{z_1^*}^{X_{p_1^{\beta_1}}}\cdot\varepsilon_{z_2^*}^{X_{p_2^{\beta_2}}}\cdot\ldots\cdot\varepsilon_{z_r^*}^{X_{p_r^{\beta_r}}}+\varepsilon_{z_1^*}^{Y_{p_1^{\beta_1}}}\cdot\varepsilon_{z_2^*}^{Y_{p_2^{\beta_2}}}\cdot\ldots\cdot\varepsilon_{z_r^*}^{Y_{p_r^{\beta_r}}}\right)\\ &= \frac{1}{m}\left(\varepsilon_{z_1}^{X_{p_1^{\beta_1}}}\cdot\varepsilon_{z_2}^{X_{p_2^{\beta_2}}}\cdot\ldots\cdot\varepsilon_{z_r}^{X_{p_r^{\beta_r}}}+\varepsilon_{z_1}^{Y_{p_1^{\beta_1}}}\cdot\varepsilon_{z_2}^{Y_{p_2^{\beta_2}}}\cdot\ldots\cdot\varepsilon_{z_r}^{Y_{p_r^{\beta_r}}}\right)\\ &= \varepsilon_{\lambda(Z_1\times\ldots\times Z_i\times\ldots\times Z_r)}.\end{aligned}$$

O termo geral da soma dos λ-produtos é dado por:

$$\frac{1}{m}\left(\sum_{(s_1,\ldots,s_r)\in(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}})}\delta_1^{-z_1s_1}\cdot\ldots\cdot\delta_r^{-z_rs_r}\right)\sigma_{\lambda(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*)}(x), \tag{4.19}$$

onde, de acordo com a Observação 4.1.10, $\lambda(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*)$ é uma classe l-ciclotômica de A.

Afirmação: Para $s=(s_1,\ldots,s_r)$ e $W_{bp_i^{\beta_i}} = \left(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}}\right)$, em (4.19), o coeficiente de $\sigma_{\lambda(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*)}(x)$ pode ser reescrito como

$$\frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}}\delta_1^{-z_1s_1}\cdot\ldots\cdot\delta_r^{-z_rs_r} = \frac{1}{m}\sum_{t\in C_{bp_1^{\beta_1}\ldots.p_r^{\beta_r}}}\delta^{-\lambda(z_1,\ldots,z_r)t}.$$

De fato, como δ_i é uma raiz $p_i^{\alpha_i}$-ésima primitiva da unidade em alguma extensão de $\mathbb{F}_{l^2}$, que contém uma raiz m-ésima primitiva da unidade, de acordo com a Notação (4.1.1), vamos assumir que δ é a raiz m-ésima em questão. Logo

$$1=(\delta)^m=\left(\delta^{\overline{m}_i}\right)^{p_i^{\alpha_i}}.$$

Assim, vamos denotar $\delta_i=\delta^{\overline{m}_i}$, para cada $1\leq i\leq r$. Além disso, de acordo com a hipótese geral (4.1), $mdc(\overline{m}_i,p_i)=1$, para todo $1\leq i\leq r$. Logo definimos naturalmente o isomorfismo

$$\begin{array}{rccc}\psi: & A_i & \longrightarrow & A_i\\ & s_i & \mapsto & s_i\overline{m}_i,\end{array} \tag{4.20}$$

que pode ser estendida para

$$\begin{array}{rccc}\psi^*: & A_1\times A_2\times\ldots\times A_n & \longrightarrow & A_1\times A_2\times\ldots\times A_n\\ & (s_1,\ldots,s_r) & \mapsto & (s_1\overline{m}_1,\ldots,s_r\overline{m}_r)\end{array} \tag{4.21}$$

Então

$$\begin{aligned}
\frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}} \delta_1^{-z_1 s_1}\cdot\ldots\cdot\delta_r^{-z_r s_r} &= \frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}} \delta^{-z_1\overline{m}_1 s_1}\cdot\ldots\cdot\delta^{-z_r\overline{m}_r s_r}\\
&= \frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}} \delta^{\sum_{i=1}^r -z_i\overline{m}_i s_i}\\
&= \frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}} \delta^{\sum_{i=1}^r -z_i\overline{m}_i^2 s_i}\\
&= \frac{1}{m}\sum_{s\in W_{bp_i^{\beta_i}}} \delta^{-\lambda(z_1,\ldots,z_r)\lambda(s_1,\ldots,s_r)}\\
&= \frac{1}{m}\sum_{t\in C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}}} \delta^{-\lambda(z_1,\ldots,z_r)t},
\end{aligned}$$

e assim verificamos a afirmação, ou seja, o termo geral da soma dos λ-produtos (4.19) pode ser reescrito como

$$\frac{1}{m}\left(\varepsilon_{\lambda(z_1\times\ldots\times z_r)}^{C_{bp_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}}}\sigma_{\lambda\left(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*\right)}(x)\right).$$

Desde que $\lambda\left(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*\right)$ cobre todas as classes l-ciclotômicas, logo a soma dos λ-produtos (4.17) é dada por

$$=\frac{1}{m}\left(\sum \varepsilon_{\lambda(z_1\times\ldots\times z_r)}^{\lambda\left(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}}\right)}\sigma_{\lambda\left(Z_1\times\ldots\times Z_r\cup Z_1^*\times\ldots\times Z_r^*\right)}(x)\right)$$

onde o somatório percorre o conjunto de todos os representantes das classes l-ciclotômicas. Como

$$\left(\varepsilon_{\lambda(z_1\times\ldots\times z_r)}^{\lambda\left(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}}\right)}\right)^l = \varepsilon_{\lambda(z_1\times\ldots\times z_r)}^{\lambda\left(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}}\right)}, \tag{4.22}$$

então $\varepsilon_{\lambda(z_1\times\ldots\times z_r)}^{\lambda(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}})}\in\mathbb{F}_l$.

Portanto, pela Definição 4.2.2, $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r}} = \lambda\left(\theta^*_{p_1^{\beta_1}}\otimes\ldots\otimes\theta^*_{p_r^{\beta_r}}\right)+\lambda\left(\theta^{**}_{p_1^{\beta_1}}\otimes\ldots\otimes\theta^{**}_{p_r^{\beta_r}}\right)$ é o idempotente primitivo em $\mathcal{R}_m$, correspondente a classe l-ciclotômica $\lambda\left(X_{p_1^{\beta_1}}\times\ldots\times X_{p_r^{\beta_r}}\cup Y_{p_1^{\beta_1}}\times\ldots\times Y_{p_r^{\beta_r}}\right) = C_{bp_1^{\beta_1}\ldots p_r^{\beta_r}}$. ∎

Corolário 4.2.5. *Se as i-ésimas entradas da primeira parte de*

$$C_1 = \lambda\left(X_1 \times ... \times X_r \cup Y_1 \times ... \times Y_r\right) e$$

$$C_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(X_{p_1^{\beta_1}} \times ... \times X_{p_r^{\beta_r}} \cup Y_{p_1^{\beta_1}} \times ... \times Y_{p_r^{\beta_r}}\right), 0 \leq \beta_i \leq \alpha_i - 1,$$

são N_i *e* $R_{p_i^{\beta_i}}\left(ou\ N_{p_i^{\beta_i}}\right)$, *então* $\theta_{bp_1^{\beta_1}p_2^{\beta_2}\cdot...\cdot p_r^{\beta_r}} = \lambda\left(\theta^*_{p_1^{\beta_1}} \otimes ... \otimes \theta^*_{p_r^{\beta_r}}\right) + \lambda\left(\theta^{**}_{p_1^{\beta_1}} \otimes ... \otimes \theta^{**}_{p_r^{\beta_r}}\right)$ *onde, para* $1 \leq i \leq r$, $\theta^*_{p_i^{\beta_i}}$ *e* $\theta^{**}_{p_i^{\beta_i}}$ *são os idempotentes primitivos correspondentes as classes* l^2*-ciclotômicas* $N_{p_i^{\beta_i}}\left(ou\ R_{p_i^{\beta_i}}\right)$ *e* $R_{p_i^{\beta_i}}\left(ou\ N_{p_i^{\beta_i}}\right)$, *respectivamente.*

Descrevemos nesta seção a demonstração do Teorema 4.2.4 conforme apresentado no artigo [16]. No entanto, pelos exemplos que apresentamos no Capítulo 6, observamos que os coeficientes do termo geral (4.19) podem estar incompletos. A nossa "conjectura", diante dos exemplos que exibimos no Capítulo 6, é que na expressão (4.19), os coeficientes das classes l-ciclotômicas diferentes de C_0 deveriam aparecer divididos por 2, uma vez que

$$\lambda\left(Z_1 \times \ldots \times Z_r \cup Z_1^* \times \ldots \times Z_r^*\right) = \lambda\left(Z_1^* \times \ldots \times Z_r^* \cup Z_1 \times \ldots \times Z_r\right),$$

onde a classe do C_0 possui uma única maneira de ser escrita. No entanto, até o momento não temos evidências suficientes para propor uma nova demonstração.

Capítulo 5

Códigos Abelianos Binários Minimais

Sejam $\mathbb{F}_2$ o corpo finito com 2 elementos e G um grupo finito de ordem ímpar. Um ideal minimal de $\mathbb{F}_2G$ será dito um **código abeliano binário minimal**. Neste capítulo apresentamos as expressões dos idempotentes primitivos geradores dos códigos binários cíclicos de comprimento p^mq^n, pq e $p_1p_2p_3$, onde p, q, p_1, p_2 e p_3 são todos primos ímpares distintos dois a dois. Iniciamos com dois resultados técnicos.

5.1 Resultados Auxiliares

Lema 5.1.1. *Sejam p um número primo positivo e $r, s \in \mathbb{N}^*$. Então*

$$\mathbb{F}_{p^r} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong mdc(r,s) \cdot \mathbb{F}_{p^{mmc(r,s)}}.$$

Demonstração. Seja L um fecho algébrico de $\mathbb{F}_p$ que contém $\mathbb{F}_{p^r}$ e $\mathbb{F}_{p^s}$. Como $\mathbb{F}_{p^r}$ é uma extensão separável de $\mathbb{F}_p$, pelo Teorema do Elemento Primitivo [14, Proposição V.6.15], existe $\alpha \in L$ tal que $\mathbb{F}_{p^r} = \mathbb{F}_p(\alpha)$. Assim, para o polinômio minimal $p(x)$ de α sobre $\mathbb{F}_p$ temos

$$\mathbb{F}_{p^r} \cong \frac{\mathbb{F}_p[x]}{\langle p(x) \rangle}.$$

Logo

$$\mathbb{F}_{p^r} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong \frac{\mathbb{F}_p[x]}{\langle p(x) \rangle} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong \frac{\mathbb{F}_{p^s}[x]}{\langle p(x) \rangle} \cong \bigoplus_{k=1}^{m} \frac{\mathbb{F}_{p^s}[x]}{\langle p_k(x) \rangle},$$

onde $p(x) = \prod_{k=1}^{m} p_k(x)$ é a decomposição de $p(x)$ em polinômios irredutíveis sobre $\mathbb{F}_{p^s}$. Para

$1 \leq k \leq m$, seja α_k uma raiz de $p_k(x)$. Então

$$\mathbb{F}_{p^r} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong \bigoplus_{k=1}^{m} \frac{\mathbb{F}_{p^s}[x]}{\langle p_k(x) \rangle} \cong \bigoplus_{k=1}^{m} \mathbb{F}_{p^s}(\alpha_k).$$

Agora, como $\mathbb{F}_{p^r}$ é uma extensão normal de $\mathbb{F}_p$, então todas as outras raízes de $p(x)$ estão em $\mathbb{F}_{p^r}$. Como α é uma raiz de $p(x)$, temos $\alpha_k \in \mathbb{F}_{p^r}$, para todo $1 \leq k \leq m$. Assim, $\mathbb{F}_{p^s}(\alpha_k) = \mathbb{F}_{p^s}(\mathbb{F}_{p^r}) = \mathbb{F}_{p^s} \cdot \mathbb{F}_{p^r}$, conforme a notação dada em [14, página 233], para todo k. Logo

$$\mathbb{F}_{p^r} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^s} \cong m\,(\mathbb{F}_{p^s} \cdot \mathbb{F}_{p^r}).$$

O menor subcorpo de L que contém $\mathbb{F}_{p^r}$ e $\mathbb{F}_{p^s}$ é o corpo $\mathbb{F}_{p^l}$, onde $l = mmc(r,s)$. Então $(\mathbb{F}_{p^s} \cdot \mathbb{F}_{p^r}) = \mathbb{F}_{p^l}$. Por fim, basta verficarmos que $m = \frac{rs}{mmc(r,s)} = mdc(r,s)$. ∎

Observação 5.1.2. *Qualquer extensão K de grau 2 do corpo primo $\mathbb{F}_2$ é isomorfa a um corpo de decomposição do polinômio $x^2 + x + 1$ sobre $\mathbb{F}_2$. Assim, existe $a \in K \setminus \{0,1\}$ satisfazendo $a^4 = a$. Mais ainda, para qualquer extensão L de $\mathbb{F}_2$ de grau par, existe um subcorpo $K \subset L$, com quatro elementos, que satisfaz a mesma condição acima.*

Lema 5.1.3. *Sejam $r, s \in \mathbb{N}$ elementos não nulos tais que $mdc(r,s) = 2$. Sejam $u \in \mathbb{F}_{2^r}$ e $v \in \mathbb{F}_{2^s}$ elementos que satisfaçam a equação $x^2 + x + 1 = 0$. Então*

$$\mathbb{F}_{2^r} \otimes_{\mathbb{F}_2} \mathbb{F}_{2^s} \cong \mathbb{F}_{2^{\frac{rs}{2}}} \oplus \mathbb{F}_{2^{\frac{rs}{2}}} \tag{5.1}$$

e $e_1 = (u \otimes v) + (u^2 \otimes v^2)$ e $e_2 = (u \otimes v^2) + (u^2 \otimes v)$ são idempotentes primitivos geradores das componentes simples de (5.1).

Demonstração. É fácil ver que os elementos u, $u^2 \in \mathbb{F}_{2^r}^* = \mathbb{F}_{2^r} \setminus \{0\}$, (respectivamente v, $v^2 \in \mathbb{F}_{2^s}^*$) são linearmente independentes sobre $\mathbb{F}_2$. Consequentemente, é simples verificar que os elementos $(u \otimes v), (u^2 \otimes v^2), (u \otimes v^2)$ e $(u^2 \otimes v)$ são linearmente independentes em
$\mathbb{F}_{2^r} \otimes \mathbb{F}_{2^s}$.

Defina $0 \neq e_1 = (u \otimes v) + (u^2 \otimes v^2)$ e $0 \neq e_2 = (u \otimes v^2) + (u^2 \otimes v)$. Verificamos

$$\begin{aligned} e_1 \cdot e_2 &= \left[(u \otimes v) + \left(u^2 \otimes v^2\right)\right] \cdot \left[\left(u \otimes v^2\right) + \left(u^2 \otimes v\right)\right] \\ &= (u \otimes v)\left(u \otimes v^2\right) + (u \otimes v)\left(u^2 \otimes v\right) + \left(u^2 \otimes v^2\right)\left(u \otimes v^2\right) + \left(u^2 \otimes v^2\right)\left(u^2 \otimes v\right) \\ &= \left(u^2 \otimes v^3\right) + \left(u^3 \otimes v^2\right) + \left(u^3 \otimes v^4\right) + \left(u^4 \otimes v^3\right) \\ &= \left(u^2 \otimes 1\right) + \left(1 \otimes v^2\right) + (1 \otimes v) + (u \otimes 1) \\ &= \left(u^2 + u \otimes 1\right) + \left(1 \otimes v + v^2\right). \end{aligned} \tag{5.2}$$

Como por hipótese, u e v são raízes de $f(x) = x^2 + x + 1$, temos $u^2 + u = 1$ e $v^2 + v = 1$, que substituindo em (5.2) nos dá

$$(1 \otimes 1) + (1 \otimes 1) = (2 \otimes 2) = (0 \otimes 0).$$

Também,

$$\begin{aligned} e_1 + e_2 &= \left[(u \otimes v) + \left(u^2 \otimes v^2\right)\right] + \left[\left(u \otimes v^2\right) + \left(u^2 \otimes v\right)\right] \\ &= \left(u + u^2 \otimes v + v^2\right) \\ &= (1 \otimes 1). \end{aligned}$$

Além disso,

$$\begin{aligned} e_1 \cdot e_1 &= \left[(u \otimes v) + \left(u^2 \otimes v^2\right)\right] \cdot \left[(u \otimes v) + \left(u^2 \otimes v^2\right)\right] \\ &= \left(u^2 \otimes v^2\right) + \underbrace{\left(u^3 \otimes v^3\right) + \left(u^3 \otimes v^3\right)}_{u^3=v^3=1} + \left(u^4 \otimes v^4\right) \\ &= \left(u^2 \otimes v^2\right) + (u \otimes v) = e_1. \end{aligned}$$

De forma análoga, verificamos a igualdade $e_2^2 = e_2$.

