PEDRO LEONARDO PINTO DE SOUZA

CÓDIGOS DE GRUPO, LCD E AUTO-ORTOGONAIS CONSTRUÍDOS A PARTIR DE P-GRUPOS ABELIANOS FINITOS

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*.

Orientadora: Marinês Guerreiro.

VIÇOSA - MINAS GERAIS
2023

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
S729c
2023

Souza, Pedro Leonardo Pinto de, 1995-
Códigos de grupo, LCD e auto-ortogonais construídos a partir de p-grupos abelianos finitos / Pedro Leonardo Pinto de Souza. – Viçosa, MG, 2023.
1 dissertação eletrônica (108 f.)

Orientador: Marinês Guerreiro.
Dissertação (mestrado) - Universidade Federal de Viçosa, Departamento de Matemática, 2023.
Referências bibliográficas: f. 107-108.
DOI: https://doi.org/10.47328/ufvbbt.2023.548
Modo de acesso: World Wide Web.

1. Grupos abelianos. 2. Teoria dos grupos. I. Guerreiro, Marinês, 1967-. II. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. III. Título.

CDD 22. ed. 512.25

Bibliotecário(a) responsável: Euzébio Luiz Pinto CRB-6/3317

PEDRO LEONARDO PINTO DE SOUZA

CÓDIGOS DE GRUPO, LCD E AUTO-ORTOGONAIS CONSTRUÍDOS A PARTIR DE P-GRUPOS ABELIANOS FINITOS

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

APROVADA: 10 de agosto de 2023

Assentimento:

gov.br Documento assinado digitalmente
PEDRO LEONARDO PINTO DE SOUZA
Data: 14/08/2023 15:52:20-0300
Verifique em https://validar.iti.gov.br

Pedro Leonardo Pinto de Souza
Autor

gov.br Documento assinado digitalmente
MARINES GUERREIRO
Data: 14/08/2023 16:20:51-0300
Verifique em https://validar.iti.gov.br

Marinês Guerreiro
Orientadora

AGRADECIMENTOS

Agradeço, primeiramente, aos meus pais, Ivete e Ernani, por serem os principais responsáveis para que mais esta etapa se concretizasse. Em especial à minha mãe, por todo amor e por sempre ser mais do que eu precisava, não importando o quão difícil fosse. Dedico esse mestrado à você! Agradeço à minha irmã Júlia, por todo apoio, paciência com meus esquecimentos e pela disposição em me ouvir falar sem parar.

Agradeço à minha amiga e companheira, Stefani, por todo amor e carinho. Obrigado por ser tão paciente e me ajudar a lidar com minha cabeça, por vezes, melhor do que eu mesmo. Seu apoio e companheirismo fez esses anos de mestrado parecerem fáceis.

Agradeço à toda minha família, aos meus primos e primas mais próximos. Minhas tias Suzete, Ivone, Elizete e Beatriz; meus tios Tarcísio, Breno e Nenem. Em especial à minha tia Suzete, por tornar a minha vinda e estadia em Viçosa possíveis. Sem você esse mestrado não existiria.

Agradeço aos meus amigos por todo suporte e companheirismo. Em especial ao Hugo, Janaína, Diego e Natália, que mesmo de longe estiveram comigo o tempo todo. Ao João, por tornar Viçosa um lugar familiar e mais agradável, além de todas as conversas e indicações de entretenimento de qualidade. Agradeço a todos os amigos do mestrado, especialmente ao Carlos, por ser o companheiro de mestrado e por toda ajuda nesse tempo.

Agradeço aos professores da graduação Edney e Vinícius, por todo incentivo e ajuda. Obrigado por toda a confiança e todo o trabalho que desempenharam comigo. Vocês sempre farão parte da minha base sólida. Agradeço também à professora Ana Paula, por ser a minha primeira inspiração e por me guiar naqueles que seriam os primeiros passos em direção a este momento.

Agradeço enormemente à minha orientadora, Marinês Guerreiro, por aceitar me orientar e por toda paciência e disponibilidade. Obrigado por me ensinar, incentivar e me inspirar.

Agradeço aos membros da banca avaliadora por aceitarem o convite e por todas as contribuições para a melhoria deste trabalho.

À Universidade Federal de Viçosa, pela oportunidade de realizar a pós-graduação.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

À Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG), pela concessão da bolsa de estudos.

"Lembra que o sono é sagrado e alimenta de horizontes o tempo acordado de viver."

Alberto de Castro Guedes

RESUMO

SOUZA, Pedro Leonardo Pinto de, M.Sc., Universidade Federal de Viçosa, agosto de 2023. **Códigos de grupo, LCD e auto-ortogonais construídos a partir de p-grupos abelianos finitos**. Orientador: Marinês Guerreiro.

Neste trabalho descrevemos os idempotentes primitivos da álgebra de grupo $\mathbb{F}_qG = \mathbb{F}_q(C_{p^m} \times C_{p^n})$, em que C_{p^m} e C_{p^n} são, respectivamente, grupos cíclicos de ordem p^m e p^n. Para tanto, elaboramos alguns exemplos nos quais calculamos os elementos idempotentes a partir da teoria de corpos finitos. Além disso, calculamos os idempotentes, por meio de exemplos, a partir da teoria de grupos. Nosso objetivo é mostrar, na prática, como devemos transitar seguramente entre essas diferentes abordagens, evidenciando as relações entre elas e as consequências nos cálculos dos idempotentes, gerados pela diferença das hipóteses adotadas em cada caso. Por fim, descrevemos todos os códigos abelianos LCD e auto-ortogonais da álgebra de grupo $\mathbb{F}_qG$ a partir dos idempotentes primitivos previamente calculados.

Palavras-chave: Códigos. Idempotentes. Primitivos.

ABSTRACT

SOUZA, Pedro Leonardo Pinto de, M.Sc., Universidade Federal de Viçosa, August, 2023. **Group, LCD and self-orthogonal codes built from finite abelian p-groups**. Adviser: Marinês Guerreiro.

In this work we describe the primitive idempotents of the group algebra $\mathbb{F}_q G = \mathbb{F}_q(C_{p^m} \times C_{p^n})$, with C_{p^m} and C_{p^n} cyclic groups of order p^m and p^n, respectively. To do so, we elaborate on some examples in which we calculate the idempotent elements using finite field theory. Additionally, we calculate these elements in some examples using group theory. Our goal is to demonstrate in practice how to safely navigate between these different approaches, highlighting the relationships between them and the consequences in the computation of idempotents, arising from the differences in the assumptions made in each case. Finally, we describe all linear codes with complementary dual (LCD) and all self-orthogonal abelian codes in the group algebra $\mathbb{F}_q G$ based on the previously computed primitive idempotents.

Keywords: Codes. Idempotents. Primitives.