Por fim, de acordo com o Lema 5.1.1, temos

$$\mathbb{F}_{2^r} \otimes \mathbb{F}_{2^s} \cong 2\mathbb{F}_{2^{\frac{rs}{mdc(r,s)}}} \cong 2\mathbb{F}_{2^{\frac{rs}{2}}} \cong \mathbb{F}_{2^{\frac{rs}{2}}} \oplus \mathbb{F}_{2^{\frac{rs}{2}}}.$$

Como a álgebra $\mathbb{F}_{2^r} \otimes \mathbb{F}_{2^s}$ se decompõe em uma soma direta de dois corpos, ou seja, em duas componentes simples e, além disso, e_1 e e_2 são idempotentes ortogonais cuja a soma é igual $(1 \otimes 1)$, então estes idempotentes também são primitivos. ■

5.2 Códigos Abelianos Minimais Binários

Em [11], foram determinados todos os códigos minimais sob as seguintes hipóteses:

$$\begin{aligned} &G \text{ é um grupo abeliano finito de expoente } p^m \text{ (ou } 2p^m\text{, com } p \text{ ímpar),} \\ &\mathbb{F}_q \text{ é um corpo finito com } q \text{ elementos, onde } q \text{ tem ordem multiplicativa } \varphi(p^m) \ mod\, p^m. \end{aligned} \tag{5.3}$$

Em [6], estas idéias foram aplicadas para grupos da forma $G_p \times G_q$, onde G_p e G_q denotam grupos abelianos, o primeiro um p-grupo e o segundo um q-grupo, que satisfazem as seguintes condições, que, em particular, satisfazem (5.3):

$$\begin{aligned} &mdc(p-1,\, q-1) = 2, \\ &\overline{2} \text{ gera o grupo das unidades de } \mathbb{Z}_{p^2} \text{ e } \mathbb{Z}_{q^2} \\ &mdc(p-1, q) = mdc(p, q-1) = 1. \end{aligned} \tag{5.4}$$

Observação 5.2.1. *Em* (5.4)*, a primeira hipótese nos garante que pelo menos um dos números primos p e q é da forma $4k+3$, onde $k \in \mathbb{N}$.*

5.2.1 Idempotentes Primitivos

Seja G um grupo de ordem ímpar. Para um subgrupo $H \leq G$, definimos $\widehat{H} = \dfrac{1}{|H|}\sum_{h\in H} h$, da mesma forma que (3.3) e, para um elemento $x \in G$, $\widehat{x} = \widehat{\langle x\rangle}$. Ainda, conforme foi definido na página 31, denote por $S_{cc}(G)$ o conjunto dos subgrupos N de G tais que $G/N \neq 1$ é cíclico.

Teorema 5.2.2. *Sejam G_p e G_q p e q-grupos abelianos, respectivamente, satisfazendo as condições em* (5.4)*. Então o conjunto completo de idempotentes ortogonais e primitivos em $\mathbb{F}_2(G_p \times G_q)$ é dado pelos elementos:*

$$\begin{array}{rl} \widehat{G_p}\cdot\widehat{G_q}, & \\ \widehat{G_p}\cdot e_K, & K \in S_{cc}(G_q), \\ e_H\cdot\widehat{G_q}, & H \in S_{cc}(G_p), \\ e_1(H,K),\ e_2(H,K), & H \in S_{cc}(G_p), K \in S(G_q). \end{array}$$

Demonstração. Sejam G_p e G_q grupos abelianos , o primeiro um p-grupo e o segundo um q-grupo e defina $G = G_p \times G_q$. Para cada subgrupo H de G_p tal que $G_p/H \neq 1$ é cíclico, considere o idempotente $e_H = \widehat{H} - \widehat{H^*}$ como na Observação 3.3.2 e, similarmente, considere idempotentes primitivos da forma $e_K = \widehat{K} - \widehat{K^*}$, onde K é um subgrupo co-cíclico de G_q.

Claramente $\widehat{G_p}\cdot\widehat{G_q} = \widehat{G_p \times G_q}$ é um idempotente primitivo. De fato, $\mathbb{F}_2G$ é uma álgebra comutativa, logo $\left(\widehat{G_p \times G_q}\right)^2 = \left(\widehat{G_p}\cdot\widehat{G_q}\right)^2 = \widehat{G_p}^2\cdot\widehat{G_q}^2 = \widehat{G_p}\cdot\widehat{G_q} = \widehat{G_p \times G_q}$. Ainda, $(\mathbb{F}_2G)\,\widehat{G_p \times G_q} \cong \mathbb{F}_2\left(\frac{G_p\times G_q}{G_p\times G_q}\right) \cong \mathbb{F}_2$, de acordo com [22, Proposição 3.6.7]. Logo $\widehat{G_p \times G_q}$ é um idempotente primitivo.

Afirmamos que os idempotentes da forma $\widehat{G_p}\cdot e_K$ são primitivos. De fato, temos $(\mathbb{F}_2G)\,\widehat{G_p}\cdot e_K = \left(\mathbb{F}_2G\cdot\widehat{G_p}\right)e_K \cong (\mathbb{F}_2G_q)\,e_K$ que é um corpo, pelo Teorema 3.3.4. De forma similiar, os idempotentes da forma $e_H\cdot\widehat{G_q}$ são primitivos.

Por fim, desejamos mostrar que um idempotente da forma $e_H\cdot e_K$ decompõe-se como soma de dois idempotentes primitivos em $\mathbb{F}_2G$.

Para verificarmos esta afirmação, tome $a \in H^*\backslash H$ $(b \in K^* \setminus K)$. Observe que aH (bK) é um gerador do grupo cíclico H^*/H (K^*/K), respectivamente. Defina

$$u(a) = \begin{cases} a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & \text{se } p \equiv 1\,(mod\ 4) \text{ ou} \\ 1 + a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}, & \text{se } p \equiv 3\,(mod\ 4) \end{cases} \tag{5.5}$$

e

$$u'(a) = \begin{cases} a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & \text{se } p \equiv 1\,(mod\ 4) \text{ ou} \\ 1 + a^2 + a^{2^3} + \cdots + a^{2^{p-2}}, & \text{se } p \equiv 3\,(mod\ 4) \end{cases} \tag{5.6}$$

Denote $\left(u\widehat{H}\right)^2 = u'\widehat{H}$. Verifiquemos $\left(u'\widehat{H}\right)^2 = u\widehat{H}$ e $\left(u\widehat{H}\right)^2 + u\widehat{H} + e_H = 0$, ou seja, $u\widehat{H}$ satistaz o polinômio $x^2 + x + 1$, onde e_H é identidade em $(\mathbb{F}_2 G_p)\, e_H$. De fato, de acordo com (5.5), $u\widehat{H} = a^{2^0} + a^{2^2} + \cdots + a^{2^{p-3}}$. Assim

$$u'\widehat{H} = \left(u\widehat{H}\right)^2 = a^{2^0 \cdot 2} + a^{2^2 \cdot 2} + \ldots + a^{2^{p-3} \cdot 2},$$

uma vez que $car\,(\mathbb{F}_2) = 2$. Logo

$$\left(u'\widehat{H}\right)^2 = \left(u\widehat{H}\right)^4 = a^{2^1 \cdot 2} + a^{2^3 \cdot 2} + \ldots + a^{2^{p-2} \cdot 2} = a^{2^2} + a^{2^4 \cdot} + \ldots + a^{2^{p-1}}.$$

Por (5.4), $\langle \overline{2} \rangle = U\,(\mathbb{Z}_p)$, ou seja, $2^{\varphi(p)} = 2^{p-1} \equiv 1 (mod\ p)$. Assim

$$\left(u'\widehat{H}\right)^2 = \left(u\widehat{H}\right)^4 = a^{2^2} + a^{2^4 \cdot} + \cdots + a^{2^0} = u\widehat{H}.$$

Por fim,

$$\left(u\widehat{H}\right)^2 + u\widehat{H} + e_H = \left(a^{2^0} + a^{2^1} + \cdots + a^{2^{p-3}} + a^{2^{p-2}}\right)\widehat{H} + e_H \tag{5.7}$$

Como aH gera H^*/H, logo $\left(\sum_{i \in \{0,\ldots,p-2\}} a^{2^i}\widehat{H}\right) + \widehat{H} = \widehat{H^*} \Rightarrow \sum_{i \in \{0,\ldots,p-2\}} a^{2^i}\widehat{H} = \widehat{H^*} - \widehat{H}$.
Como definido anteriormente, $e_H = \widehat{H} - \widehat{H^*}$, ou seja, $\widehat{H^*} - \widehat{H} = -e_H$. Substituindo em (5.7), obtemos

$$\left(u\widehat{H}\right)^2 + u\widehat{H} + e_H = -e_H + e_H = 0$$

É fácil verificarmos

$$u\widehat{H}\left(\widehat{H} - \widehat{H^*}\right) = u\widehat{H} - u\widehat{H^*} = u\widehat{H} - \varepsilon(u)\widehat{H^*},$$

onde $\varepsilon(u)$ é o número de somandos $\widehat{H^*}$ em u, o qual é sempre par. Assim

$$u\widehat{H}\left(\widehat{H} - \widehat{H^*}\right) = u\widehat{H}.$$

Da mesma forma, $u'\widehat{H}\left(\widehat{H} - \widehat{H^*}\right) = \left(u\widehat{H}\right)\left[\left(u\widehat{H}\right)\left(\widehat{H} - \widehat{H^*}\right)\right] = u\widehat{H}u\widehat{H} = u'\widehat{H}$.
Logo, concluímos que $u\widehat{H}$ e $u'\widehat{H} \in \mathbb{F}_2 G_p\left(\widehat{H} - \widehat{H^*}\right)$.

Analogamente, $v\widehat{K}$ e $v'\widehat{K} \in \mathbb{F}_2 G_q\left(\widehat{K} - \widehat{K^*}\right)$.

Em [11, página 390], se $[G : H] = p^r$, então a dimensão do ideal gerado por um idempotente da forma e_H é

$$dim_{\mathbb{F}}(\mathbb{F}G)e_H \;=\; dim_{\mathbb{F}}\mathbb{F}[G/H] - dim_{\mathbb{F}}\mathbb{F}[G/H^*] = p^{r-1}(p-1). \tag{5.8}$$

De acordo com (5.8), temos $dim_{\mathbb{F}}(\mathbb{F}_2G_p)e_H = p^{r-1}(p-1)$ e $dim_{\mathbb{F}}(\mathbb{F}_2G_q)e_K = q^{s-1}(q-1)$, onde $p^r = [G_p : H]$ e $q^s = [G_q : K]$. Assim

$$(\mathbb{F}_2G_p)\, e_H \cong \mathbb{F}_{2^{p^{r-1}(p-1)}} = \mathbb{F}_{2^{\varphi(p^r)}} \quad \text{e} \quad (\mathbb{F}_2G_q)\, e_K \cong \mathbb{F}_{2^{q^{s-1}(q-1)}} = \mathbb{F}_{2^{\varphi(q^s)}}.$$

Como $mdc\left(\varphi\left(p^r\right), \varphi\left(q^s\right)\right) = mdc\left(p^r(p-1), q^s(q-1)\right) = 2$, conforme (5.4), então as hipóteses do Lema 5.1.3 são satisfeitas, ou seja,

$$\mathbb{F}_2\left(G_p \times G_q\right) e_H e_K \cong \left(\mathbb{F}_2G_p\right) e_H \otimes \left(\mathbb{F}_2G_q\right) e_K \cong \mathbb{F}_{2^{\varphi(p^r)}} \otimes \mathbb{F}_{2^{\varphi(q^s)}} \cong 2\mathbb{F}_{2^{\frac{\varphi(p^r)\varphi(q^s)}{2}}},$$

onde

$$\begin{aligned} e_1 = e_1(H,K) &= u\widehat{H}\cdot v\widehat{K} \;+\; u'\widehat{H}\cdot v'\widehat{K} \\ e_2 = e_2(H,K) &= u\widehat{H}\cdot v'\widehat{K} \;+\; u'\widehat{H}\cdot v\widehat{K} \end{aligned}$$

são idempotentes ortogonais primitivos tais que $e_1 + e_2 = e_H e_K$. ∎

5.2.2 Códigos em $\mathbb{F}_2\left(\mathcal{C}_p \times \mathcal{C}_q\right)$

Sejam $p \neq q$ primos ímpares. Consideremos o grupo $G = \langle g \,/\, g^{pq} = 1\rangle$ e vamos denotar $a = g^q$, $b = g^p$ e $G = \mathcal{C}_p \times \mathcal{C}_q$, onde $\mathcal{C}_p = \langle a\rangle$ e $\mathcal{C}_q = \langle b\rangle$. Como caso particular do Teorema 5.2.2, nesta seção vamos descrever todos os idempotentes primitivos de $\mathbb{F}_2\left(\mathcal{C}_p \times \mathcal{C}_q\right)$ e as classes 2-ciclotômicas de G.

Teorema 5.2.3. *Seja $G = \langle a\rangle \times \langle b\rangle$ como acima e assuma que p e q satisfazem* (5.4). *Então os idempotentes primitivos de $\mathbb{F}_2G$ são*

$$e_0 = \widehat{G}, \quad e_1 = \widehat{a}\left(1 - \widehat{b}\right), \quad e_2 \,=\, (1-\widehat{a})\,\widehat{b}, \quad e_3 \,=\, uv + u^2v^2 \;\; e \;\; e_4 \,=\, uv^2 + u^2v,$$

onde $u = u(a)$ e $v = v(b)$ são como em (5.5).

Demonstração. É simples verificar que

$$\begin{aligned}
\mathbb{F}_2\left(\langle a\rangle \times \langle b\rangle\right) &\cong \left(\mathbb{F}_2G\right)\langle a\rangle \otimes \left(\mathbb{F}_2G\right)\langle b\rangle \\
&\cong \left[\left(\mathbb{F}_2G\right)\widehat{a} \oplus \left(\mathbb{F}_2G\right)(1-\widehat{a})\right] \otimes \left[\left(\mathbb{F}_2G\right)\widehat{b} \oplus \left(\mathbb{F}_2G\right)\left(1-\widehat{b}\right)\right] \\
&\cong \left[\left(\mathbb{F}_2G\right)\widehat{a} \otimes \left(\mathbb{F}_2G\right)\widehat{b}\right] \oplus \left[\left(\mathbb{F}_2G\right)\widehat{a} \otimes \left(\mathbb{F}_2G\right)\left(1-\widehat{b}\right)\right] \qquad (5.9) \\
&\oplus \left[\left(\mathbb{F}_2G\right)(1-\widehat{a}) \otimes \left(\mathbb{F}_2G\right)\widehat{b}\right] \oplus \left[\left(\mathbb{F}_2G\right)(1-\widehat{a}) \otimes \left(\mathbb{F}_2G\right)\left(1-\widehat{b}\right)\right] \\
&\cong \left(\mathbb{F}_2G\right)\widehat{ab} \oplus \left(\mathbb{F}_2G\right)\widehat{a}\left(1-\widehat{b}\right) \oplus \left(\mathbb{F}_2G\right)(1-\widehat{a})\,\widehat{b} \oplus \left(\mathbb{F}_2G\right)(1-\widehat{a})\left(1-\widehat{b}\right)
\end{aligned}$$

Como $(1-\widehat{a})$ e $\left(1-\widehat{b}\right)$ não são idempotentes principais em $\mathbb{F}_2\langle a\rangle$ e $\mathbb{F}_2\langle b\rangle$, respectivamente, de acordo com Teorema 5.2.2, o produto $(1-\widehat{a})\left(1-\widehat{b}\right)$ decompõe-se em $e_3 = uv + u^2v^2$ e $e_4 = uv^2 + u^2v$, onde $(1-\widehat{a})\left(1-\widehat{b}\right) = e_3 + e_4$. Assim, substituindo em (5.9), obtemos

$$\mathbb{F}\left(\langle a\rangle \times \langle b\rangle\right) \cong \left(\mathbb{F}_2G\right)\widehat{ab} \oplus \left(\mathbb{F}_2G\right)\widehat{a}\left(1-\widehat{b}\right) \oplus \left(\mathbb{F}_2G\right)(1-\widehat{a})\,\widehat{b} \oplus \left(\mathbb{F}_2G\right)e_3 \oplus \left(\mathbb{F}_2G\right)e_4.$$

■

Agora vamos descrever as classes 2-ciclotômicas de G. Aqui utilizaremos a relação definida em (3.2). Para cada $0 \leq i \leq pq-1$, escrevemos

$$g^i = g^{(i_1,i_2)},\ \text{onde } i_1 \equiv i\,(mod\ p) \text{ e } i_2 \equiv i\,(mod\ q), \qquad (5.10)$$

e, dados conjuntos $X \subset \mathbb{Z}_p$ e $Y \subset \mathbb{Z}_q$, escrevemos $g^j \in (X,Y)$ para indicar $g^j = g^{(j_1,j_2)}$, com $(j_1,j_2) \in (X,Y)$.

Para um primo $p > 0$, nesta seção, escrevemos Q^p para o conjunto dos resíduos quadráticos módulo p, N^p para o conjuntos dos resíduos não quadráticos módulo p.

Lema 5.2.4. *Seja G um grupo abeliano de ordem pq como no Teorema 5.2.3. Então as classes 2-ciclotômicas de G são:*

$$\begin{aligned}
C_1 &= \{1\} \\
C_g &= \left\{g, g^2, g^{2^2}, \ldots, g^{2^{\frac{(p-1)(q-1)}{2}-1}}\right\} \\
&= \left\{g^{(i,j)} \,/\, (i,j) \in (Q^p,Q^q) \cup (N^p,N^q)\right\} \\
C_a &= C_{g^q} = \left\{g^q, g^{2q}, g^{2^2q}, g^{2^3q}, \ldots, g^{2^{p-2}q}\right\} \\
&= \left\{g^{(i,j)} \,/\, (i,j) \in (Q^p,0) \cup (N^p,0)\right\} \\
C_b &= C_{g^p} = \left\{g^p, g^{2p}, g^{2^2p}, g^{2^3p}, \ldots, g^{2^{q-2}p}\right\} \\
&= \left\{g^{(i,j)} \,/\, (i,j) \in (0,Q^q) \cup (0,N^q)\right\}
\end{aligned}$$

onde

$$\begin{aligned}(a)\ C_{g^{p+q}} &= \left\{ g^{p+q}, g^{2(p+q)}, g^{2^2(p+q)}, \ldots, g^{\left(2^{\frac{(p-1)(q-1)}{2}-1}\right)(p+q)} \right\} \\ &= \left\{ g^{(i,j)} \ / \ (i,j) \in (Q^p, N^q) \cup (N^p, Q^q) \right\},\end{aligned}$$

se $p \equiv 3 \ (mod\, 4)$ *e* $q \equiv 3 \ (mod\, 4)$ *ou*

$$\begin{aligned}(b)\ C_{g^{-1}} &= \left\{ g^{-1}, g^{-2}, g^{-2^2}, \ldots, g^{-\left(2^{\frac{(p-1)(q-1)}{2}-1}\right)} \right\} \\ &= \left\{ g^{(i,j)} \ / \ (i,j) \in (Q^p, N^q) \cup (N^p, Q^q) \right\},\end{aligned}$$

se $p \equiv 1 \ (mod\, 4)$ *e* $q \equiv 3 \ (mod\, 4)$.

Demonstração. Desde $\bar{2}$ gera $U(\mathbb{Z}_p)$ e $U(\mathbb{Z}_q)$, o menor inteiro positivo i tal que $(g^q)^{2^i} = g^q$ é $p-1$ e, similarmente, o menor inteiro positivo j tal que $(g^p)^{2^j} = g^p$ é $q-1$. Assim $|C_a| = p-1$ e $|C_b| = q-1$. Pelo Teorema 4.1.5, temos $|C_g| = \dfrac{(p-1)(q-1)}{2}$.

Usando a notação (5.10), podemos escrever

$$C_g = \left\{ g^{(i,j)} \ / \ i \equiv 2^k \, (mod\ p),\ j \equiv 2^k \, (mod\ q), 0 \leq k \leq |C_g| - 1 \right\}.$$

De acordo com a Observação 1.1.7 e a Hipótese (5.4), $\overline{2} \in N^p\,(N^q)$, ou seja, $(2,2) \in (N^p, N^q)$. Assim, afirmamos que todos os elementos em C_g são da forma $g^{2^i} = g^{(i_1,i_2)}$, com (i_1, i_2) percorrendo todo o conjunto $(Q^p, Q^q) \cup (N^p, N^q)$. De fato, como $(2,2) \in (N^p, N^q)$, da Definição 1.1.2 e do Teorema 1.1.3, $(2^i, 2^j) \in (N^p, N^q)$ se, e somente se, i e j são ímpares. Além disso, conforme [17, Teorema 79], temos

$$|(Q^p, Q^q) \cup (N^p, N^q)| = \frac{(p-1)}{2}\frac{(q-1)}{2} + \frac{(p-1)}{2}\frac{(q-1)}{2} = \frac{(p-1)(q-1)}{2} = |C_g|.$$

Observemos que $C_{g^q} \subset \left\{ g^{\left(2^i q, 0\right)} \ / \ i \in \mathbb{N} \right\}$. Como $\bar{2}$ gera $U\,(\mathbb{Z}_p)$ e q é invertível $mod\, p$, podemos escrever

$$C_{g^q} = \left\{ g^{\left(2^i q, 0\right)} \ / \ \left(2^i q, 0\right) \in (Q^p, 0) \cup (N^p, 0) \right\}.$$

Similarmente,

$$C_{g^p} = \left\{ g^{\left(0, 2^i p\right)} / \left(0, 2^i p\right) \in (0, Q^q) \cup (0, N^q) \right\}.$$

Para determinar a última classe 2-ciclotômica, vamos considerar dois casos.

Caso 1: $p \equiv 3\,(mod\,4)$ e $q \equiv 3\,(mod\,4)$. Pelo Teorema 1.1.4, temos $p \in Q^q$ se, e somente se, $q \in N^p$. Assim o elemento $g^{p+q} = g^{(q,p)} \in (N^p, Q^q) \cup (Q^p, N^q)$ e $g^{p+q} \notin C_g$. Observe $1 \neq g^{p+q} \notin C_{g^p} \cup C_{g^q}$. Consequentemente, neste caso, a quinta classe 2-ciclotômica é:

$$C_{g^{p+q}} = \left\{ g^{p+q}, g^{2(p+q)}, g^{2^2(p+q)}, \ldots, g^{\left(2^{\frac{(p-1)(q-1)}{2}-1}\right)(p+q)} \right\}.$$

Caso 2: $p \equiv 1\,(mod\,4)$ e $q \equiv 3\,(mod\,4)$. Pelo Lema 1.1.8, temos $-1 \in Q^p$ e $-1 \in N^q$. Então $g^{-1} = g^{(-1,-1)} \in (Q^p, N^q)$ e $g^{-1} \notin C_g$. Considerando a ordem dos elementos em C_a e C_b, temos $1 \neq g^{-1} \notin C_{g^p} \cup C_{g^q}$.

Portanto, podemos descrever a quinta classe 2-ciclotômica como:

$$C_{g^{-1}} = \left\{ g^{-1}, g^{-2}, g^{-2^2}, \ldots, g^{-\left(2^{\frac{(p-1)(q-1)}{2}-1}\right)} \right\}.$$

■

Observação 5.2.5. *Para um elemento $x \in G$, escreveremos $\mathcal{S}_x = \sum_{h \in \mathcal{C}_x} h$, para denotar a soma de todos os elementos na classe 2-ciclotômica de x em G. Logo podemos escrever:*

Para o **Caso 1**:

$$e_3 = \mathcal{S}_g + \mathcal{S}_{g^p} + \mathcal{S}_{g^q} \quad \text{e} \quad e_4 = \mathcal{S}_{g^{p+q}} + \mathcal{S}_{g^p} + \mathcal{S}_{g^q}. \tag{5.11}$$

Para **Caso 2**:

$$e_3 = \mathcal{S}_g + \mathcal{S}_{g^q} \quad \text{e} \quad e_4 = \mathcal{S}_{g^{-1}} + \mathcal{S}_{g^q}. \tag{5.12}$$

Vamos verificar a igualdade e_3 para o **Caso 1**. Para o **Caso 2** o racíocinio é análogo. De acordo com o Teorema 5.2.3 temos

$$e_3 = uv + u^2v^2, \text{ com } u \text{ e } v \text{ definidos em (5.5) e (5.6) respectivamente.}$$

Na introdução desta seção, definimos $a = g^q$ e $b = g^p$. Assim

$$\begin{aligned} uv &= \left(1 + g^{2p} + g^{2^3p} + \cdots + g^{2^{q-2}p}\right) + \left(g^{2^0q} + g^{2^0q}g^{2p} + \cdots + g^{2^0q}g^{2^{q-2}p}\right) + \cdots + \\ &+ \left(g^{2^{p-3}q} + g^{2^{p-3}q}g^{2p} + \cdots g^{2^{p-3}q}g^{2^{q-2}p}\right). \\ u^2v^2 &= \left(1 + g^{2^0p} + g^{2^2p} + \cdots + g^{2^{q-3}p}\right) + \left(g^{2^1q} + g^{2^1q}g^{2^0p} + \cdots + g^{2^1q}g^{2^{q-3}p}\right) + \cdots + \\ &+ \left(g^{2^{p-2}q} + g^{2^{p-2}q}g^{2^0p} + \cdots g^{2^{p-2}q}g^{2^{q-3}p}\right). \end{aligned}$$

Logo

$$uv + u^2v^2 = \underbrace{g^{2^0p} + g^{2^1p} + g^{2^2p} + \cdots + g^{2^{q-2}p}}_{\mathcal{S}_{g^p}} + \underbrace{g^{2^0q} + g^{2^1q} + g^{2^2q} + \cdots + g^{2^{p-2}q}}_{\mathcal{S}_{g^q}} +$$

$$+g^{2^0q}g^{2^1p}+\cdots+g^{2^0q}g^{2^{q-2}p}+g^{2^1q}g^{2^0p}+\cdots g^{2^1q}g^{2^{q-3}p}+\cdots g^{2^{p-2}q}g^{2^0p}+\cdots+g^{2^{p-2}q}g^{2^{q-3}p} \quad (5.13)$$

Dado um elemento arbitrário na última linha, verificamos que ele pode ser reescrito como

$$g^{2^iq}g^{2^jp} = g^{2^iq+2^jp}, \text{ com } 0 \leq i \leq p-2 \text{ e } 1 \leq j \leq q-3.$$

Observamos, neste caso, que se i é um número par, então j é um número ímpar. Assim, utilizando a notação (5.10), temos

$$g^{2^iq+2^jp} = g^{\left(2^iq, 2^jp\right)}, \text{ onde } 2^iq \equiv 2^iq + 2^jp \,(mod\ p) \text{ e } 2^jp \equiv 2^iq + 2^jp \,(mod\ q).$$

No **Caso 1**, pelo Teorema 1.1.4 e do fato de que $\overline{2} \in N^p$ e $\overline{2} \in N^q$, logo

$$\begin{array}{rcl} i \text{ é par e } j \text{ é ímpar} & \Rightarrow & \left(2^ip, 2^jq\right) \in (Q_p, Q_q) \\ i \text{ é ímpar e } j \text{ é par} & \Rightarrow & \left(2^ip, 2^jq\right) \in (N_p, N_q) \end{array}$$

Por fim, existem $\dfrac{(p-1)(q-1)}{2} = |C_g|$ elementos em (5.13). De fato, o expoente j ora percorre os números pares entre 0 e $q-3$, ora percorre os números ímpares entre 1 e $q-2$. O mesmo ocorre para $0 \leq i \leq p-2$. Assim existem $\dfrac{(p-1)(q-1)}{2} = |C_g|$ elementos. Logo, concluímos

$$g^{2^0q}g^{2^1p} + \cdots + g^{2^0q}g^{2^{q-2}p} + g^{2^1q}g^{2^0p} + \cdots g^{2^1q}g^{2^{q-3}p} + \cdots g^{2^{p-2}q}g^{2^0p} + \cdots + g^{2^{p-2}q}g^{2^{q-3}p} = \mathcal{S}_g$$

e, portanto,

$$e_3 = uv + u^2v^2 = \mathcal{S}_g + \mathcal{S}_{g^p} + \mathcal{S}_{g^q}.$$

O Teorema 5.2.2 nos permite explicitar os idempotentes primitivos para os casos $\mathcal{C}_{p^m} \times \mathcal{C}_{q^n}$, $m \geq 2$ e $n \geq 2$. Além disso, utilizando técnicas similares, podemos também considerar os idempotentes primitivos quando o grupo é do tipo $\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}$, onde p_1, p_2 e p_3 são primos ímpares distintos.

5.2.3 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p^m} \times \mathcal{C}_{q^n}\right)$, para $m \geq 2, n \geq 2$

Teorema 5.2.6. *Sejam p e q números primos que satisfazem (5.4) e $G = \langle a \rangle \times \langle b \rangle$, com $\langle a \rangle = \mathcal{C}_{p^m}$ e $\langle b \rangle = \mathcal{C}_{q^n}$. Então os códigos minimais de $\mathbb{F}_2 G$ são gerados pelos seguintes idempotentes primitivos*

$$e_0 = \widehat{a}\widehat{b},\ \ e_{0j} = \widehat{a}\left(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}}\right),\ \ e_{i0} = \left(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}}\right)\widehat{b},\ \ e_{ij}^{*} = uv + u^2v^2 \ \text{ e } \ e_{ij}^{**} = uv^2 + u^2v,$$

onde

$$\begin{aligned} u &= \widehat{a^{p^i}}\left(a^{2^0 p^{i-1}} + a^{2^2 p^{i-1}} + \cdots + a^{2^{p-3} p^{i-1}}\right),\ \textit{se } p \equiv 1\,(\textit{mod } 4)\ \textit{ ou} \\ u &= \widehat{a^{p^i}}\left(1 + a^{2^0 p^{i-1}} + a^{2^2 p^{i-1}} + \cdots + a^{2^{p-3} p^{i-1}}\right),\ \textit{se } p \equiv 3\,(\textit{mod } 4) \end{aligned}$$

e

$$\begin{aligned} v &= \widehat{b^{q^j}}\left(b^{2^0 q^{j-1}} + b^{2^2 q^{j-1}} + \cdots + b^{2^{q-3} q^{j-1}}\right),\ \textit{se } q \equiv 1\,(\textit{mod } 4)\ \textit{ ou} \\ v &= \widehat{b^{q^j}}\left(1 + b^{2^0 q^{j-1}} + b^{2^2 q^{j-1}} + \cdots + b^{2^{q-3} q^{j-1}}\right),\ \textit{se } q \equiv 3\,(\textit{mod } 4) \end{aligned}$$

Demonstração. Pelo Lema 5.1.1 e o Teorema 3.2.3, obtemos

$$\begin{aligned} \mathbb{F}_2\mathcal{C}_{p^m} &= \mathbb{F}_2\mathcal{C}_{p^m} \cdot \widehat{a} \oplus \bigoplus_{i=1}^{m} \mathbb{F}_2\mathcal{C}_{p^m} \cdot \left(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}}\right) \cong \mathbb{F}_2 \oplus \bigoplus_{i=1}^{m} \mathbb{F}_{2^{(p^i - p^{i-1})}}, \\ \mathbb{F}_2\mathcal{C}_{q^n} &= \mathbb{F}_2\mathcal{C}_{q^n} \cdot \widehat{b} \oplus \bigoplus_{j=1}^{n} \mathbb{F}_2\mathcal{C}_{q^n} \cdot \left(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}}\right) \cong \mathbb{F}_2 \oplus \bigoplus_{j=1}^{n} \mathbb{F}_{2^{(q^j - q^{j-1})}}. \end{aligned}$$

onde $\mathbb{F}_2\mathcal{C}_{p^m}\left(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}}\right) \cong \mathbb{F}_{2^{(p^i - p^{i-1})}}$ e $\mathbb{F}_2\mathcal{C}_{q^n}\left(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}}\right) \cong \mathbb{F}_{2^{(q^j - q^{j-1})}}$, conforme (5.8).

O ideal $I_0 = \langle e_0 \rangle = \left\langle \hat{a}\hat{b} \right\rangle$ é minimal, pois é gerado pelo idempotente primitivo principal. Os ideais $I_{i0} = \langle e_{i0} \rangle$ e $I_{0j} = \langle e_{0j} \rangle$ também são minimais de acordo com o Teorema 5.2.2.