SUMÁRIO

1 INTRODUÇÃO

A velocidade extraordinária no desenvolvimento de microcomputadores com capacidades de processamento de dados cada vez maiores elevou significativamente a qualidade e a quantidade de transmissão desses dados, impulsionando, quase que naturalmente, o desenvolvimento de códigos corretores de erros com maiores capacidades de detecção e correção. Contudo, essa é apenas uma condição necessária, mas não suficiente para a eficiência de tais códigos.

Um código corretor de erros (cíclico ou abeliano) pode ser construído, teoricamente, como um subespaço vetorial sobre um corpo finito, como um ideal num anel quociente de um anel de polinômios (em uma ou mais indeterminadas) e também estudado como uma extensão de um corpo finito. Mais recentemente, a partir dos trabalhos [4] e [9], dentre muitos outros, se tem procurado estudar esses códigos como ideias de uma álgebra de grupo, não só para grupos cíclicos e abelianos. Deste modo, para se extrair o máximo de informações possíveis sobre um código, é importante que se saiba transitar com segurança entre essas diferentes abordagens e conhecer a relação entre elas. Este é um dos objetivos desta dissertação.

Em muitos trabalhos sobre códigos se menciona a estrutura algébrica de álgebra de grupo, mas efetivamente não se usa essa estrutura para, por exemplo, o cálculo dos parâmetros de um código. Tanto na abordagem via anéis de polinômios quanto na de álgebra de grupos, um código é um ideal gerado por um idempotente. A estrutura de grupo subjacente à álgebra de grupo é um auxiliar importante na identificação dos diferentes idempotentes geradores de códigos e o reticulado de subgrupos pode ser utilizado para classificar os códigos a menos de equivalência, como feito em [8].

O aprimoramento da aplicabilidade da Teoria de Álgebras de Grupo à Teoria de Códigos, nas últimas décadas, permitiu estabelecer assertivamente sob quais condições os idempotentes de uma álgebra de grupo são primitivos ou não. Uma das aplicações destes resultados é identificar possíveis equívocos em afirmações a respeito de produtos de idempotentes primitivos, conforme [22, p. 167].

Sejam $\mathbb{F}_q$ um corpo finito com q elementos e G um p-grupo abeliano finito, com q relativamente primo com p. Um idempotente primitivo de uma álgebra de grupo $\mathbb{F}_qG$ é um elemento $e \in \mathbb{F}_qG$, tal que $e^2 = e$ e é gerador de um ideal minimal desta álgebra de grupo. Uma das motivações que levam ao estudo destes elementos é o fato de que um idempotente da álgebra de grupo $\mathbb{F}_qG$ pode escrito como soma de idempotentes primitivos,

segundo [2], [3] e [19].

Neste trabalho, descrevemos os idempotentes primitivos da álgebra de grupo $\mathbb{F}_qG = \mathbb{F}_q(C_{p^m} \times C_{p^n})$, em que C_{p^m} e C_{p^n} são, respectivamente, grupos cíclicos de ordem p^m e p^n. Para tanto, elaboramos alguns exemplos nos quais calculamos os elementos idempotentes sob as hipóteses e a técnica adotada em [15]. Além disso, calculamos os idempotentes, por meio de exemplos, sob as hipóteses e a técnica adotada em [8] e [9]. Nosso objetivo é mostrar, na prática, como devemos transitar seguramente entre essas diferentes abordagens, evidenciando as relações entre elas e as consequências nos cálculos dos idempotentes, gerados pela diferença das hipóteses adotadas em cada caso. Por fim, descrevemos todos os códigos abelianos LCD e auto-ortogonais da álgebra de grupo $\mathbb{F}_qG$ a partir dos idempotentes primitivos previamente calculados, de acordo com [15].

Apesentamos, no Capítulo 2, a base teórica que fundamenta os resultados referentes à álgebras de grupo que mostramos nesta dissertação. Começamos por apresentar, na Seção 2.1, definições e resultados da teoria de corpos finitos, como a existência e a unicidade (a menos de isomorfismos) de corpos finitos, extensões de corpos ciclotômicas e a decomposição de polinômios ciclotômicos sobre corpos finitos. Esses resultados são primordiais para o cálculo dos idempotentes primitivos por meio da técnica adotada por [5], [14] e [15], que veremos no Capítulo 4. Na Seção 2.2 introduzimos os principais resultados da teoria de módulos que são necessárias para definir uma álgebra de grupo, especialmente a semissimplicidade, pois a partir dela temos uma caracterização de um idempotente primitivo [21]. Na Seção 2.3 apresentamos o Teorema de Wedderburn-Artin em sua forma mais geral, dada por [21]. Este Teorema é um dos resultados mais importante deste trabalho, visto que a partir dele é possível transitar entre as diferentes abordagens que tratamos dos códigos aqui. Na Seção 2.4, introduzimos alguns resultados de anéis de polinômios que usamos, principalmente, nos Capítulos 4 e 5.

No Capítulo 3, apresentamos outros resultados importantes a respeito de álgebras de grupo que utilizamos nesta dissertação. Iniciamos, pela Seção 3.1, com as definições básicas e alguns resultados que estabelecem isomorfismos essenciais para se trabalhar com os elementos de uma álgebra de grupo de maneiras diferentes. Além disso, apresentamos como é a estrutura de um ideal de uma álgebra de grupo. Na Seção 3.2 particularizamos os conceitos de semissimplicidade para álgebras de grupo finitas, exibimos uma versão do Teorema de Wedderburn-Artin mais direcionada para nossos propósitos e discutimos alguns dos principais resultados usados na construção das álgebras de grupo que nos interessam, como um corolário do Teorema de Maschke, que estabelece condições para que uma álgebra de grupo seja semissimples. Todo o trabalho feito nesta seção foi baseado em [21]. Os conceitos apresentados na Seção 3.2 foram particularizados para álgebras de grupo abelianas na Seção 3.3, conforme [21]. Primeiro, descrevemos como se dá a

decomposição de uma álgebra de grupo de um grupo cíclico em ideais minimais bilaterais. Estentendo essas ideias, apresentamos o Teorema de Perlis-Walker, o qual estabelece, como, e sob quais hipóteses, uma álgebra de grupo de um grupo abeliano, não necessariamente cíclico, se decompões como soma direta de ideais minimais bilaterais [21]. Na Seção 3.4 mostramos como são os idempotentes e os idempotentes primitivos de uma álgebra de grupo $\mathbb{F}G$, com $\mathbb{F}$ um corpo finito e G um grupo cíclico de ordem n, além de exibirmos um exemplo de como se calculam esses elementos. Por fim, na Seção 3.5, concatenamos todas as ideias a respeito da decomposição de uma álgebra de grupo como soma direta de seus ideais minimais bilaterais e apresentamos os principais resultados estabelecidos em [9], no qual são determinadas condições necessárias e suficientes para que o número de componentes simples de uma álgebra de grupo seja minimal. Os resultados da Seção 3.5 são extensivamente usados no Capítulo 4.