Para cada par i, j, o idempotente $e_{ij} = \left(\widehat{a^{p^i}} + \widehat{a^{p^{i-1}}}\right) \cdot \left(\widehat{b^{q^j}} + \widehat{b^{q^{j-1}}}\right)$ não é primitivo conforme o Teorema 5.2.2 e decompõe-se como soma de dois idempotentes primitivos, ou seja, $e_{ij}^{*} = uv + u^2v^2$ e $e_{ij}^{**} = uv^2 + u^2v$, onde u e v são definidos como afirmado no Teorema 5.2.2. Logo os ideais $I_{ij}^{*} = \langle uv + u^2v^2 \rangle$ e $I_{ij}^{**} = \langle u^2v + uv^2 \rangle$ são minimais tais

que $I_{ij}^{*} \oplus I_{ij}^{**} = \langle e_{ij} \rangle$. Portanto

$$\begin{aligned}
\mathbb{F}_2\left(\mathcal{C}_{p^m} \times \mathcal{C}_{q^n}\right) &= \mathbb{F}_2\mathcal{C}_{p^m} \otimes_{\mathbb{F}_2} \mathbb{F}_2\mathcal{C}_{q^n} \\
&\cong \left(\mathbb{F}_2 \oplus \bigoplus_{i=1}^{m} \mathbb{F}_{2^{(p^i-p^{i-1})}}\right) \otimes_{\mathbb{F}_2} \left(\mathbb{F}_2 \oplus \bigoplus_{j=1}^{n} \mathbb{F}_{2^{(q^j-q^{j-1})}}\right) \\
&= \mathbb{F}_2 \oplus \bigoplus_{i=1}^{m} \mathbb{F}_{2^{(p^i-p^{i-1})}} \oplus \bigoplus_{j=1}^{n} \mathbb{F}_{2^{(q^j-q^{j-1})}} \oplus 2 \cdot \bigoplus_{i,j} \mathbb{F}_{2^{\frac{(p^i-p^{i-1})(q^j-q^{j-1})}{2}}}.
\end{aligned}$$

■

5.2.4 Códigos em $\mathbb{F}_2\left(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}\right)$

Os métodos das seções anteriores podem ser estendidos para o caso geral, mas os cálculos tornam-se muito mais complexos. Como uma ilustração, mostramos abaixo como obter os idempotentes primitivos quando $|G|$ envolve três primos distintos.

Teorema 5.2.7. *Sejam p_1, p_2 e p_3 três primos ímpares distintos tais que $mdc\left(p_i - 1,\, p_j - 1\right) = 2$, para $1 \leq i \neq j \leq 3$, e $\overline{2}$ um gerador do grupo $U\left(\mathbb{Z}_{p_i}\right)$. Então os idempotentes primitivos da álgebra de grupo $\mathbb{F}_2G$, para $G = \mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}$, com $\mathcal{C}_{p_1} = \langle a \rangle$, $\mathcal{C}_{p_2} = \langle b \rangle$ e $\mathcal{C}_{p_3} = \langle c \rangle$, são*

$$\begin{aligned}
e_0 &= \hat{a}\hat{b}\hat{c} & e_1 &= \hat{a}\hat{b}\left(1-\hat{c}\right) \\
e_2 &= \hat{a}\left(1-\hat{b}\right)\hat{c} & e_3 &= \left(1-\hat{a}\right)\hat{b}\hat{c} \\
e_4 &= \left(uv + u^2v^2\right)\hat{c} & e_5 &= \left(u^2v + uv^2\right)\hat{c} \\
e_6 &= \left(uw + u^2w^2\right)\hat{b} & e_7 &= \left(u^2w + uw^2\right)\hat{b} \\
e_8 &= \left(vw + v^2w^2\right)\hat{a} & e_9 &= \left(v^2w + vw^2\right)\hat{a} \\
e_{10} &= \left(1-\hat{a}\right)\left(1-\hat{b}\right)\left(1-\hat{c}\right) & e_{11} &= \left(1-\hat{a}\right)\left(1-\hat{b}\right)\left(1-\hat{c}\right) \\
&\quad + u^2v^2w + uvw^2 & &\quad + u^2v^2w^2 + uvw \\
e_{12} &= \left(1-\hat{a}\right)\left(1-\hat{b}\right)\left(1-\hat{c}\right) & e_{13} &= \left(1-\hat{a}\right)\left(1-\hat{b}\right)\left(1-\hat{c}\right) \\
&\quad + u^2vw^2 + uv^2w^2 & &\quad + uv^2w + u^2vw^2
\end{aligned}$$

onde $u = u(a), v = v(b)$ e $w = w(c)$ são definidos como em (5.5), respectivamente

Demonstração. De acordo com o Teorema 4.1.11, existem 14 classes 2-ciclotômicas, ou seja, existem 14 componentes simples em $\mathbb{F}_2G$.

Pelos Teoremas 5.2.3 e 3.2.3, para cada $i = 1, 2, 3$, $\mathbb{F}_2\mathcal{C}_{p_i}$ contém dois idempotentes primitivos, a saber, $\widehat{\mathcal{C}_{p_i}}$ e $1 - \widehat{\mathcal{C}_{p_i}}$. Logo

$$\mathbb{F}_2\mathcal{C}_{p_1} \cong \left(\mathbb{F}_2\mathcal{C}_{p_1}\right) \cdot \widehat{a} \,\oplus\, \left(\mathbb{F}_2\mathcal{C}_{p_1}\right) \cdot \left(1 - \widehat{a}\right) \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^{p_1-1}}.$$

$$\mathbb{F}_2\mathcal{C}_{p_2} \cong (\mathbb{F}_2\mathcal{C}_{p_2}) \cdot \widehat{b} \oplus (\mathbb{F}_2\mathcal{C}_{p_2}) \cdot \left(1 - \widehat{b}\right) \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^{p_2-1}}.$$
$$\mathbb{F}_2\mathcal{C}_{p_3} \cong (\mathbb{F}_2\mathcal{C}_{p_3}) \cdot \widehat{c} \oplus (\mathbb{F}_2\mathcal{C}_{p_3}) \cdot (1 - \widehat{c}) \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^{p_3-1}}.$$

De acordo com o Teorema 5.2.2, os idempotentes de $\mathbb{F}_2G$ são dados por

$$\begin{array}{ll} E_0 = \hat{a}\ \hat{b}\ \hat{c} & E_1 = (1-\hat{a})\ \hat{b}\ \hat{c} \\ E_2 = \hat{a}\ \left(1-\hat{b}\right)\ \hat{c} & E_3 = \hat{a}\ \hat{b}\ (1-\hat{c}) \\ E_4 = (1-\hat{a})\ \left(1-\hat{b}\right)\ \hat{c} & E_5 = \hat{a}\ \left(1-\hat{b}\right)\ (1-\hat{c}) \\ E_6 = (1-\hat{a})\ \hat{b}\ (1-\hat{c}) & E_7 = (1-\hat{a})\ \left(1-\hat{b}\right)\ (1-\hat{c}) \end{array} \tag{5.14}$$

Observe que

$$\begin{aligned} \sum_{i=0}^{7} E_i &= \hat{a}\hat{b}\hat{c} + (1-\hat{a})\,\hat{b}\hat{c} + \hat{a}\left(1-\hat{b}\right)\hat{c} + \hat{a}\hat{b}\,(1-\hat{c}) + (1-\hat{a})\left(1-\hat{b}\right)\hat{c} \\ &+ \hat{a}\left(1-\hat{b}\right)(1-\hat{c}) + (1-\hat{a})\,\hat{b}\,(1-\hat{c}) + (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c}) \\ &= 8\hat{a}\hat{b}\hat{c} + 4\hat{a}\hat{c} + 4\hat{b}\hat{c} + 4\hat{a}\hat{b} + 2\hat{a} + 2\hat{b} + 2\hat{c} + 1 \\ &= 1. \end{aligned}$$

Além disso, os ideais $\mathbb{F}_2G \cdot \hat{a}\hat{b}\hat{c}$, $\mathbb{F}_2G \cdot (1-\hat{a})\,\hat{b}\hat{c}$, $\mathbb{F}_2G \cdot \hat{a}\left(1-\hat{b}\right)\hat{c}$ e $\mathbb{F}_2G \cdot \hat{a}\hat{b}\,(1-\hat{c})$ são minimais. De fato,

$$\begin{aligned} \mathbb{F}_2G \cdot \hat{a}\hat{b}\hat{c} &= \mathbb{F}_2G \cdot \widehat{G} \ \cong\ \mathbb{F}_2 \\ \mathbb{F}_2G \cdot (1-\hat{a})\,\hat{b}\hat{c} &\cong \mathbb{F}_2G \cdot \left(1 - \widehat{\mathcal{C}_{p_1}}\right)\widehat{\mathcal{C}_{p_2}}\widehat{\mathcal{C}_{p_3}} \cong \mathbb{F}_2\mathcal{C}_{p_1} \cdot \left(1 - \widehat{\mathcal{C}_{p_1}}\right) \ \cong\ \mathbb{F}_{2^{p_1-1}} \\ \mathbb{F}_2G \cdot \hat{a}\left(1-\hat{b}\right)\hat{c} &\cong \mathbb{F}_2G \cdot \widehat{\mathcal{C}_{p_1}}\left(1 - \widehat{\mathcal{C}_{p_2}}\right)\widehat{\mathcal{C}_{p_3}} \cong \mathbb{F}_2\mathcal{C}_{p_2} \cdot \left(1 - \widehat{\mathcal{C}_{p_2}}\right) \ \cong\ \mathbb{F}_{2^{p_2-1}} \\ \mathbb{F}_2G \cdot \hat{a}\hat{b}\,(1-\hat{c}) &\cong \mathbb{F}_2G \cdot \widehat{\mathcal{C}_{p_1}}\widehat{\mathcal{C}_{p_2}}\left(1 - \widehat{\mathcal{C}_{p_3}}\right) \cong\ \mathbb{F}_2\mathcal{C}_{p_3} \cdot \left(1 - \widehat{\mathcal{C}_{p_3}}\right) \ \cong\ \mathbb{F}_{2^{p_3-1}}. \end{aligned}$$

No que segue, vamos omitir o índice $\mathbb{F}_2$ do produto tensorial. De acordo com o

Teorema 1.2.3, obtemos

$$\begin{aligned}
\mathbb{F}_2G &\cong \mathbb{F}_2\mathcal{C}_{p_1} \otimes \mathbb{F}_2\mathcal{C}_{p_2} \otimes \mathbb{F}_2\mathcal{C}_{p_3} \\
&\cong (\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \oplus \mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a})) \otimes \left(\mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \oplus \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right)\right) \otimes (\mathbb{F}_2\mathcal{C}_{p_3}\hat{c} \oplus \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c})) \\
&\cong \left(\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \otimes \mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c}\right) \oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \otimes \mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c})\right) \\
&\oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c}\right) \oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c})\right) \\
&\oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c}\right) \oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c})\right) \\
&\oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c}\right) \\
&\oplus \left(\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c})\right)
\end{aligned}$$

De acordo com a Observação 5.1.2, existe um elemento $0 \neq u \in \mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \cong \mathbb{F}_{2^{p_1-1}}$ tal que $u^3 = (1-\hat{a})$ e $u \neq (1-\hat{a})$, ou seja, u não desempenha o papel de identidade no ideal minimal $\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a})$. Da mesma forma, existe $0 \neq v \in \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \cong \mathbb{F}_{2^{p_2-1}}$ tal que $v^3 = \left(1-\hat{b}\right)$ e $v \neq \left(1-\hat{b}\right)$ e, por fim, $0 \neq w \in \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c}) \cong \mathbb{F}_{2^{p_3-1}}$ tal que $w^3 = (1-\hat{c})$ e $w \neq (1-\hat{c})$. Assim,

$$\begin{aligned}
&\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c} \cong (\mathbb{F}_2G)e_3^{ab}\hat{c} \oplus (\mathbb{F}_2G)e_4^{ab}\hat{c}, \\
&\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\hat{b} \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c}) \cong (\mathbb{F}_2G)e_3^{ac}\hat{b} \oplus (\mathbb{F}_2G)e_4^{ac}\hat{b}, \\
&\mathbb{F}_2\mathcal{C}_{p_1}\hat{a} \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}(1-\hat{c}) \cong (\mathbb{F}_2G)e_3^{bc}\hat{a} \oplus (\mathbb{F}_2G)e_4^{bc}\hat{a},
\end{aligned}$$

são decomposições em componentes simples, onde $e_3^{ab} = uv + u^2v^2$, $e_4^{ab} = u^2v + uv^2$, $e_3^{ac} = uw + u^2w^2$, $e_4^{ac} = u^2w + uw^2$, $e_3^{bc} = vw + v^2w^2$ e $e_4^{bc} = v^2w + vw^2$.

De fato, vamos verificar a primeira decomposição. O racícionio é análogo para as demais. Temos

$$\begin{aligned}
\mathbb{F}_2\mathcal{C}_{p_1}(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}\hat{c} &\cong (\mathbb{F}_2G)(1-\hat{a})\left(1-\hat{b}\right)\hat{c} \\
&\cong \mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2})(1-\hat{a})\left(1-\hat{b}\right).
\end{aligned}$$

Pelo Teorema 5.2.3, o ideal acima decompõe-se em duas componentes simples. Logo

$$\mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2})(1-\hat{a})\left(1-\hat{b}\right) \cong \mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2})e_3^{ab} \oplus \mathbb{F}_2(\mathcal{C}_{p_1} \times \mathcal{C}_{p_2})e_4^{ab}. \tag{5.15}$$

Assim, reescrevendo (5.15), obtemos

$$(\mathbb{F}_2G)\,(1-\hat{a})\left(1-\hat{b}\right)\widehat{c} \cong (\mathbb{F}_2G)e_3^{ab}\hat{c} \oplus (\mathbb{F}_2G)e_4^{ab}\hat{c}.$$

Por fim, vamos mostrar que o ideal

$$\mathbb{F}_2\mathcal{C}_{p_1}\,(1-\hat{a}) \otimes \mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right) \otimes \mathbb{F}_2\mathcal{C}_{p_3}\,(1-\hat{c})$$

decompõe-se em quatro componentes simples. De fato,

$$\begin{aligned}
\mathbb{F}_2G\,(1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c}) &\cong \mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\times\mathcal{C}_{p_3}\right)(1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c}) \\
&\cong \left[\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)(1-\hat{a})\left(1-\hat{b}\right)\right]\otimes\left(\mathbb{F}_2\mathcal{C}_{p_3}\right)(1-\hat{c}) \\
&\cong \left[\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)e_3^{ab}\oplus\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)e_4^{ab}\right]\otimes\left(\mathbb{F}_2\mathcal{C}_{p_3}\right)(1-\hat{c}) \\
&\cong (\mathbb{F}_2G)\,e_3^{ab}\,(1-\hat{c})\oplus(\mathbb{F}_2G)\,e_4^{ab}\,(1-\hat{c}) \qquad (5.16)
\end{aligned}$$

Devemos verificar que as componentes em (5.16) não são simples. Vejamos

$$\mathbb{F}_2\mathcal{C}_{p_1}\,(1-\hat{a})\otimes\mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right)\cong\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)(1-\hat{a})\left(1-\hat{b}\right)\cong\mathbb{F}_{2^{p_1-1}}\otimes\mathbb{F}_{2^{p_2-1}}. \quad (5.17)$$

Existem $u\in\mathbb{F}_{2^{p_1-1}}$ e $v\in\mathbb{F}_{2^{p_2-1}}$, tais que $u^3=1$ e $v^3=1$. Logo, por (5.17), e sem perda de generalidade, afirmamos $1\otimes 1=u^3\otimes v^3=(uv)^3=(1-\hat{a})\left(1-\hat{b}\right)$. Além disso, $uv\neq e_3^{ab}=uv+u^2v^2$. Assim, defina $\alpha=uve_3^{ab}=uv+u^2v+uv^2$. Então, das considerações anteriores, verificamos

$$\alpha^3=\alpha^2\alpha=u^3v^3\left(e_3^{ab}\right)^2=(1-\hat{a})\left(1-\hat{b}\right)e_3^{ab}=\left(e_3^{ab}+e_4^{ab}\right)e_3^{ab}=e_3^{ab}, \qquad (5.18)$$

onde, de acordo com o Teorema 5.2.3, e_3^{ab} é um idempotente primitivo em $\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)(1-\hat{a})\left(1-\hat{b}\right)$. Similarmente, $\left(u^2v^2\right)^3=\left((uv)^3\right)^2=(1-\hat{a})\left(1-\hat{b}\right)$, e o elemento $\alpha^2=u^2v^2e_3^{ab}=u^2v^2+u^2v+uv^2$ satisfaz as mesmas condições do parágrafo anterior.

Afirmamos que os elementos $A=\alpha w+\alpha^2w^2$ e $B=\alpha^2w+\alpha w^2$ são idempotentes

primitivos de $\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)e_3^{ab}\otimes\mathbb{F}_2\mathcal{C}_{p_3}\left(1-\hat{c}\right)\cong\left(\mathbb{F}_2G\right)e_3^{ab}\left(1-\hat{c}\right)$. Vejamos

$$\begin{aligned}
A+B &= \alpha w+\alpha^2w^2+\alpha^2w+\alpha w^2\\
&= \alpha\left(w+w^2\right)+\alpha^2\left(w+w^2\right)\\
&= \left(\alpha+\alpha^2\right)+\underbrace{\left(w+w^2\right)}_{w^2+w+1=0}\\
&= \left(\alpha+\alpha^2\right)\cdot\left(1-\hat{c}\right)\\
&= \left(uv+u^2v^2+2u^2v+2uv^2\right)\cdot\left(1-\hat{c}\right)\\
&= \underbrace{\left(uv+u^2v^2\right)}_{e_3^{ab}}\cdot\left(1-\hat{c}\right)\\
&= e_3^{ab}\cdot\left(1-\hat{c}\right)
\end{aligned}$$

onde, em (5.16), $e_3^{ab}\left(1-\hat{c}\right)$ desempenha o papel de identidade no primeiro somando.

$$\begin{aligned}
AB &= \left(\alpha w+\alpha^2w^2\right)\left(\alpha^2w+\alpha w^2\right)\\
&= \alpha^3w^2+\alpha^2w^3+\alpha^4w^3+\alpha^3w^4\\
&= \alpha^3w^2+\alpha^2+\alpha^4+\alpha^3w\\
&= \underbrace{\alpha^3(w^2+w)}_{\alpha^3=1\text{ e }w^2+w=1}+\underbrace{\alpha^4+\alpha^2}_{\alpha^2(\alpha^2+1)=1}\\
&= 0
\end{aligned}\tag{5.19}$$

Por fim,

$$A^2=\left(\alpha w+\alpha^2w^2\right)^2=\alpha^2w^2+\alpha^4w^4=A\text{ e }B^2=\left(\alpha^2w+\alpha w^2\right)^2=\alpha^4w^2+\alpha^2w^4=B$$

Similarmente, em $\mathbb{F}_2\mathcal{C}_{p_1}\left(1-\hat{a}\right)\otimes\mathbb{F}_2\mathcal{C}_{p_2}\left(1-\hat{b}\right)$, temos $\left(uv^2\right)^3=\left(1-\hat{a}\right)\left(1-\hat{b}\right)$ e $uv^2\neq e_4^{ab}$. Defina $\beta=uv^2e_4^{ab}=uv^2+u^2v^2+uv$. Como foi feito para A e B, os elementos $C=\beta w+\beta^2w^2$ e $D=\beta^2w+\beta w^2$ são os idempotentes primitivos de $\mathbb{F}_2\left(\mathcal{C}_{p_1}\times\mathcal{C}_{p_2}\right)e_4^{ab}\otimes\mathbb{F}_2\mathcal{C}_{p_3}\left(1-\hat{c}\right)$.

Finalmente, afirmamos que A,B,C e D são idempotentes ortogonais e que

$A+B+C+D=(1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})$. De fato:

$$\begin{aligned}
A &= \alpha w+\alpha^2w^2=(uv+u^2v+uv^2)w+(uv+u^2v+uv^2)^2w^2=uvw+u^2vw\\
&+ uv^2w+u^2v^2w^2+uv^2w^2+u^2vw^2\\
&= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})+u^2v^2w+uvw^2,\\
B &= \alpha^2w+\alpha w^2=(uv+u^2v+uv^2)^2w+(uv+u^2v+uv^2)w^2=u^2v^2w+uv^2w+u^2vw\\
&+ uvw^2+u^2vw^2+uv^2w^2\\
&= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})+u^2v^2w^2+uvw,
\end{aligned}$$

$$\begin{aligned}
C &= \beta w+\beta^2w^2=\left(uv^2+u^2v^2+uv\right)w+\left(uv^2+u^2v^2+uv\right)^2w^2=uv^2w+u^2v^2w\\
&+ uvw+u^2vw^2+uvw^2+u^2v^2w^2\\
&= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})+u^2vw+uv^2w^2,\\
D &= \beta^2w+\beta w^2=\left(uv^2+u^2v^2+uv\right)^2w+\left(uv^2+u^2v^2+uv\right)w^2=u^2vw+uvw\\
&+ u^2v^2w+uv^2w^2+u^2v^2w^2+uvw^2\\
&= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})+uv^2w+u^2vw^2.
\end{aligned}$$

Logo,

$$\begin{aligned}
A+B+C+D &= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})\left[(1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})\right]\\
&= (1-\hat{a})\left(1-\hat{b}\right)(1-\hat{c})\,.
\end{aligned}$$

Por fim, os idempotentes A, B, C e D são ortogonais. De fato, em (5.19) já mostramos que $AB=0$. Vamos verificar que $AC=0$. A verificação para os demais casos é análoga.

$$\begin{aligned}
AC &= \alpha\beta w^2+\alpha\beta^2+\alpha^2\beta+\alpha^2\beta^2w\\
&= \alpha\beta\left(w^2+\alpha+\beta+\alpha\beta w\right)=0,
\end{aligned}$$

pois

$$\begin{aligned}
\alpha\beta &= \left(uv+u^2v+uv^2\right)\left(uv^2+u^2v^2+uv\right)=u^2+1+u^2v^2+1+u+v^2+u^2v+v+u^2\\
&= u^2v^2+u+u^2v+v^2+v=u^2\left(v^2+v\right)+u+1=u^2+u+1=0
\end{aligned}$$

Portanto, podemos reescrever a tabela (5.14) da seguinte forma

$$\begin{array}{ll} E_0=\hat{a}\ \hat{b}\ \hat{c} & E_1=(1-\hat{a})\ \hat{b}\ \hat{c} \\ E_2=\hat{a}\ \left(1-\hat{b}\right)\ \hat{c} & E_3=\hat{a}\ \hat{b}\ (1-\hat{c}) \\ E_4=e_4+e_5 & E_5=e_6+e_7 \\ E_6=e_8+e_9 & E_7=e_{10}+e_{11}+e_{12}+e_{13} \end{array} \tag{5.20}$$

onde os e_i, para cada $0\leq i\leq 13$, são dados conforme o enuncionado do Teorema. ■

5.3 Idempotentes Primitivos de $\mathbb{F}_2\left(\mathcal{C}_{121}\times\mathcal{C}_{169}\right)$

Finalizamos este capítulo explicitando o cálculo de idempotentes primitivos para uma álgebra do tipo $\mathbb{F}_2\left(\mathcal{C}_{p^2}\times\mathcal{C}_{q^2}\right)$, a partir da técnica apresentada na Seção (5.2.3).

É fácil ver que $\overline{2}$ gera $U\left(\mathbb{Z}_{121}\right)$ e $U\left(\mathbb{Z}_{169}\right)$. Além disso, as demais hipóteses de (5.4) são satisfeitas.

Os subgrupos de $\mathcal{C}_{121}=\langle a\rangle$ e $\mathcal{C}_{169}=\langle b\rangle$ são dados respectivamente por $\langle a\rangle$, $\langle a^{11}\rangle$ e $\langle a^{121}\rangle$ e $\langle b\rangle$, $\langle b^{13}\rangle$ e $\langle b^{169}\rangle$. Assim, os idempotentes primitivos de $\mathbb{F}_2\left(\mathcal{C}_{121}\times\mathcal{C}_{169}\right)$ são dados por:

$$\begin{aligned} e_0 &= \widehat{a}\widehat{b}=\widehat{\langle a\rangle}\widehat{\langle b\rangle}=\left(\sum_{i=0}^{120}a^i\right)\left(\sum_{j=0}^{168}b^j\right) \\ &= a^{120}b^{168}+a^{120}b^{167}+a^{119}b^{168}+\ldots+ab^2+b^3+a^2+ab+b^2+a+b+1 \end{aligned}$$

$$\begin{aligned} e_{02} &= \widehat{a}\left(\widehat{b^{169}}+\widehat{b^{13}}\right)=\widehat{\langle a\rangle}\left(\widehat{\langle b^{169}\rangle}+\widehat{\langle b^{13}\rangle}\right)=\left(\sum_{i=0}^{120}a^i\right)\left(1+\sum_{j=0}^{12}b^{13j}\right) \\ &= a^{120}b^{156}+a^{119}b^{156}+a^{118}b^{156}+\ldots+a^4b^{13}+a^3b^{13}+a^2b^{13}+ab^{13}+b^{13} \end{aligned}$$

$$\begin{aligned} e_{01} &= \widehat{a}\left(\widehat{b^{13}}+\widehat{b}\right)=\widehat{\langle a\rangle}\left(\widehat{\langle b^{13}\rangle}+\widehat{\langle b\rangle}\right)=\left(\sum_{i=0}^{120}a^i\right)\left(\sum_{j=0}^{12}b^{13j}+\sum_{j=0}^{168}b^j\right) \\ &= a^{120}b^{168}+a^{120}b^{167}+a^{119}b^{168}+\ldots+b^4+a^2b+ab^2+b^3+ab+b^2+b \end{aligned}$$

$$\begin{aligned} e_{20} &= \left(\widehat{a^{121}}+\widehat{a^{11}}\right)\widehat{b}=\left(\widehat{\langle a^{121}\rangle}+\widehat{\langle a^{11}\rangle}\right)\widehat{\langle b\rangle}=\left(1+\sum_{j=0}^{10}a^{11j}\right)\left(\sum_{i=0}^{168}b^i\right) \\ &= a^{10}b^{168}+a^{10}b^{167}+a^9b^{168}+a^{10}b^{166}+\ldots+a^2b+ab^2+a^2+ab+a \end{aligned}$$

$$\begin{aligned} e_{10} &= \left(\widehat{a^{11}}+\widehat{a}\right)\widehat{b}=\left(\widehat{\langle a^{11}\rangle}+\widehat{\langle a\rangle}\right)\widehat{\langle b\rangle}=\left(\sum_{j=0}^{10}a^{11j}+\sum_{j=0}^{120}a^{j}\right)\left(\sum_{i=0}^{168}b^{i}\right)\\ &= a^{120}b^{168}+a^{120}b^{167}+a^{119}b^{168}+\ldots+a^{12}b+a^{11}b^2+a^{12}+a^{11}b+a^{11}\end{aligned}$$

Agora vamos expressar os elementos u e v, conforme definido no Teorema (5.2.6).

$$\begin{aligned} u_2 &= \left\langle a^{121}\right\rangle\left(1+a^{2^0 11}+a^{2^2 11}+\ldots+a^{2^8 11}\right)=\left(1+a^{2^0 11}+a^{2^2 11}+\ldots+a^{2^8 11}\right)\\ &= a^{99}+a^{55}+a^{44}+a^{33}+a^{11}+1\\ v_2 &= \left\langle b^{169}\right\rangle\left(b^{2^0 13}+b^{2^2 13}+\ldots+a^{2^{10} 13}\right)=\left(b^{2^0 13}+b^{2^2 13}+\ldots+b^{2^{10} 13}\right)\\ &= b^{156}+b^{130}+b^{117}+b^{52}+b^{39}+b^{13}\end{aligned}$$

$$\begin{aligned} u_1 &= \left\langle a^{11}\right\rangle\left(1+a^{2^0}+a^{2^2}+\ldots+a^{2^8}\right)=\left(\sum_{i=0}^{10}a^{11i}\right)\left(1+a^{2^0}+a^{2^2}+\ldots+a^{2^8}\right)\\ &= a^{119}+a^{115}+a^{114}+\ldots+a^{14}+a^{12}+a^{11}+a^9+a^5+a^4+a^3+a+1\\ v_1 &= \left\langle b^{13}\right\rangle\left(b^{2^0}+b^{2^2}+\ldots+a^{2^{10}}\right)=\left(\sum_{j=0}^{12}b^{13j}\right)\left(b^{2^0}+b^{2^2}+\ldots+a^{2^{10}}\right)\\ &= b^{168}+b^{166}+b^{165}+b^{160}+b^{159}+\ldots+b^{14}+b^{12}+b^{10}+b^9+b^4+b^3+b\end{aligned}$$

Então

$$\begin{aligned} e_{22}^{*} &= u_2v_2+u_2^2v_2^2\\ &= a^{99}b^{156}+a^{110}b^{143}+a^{88}b^{143}+\ldots+a^{33}b^{13}+b^{39}+b^{26}+a^{11}b^{13}+b^{13}\\ e_{22}^{**} &= u_2v_2^2+u_2^2v_2\\ &= a^{110}b^{156}+a^{88}b^{156}+a^{99}b^{143}+\ldots+b^{39}+a^{11}b^{26}+a^{22}b^{13}+b^{26}+b^{13}\\ e_{12}^{*} &= u_1v_2+u_1^2v_2^2\\ &= a^{119}b^{156}+a^{115}b^{156}+a^{114}b^{156}+\ldots+a^5b^{13}+a^4b^{13}+a^3b^{13}+ab^{13}+b^{13}\\ e_{12}^{**} &= u_1v_2^2+u_1^2v_2\\ &= a^{120}b^{156}+a^{118}b^{156}+a^{117}b^{156}+\ldots+a^8b^{13}+a^7b^{13}+a^6b^{13}+a^2b^{13}+b^{13}\\ e_{21}^{*} &= u_2v_1+u_2^2v_1^2\\ &= a^{110}b^{167}+a^{110}b^{164}+a^{110}b^{163}+\ldots+b^8+b^7+b^6+b^5+b^4+b^3+b^2+b\\ e_{21}^{**} &= u_2v_1^2+u_2^2v_1\\ &= a^{110}b^{168}+a^{110}b^{166}+a^{110}b^{165}+\ldots+b^8+b^7+b^6+b^5+b^4+b^3+b^2+b\\ e_{11}^{*} &= u_1v_1+u_1^2v_1^2\\ &= a^{120}b^{167}+a^{119}b^{168}+a^{119}b^{166}+\ldots+a^3b+a^2b^2+ab^3+b^4+b^3+ab+b^2+b\\ e_{11}^{**} &= u_1v_1^2+u_1^2v_1\\ &= a^{120}b^{168}+a^{120}b^{166}+a^{119}b^{167}+\ldots+a^2b^3+b^5+b^4+a^2b+ab^2+b^3+b^2+b\end{aligned}$$

Capítulo 6

Comparação de técnicas para códigos de comprimento $p^n q$

Neste capítulo, l, p e q são primos distintos dois a dois, tais que $mdc\,(l, p^n q) = 1$ e l satisfaz a hipótese geral (4.1). Para códigos de comprimento $p^n q$ sobre um corpo de característica $l \neq 2$, as técnicas de álgebras de grupo não nos permitem ainda dar uma descrição completa dos idempotentes primitivos. No entanto, com o auxílio da abordagem polinomial feita por Bakshi e Raka em [2], conseguimos explicitar tais idempotentes. Desta forma, podemos dizer que estas duas técnicas se complementam.

Apresentamos ainda as expressões dos idempotentes primitivos para códigos de comprimento 245, de acordo com ambas as técnicas. Em seguida, generalizamos estes resultados para códigos de comprimento $p^n q$, onde conseguimos identificar possíveis erros nas expressões dos idempotentes primitivos dados pela λ-técnica, descrita no Capítulo 4.

6.1 Exemplos Comparativos

Exibiremos neste capítulo exemplos comparativos entre as duas técnicas apresentadas neste trabalho.

6.1.1 Idempotentes Primitivos de $\mathcal{R}_{245} = \dfrac{\mathbb{F}_3[x]}{\langle x^{245} - 1 \rangle}$

Vamos expressar os idempotentes primitivos do anel quociente $\mathcal{R}_{245} = \dfrac{\mathbb{F}_3[x]}{\langle x^{245} - 1 \rangle}$, a partir da λ-técnica.

Todos os cálculos deste capítulo foram realizados com o auxílio do software MAPLE.

Como $245 = 7^2 5$, verifica-se que 3 é raiz primitiva módulo 49 e módulo 5. Pelo Teorema 4.1.11, existem oito classes 3-ciclotômicas módulo 245, ou seja, oito idempotentes primitivos em $\mathcal{R}_{245}$. Para expressá-los, calcularemos as classes 3^2-ciclotômicas módulo 49 e módulo 5. Denotaremos por R_1 e N_1 os conjuntos de resíduos quadráticos e não quadráticos módulo 49, respectivamente. Além disso, defina $R_7 = \{r \cdot 7 / r \in R_1\}$ e $N_7 = \{n \cdot 7 / n \in N_1\}$. Por fim, sejam R_2 e N_2 os conjuntos de resíduos quadráticos e não quadráticos módulo 5, respectivamente. Assim as classes 3^2-ciclotômicas são os conjuntos

$$\begin{array}{rcl} R_1 & = & \{1,2,4,8,9,11,15,16,18,22,23,25,29,30,32,36,37,39,43,44,46\} \\ N_1 & = & \{3,5,6,10,12,13,17,19,20,24,26,27,31,33,34,38,40,41,45,47,48\} \\ R_7 & = & \{7,14,28\} \\ N_7 & = & \{21,35,42\} \\ R_2 & = & \{1,4\} \\ N_2 & = & \{2,3\} \\ C_0 & = & \{0\} \end{array} \tag{6.1}$$

onde $C_0 = \{0\}$ denota as classes 3^2-ciclotômicas do zero módulo 49 e módulo 5 e também denotará a classe 3-ciclotômica do zero módulo 245.