As principais ideias e argumentações desta dissertação encontram-se no Capítulo 4. Começamos por firmar algumas considerações e convenções que são utilizadas ao longo de todo o capítulo. Na Seção 4.1, descrevemos, a partir da abordagem dada em [15], os idempotentes primitivos de uma álgebra de grupo de um grupo abeliano finito e calculamos estes elementos em um exemplo particular. Além disso, apresentamos alguns resultados importantes enunciados em [15], que são demonstrados e discutidos mais detalhadamente em [5] e [14]. Ainda na Seção 4.1, discutimos, de acordo com a abordagem dada em [9], os resultados necessários para se calcular os idempotentes primitivos por meio da estrutura do grupo e calculamos esses elementos em um exemplo particular. Concluímos a Seção 4.1 discutindo as particularidades observadas nos cálculos desses elementos, quando obtidos a partir da teoria de grupos e a partir da teoria de corpos finitos. Na Seção 4.2, estendemos as ideias apresentadas na Seção 4.1, em ambas as abordagens, generalizando alguns resultados e demonstrando grande parte deles, conforme [8] e [15]. Antes, porém, discutimos, na Subseção 4.2.1, quem são os subgrupos dos grupos $C_{p^2} \times C_p$ e $C_{p^2} \times C_{p^2}$, com o objetivo de conhecer melhor a estrutura dos subgrupos nestes casos particulares para utilizá-los na construção de exemplos na abordagem da teoria de grupos dada em [8]. Por fim, discutimos, num espectro mais geral, as particularidades observadas nos cálculos dos idempotentes primitivos quando se usa a teoria de grupos e a teoria de corpos finitos. Utilizamos exemplos mais elaborados para descrever os idempotentes primitivos em cada caso.

No Capítulo 5, definimos os códigos de grupo e descrevemos todos os códigos abelianos com complementar dual (LCD) e auto-ortogonais abelianos, de acordo com [15]. Na Seção 5.1 introduzimos os principais conceitos a respeito dos códigos corretores de erros e todos os códigos que tratamos nesta dissertação, com base em [2], [3], [11], [12], [18] e [19]. Além disso, introduzimos alguns conceitos que usamos na demonstração de

resultados da Seção 5.2, conforme [6], [15] e [21]. Na seção 5.2, definimos os códigos LCD e auto-ortogonais (de acordo com [15]) e descrevemos todos os códigos desta forma, que são gerados pelos idempotentes primitivos encontrados nos Teoremas 4.2.1, 4.2.2 e 4.2.2.

2 PRELIMINARES ALGÉBRICOS

Neste capítulo, apresentamos os principais conceitos, propriedades e resultados, relativos às estruturas algébricas, que são essenciais para a teoria de códigos. Além disso, firmamos algumas notações que serão usadas ao longo de todo o texto. Este capítulo foi estruturado com base nas referências [13], [16], [20] e [21], as quais também indicamos para maiores detalhes e demonstrações dos resultados que optamos por omitir aqui.

2.1 CORPOS FINITOS

Apresentamos, nesta seção, alguns resultados da teoria de corpos finitos que abordam a construção desses corpos por meio das extensões ciclotômicas e o comportamento das raízes dos polinômios ciclotômicos.

Teorema 2.1.1. *Para todo primo positivo p e todo inteiro positivo n existe um corpo finito com $q = p^n$ elementos. Todo corpo com $q = p^n$ elementos é isomorfo ao corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}$.*

Teorema 2.1.2. *Seja $\mathbb{F}_q$ um corpo finito, com $q = p^n$ elementos, para p finito e $n \in \mathbb{N}^*$. Então todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, em que m é um divisor de n. Reciprocamente, se m é um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Convencionamos, a partir de agora, que $\mathbb{F}_q$ denota um corpo finito com q elementos ao longo de todo o texto.

Teorema 2.1.3. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ de elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Definição 2.1.1. O gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado **elemento primitivo** de $\mathbb{F}_q$.

Observação 2.1.1. A ordem de $\mathbb{F}_q^*$ é igual a $q-1$. Por [16, Teorema 1.15(v)], $\mathbb{F}_q^*$ possui $\phi(q-1)$ geradores, em que ϕ é a função de Euler. Assim, da Definição 2.1.1, $\mathbb{F}_q$ possui $\phi(q-1)$ elementos primitivos.

Definição 2.1.2. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então os elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ são chamados **conjugados** de α com respeito a $\mathbb{F}_q$.

Corolário 2.1.1. *Seja $\alpha \in \mathbb{F}_{q^m}$. Então o **polinômio minimal** de α sobre $\mathbb{F}_q$ é*

$$irr(\alpha, \mathbb{F}_q) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\ldots(x-\alpha^{q^{s-1}}),$$

em que s é o menor inteiro positivo tal que $\alpha^{q^s} = \alpha$.

Observação 2.1.2. Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito a $\mathbb{F}_q$ são distintos se, e somente se, o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau s. Caso contrário, o grau r deste polinômio minimal é um divisor próprio de s e, então, os conjugados de α com respeito a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{r-1}}$, cada um repetido s/r vezes.

Teorema 2.1.4. *Os conjugados de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ possuem a mesma ordem no grupo multiplicativo $\mathbb{F}_q^*$.*

Definição 2.1.3. Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o **traço** $\mathrm{Tr}_{F/K}(\alpha)$ de α sobre K é definido por

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Se K é o subcorpo primo de F, então $\mathrm{Tr}_{F/K}(\alpha)$ é chamado **traço absoluto** de α e simplesmente denotado por $\mathrm{Tr}_F(\alpha)$.

2.1.1 Raízes da unidade e polinômios ciclotômicos

Definição 2.1.4. Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre um corpo $\mathbb{F}$ é chamado n-**ésimo corpo ciclotômico** sobre $\mathbb{F}$ e denotado por $\mathbb{F}^{(n)}$. As raízes de $x^n - 1$ em $\mathbb{F}^{(n)}$ são chamadas **raízes n-ésimas da unidade** sobre $\mathbb{F}$ e o conjunto de todas as raízes é denotado por $\mathbb{E}^{(n)}$.

O conjunto das raízes $\mathbb{E}^{(n)}$ estabelece uma relação com a característica do corpo $\mathbb{F}$.

Teorema 2.1.5. *Seja n um inteiro positivo e $\mathbb{F}$ um corpo de característica p. Então:*

(i) Se p não divide n, então $\mathbb{E}^{(n)}$ é um grupo cíclico de ordem n com respeito a multiplicação em $\mathbb{F}^{(n)}$.

(ii) Se p divide n, escreva $n = mp^{\mathrm{e}}$, com inteiros positivos e, *m, e m não divisível por p. Então $\mathbb{F}^{(n)} = \mathbb{F}^{(m)}$, $\mathbb{E}^{(n)} = \mathbb{E}^{(m)}$ e as raízes de $x^n - 1$ em $\mathbb{F}^{(n)}$ são os elementos de $\mathbb{E}^{(m)}$, cada uma com multiplicidade p^e.*

Definição 2.1.5. Sejam $\mathbb{F}$ um corpo de característica p e n um inteiro positivo não divisível por p. Então um gerador do grupo cíclico $\mathbb{E}^{(n)}$ é chamado **raiz n-ésima primitiva da unidade** sobre $\mathbb{F}$.

Observação 2.1.3. Por [16, Teorema 1.15(v)] — sob as condições da Definição 2.1.5 — existem exatamente $\phi(n)$ raízes n-ésimas primitivas da unidade diferentes sobre $\mathbb{F}$. Se ξ é uma delas, então todas as raízes n-ésimas primitivas da unidade sobre $\mathbb{F}$ são dadas por ξ^s, em que $1 \leq s \leq n$ e $mdc(s, n) = 1$.

Definição 2.1.6. Sejam $\mathbb{F}$ um corpo de característica p, n um inteiro positivo não divisível por p e ξ a raiz n-ésima primitiva da unidade sobre $\mathbb{F}$. Então o polinômio

$$\Phi_n(x) = \prod_{\substack{s=1 \\ mdc(s,n)=1}}^{n} (x - \xi^s)$$

é chamado **n-ésimo polinômio ciclotômico** sobre $\mathbb{F}$.

O grau de $\Phi_n(x)$ é $\phi(n)$ e seus coeficientes pertencem obviamente ao corpo ciclotômico de grau n sobre $\mathbb{F}$.

Teorema 2.1.6. *Sejam $\mathbb{F}$ um corpo de característica p e n um inteiro positivo não divisível por p. Então:*

(i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$;

(ii) os coeficientes de $\Phi_n(x)$ pertencem ao subcorpo primo de $\mathbb{F}$. Se o subcorpo primo de $\mathbb{F}$ é o corpo dos racionais, então os coeficientes de $\Phi(x)$ pertencem a $\mathbb{Z}$.

Demonstração. (i) Cada raiz n-ésima da unidade sobre $\mathbb{F}$ é uma raiz primitiva d-ésima da unidade sobre $\mathbb{F}$, para exatamente um divisor positivo d de n. Em particular, se ξ é uma raiz primitiva n-ésima da unidade sobre $\mathbb{F}$, e ξ^s é uma raiz arbitrária n-ésima da unidade sobre $\mathbb{F}$, então $d = \dfrac{n}{mdc(s,n)}$, isto é, d é a ordem de ξ^s em $E^{(n)}$. Como

$$x^n - 1 = \prod_{s=1}^{n} (x - \xi^s),$$

o resultado segue ao agruparmos, para cada d que divide n, os fatores $(x - \xi^s)$ para os quais ξ^s é uma raiz d-ésima primitiva da unidade sobre $\mathbb{F}$.

(ii) A prova segue por indução sobre n. Com efeito, $\Phi_n(x)$ é um polinômio mônico, assim, para $n = 1$, temos $\Phi_1(x) = x - 1$, e a afirmação é obviamente válida. Para $n > 1$, suponha a proposição válida, para todos os $\Phi_d(x)$, com $1 \leqslant d < n$. Então, a partir de (i), $\Phi_n(x) = \dfrac{x^n - 1}{f(x)}$, em que $f(x) = \prod_{d|n, d<n} \Phi_d(x)$. Pela hipótese de indução, $f(x)$ é um polinômio com coeficientes no subcorpo primo de $\mathbb{F}$, ou em $\mathbb{Z}$, caso a característica de $\mathbb{F}$ seja 0. Usando o algoritmo de Briot-Ruffini para calcular a divisão de $x^n - 1$ pelo polinômio mônico $f(x)$, vemos facilmente que os coeficientes de $\Phi_n(x)$ pertencem ao subcorpo primo de $\mathbb{F}$, ou a $\mathbb{Z}$, respectivamente.

■

Teorema 2.1.7. *O corpo ciclotômico $\mathbb{F}^{(n)}$ é uma extensão algébrica simples de $\mathbb{F}$. Além disso:*

(i) Se $\mathbb{F} = \mathbb{Q}$, então o polinômio ciclotômico Φ_n é irredutível sobre $\mathbb{F}$ e $[\mathbb{F}^{(n)} : \mathbb{F}] = \phi(n)$.

(ii) Se $\mathbb{F} = \mathbb{F}_q$, com $mdc(q, n) = 1$, então Φ_n se decompõe em $\dfrac{\phi(n)}{d}$ polinômios irredutíveis distintos e mônicos em $\mathbb{F}[x]$ com o mesmo grau d. O corpo $\mathbb{F}^{(n)}$ é o corpo de decomposição de qualquer um desses fatores irredutíveis sobre $\mathbb{F}$, e $[\mathbb{F}^{(n)} : \mathbb{F}] = d$, em que d é o menor inteiro positivo tal que $q^d \equiv 1 (\text{mod } n)$, em outras palavras, d é a ordem da classe de q em $\mathbb{Z}_n$, que denotamos por $d = o(q)$.

Demonstração. Se existe uma raiz primitiva ξ de ordem n sobre $\mathbb{F}$, então $\mathbb{F}^{(n)} = \mathbb{F}(\xi)$. Caso contrário, temos a situação descrita no caso (ii) do Teorema 2.1.5, daí $\mathbb{F}^{(n)} = \mathbb{F}^{(m)}$ e o resultado segue novamente. Quanto às demais afirmações, podemos encontrar a prova de (i) em [13, Proposição 8.3]; vamos provar apenas (ii), o caso mais importante para nossos propósitos. Seja η uma raiz n-ésima primitiva da unidade sobre $\mathbb{F}_q$. Então $\eta \in \mathbb{F}_{q^k}$ se, e somente se, $\eta^{q^k} = \eta$, e essa última identidade é equivalente a $q^k \equiv 1 \ (\text{mod} n)$. O menor inteiro positivo para o qual isso vale é $k = d$, para algum divisor d de n, assim, $\eta \in \mathbb{F}_{q^d}$. Consequentemente, η não pode pertencer a nenhum subcorpo próprio de $\mathbb{F}_{q^d}$ Assim, o polinômio minimal de η sobre $\mathbb{F}_q$ tem grau d e, como η é uma raiz arbitrária de Φ_n, os resultados desejados seguem. ■

Suponhamos $1, \xi, \xi^s, \ldots, \xi^{n-1}$ as raízes de $x^n - 1$ sobre $\mathbb{F}$. Para $i = 0, 1, \ldots, n-1$, os conjugados de ξ^i são $\xi^i, \xi^{iq}, \xi^{iq^2}, \ldots, \xi^{iq^{s-1}}$, com s o menor inteiro positivo tal que $\xi^{iq^s} = \xi^i$. Note

$$\xi^{iq^s} = \xi^i \iff \xi^{iq^s - i} = 1 \iff n \mid (iq^s - i) \iff iq^s \equiv i (\text{mod } n).$$

Portanto, podemos usar a condição $iq^s \equiv i \ (\text{mod } n)$ para determinar os conjugados de ξ. Assim, o polinômio minimal da raiz ξ^i (e, portanto, também o das raízes $\xi^{iq}, \ldots, \xi^{iq^{s-1}}$) é o produto

$$m_{\xi^i}(x) = (x - \xi^i)(x - \xi^{iq})(x - \xi^{iq^2}) \ldots (x - \xi^{iq^{s-1}}),$$

com s o menor inteiro positivo tal que $iq^s \equiv i \ (mod \ n)$.