Conforme foi visto na demonstração da Proposição 4.1.9, existem $a_1 \in R_1\,(N_1)$ e $b_1 \in R_2\,(N_2)$ tais que

$$\lambda\,(a_1, b_1) = a_1 \cdot 5 + b_1 \cdot 49 \equiv 1\,(mod\,245)$$

Para $a_1 = 10 \in N_1$ e $b_1 = 4 \in R_2$, a congruência acima é válida. Assim

$$C_1 = \lambda\,(N_1 \times R_2 \cup R_1 \times N_2)\,. \tag{6.2}$$

Observação 6.1.1. *Para o anel* $\mathcal{R}_{35} = \dfrac{\mathbb{F}_3[x]}{\langle x^{35} - 1\rangle}$, *a classe l-ciclotômica*

$$C_1 = \lambda\,(R_1 \times R_2 \cup N_1 \times N_2)\,, \tag{6.3}$$

onde, em comparação com a expressão (6.2)*, verificamos que as afirmações dadas em [16, Exemplo 4.1] podem não estar completas.*

Pela descrição dada na Proposição 4.1.9, as classes 3-ciclotômicas módulo 245 são

$$\begin{array}{ll} C_1 = \lambda\,(N_1 \times R_2 \cup R_1 \times N_2) & C_2 = \lambda\,(R_1 \times R_2 \cup N_1 \times N_2) \\ C_7 = \lambda\,(R_7 \times R_2 \cup N_7 \times N_2) & C_{14} = \lambda\,(N_7 \times R_2 \cup R_7 \times N_2) \\ C_{49} = \lambda\,(C_0 \times R_2 \cup C_0 \times N_2) & C_5 = \lambda\,(R_1 \times C_0 \cup N_1 \times C_0) \\ C_{35} = \lambda\,(R_7 \times C_0 \cup N_7 \times C_0) & C_0 = \lambda\,(C_0 \times C_0) = \{0\} \end{array} \tag{6.4}$$

De acordo com a notação dada na Observação 4.2.3 e em [16, Exemplo 4.1], os idem-

potentes primitivos correspondentes as classes l^2-ciclotômicas módulo p^n, onde p é um primo positivo, são dados por:

$$\begin{aligned}
\theta_0 &= \frac{1}{p^n}\left[\sigma_{C_0}(x)+\sum_{i=0}^{n-1}\left(\sigma_{R_{p^i}}(x)+\sigma_{N_{p^i}}(x)\right)\right],\\
\theta^*_{p^j} &= \frac{1}{p^n}\left\{\frac{\varphi\left(p^{n-j}\right)}{2}\left[\sigma_{C_0}(x)+\sum_{i=n-j}^{n-1}\left(\sigma_{R_{p^i}}(x)+\sigma_{N_{p^i}}(x)\right)\right]\right.\\
&+ \left.\frac{1}{p^j}\left(\mathcal{A}\sigma_{R_{p^{n-j-1}}}(x)+\overline{\mathcal{A}}\sigma_{N_{p^{n-j-1}}}(x)\right)\right\} \text{ e} \qquad (6.5)\\
\theta^{**}_{p^j} &= \frac{1}{p^n}\left\{\frac{\varphi\left(p^{n-j}\right)}{2}\left[\sigma_{C_0}(x)+\sum_{i=n-j}^{n-1}\left(\sigma_{R_{p^i}}(x)+\sigma_{N_{p^i}}(x)\right)\right]\right.\\
&+ \left.\frac{1}{p^j}\left(\overline{\mathcal{A}}\sigma_{R_{p^{n-j-1}}}(x)+\mathcal{A}\sigma_{N_{p^{n-j-1}}}(x)\right)\right\},
\end{aligned}$$

onde $\mathcal{A}=\dfrac{-p^{n-1}\left(1+\sqrt{p}\right)}{2}$ $\left(\text{ou } \dfrac{-p^{n-1}\left(1+\sqrt{-p}\right)}{2}\right)$ e $\overline{\mathcal{A}}=\dfrac{-p^{n-1}\left(1-\sqrt{p}\right)}{2}$ $\left(\text{ou } \dfrac{-p^{n-1}\left(1-\sqrt{-p}\right)}{2}\right)$ quando $p\equiv 1\ (mod\ 4)$ (ou $p\equiv 3\ (mod\ 4)$).

Logo, os idempotentes primitivos relacionados as classes 3^2-ciclotômicas (6.1) são dados por:

$$\begin{aligned}
\theta_{C_0} &= \frac{1}{49}\left[\sigma_{C_0}(x)+\sigma_{R_1}(x)+\sigma_{R_7}(x)+\sigma_{N_1}(x)+\sigma_{N_7}(x)\right],\\
\theta^*_{7^0} &= \frac{1}{49}\left[\mathcal{A}\sigma_{R_7}(x)+\overline{\mathcal{A}}\sigma_{N_7}(x)\right],\\
\theta^{**}_{7^0} &= \frac{1}{49}\left[\overline{\mathcal{A}}\sigma_{R_7}(x)+\mathcal{A}\sigma_{N_7}(x)\right],\\
\theta^*_{7} &= \frac{1}{343}\left[\mathcal{A}\sigma_{R_1}(x)+\overline{\mathcal{A}}\sigma_{N_1}(x)\right],\\
\theta^{**}_{7} &= \frac{1}{343}\left[\overline{\mathcal{A}}\sigma_{R_1}(x)+\mathcal{A}\sigma_{N_1}(x)\right],\\
\theta_{C_0} &= \frac{1}{5}\left[\sigma_{C_0}(x)+\sigma_{R_2}(x)+\sigma_{N_2}(x)\right],\\
\theta^*_{5^0} &= \frac{1}{5}\left[2\sigma_{C_0}(x)+\mathcal{B}\sigma_{R_2}(x)+\overline{\mathcal{B}}\sigma_{N_2}(x)\right],\\
\theta^{**}_{5^0} &= \frac{1}{5}\left[2\sigma_{C_0}(x)+\overline{\mathcal{B}}\sigma_{R_2}(x)+\mathcal{B}\sigma_{N_2}(x)\right],
\end{aligned}$$

onde $\mathcal{A}=\dfrac{-7(1+\sqrt{-7})}{2}$, $\overline{\mathcal{A}}=\dfrac{-7(1-\sqrt{-7})}{2}$, $\mathcal{B}=\dfrac{-1-\sqrt{5}}{2}$ e $\overline{\mathcal{B}}=\dfrac{-1+\sqrt{5}}{2}$.

De acordo com o Teorema 4.2.4 e o Corolário 4.2.5, apresentamos as expressões dos

oito idempotentes primitivos do anel $\mathcal{R}_{245} = \dfrac{\mathbb{F}_3[x]}{\langle x^{245}-1\rangle}$:

$$\begin{aligned}
\theta_1 &= \lambda(\theta_{7^0}^* \otimes \theta_{5^0}^*) + \lambda(\theta_{7^0}^{**} \otimes \theta_{5^0}^{**}) \\
&= \frac{4}{245}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_{35}}(x) + \frac{2}{245}\left(\overline{\mathcal{A}}\mathcal{B}+\mathcal{A}\overline{\mathcal{B}}\right)\sigma_{C_{14}}(x) + \frac{2}{245}\left(\mathcal{A}\mathcal{B}+\overline{\mathcal{A}}\,\overline{\mathcal{B}}\right)\sigma_{C_7}(x), \\
\theta_2 &= \lambda(\theta_{7^0}^{**} \otimes \theta_{5^0}^*) + \lambda(\theta_{7^0}^* \otimes \theta_{5^0}^{**}) \\
&= \frac{4}{245}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_{35}}(x) + \frac{2}{245}\left(\overline{\mathcal{A}}\mathcal{B}+\mathcal{A}\overline{\mathcal{B}}\right)\sigma_{C_7}(x) + \frac{2}{245}\left(\mathcal{A}\mathcal{B}+\overline{\mathcal{A}}\,\overline{\mathcal{B}}\right)\sigma_{C_{14}}(x), \\
\theta_7 &= \lambda(\theta_7^{**} \otimes \theta_{5^0}^*) + \lambda(\theta_7^* \otimes \theta_{5^0}^{**}) \\
&= \frac{4}{1715}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_5}(x) + \frac{2}{1715}\left(\overline{\mathcal{A}}\mathcal{B}+\mathcal{A}\overline{\mathcal{B}}\right)\sigma_{C_2}(x) + \frac{2}{1715}\left(\mathcal{A}\mathcal{B}+\overline{\mathcal{A}}\,\overline{\mathcal{B}}\right)\sigma_{C_1}(x), \\
\theta_{14} &= \lambda(\theta_7^* \otimes \theta_{5^0}^*) + \lambda(\theta_7^{**} \otimes \theta_{5^0}^{**}) \\
&= \frac{4}{1715}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_5}(x) + \frac{2}{1715}\left(\overline{\mathcal{A}}\mathcal{B}+\mathcal{A}\overline{\mathcal{B}}\right)\sigma_{C_1}(x) + \frac{2}{1715}\left(\mathcal{A}\mathcal{B}+\overline{\mathcal{A}}\,\overline{\mathcal{B}}\right)\sigma_{C_2}(x), \\
\theta_{49} &= \lambda(\theta_{C_0} \otimes \theta_{5^0}^*) + \lambda(\theta_{C_0} \otimes \theta_{5^0}^{**}) \\
&= \frac{4}{245}\sigma_{C_0}(x) + \frac{2}{245}(\mathcal{B}+\overline{\mathcal{B}})\sigma_{C_{49}}(x) + \frac{8}{245}\sigma_{C_5}(x) + \frac{2}{245}(\mathcal{B}+\overline{\mathcal{B}})\sigma_{C_2}(x) \\
&+ \frac{2}{245}\left(\mathcal{B}+\overline{\mathcal{B}}\right)\sigma_{C_1}(x) + \frac{8}{245}\sigma_{C_{35}}(x) + \frac{2}{245}\left(\mathcal{B}+\overline{\mathcal{B}}\right)\sigma_{C_7}(x) + \frac{2}{245}\left(\mathcal{B}+\overline{\mathcal{B}}\right)\sigma_{C_{14}}(x), \\
\theta_5 &= \lambda(\theta_{7^0}^{**} \otimes \theta_{C_0}) + \lambda(\theta_{7^0}^* \otimes \theta_{C_0}) \\
&= \frac{2}{245}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_{35}}(x) + \frac{2}{245}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_7}(x) + \frac{2}{245}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_{14}}(x), \\
\theta_{35} &= \lambda(\theta_7^{**} \otimes \theta_{C_0}) + \lambda(\theta_7^* \otimes \theta_{C_0}) \\
&= \frac{2}{1715}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_5}(x) + \frac{2}{1715}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_2}(x) + \frac{2}{1715}\left(\mathcal{A}+\overline{\mathcal{A}}\right)\sigma_{C_1}(x), \\
\theta_0 &= \lambda(\theta_{C_0} \otimes \theta_{C_0}) \\
&= \frac{1}{245}\sigma_{C_0}(x) + \frac{2}{245}\sigma_{C_{49}}(x) + \frac{2}{245}\sigma_{C_5}(x) + \frac{2}{245}\sigma_{C_2}(x) + \frac{2}{245}\sigma_{C_1}(x) + \frac{2}{245}\sigma_{C_{35}}(x) \\
&+ \frac{2}{245}\sigma_{C_7}(x) + \frac{2}{245}\sigma_{C_{14}}(x).
\end{aligned}$$

Necessitamos do seguinte resultado para calcularmos os valores dos coeficientes.

Corolário 6.1.2 ([2], Corolário, página 445)**.** *Se p, q, e l são primos ímpares distintos, l é uma raiz primitiva módulo p^n e módulo q, $mdc\left(\dfrac{\varphi(p^n)}{2}, \dfrac{\varphi(q)}{2}\right) = 1$, então $-pq$ é um resíduo quadrático módulo l se $l^{\frac{\varphi(p^n q)}{4}} \not\equiv -1 \,(mod\, p^n q)$ e pq é resíduo quadrático módulo l se $l^{\frac{\varphi(p^n q)}{4}} \equiv -1 \,(mod\, p^n q)$.*

Assim, em $\mathbb{F}_3$, $\mathcal{A}\mathcal{B} + \overline{\mathcal{A}}\,\overline{\mathcal{B}} = 1$, $\overline{\mathcal{A}}\mathcal{B} + \mathcal{A}\overline{\mathcal{B}} = 0$, $\mathcal{A} + \overline{\mathcal{A}} = 2$ e $\mathcal{B} + \overline{\mathcal{B}} = 2$. Logo, os

idempotentes podem ser reescritos como:

$$\begin{aligned}
\theta_1 &= \lambda\left(\theta_{7^0}^{*}\otimes\theta_{5^0}^{*}\right)+\lambda\left(\theta_{7^0}^{**}\otimes\theta_{5^0}^{**}\right)=\sigma_{C_{35}}(x)+\sigma_{C_7}(x),\\
\theta_2 &= \lambda\left(\theta_{7^0}^{**}\otimes\theta_{5^0}^{*}\right)+\lambda\left(\theta_{7^0}^{*}\otimes\theta_{5^0}^{**}\right)=\sigma_{C_{35}}(x)+\sigma_{C_{14}}(x),\\
\theta_7 &= \lambda\left(\theta_{7}^{**}\otimes\theta_{5^0}^{*}\right)+\lambda\left(\theta_{7}^{*}\otimes\theta_{5^0}^{**}\right)=\sigma_{C_5}(x)+\sigma_{C_1}(x),\\
\theta_{14} &= \lambda\left(\theta_{7}^{*}\otimes\theta_{5^0}^{*}\right)+\lambda\left(\theta_{7}^{**}\otimes\theta_{5^0}^{**}\right)=\sigma_{C_5}(x)+\sigma_{C_2}(x),\\
\theta_{49} &= \lambda\left(\theta_{C_0}\otimes\theta_{5^0}^{*}\right)+\lambda\left(\theta_{C_0}\otimes\theta_{5^0}^{**}\right) \qquad (6.6)\\
&= 2\sigma_{C_0}(x)+2\sigma_{C_{49}}(x)+\sigma_{C_5}(x)+2\sigma_{C_2}(x)+2\sigma_{C_1}(x)+\sigma_{C_{35}}(x)+2\sigma_{C_7}(x)+2\sigma_{C_{14}}(x),\\
\theta_5 &= \lambda\left(\theta_{7^0}^{**}\otimes\theta_{C_0}\right)+\lambda\left(\theta_{7^0}^{*}\otimes\theta_{C_0}\right)=2\sigma_{C_{35}}(x)+2\sigma_{C_7}(x)+2\sigma_{C_{14}}(x),\\
\theta_{35} &= \lambda\left(\theta_{7}^{**}\otimes\theta_{C_0}\right)+\lambda\left(\theta_{7}^{*}\otimes\theta_{C_0}\right)=2\sigma_{C_5}(x)+2\sigma_{C_2}(x)+2\sigma_{C_1}(x),\\
\theta_0 &= \lambda\left(\theta_{C_0}\otimes\theta_{C_0}\right)\\
&= 2\sigma_{C_0}(x)+\sigma_{C_{49}}(x)+\sigma_{C_5}(x)+\sigma_{C_2}(x)+\sigma_{C_1}(x)+\sigma_{C_{35}}(x)+\sigma_{C_7}(x)+\sigma_{C_{14}}(x).
\end{aligned}$$

6.1.2 Idempotentes Primitivos de $\mathbb{F}_3\left(\mathcal{C}_{49}\times\mathcal{C}_5\right)$

Vamos expressar os idempotentes primitivos da álgebra de grupo $\mathbb{F}_3\left(\mathcal{C}_{49}\times\mathcal{C}_5\right)$, desta vez a partir da técnica apresentada na Seção 3.2.

Como afirmado na seção anterior, $\overline{3}$ gera $U\left(\mathbb{Z}_{49}\right)$ e $U\left(\mathbb{Z}_5\right)$. Além disso, as demais hipóteses de (5.4) são satisfeitas.

Para $\mathcal{C}_{245}=\langle g\rangle$, os subgrupos de $\mathcal{C}_{49}=\langle a\rangle=\langle g^5\rangle$ e $\mathcal{C}_5=\langle b\rangle=\langle g^{49}\rangle$ são dados respectivamente por $\langle a\rangle$, $\langle a^7\rangle$ e $\langle a^{49}\rangle$ e $\langle b\rangle$ e $\langle b^5\rangle$. Assim a decomposição da álgebra de grupo $\mathbb{F}_3\mathcal{C}_{245}$ é dada por:

$$\begin{aligned}
\mathbb{F}_3\left(\mathcal{C}_{49}\times\mathcal{C}_5\right) &\cong \mathbb{F}_3\mathcal{C}_{49}\otimes\mathbb{F}_3\mathcal{C}_5\\
&\cong \left[\mathbb{F}_3\widehat{a}\oplus\mathbb{F}_3\left(\widehat{a^7}-\widehat{a}\right)\oplus\mathbb{F}_3\left(1-\widehat{a^7}\right)\right]\otimes\left[\mathbb{F}_3\widehat{b}\oplus\mathbb{F}_3\left(1-\widehat{b}\right)\right]\\
&\cong \mathbb{F}_3\widehat{a}\widehat{b}\oplus\mathbb{F}_3\widehat{a}\left(1-\widehat{b}\right)\oplus\mathbb{F}_3\left(\widehat{a^7}-\widehat{a}\right)\widehat{b}\oplus\mathbb{F}_3\left(\widehat{a^7}-\widehat{a}\right)\left(1-\widehat{b}\right)\\
&\oplus \mathbb{F}_3\left(1-\widehat{a^7}\right)\widehat{b}\oplus\mathbb{F}_3\left(1-\widehat{a^7}\right)\left(1-\widehat{b}\right)\\
&\cong \mathbb{F}_3\widehat{a}\widehat{b}\oplus\mathbb{F}_3\left(\widehat{a}-\widehat{G}\right)\oplus\mathbb{F}_3\left(\widehat{a^7}\widehat{b}-\widehat{G}\right)\oplus\mathbb{F}_3\left(\widehat{a^7}-\widehat{a}\right)\left(1-\widehat{b}\right)\\
&\oplus \mathbb{F}_3\left(\widehat{b}-\widehat{a^7}\widehat{b}\right)\oplus\mathbb{F}_3\left(1-\widehat{a^7}\right)\left(1-\widehat{b}\right) \qquad (6.7)
\end{aligned}$$

Os idempotentes são dados por

$$\begin{aligned}
e_0 &= \frac{1}{245}\widehat{a}\widehat{b}=\frac{1}{245}\widehat{g^5}\widehat{g^{49}}=\frac{1}{245}\left(\sum_{i=0}^{48}g^{5i}\right)\left(\sum_{j=0}^{4}g^{49j}\right)\\
&= 2g^{244}+2g^{243}+2g^{242}+2g^{241}+2g^{240}+\ldots+2g^4+2g^3+2g^2+2g+2
\end{aligned}$$

$$\begin{aligned} e_1 &= \widehat{a} - \widehat{G} = \frac{1}{49}\widehat{g^5} - \frac{1}{245}\widehat{g} = \frac{1}{49}\left(\sum_{i=0}^{48} g^{5i}\right) - \frac{1}{245}\left(\sum_{i=0}^{48} g^{5i}\right)\left(\sum_{j=0}^{4} g^{49j}\right) \\ &= g^{244} + g^{243} + g^{242} + g^{241} + 2g^{240} + \ldots + 2g^5 + g^4 + g^3 + g^2 + g + 2 \end{aligned}$$

$$\begin{aligned} e_2 &= \widehat{a^7}\widehat{b} - \widehat{G} = \widehat{g^{35}}\widehat{g^{49}} - \widehat{g} = \frac{1}{7}\left(\sum_{i=0}^{6} g^{35i}\right)\frac{1}{5}\left(\sum_{j=0}^{4} g^{49j}\right) - \frac{1}{245}\left(\sum_{k=0}^{244} g^{k}\right) \\ &= g^{244} + g^{243} + g^{242} + g^{241} + g^{240} + \ldots + g^5 + g^4 + g^3 + g^2 + g \end{aligned}$$

$$\begin{aligned} e_3 &= \widehat{b} - \widehat{a^p}\widehat{b} = \widehat{g^{49}} - \widehat{g^{35}}\widehat{g^{49}} = \frac{1}{5}\left(\sum_{i=0}^{4} g^{49i}\right) - \frac{1}{7}\left(\sum_{j=0}^{6} g^{35j}\right)\frac{1}{5}\left(\sum_{i=0}^{4} g^{49i}\right) \\ &= g^{238} + g^{231} + g^{224} + g^{217} + g^{210} + \ldots + g^{35} + g^{28} + g^{21} + g^{14} + g^7 \end{aligned}$$

Do Teorema 5.2.2, temos que

$$\begin{aligned} e_4 &= \left(\widehat{a^7} - \widehat{a}\right)\left(1 - \widehat{b}\right) = \left(\frac{1}{7}\sum_{i=0}^{6} g^{35i} - \frac{1}{49}\sum_{j=0}^{48} g^{5j}\right)\left(1 - \frac{1}{5}\sum_{k=0}^{4} g^{49k}\right) \\ &= 2g^{244} + 2g^{243} + 2g^{242} + 2g^{241} + g^{240} + \ldots + g^5 + 2g^4 + 2g^3 + 2g^2 + 2g \end{aligned}$$

e

$$\begin{aligned} e_5 &= \left(1 - \widehat{a^7}\right)\left(1 - \widehat{b}\right) = \left(1 - \frac{1}{7}\sum_{i=0}^{6} g^{35i}\right)\left(1 - \frac{1}{5}\sum_{k=0}^{4} g^{49k}\right) \\ &= 2g^{238} + 2g^{231} + 2g^{224} + 2g^{217} + g^{210} + \ldots + 2g^{28} + 2g^{21} + 2g^{14} + 2g^7 \end{aligned}$$

não são idempotentes primitivos em $\mathbb{F}_3\left(\mathcal{C}_{49} \times \mathcal{C}_5\right)$. Assim $e_4 = e_4^* + e_4^{**}$ e $e_5 = e_5^* + e_5^{**}$ onde

$$\begin{aligned} e_4^* &= 2g^{243} + 2g^{240} + 2g^{239} + 2g^{237} + 2g^{235} + \ldots + 2g^9 + 2g^5 + 2g^4 + 2g^3 + 2g \\ e_4^{**} &= 2g^{244} + 2g^{242} + 2g^{241} + 2g^{240} + 2g^{236} + \ldots + 2g^{10} + 2g^8 + 2g^6 + 2g^5 + 2g^2 \end{aligned}$$

e

$$\begin{aligned} e_5^* &= 2g^{231} + 2g^{210} + 2g^{203} + 2g^{189} + 2g^{175} + \ldots + 2g^{63} + 2g^{35} + 2g^{28} + 2g^{21} + 2g^7 \\ e_5^{**} &= 2g^{238} + 2g^{224} + 2g^{217} + 2g^{210} + 2g^{182} + \ldots + 2g^{70} + 2g^{56} + 2g^{42} + 2g^{35} + 2g^{14} \end{aligned}$$

Portanto, os idempotentes primitivos de $\mathbb{F}_3\left(\mathcal{C}_{49} \times \mathcal{C}_5\right)$ podem ser expressos da seguinte

forma:

$$\begin{aligned}
e_0 &= 2\mathcal{S}_1+2\mathcal{S}_g+2\mathcal{S}_{g^2}+2\mathcal{S}_{g^7}+2\mathcal{S}_{g^{14}}+2\mathcal{S}_{g^{49}}+2\mathcal{S}_{g^5}+2\mathcal{S}_{g^{35}}\\
e_1 &= 2\mathcal{S}_1+\mathcal{S}_g+\mathcal{S}_{g^2}+\mathcal{S}_{g^7}+\mathcal{S}_{g^{14}}+\mathcal{S}_{g^{49}}+2\mathcal{S}_{g^5}+2\mathcal{S}_{g^{35}}\\
e_2 &= \mathcal{S}_g+\mathcal{S}_{g^2}+\mathcal{S}_{g^5}\\
e_3 &= \mathcal{S}_{g^7}+\mathcal{S}_{g^{14}}+\mathcal{S}_{g^{35}}\\
e_4^* &= 2\mathcal{S}_g+2\mathcal{S}_{g^5}\\
e_4^{**} &= 2\mathcal{S}_{g^2}+2\mathcal{S}_{g^5}\\
e_5^* &= 2\mathcal{S}_{g^7}+2\mathcal{S}_{g^{35}}\\
e_5^{**} &= 2\mathcal{S}_{g^{14}}+2\mathcal{S}_{g^{35}}.
\end{aligned} \tag{6.8}$$

Agora apresentamos uma tabela comparativa entre os idempotentes primitivos calculados a partir de ambas as técnicas.

$\frac{\mathbb{F}_3[x]}{\langle x^{245}-1\rangle}$	$\mathbb{F}_3\left(\mathcal{C}_{49}\times\mathcal{C}_5\right)$
$\theta_1=\sigma_{C_{35}}+\sigma_{C_7}$	$\mathrm{e}_5^*=\mathcal{S}_{g^{35}}+\mathcal{S}_{g^7}$
$\theta_2=\sigma_{C_{35}}+\sigma_{C_{14}}$	$\mathrm{e}_5^{**}=\mathcal{S}_{g^{35}}+\mathcal{S}_{g^{14}}$
$\theta_7=\sigma_{C_5}+\sigma_{C_1}$	$\mathrm{e}_4^*=\mathcal{S}_{g^5}+\mathcal{S}_g$
$\theta_{14}=\sigma_{C_5}+\sigma_{C_2}$	$\mathrm{e}_4^{**}=\mathcal{S}_{g^5}+\mathcal{S}_{g^2}$
$\theta_{49}=2\sigma_{C_0}+\sigma_{C_{49}}+\sigma_{C_5}+\sigma_{C_2}$ $+\sigma_{C_1}+\sigma_{C_{35}}+\sigma_{C_7}+\sigma_{C_{14}}$	$\mathrm{e}_1=2\mathcal{S}_1+\mathcal{S}_{g^{49}}+2\mathcal{S}_{g^5}+\mathcal{S}_{g^2}$ $+\mathrm{S}_g+2\mathcal{S}_{g^{35}}+\mathcal{S}_{g^7}+\mathcal{S}_{g^{14}}$
$\theta_5=\sigma_{C_{35}}+\sigma_{C_7}+\sigma_{C_{14}}$	$\mathrm{e}_3=\mathcal{S}_{g^{35}}+\mathcal{S}_{g^7}+\mathcal{S}_{g^{14}}$
$\theta_{35}=\sigma_{C_5}+\sigma_{C_2}+\sigma_{C_1}$	$\mathrm{e}_2=\mathcal{S}_{g^5}+\mathcal{S}_{g^2}+\mathcal{S}_{g^1}$
$\theta_0=2\sigma_{C_0}+\sigma_{C_{49}}+\sigma_{C_5}+\sigma_{C_2}$ $+\sigma_{C_1}+\sigma_{C_{35}}+\sigma_{C_7}+\sigma_{C_{14}}$	$\mathrm{e}_0=2\mathcal{S}_1+\mathcal{S}_{g^{49}}+\mathcal{S}_{g^5}+\mathcal{S}_{g^2}$ $+\mathrm{S}_g+\mathcal{S}_{g^{35}}+\mathcal{S}_{g^7}+\mathcal{S}_{g^{14}}$

Tabela 6.1: Idempotentes primitivos

Comparando os idempotentes primitivos dados por ambas abordagens, encontramos diferenças entre as expressões correspondentes, o que nos sugere possíveis falhas na λ-técnica, uma vez que todos os idempotentes primitivos encontrados a partir da técnica de álgebras de grupo, foram testados no software MAPLE com êxito.

6.2 Idempotentes Primitivos em $\mathbb{F}_l\left(\mathcal{C}_{p^n}\times\mathcal{C}_q\right)$

Nesta seção buscamos identificar os possíveis erros na λ-técnica para a expressão dos idempotentes primitivos, utilizando as expressões dadas pela técnica de álgebra de grupo.

Se $\mathcal{C}_{p^nq}=\langle g\rangle$, onde $\mathcal{C}_{p^n}=\langle a\rangle=\langle g^q\rangle$ e $\mathcal{C}_q=\langle b\rangle=\left\langle g^{p^n}\right\rangle$, considere a seguinte decomposição em ideais da álgebra de grupo $\mathbb{F}_l\left(\mathcal{C}_{p^n}\times\mathcal{C}_q\right)$, a partir dos resultados vistos

na Seção 3.2

$$\begin{aligned}\mathbb{F}_l\left(\mathcal{C}_{p^nq}\right) &\cong \mathbb{F}_l\mathcal{C}_{p^n}\otimes\mathbb{F}_l\mathcal{C}_q\\ &\cong \left[\mathbb{F}_l\mathcal{C}_{p^n}\widehat{a}\oplus\ldots\oplus\mathbb{F}_l\mathcal{C}_{p^n}\left(1-\widehat{a^{p^{n-1}}}\right)\right]\otimes\left[\mathbb{F}_l\mathcal{C}_q\widehat{b}\oplus\mathbb{F}_l\mathcal{C}_q\left(1-\widehat{b}\right)\right]\\ &\cong \mathbb{F}_l\mathcal{C}_{p^nq}\widehat{a}\widehat{b}\oplus\ldots\oplus\mathbb{F}_l\mathcal{C}_{p^nq}\left(\widehat{a^{n-j}}-\widehat{a^{n-(j+1)}}\right)\left(1-\widehat{b}\right)\oplus\ldots\oplus\mathbb{F}_l\mathcal{C}_{p^nq}\widehat{a}\left(1-\widehat{b}\right).\end{aligned}$$

De acordo com o Lema 5.1.1, para todo $0\leq j\leq n-1$, os idempotentes da forma $\widehat{a}\widehat{b}$, $\left(\widehat{a^{n-j}}-\widehat{a^{n-(j+1)}}\right)\widehat{b}$ e $\widehat{a}\left(1-\widehat{b}\right)$ são primitivos. Já os idempotentes da forma $e^{n-j}=\left(\widehat{a^{n-j}}-\widehat{a^{n-(j+1)}}\right)\left(1-\widehat{b}\right)$ não são primitivos. Dos resultados vistos no Capítulo 4, juntamente com os resultados de [2], podemos fornecer uma expressão para e^{n-j} como soma de idempotentes primitivos.

Considerando a notação estabelecida na Observação 5.2.5 e a hipótese geral (4.1), temos os seguintes resultados

Lema 6.2.1.

(i) $\displaystyle\sum_{i=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^i=\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i+\mathcal{S}_{g^{qp^{n-j-1}}}.$

(ii) $\displaystyle\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i=\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{p^iq}}.$

Demonstração. De fato, para (i), temos

$$\begin{aligned}\sum_{i=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^i &= \sum_{i\in\mathbb{Z}^*_{p^{j+1}}}\left(g^{qp^{n-j-1}}\right)^i\\ &= \sum_{r\in\mathbb{Z}^*_{p^{j+1}}-U\left(\mathbb{Z}_{p^{j+1}}\right)}\left(g^{qp^{n-j-1}}\right)^r+\sum_{s\in U\left(\mathbb{Z}_{p^{j+1}}\right)}\left(g^{qp^{n-j-1}}\right)^s\\ &= \sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i+\mathcal{S}_{g^{qp^{n-j-1}}}.\end{aligned}$$

uma vez que todo elemento da forma $g^{\left(qp^{n-j-1}\right)s}$, onde $s\in U\left(\mathbb{Z}^*_{p^{j+1}}\right)$, pode ser escrito da forma $g^{\left(qp^{n-j-1}\right)l^t}$ pois, pelo Teorema 4.1.4, l gera $U\left(\mathbb{Z}_{p^{j+1}}\right)$, para todo $0\leq j\leq n-1$. Além disso, pela Proposição 4.1.9, temos

$$\left|U\left(\mathbb{Z}_{p^{j+1}}\right)\right|=p^j(p-1)=\left|C_{qp^{n-j-1}}\right|.$$

O item (ii) decorre de (i). ∎

Lema 6.2.2. $\sum_{k=1}^{q-1} \left(g^{p^n}\right)^k \sum_{i=1}^{p^j-1} \left(g^{qp^{n-j}}\right)^i = \sum_{i=n-j}^{n-1} \mathcal{S}_{g^{p^i}} + \sum_{i=n-j}^{n-1} \mathcal{S}_{g^{dp^i}}$, *onde d faz o papel do elemento a dado em [2, Lema 3].*

Demonstração. É simples verificar que $\sum_{k=1}^{q-1} \left(g^{p^n}\right)^k = \mathcal{S}_{g^{p^n}}$. Logo, pelo Lema 6.2.1, item (ii), temos

$$\sum_{k=1}^{q-1} \left(g^{p^n}\right)^k \sum_{i=1}^{p^j-1} \left(g^{qp^{n-j}}\right)^i = \mathcal{S}_{g^{p^n}} \sum_{i=n-j}^{n-1} \mathcal{S}_{g^{p^i q}}.$$

Verifiquemos, para um elemento arbitrário $\mathcal{S}_{g^{p^{n-(j-w)}}}$, que

$$\mathcal{S}_{g^{p^n}} \mathcal{S}_{g^{qp^{n-(j-w)}}} = \mathcal{S}_{g^{p^{n-(j-w)}}} + \mathcal{S}_{g^{dp^{n-(j-w)}}},$$

para algum $0 \leq w \leq j-1$. De fato

$$\left(g^{p^n} + g^{lp^n} + \ldots + g^{l^{\varphi(q)-1}p^n}\right)\left(g^{p^{n-(j-w)}q} + g^{lp^{n-(j-w)}q} + \ldots + g^{l^{\varphi\left(p^{j-w}\right)-1}p^{n-(j-w)}q}\right) \quad (6.9)$$

A Equação (6.9) pode ser reescrita como

$$g^{p^{n-(j-w)}\left(p^{j-w}+q\right)} + g^{p^{n-(j-w)}\left(p^{j-w}+lq\right)} + \ldots + g^{p^{n-(j-w)}\left(l^{\varphi(q)-1}p^{j-w}+l^{\varphi\left(p^{j-w}\right)-1}q\right)}, \quad (6.10)$$

onde existem exatamente $\varphi(q)\varphi(p^{j-w}) = \varphi(qp^{j-w})$ elementos, número este igual ao número de somandos em $\mathcal{S}_{g^{p^{n-(j-w)}}} + \mathcal{S}_{g^{dp^{n-(j-w)}}}$. O argumento para provar que a equação (6.10) representa a soma $\mathcal{S}_{g^{p^{n-(j-w)}}} + \mathcal{S}_{g^{dp^{n-(j-w)}}}$ será por exclusão.