Desta forma, a determinação do polinômio minimal de ξ^i passa pela determinação do conjunto

$$C_j = \{[jq^t] \in \mathbb{Z}_n; \ t \in \mathbb{Z}, \ t \geq 0\},$$

em que cada jq^t é reduzido módulo n, e seus elementos são os expoentes a que devemos elevar ξ para achar todas as raízes do polinômio minimal de ξ^i.

Definição 2.1.7. A j**-ésima classe ciclotômica de** q **módulo** n é

$$C_j = \{j, jq, jq^2, \ldots, jq^{r_i-1}\},$$

em que cada jq^j é reduzido módulo n e r_j é o menor inteiro positivo tal que $jq^{r_j} \equiv j \ (mod\, n)$.

Proposição 2.1.1. *Os conjuntos C_i possuem as seguintes propriedades:*

(i) Se $C_i \cap C_j \neq \emptyset$, então $C_i = C_j$.

(ii) A união de todos C_i é igual a $\mathbb{Z}_n$.

Demonstração. (i) Suponha $C_i \cap C_j \neq \emptyset$. Então existem inteiros não negativos t e s, tais que

$$[iq^t] = [jq^s]. \tag{2.1}$$

Da igualdade (2.1),

$$iq^t \in [jq^s] \Longrightarrow \exists\ k \in \mathbb{Z};\ iq^t = jq^k.$$

Sem perda de generalidade, podemos supor $t \geq k$, assim

$$iq^{t-k} = j \Longrightarrow [j] = [iq^{t-k}] \in C_i. \tag{2.2}$$

Logo, $C_j \subset C_i$. Por outro lado, multiplicando a última igualdade em (2.2) por $[q^r]$, para algum inteiro r tal que $[q^{t-k+r}] = 1$, de modo que $[iq^{t-k+r}] = [i]$, obtemos

$$[i] = [iq^{t-k+r}] = [jq^r] \in C_j.$$

Logo, $C_i \subset C_j$. Portanto, vale a igualdade.

(ii) É imediato que a união de todos os C_j está contido em $\mathbb{Z}_n$, pois cada C_j está contido em $\mathbb{Z}_n$. Por outro lado, sendo $[m] \in \mathbb{Z}_n$ arbitrário, temos $[m] = [mq^0] \in C_m$. Logo $\mathbb{Z}_n$ está contido na união de todos os C_j. Portanto, vale a igualdade.

■

Teorema 2.1.8. *Sejam ξ uma raiz de $x^n - 1$ no menor corpo finito $\mathbb{F}$ de característica p que contém ξ e $m_\xi(x)$ seu polinômio minimal. Sejam ζ um elemento primitivo em $\mathbb{F}$ e $\xi = \zeta^i$. Se u é o menor elemento na i-ésima classe ciclotômica de q módulo n, então*

$$m_\xi(x) = \prod_{k \in C_u} (x - \zeta^k).$$

2.1.2 Outras classes de ciclotomia

Nem sempre é possível encontrar as classes de ciclotomia da maneira que foi abordada anteriormente, uma vez que a fatoração do polinômio $x^n - 1$, com $n \in \mathbb{N}^*$, pode não ser minimal, ou seja, igual a fatoração sobre o corpo dos racionais. Neste caso é necessário definir um conjunto auxiliar e particioná-lo, para só então encontrar as classes de ciclotomia vinculadas a cada uma dessas novas partes, como foi feito em [14] e que mostraremos a seguir.

Sejam l um número primo ímpar e $\mathbb{F}_q$ um corpo finito. Seja $\mathbb{F}_{q^t}$ uma extensão de $\mathbb{F}_q$ de grau t. Considere l e q tais que $mdc(l, q) = 1$, t a ordem multiplicativa de q módulo l. Seja v a maior potência de l tal que $l^v \mid (q^t - 1)$. Para $m \leq v$, existe a seguinte fatoração do polinômio $x^{l^m} - 1$

$$x^{l^m} - 1 = \prod_{j=1}^{l^m} (x - \xi_{l^m}^j), \tag{2.3}$$

em que ξ_{l^m} é a l^m-ésima raiz da unidade em $\mathbb{F}_{q^t}$.

Definição 2.1.8. Sejam $S = \{j;\ 1 \leq j \leq l^m\}$, $S_h = \{j = l^{m-h}u \in S;\ mdc(u, l) = 1\}$ e $\xi_{l^m}^j$, com $1 \leq j \leq l^m$, a j-ésima potência da raiz l^m-ésima primitiva da unidade. Definimos

$$\Psi_h(x) = \prod_{j \in S_h} (x - \xi_{l^m}^j),\ h = 0, 1, \ldots, m.$$

Proposição 2.1.2. *Sejam $S = \{j;\ 1 \leq j \leq l^m\}$ e $S_h = \{j = l^{m-h}u \in S;\ mdc(u, l) = 1\}$. Então*

$$S = \bigcup_{h=0}^{m} S_h.$$

Demonstração. Seja j um elemento de S. Por definição $1 \leq j \leq l^m$. Se $j = l^k$, para algum $k = 0, 1, \ldots, m$, então $j = l^k = l^{m-h}$, para algum $h = 0, 1, \ldots, m$, assim $j \in S_h$, para algum $h = 0, 1, \ldots, m$. Se $j \neq l^k$, para todo $k = 0, 1, \ldots m$, então existe, para cada $h = 0, 1, \ldots, m$, um elemento u, primo com l, tal que $j = l^k u = l^{m-h}u$. Assim, $j = l^{m-h}u \in S_h$, para cada $h = 0, 1, \ldots, m$. Logo $S \subset \bigcup_{h=0}^{m} S_h$. Portanto, vale a igualdade. ■

Para cada $j = l^{m-h}u \in S_h$, com $1 \leq h \leq m$, existe uma q-classe ciclotômica $C_{h,u} = \{j, jq, \ldots, jq^{t-1}\} \subset S_h$, desde que $q^t \equiv 1 \pmod{l^v}$. Assim, existe uma união disjunta

$$S_h = \bigcup_{u=1}^{\frac{\phi(l^h)}{t}} C_{h,u},\ \text{com } |C_{h,u}| = t \text{ e } mdc(u, l) = 1. \tag{2.4}$$

Portanto, cada q-classe ciclotômica $C_{h,u}$ corresponde a um polinômio irredutível sobre $\mathbb{F}_q$, a saber,

$$f_{h,u}(x) = \prod_{\mu=0}^{t-1}(x - \xi_{l^m}^{l^{m-h}uq^\mu}) = \prod_{\mu=0}^{t-1}(x - \xi_{l^h}^{uq^\mu}), \tag{2.5}$$

e S_0 corresponde ao polinômio irredutível $x-1$ sobre $\mathbb{F}_q$. Desta forma, pelo item (ii) do Teorema 2.1.7, o número de fatores irredutíveis de $x^{l^m}-1$ sobre $\mathbb{F}_q$ é:

$$1 + \frac{\phi(l)}{t} + \ldots + \frac{\phi(l^m)}{t} = 1 + \frac{l^m - 1}{t}.$$

2.2 MÓDULOS

A estrutura algébrica módulo é primordial no desenvolvimento da teoria dos anéis de grupo e contém todos os fatos básicos desta teoria como é dito em [21]. Nesta seção apresentamos algumas definições e resultados sobre módulos que serão utilizados no capítulo destinado a teoria dos anéis de grupo.

Definição 2.2.1. Seja R um anel. Um grupo abeliano M (escrito aditivamente) é chamado **R-módulo** (à esquerda) (ou de módulo à esquerda sobre R) se, para cada elemento $a \in R$ e cada $m \in M$, tivermos um produto $am \in M$ tal que, para todos $a, b \in R$ e $m, m_1, m_2 \in M$:

(i) $(a+b)m = am + bm$,

(ii) $a(m_1 + m_2) = am_1 + am_2$,

(iii) $a(bm) = (ab)m$,

(iv) $1m = m$,

De maneira similar, dado um anel R podemos definir um R-módulo à direita considerando a multiplicação de elementos de R por elementos de M pelo lado direito. No que se segue, a menos que seja explicitado, trataremos um R-módulo à esquerda apenas como R-módulo.

Observação 2.2.1. Seja $\mathbb{F}$ um corpo. Da definição de módulos, um $\mathbb{F}$-módulo coincide com a definição de espaço vetorial sobre um corpo $\mathbb{F}$.

Exemplo 2.2.1. Seja L um ideal à esquerda de um anel R. Como o produto de elementos de R por elementos de L está em L, então L pode ser considerado um R-módulo à esquerda. Similarmente, ideias à direita podem ser considerados R-módulos à direita. Em particular, um anel é sempre um módulo sobre si mesmo. Neste caso, consideramos ${}_RR$ um módulo à esquerda sobre o anel R e R_R um módulo à direita sobre o anel R.

Definição 2.2.2. Sejam M e N dois R-módulos. Uma função $f : M \longrightarrow N$ é dita um homomorfismo de R-módulos ou um R-homomorfismo se, para todos $m_1,\ m_2 \in M$ e todo $r \in R$, tem-se

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$;

(ii) $f(rm_1) = rf(m_1)$.

Dizemos que o R-homomorfismo f, definido em 2.2.2, é um **R-epimorfismo**, se f é sobrejetora; é um **R-monomorfismo**, se f é injetora. Além disso, se f é simultaneamente injetora e sobrejetora, então f é chamada **R-isomorfismo**.

Definição 2.2.3. Seja R um anel comutativo. Um R-módulo A é dito uma **R-álgebra** se existe uma multiplicação definida em A tal que, com a adição dada em A e esta multiplicação, A é um anel e tal que a seguinte condição é válida:

$$r(ab) = (ra)b = a(rb),$$

para todos $r \in R$ e $a, b \in A$.

Definição 2.2.4. Seja M um módulo sobre um anel R. Um conjunto não vazio $N \subset M$ é chamado **R-submódulo** de M se as seguintes condições são satisfeitas:

(i) Para todos $x, y \in N$, temos $x + y \in N$.

(ii) Para todo $r \in R$ e todo $n \in N$, temos $rn \in N$.

Se R é comutativo e M é uma R-álgebra, então dizemos que N é uma **R-subálgebra** de M se for, simultaneamente, um submódulo e um subanel de M.

Decorre da definição acima que os submódulos do ${}_RR$-módulo são seus ideias à esquerda.

Definição 2.2.5. Dizemos que M é um módulo **simples** se for não nulo e seus únicos submódulos forem $\langle 0 \rangle$ e M.

Observação 2.2.2. Seja S um subconjunto de elementos de um R-módulo M. Denotaremos por RS o conjunto de todas as somas finitas da forma

$$\sum_{i=1}^{n} x_i s_i = x_1 s_1 + x_2 s_2 + \ldots + x_n s_n,$$

com n um inteiro positivo qualquer e $x_i \in R, s_i \in S$, para $1 \leq i \leq n$.

Definição 2.2.6. Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R-módulo M é chamado **conjunto de geradores** de M, se $M = RS$, isto é, se todo elemento de M pode ser escrito como uma combinação linear (finita) de elementos de S com coeficientes em R.

Definição 2.2.7. Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R módulo M é dito **linearmente independente** (ou, as vezes, R-livre) se, para qualquer combinação linear (finita) de elementos de S com coeficientes em R,

$$r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \ldots + r_{i_t}s_{i_t} = 0 \Longrightarrow r_{i_1} = r_{i_2} = \ldots = r_{i_t} = 0.$$

Definição 2.2.8. Um conjunto $S = \{s_i\}_{i\in I}$ de elementos de um R módulo M é uma **base** de M sobre R (ou, brevemente, R**-base**) se é linearmente independente e um conjunto de geradores de M.

Definição 2.2.9. Um R-módulo M é chamado R**-livre** se tiver uma base.

Definição 2.2.10. Uma família $\{M_i\}_{i\in I}$ de submódulos de um R-módulo M é dita **independente** se, para todo índice $i \in I$ temos

$$M_i \bigcap \left(\sum_{j\neq i} M_j \right) = \langle 0 \rangle.$$

Definição 2.2.11. Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo M. Dizemos que M é a **soma direta (interna)** de um submódulo desta família e escrevemos $M = \oplus_{i\in I} M_i$ se a família é independente e gera M, isto é, se as seguintes condições são satisfeitas:

(i) Para todo $i \in I$, temos $M_i \bigcap \left(\sum_{j\neq i} M_j \right) = \langle 0 \rangle$.

(ii) $M = \sum_{i\in I} M_i$.

Observação 2.2.3. As duas condições da definição acima são equivalentes a:

(iii) Todo elemento $m \in M$ pode ser escrito unicamente como

$$m = m_{i_1} + m_{i_2} + \ldots + m_{i_t};\ m_{i_j} \in M_{i_j},\ 1 \leq j \leq t.$$

Observação 2.2.4. Em particular, se $\{m_i\}_{i\in I}$ é uma base de M, então M é a soma direta

$$M = \oplus_{i\in I} Rm_i.$$

Definição 2.2.12. Um submódulo N de um R-módulo M é um **somando direto** se existe outro submódulo N' de M tal que $M = N \oplus N'$. Um módulo que não contenha somandos diretos não triviais é chamado **indecomponível**.