O grupo $\mathcal{C}_{p^n q}$ pode ser particionado de acordo com as seguintes classes l-ciclotômicas:

$$C_1,\ C_{g^{p^n}},\ C_{g^{p^t}},\ C_{g^{p^t q}},\ \text{e}\ C_{g^{dp^t}},$$

onde $0 \leq t \leq n-1$.

Naturalmente, nenhum dos elementos em (6.10) é igual a 1, o que nos permite excluir a classe C_1. Além disso, afirmamos que nenhum dos elementos de (6.10) pertencem as classes do tipo $C_{g^{p^n}}$ e $C_{g^{p^t q}}$, além das classes $C_{g^{p^h}}$ e $C_{g^{dp^h}}$, com $h \neq n-(j-w)$, uma que vez se isso fosse possível, então os números da forma $(l^r p^{j-w} + l^s q)$, para $0 \leq r \leq \varphi(q)-1$ e $0 \leq s \leq \varphi(p^{j-w})-1$, seriam na verdade múltiplos de p ou de q, o que contradiz o fato de que $mdc(l, pq) = 1$. Portanto, os elementos dados em (6.10) estão distribuídos entre as duas classes, a saber, $\mathcal{S}_{g^{p^{n-(j-w)}}}$ e $\mathcal{S}_{g^{dp^{n-(j-w)}}}$. ∎

Agora estamos aptos para explicitar e^{n-j} como soma de idempotentes primitivos, conforme anunciamos na página 73.

$$e^{n-j} = \theta_{p^j} + \theta_{dp^j}. \tag{6.11}$$

De fato,

$$
\begin{aligned}
e^{n-j} &= \widehat{a^{n-j}} - \widehat{a^{n-j}}\widehat{b} - \widehat{a^{n-(j+1)}} + \widehat{a^{n-(j+1)}}\widehat{b} \\
&= \frac{1}{p^j}\sum_{i=0}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - \frac{1}{p^jq}\sum_{i=0}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\sum_{k=0}^{q-1}\left(g^{p^n}\right)^k - \frac{1}{p^{j+1}}\sum_{t=0}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t \\
&+ \frac{1}{p^{j+1}q}\sum_{t=0}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t\sum_{k=0}^{q-1}\left(g^{p^n}\right)^k \\
&= \frac{1}{p^{j+1}q}\left[pq\sum_{i=0}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - p\sum_{i=0}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\sum_{k=0}^{q-1}\left(g^{p^n}\right)^k - q\sum_{t=0}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t\right. \\
&+ \left.\sum_{t=0}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t\sum_{k=0}^{q-1}\left(g^{p^n}\right)^k\right] \\
&= \frac{1}{p^{j+1}q}\left[(p-1)(q-1) - (p-1)\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k + pq\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - p\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\right. \\
&- (q-1)\sum_{t=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t - p\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k \\
&+ \left.\sum_{t=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k\right] \\
&= \frac{1}{p^{j+1}q}\left[(p-1)(q-1) + pq\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - p\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - q\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\right. \\
&+ \sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i - (p-1)\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k - (q-1)\mathcal{S}_{g^{qp^{n-j-1}}} \\
&- \left.p\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k + \sum_{t=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k\right] \\
&= \frac{1}{p^{j+1}q}\left\{(p-1)(q-1)\left[1+\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^iq}}\right] - (q-1)\mathcal{S}_{g^{qp^{n-j-1}}}\right. \\
&+ \left.\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k\left[-(p-1) + \sum_{t=1}^{p^{j+1}-1}\left(g^{qp^{n-j-1}}\right)^t - p\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\right]\right\} \\
&= \frac{1}{p^{j+1}q}\left\{(p-1)(q-1)\left[1+\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^iq}}\right] - (q-1)\mathcal{S}_{g^{qp^{n-j-1}}}\right. \\
&- \left.(p-1)\left[\sum_{k=1}^{q-1}\left(g^{p^n}\right)^k + \sum_{k=1}^{q-1}\left(g^{p^n}\right)^k\sum_{i=1}^{p^j-1}\left(g^{qp^{n-j}}\right)^i\right] + \sum_{k=1}^{q-1}\left(g^{p^n}\right)^k\mathcal{S}_{g^{qp^{n-j-1}}}\right\}
\end{aligned}
$$

$$= \frac{1}{p^{j+1}q}\left\{(p-1)(q-1)\left[1+\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i q}}\right]-(q-1)\mathcal{S}_{g^{qp^{n-j-1}}}\right.$$
$$-\left.(p-1)\left[\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i}}+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{dp^i}}\right]+\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^{n-j-1}}}+\sum_{i=n-j}^{n}\mathcal{S}_{g^{dp^{n-j-1}}}\right\}.$$

De acordo com [2, Teorema 3], os idempotentes primitivos θ_{p^j} e θ_{dp^j} são dados por:

$$\theta_{p^j} = \frac{(p-1)(q-1)}{2p^{j+1}q}\left[1+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{p^i q}}\right]+\frac{A_{n-1}}{p^{n+j}q}\mathcal{S}_{g^{p^{n-j-1}}}+\frac{B_{n-1}}{p^{n+j}q}\mathcal{S}_{g^{dp^{n-j-1}}}$$
$$-\frac{(p-1)}{2p^{j+1}q}\left[\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i}}+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{dp^i}}\right]-\frac{(q-1)}{2p^{j+1}q}\mathcal{S}_{g^{p^{n-j-1}q}} \tag{6.12}$$

$$\theta_{dp^j} = \frac{(p-1)(q-1)}{2p^{j+1}q}\left[1+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{p^i q}}\right]+\frac{B_{n-1}}{p^{n+j}q}\mathcal{S}_{g^{p^{n-j-1}}}+\frac{A_{n-1}}{p^{n+j}q}\mathcal{S}_{g^{dp^{n-j-1}}}$$
$$-\frac{(p-1)}{2p^{j+1}q}\left[\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i}}+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{dp^i}}\right]-\frac{(q-1)}{2p^{j+1}q}\mathcal{S}_{g^{p^{n-j-1}q}}, \tag{6.13}$$

onde as constantes A_{n-1} e B_{n-1} são dadas por:

$$A_{n-1} := \begin{cases} \dfrac{p^{n-1}(1+\gamma)}{2},\ \gamma^2 = pq & \text{se } l^{\frac{\varphi(p^n q)}{4}} \equiv -1\ (mod\ p^n q)\,; \\ \dfrac{p^{n-1}(1+\delta)}{2},\ \delta^2 = -pq & \text{se } l^{\frac{\varphi(p^n q)}{4}} \not\equiv -1\ (mod\ p^n q)\,. \end{cases}$$

$$B_{n-1} := \begin{cases} \dfrac{p^{n-1}(1-\gamma)}{2},\ \gamma^2 = pq & \text{se } l^{\frac{\varphi(p^n q)}{4}} \equiv -1\ (mod\ p^n q)\,; \\ \dfrac{p^{n-1}(1-\delta)}{2},\ \delta^2 = -pq & \text{se } l^{\frac{\varphi(p^n q)}{4}} \not\equiv -1\ (mod\ p^n q)\,. \end{cases}$$

É simples verificar que $\theta_{p^j} + \theta_{dp^j} = e^{n-j}$, ou seja, podemos expressar todos os idempotentes primitivos da álgebra de grupo $\mathbb{F}_l(\mathcal{C}_{p^n} \times \mathcal{C}_q)$.

Agora vamos verificar quais são as expressões de θ_{p^j} e θ_{dp^j} via λ-técnica. As expressões explícitas dos idempotentes primitivos básicos são calculadas a partir de (6.5). Assim

$$\begin{aligned}
\theta_{p^j} &= \lambda\left(\theta^*_{p^j}\otimes\theta^*_{q^0}\right)+\lambda\left(\theta^{**}_{p^j}\otimes\theta^{**}_{q^0}\right)\\
&= \frac{(p-1)(q-1)}{2p^{j+1}q}\left[1+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{p^iq}}\right]+\underbrace{\frac{\overline{A_{n-1}}}{p^{n+j}q}}_{(*)}\mathcal{S}_{g^{p^{n-j-1}}}+\underbrace{\frac{\overline{B_{n-1}}}{p^{n+j}q}}_{(*)}\mathcal{S}_{g^{dp^{n-j-1}}}\\
&- \underbrace{\frac{(p-1)}{p^{j+1}q}}_{(*)}\left[\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i}}+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{dp^i}}\right]-\underbrace{\frac{(q-1)}{p^{j+1}q}}_{(*)}\mathcal{S}_{g^{p^{n-j-1}q}} \qquad (6.14)
\end{aligned}$$

$$\begin{aligned}
\theta_{dp^j} &= \lambda\left(\theta^{**}_{p^j}\otimes\theta^*_{q^0}\right)+\lambda\left(\theta^{*}_{p^j}\otimes\theta^{**}_{q^0}\right)\\
&= \frac{(p-1)(q-1)}{2p^{j+1}q}\left[1+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{p^iq}}\right]+\underbrace{\frac{\overline{B_{n-1}}}{p^{n+j}q}}_{(*)}\mathcal{S}_{g^{p^{n-j-1}}}+\underbrace{\frac{\overline{A_{n-1}}}{p^{n+j}q}}_{(*)}\mathcal{S}_{g^{dp^{n-j-1}}}\\
&- \underbrace{\frac{(p-1)}{p^{j+1}q}}_{(*)}\left[\sum_{i=n-j}^{n}\mathcal{S}_{g^{p^i}}+\sum_{i=n-j}^{n-1}\mathcal{S}_{g^{dp^i}}\right]-\underbrace{\frac{(q-1)}{p^{j+1}q}}_{(*)}\mathcal{S}_{g^{p^{n-j-1}q}}, \qquad (6.15)
\end{aligned}$$

onde as constantes $\overline{A_{n-1}}$ e $\overline{B_{n-1}}$ são dadas por:

$$\overline{A_{n-1}} := \begin{cases} p^{n-1}\left(1+\sqrt{-pq}\right), & \text{se } p=4k_1+1 \text{ e } q=4k_2+3;\\ p^{n-1}\left(1+\sqrt{pq}\right), & \text{se } p=4k_1+3 \text{ e } q=4k_2+3.\end{cases}$$

$$\overline{B_{n-1}} := \begin{cases} p^{n-1}\left(1-\sqrt{-pq}\right), & \text{se } p=4k_1+1 \text{ e } q=4k_2+3;\\ p^{n-1}\left(1-\sqrt{pq}\right), & \text{se } p=4k_1+3 \text{ e } q=4k_2+3.\end{cases}$$

Em (6.14) e (6.15), os erros da λ-técnica foram destacados por (*) em relação as expressões (6.12) e (6.13), que satisfazem a soma proposta em (6.11), onde observamos que em (6.12) e (6.13) os coeficientes estão divididos por 2. No exemplo calculado na Seção 6.1, por ambas as técnicas, observamos a mesma diferença entre os coeficientes de (6.6) e (6.8). Por estas observações e cálculos de outros exemplos que não apresentamos aqui, podemos afirmar que, para códigos de comprimento p^nq, as expressões corretas para os idempotentes primitivos são as dadas em (6.12) e (6.13).

6.3 Considerações Finais

Neste trabalho apresentamos resultados recentes para o cálculo de idempotentes primitivos a partir das técnicas polinomial e de álgebra de grupo. Ao concretizarmos alguns casos particulares, observamos que ambas as técnicas se complementam. Conseguimos identificar um possível erro no cálculo dos coeficientes dos idempotentes primitivos propostos em [16], no entanto, somente conseguimos propor a correção para códigos de comprimento $p^n q$ (Seção 6.2) com o auxílio das técnicas apresentadas.

Como sequência natural deste trabalho, identificamos vários problemas:

(i) A demonstração correta do Teorema 4.2.4.

(ii) Aprimorar a técnica de álgebra de grupo afim de expressar os idempotentes primitivos sem necessitar do auxílio das técnicas polinomiais.

(iii) Descrever idempotentes primitivos para o caso de grupos metacíclicos e nilpotentes com o auxílio das técnicas de álgebra de grupo desenvolvidas para os casos abelianos.

Referências Bibliográficas

[1] S.K. Arora and M. Pruthi *Minimal cyclic codes of length* $2p^n$. Finite Fields Appl. **5** no. 2 (1999) 177-187.

[2] G.K. Bakshi and M. Raka *Minimal Cyclic Codes of length* p^nq. Finite Fields Appl. **9** no. 4 (2003) 432-448.

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

[4] S.D. Berman, *The number of irreducible representations of a finite group over an arbitrary field*, Dokl. Akad. Nauk. (1956) 106:767-769.

[5] J.J. Bernal, Á. del Río, J.J. Simón, *An intrinsical description of group codes*, Designs, Codes and Cryptography **51**, nº 3 (2009) 289-300

[6] G. Chalom, R. A. Ferraz, M. Guerreiro and C. Polcino Milies *Minimal Binary Abelian Codes of length* p^mq^n. preprint in arXiv:1205.5699.

[7] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

[8] F. S. Dutra, *Sobre Códigos Diedrais e Quatérnios*, Tese de Doutoramento, ICEX-UFMG, Belo Horizonte, 2006.

[9] R. Ferraz *Simple components and central units in group algebras*. J. Algebra, **279** (2004) 191-203.

[10] R. A. Ferraz, M. Guerreiro and C. Polcino Milies *G-equivalence in group algebras and minimal abelian codes*. preprint in arXiv:1203.5742.

[11] R. Ferraz, C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields and their Appl., **13**, (2007) 382-393.

[12] E. Goodaire, E. Jespers, C. P. Milies, *Alternative Loop Rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.

[13] A. Hefez e M.L.T. Vilela, *Códigos Corretores de Erros*, IMPA, Rio de Janeiro, 2002.

[14] T. W. Hungerford, *Algebra*, Springer-Verlag, 1974.

[15] I. M. Isaacs, *Character theory of finite groups*, Dover Publications, New York, 1994.

[16] P. Kumar e S.K. Arora *λ-Mapping and Primitive Idempotents in semi simple ring R_m.* Communications in Algebra, to appear

[17] E. Landau, *Elementary Number Theory*, 2nd Edition, Chelsea Publishing Company, New York, 1966.

[18] F.J. MacWilliams, *Binary codes which are ideals in the group algebra of an abelian group*, Bell System Technical Journal, July-August (1970) 987-1011.

[19] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, The Mathematical Association of America, Vol. 21, 1983.

[20] P.A. Martin, *Grupos, Corpos e Teoria de Galois*, Editora Livraria da Física, São Paulo, 2010.

[21] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th Edition, John Wiley, New York, 1991.

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

[23] M. Pruthi and S.K. Arora *Minimal cyclic codes of prime power length.* Finite Fields Appl. **3** no. 2 (1997) 99-113.

[24] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, 1995.

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

[26] E. Witt, *Die algebraische struktur des gruppenringes eine endlichen gruppe über einen zahlenkörper*, J. Für Math, (1952) 190:231-245.