Definição 2.2.13. Seja $\{M_i\}_{i\in I}$ uma família de R-módulos. A **soma direta (externa)** de módulos desta família, que denotamos por $\oplus_{i\in I}M_i$, é o conjunto de todos os elementos da forma $\{m_i\}_{i\in I}$, com $m_i \in M_i$, para todo $i \in I$, e $m_i = 0$, para quase todo $i \in I$ (exceto para um número finito de índices). Com a adição e a multiplicação de R definida componente a componente, este conjunto é também um R-módulo.

Dado um anel R, denotaremos por $R^{(I)}$ o conjunto de todas as famílias $(r_i)_{i\in I}$, com $r_i \in R$, para todo $i \in I$, e $r_i = 0$ para quase todo $i \in I$ (exceto para um número finito de índices). Note que $R^{(I)}$ é uma soma direta $\oplus_{i\in I}R_i$, em que cada somando é igual a R.

Proposição 2.2.1. *Se M é um R-módulo com base $S = \{s_i\}_{i\in I}$, então M é isomorfo a $R^{(I)}$.*

Proposição 2.2.2. *Seja R um anel. Todo R-módulo M é uma imagem epimórfica de um R-módulo livre, ou seja, para todo R-módulo M, existe um R-módulo livre F e um epimorfismo de R módulos $\varphi : F \longrightarrow \varphi(F)$ tal que $M = \varphi(F)$.*

2.2.1 Semissimplicidade

Uma das razões pela qual diversos resultados acerca dos códigos de grupo foram estabelecidos é a semissimplicidade. A partir dela dela é possível decompor um R-módulo, de modo a obter propriedades importantes dos códigos construídos sobre álgebras de grupo. Os resultados apresentados nesta subseção foram baseados em [21].

Definição 2.2.14. Um R-módulo M é dito **semissimples** se todo submódulo de M é um somando direto.

Teorema 2.2.1. *Seja M um R-módulo. Então as condições abaixo são equivalentes.*

(i) M é semissimples.

(ii) M é um somando direto de submódulos simples.

(iii) M é a soma (não necessariamente direta) de submódulos simples.

Definição 2.2.15. Um anel R é chamado **semissimples** se o módulo ${}_RR$ é semissimples.

Corolário 2.2.1. *Um módulo quociente L de um módulo semissimples M é isomorfo a um submódulo de M e, consequentemente, é semissimples.*

Teorema 2.2.2. *Seja R um anel. Então as seguintes condições são equivalentes:*

(i) Todo R-módulo é semissimples.

(ii) R é um anel semissimples.

(iii) R é a soma direta de um número finito de ideais minimais à esquerda.

Demonstração. (i) $\Longrightarrow$ (ii) Suponha que todo R-módulo seja semissimples. Em particular, ${}_RR$ é semissimples. Logo, pela definição de anel semissimples, R é um anel semissimples.

(ii) $\Longrightarrow$ (iii) Suponha R um anel semissimples. Pelo Teorema 2.2.1 segue ${}_RR$ uma soma direta de submódulos simples e, como seus submódulos são ideais à esquerda de R, então $R = \oplus_{i\in I} L_i$, com L_i um ideal à esquerda de R, para todo $i \in I$. Como L_i é simples, então L_i não possui ideais próprios, logo é minimal, para todo $i \in I$. Deste modo, R é a soma direta de ideais minimais à esquerda de R. Resta provar que esta soma é finita. Note que $1 \in R$, assim, podemos escrevê-lo como $1 = x_{i_1} + x_{i_2} + \ldots + x_{i_n}$, com $x_{i_j} \in L_{i_j}$ e $1 \leq j \leq n$. Daí, dado $r \in R$ arbitrário, temos $r = r1 = rx_{i_1} + rx_{i_2} + \ldots + rx_{i_n}$, com $rx_{i_j} \in L_{i_j}$ e $1 \leq j \leq n$. Logo $R \subset \oplus_{j=1}^{n} L_{i_j}$. Além disso, temos $\oplus_{j=1}^{n} L_{i_j} \subset \oplus_{i\in I} L_i$. Portanto, $R = \oplus_{j=1}^{n} L_{i_j}$.

(iii) $\Longrightarrow$ (ii) Suponha R uma soma direta de ideais minimais à esquerda. Pelo Teorema 2.2.1, R é semissimples.

(ii) $\Longrightarrow$ (i) Seja M um R-módulo. Pela Proposição 2.2.2, existe um R-módulo livre F e um epimorfismo $\varphi : F \longrightarrow \varphi(F)$ tal que $M = \varphi(F)$. Daí, existe uma base $\{a_i\}_{i\in I}$ de F sobre R. Da Definição 2.2.11, $F = \oplus_{i\in I} Ra_i$. Como F é livre, pela Proposição 2.2.1, F é isomorfo a uma soma direta de cópias de R, ou seja, $F = \oplus_{i\in I} Ra_i \cong R^{(I)}$, logo cada $Ra_i \cong R$ é semissimples e, pelo Teorema 2.2.1, F é semissimples. Pelo Corolário 2.2.1, temos $F/Ker\varphi$ um quociente semissimples, mais ainda, $F/Ker\varphi$ é a soma direta de submódulos simples. Como $M \cong F/Ker\varphi$ (Pelo 1º Teorema dos Isomorfismos), então M é, também, a soma direta de submódulos simples. Portanto, M é semissimples.

■

Exemplo 2.2.2. Seja $M_n(D)$ o anel completo das matrizes $n \times n$ sobre um corpo de divisão D. Vamos mostrar que este é um anel semisimples. De fato, considere

$$L_1 = \begin{bmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ & & \cdots & \\ D & 0 & \cdots & 0 \end{bmatrix}, \ldots, L_n = \begin{bmatrix} 0 & 0 & \cdots & D \\ 0 & 0 & \cdots & D \\ & & \cdots & \\ 0 & 0 & \cdots & D \end{bmatrix}.$$

É fácil ver que $L_i, 1 \leq i \leq n$, é um ideal minimal à esquerda de $M_n(D)$ e que $M_n(D) = L_1 \oplus L_2 \oplus \cdots \oplus L_n$. Logo, $M_n(D)$ é semisimples.

Teorema 2.2.3. *Seja R um anel. Então R é semissimples se, e somente se, todo ideal à esquerda L de R é da forma $L = Re$, em que $e \in R$ é um idempotente.*

Demonstração. Seja R um anel semissimples e L um ideal à esquerda de R. Daí existe L' ideal à esquerda de R tal que $R = L \oplus L'$. Como $1 \in R$, podemos escrevê-lo como $1 = x + y$, com $x \in L$ e $y \in L'$. Assim, $x = x1 = x(x + y) = x^2 + xy$. Deste modo, $xy = x - x^2$, logo $xy \in L$. Além disso, $y \in L'$ e $x \in R$ implica em $xy \in L'$. Como $R = L \oplus L'$, segue $L \cap L' = \{0\}$ e, consequentemente, $0 = xy = x - x^2$. Logo $x^2 = x$, isto é, x é um idempotente de R. Resta provar que $L = Rx$.

Dado $a \in L$, temos $a = a1 = a(x + y) = ax + ay$. Daí, $ay = a - ax \in L$, além disso, $ay \in L'$. Deste modo, $ay \in L \cap L' = \{0\}$ e isso implica em $0 = ay = a - ax$. Assim, $a = ax \in Rx$, logo $L \in Rx$. Segue, da hipótese, $Rx \subset L$. Portanto $L = Rx$, com x um idempotente de R.

Reciprocamente, assuma que todo ideal à esquerda L de R seja gerado por um idempotente de R. Por hipótese $L = Re$, para cada ideal $L \subset R$ e $e \in R$ um idempotente. Seja $1 - e \in R$, temos $(1 - e)^2 = 1 - e$, ou seja, $1 - e$ é um idempotente de R. Daí, $L' = R(1 - e)$ é um ideal à esquerda de R.

Note que, para todo $x \in R$, temos $x = x + xe - xe = xe + x(1 - e)$, logo $R = Re + R(1 - e)$. Tome $x \in Re \cap R(1 - e)$. Temos $x = re + s(1 - e)$, com $r, s \in R$. Assim, $xe = ree = re^2 = re = x$ e $xe = s(1 - e)e = se - se^2 = 0$. Logo $x = xe = 0$, consequentemente, $Re \cap R(1 - e) = \{0\}$. Portanto, $R = Re \oplus R(1 - e) = L \oplus L'$, com L um somando direto de R e, pelo Teorema 2.2.2, R é semissimples. ■

Teorema 2.2.4. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples como soma direta de ideais à esquerda minimais. Então existe uma família $\{e_1, e_2, \ldots, e_t\}$ de elementos de R tais que*

(i) $e_i \neq 0$ *é um elemento idempotente para* $1 \leq i \leq t$.

(ii) Se $i \neq j$, *então* $e_i e_j = 0$.

(iii) $1 = e_1 + e_2 + \ldots + e_t$.

(iv) e_i *não pode ser escrito como* $e_i = e_i' + e_i''$, *em que* e_i' *e* e_i'' *são idempotentes tais que* $e_i', e_i'' \neq 0$ *e* $e_i' e_i'' = 0$, *com* $1 \leq i \leq t$.

Demonstração. Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples como soma direta de ideais à esquerda minimais. Escreva $1 = e_1 + e_2 + \ldots + e_t$, com $e_i \in L_i$, para

$1 \leq i \leq t$. Temos

$$\begin{aligned} e_i = e_i 1 &= e_i(e_1 + e_2 + \ldots + e_i + \ldots + e_t) \\ &= e_i e_1 + e_i e_2 + \ldots + e_i^2 + \ldots + e_i e_t \\ &= e_i^2 + e_i(e_1 + e_2 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_t), \end{aligned}$$

para todo $i = 1, 2, \ldots, t$. Assim,

$$e_i(e_1 + e_2 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_t) = e_i - e_i^2 \in L_i,$$

para todo $i = 1, 2, \ldots, t$. Como $e_i(e_1 + e_2 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_t) \in L_1 \oplus \ldots \oplus L_{i-1} \oplus L_{i+1} \oplus \ldots \oplus L_t$, então $e_i - e_i^2 \in L_i \cap (L_1 \oplus \ldots \oplus L_{i-1} \oplus L_{i+1} \oplus \ldots \oplus L_t)$. Por hipótese $L_i \cap (L_1 \oplus \ldots \oplus L_{i-1} \oplus L_{i+1} \oplus \ldots \oplus L_t) = \{0\}$, assim $e_i - e_i^2 = 0$, logo $e_i = e_i^2$, para todo $i = 1, 2, \ldots, t$, ou seja, e_i é um idempotente de R, para todo $i = 1, 2, \ldots, t$. Desta forma, $e_i = e_i^2 + e_i(e_1 + e_2 + \ldots + e_{i-1} + e_{i+1} + \ldots + e_t)$ implica em $e_i e_j = 0$, para $1 \leq i, j \leq t$. Isto prova os itens (i), (ii) e (iii).

Por hipótese e pelo Teorema 2.2.3, temos $L_i = Re_i$, para cada $i = 1, 2 \ldots, t$. Suponha que existam idempotentes e_i' e e_i'' de R tais que $e_i = e_i' + e_i''$ e $e_i' e_i'' = 0$. Daí, Re_i' e Re_i'' são ideais minimais à esquerda de R. Deste modo, $L_i = Re_i = Re_i' + Re_i''$. Se $e_i \in Re_i' \cap Re_i''$, então $e_i = re_i' = se_i''$, para $r, s \in R$. Assim, $e_i e_i' = re_i' e_i' = r(e_i')^2 = re_i' = e_i$ e $e_i e_i' = se_i'' e_i = 0$, logo $e_i = e_i e_i' = 0$, donde $Re_i' \cap Re_i'' = \{0\}$ e, consequentemente, $L_i = Re_i' \oplus Re_i''$, com $Re_i', Re_i'' \neq \langle 0 \rangle$, o que contradiz a minimalidade de L_i, para cada $i = 1, 2, \ldots, t$. Isto prova o item (iv).

Reciprocamente, suponha que exista uma família $\{e_1, e_2, \ldots, e_t\}$ de idempotentes de R satisfazendo os itens $(i), (ii), (iii)$ e (iv). Mostremos que $R = \oplus_{i=1}^t L_i$ é uma decomposição de um anel semissimples como uma soma direta de ideais minimais à esquerda de R. Primeiramente suponha, para todo $1 \leq i \leq t$, que L_i não seja um ideal minimal. Desta forma, existe J_i ideal de R tal que $J_i \subset L_i$, para $1 \leq i \leq t$. Como ${}_RR$ é semissimples e L_i é um submódulo de ${}_RR$, para todo $1 \leq i \leq t$, segue do Teorema 2.2.2, L_i semissimples, para todo $1 \leq i \leq t$. Daí, existe J_i' ideal de L_i tal que $L_i = J_i \oplus J_i'$. Reproduzindo os passos da primeira parte da demonstração do Teorema 2.2.3, conclui-se $e_i = e_i' + e_i''$, com e_i', e_i'' tais que $e_i', e_i'' \neq 0$ e $e_i' e_i'' = 0$, contradizendo o item (iv). Logo $L_i = Re_i$, para cada $1 \leq i \leq t$, e é um ideal minimal. Do item (iii), da mesma forma como feito no Teorema 2.2.2, temos $R = L_1 + L_2 + \ldots + L_t$. Resta provar que esta soma é direta. Para tanto, tome $x \in L_i \cap (\sum_{j \neq i} L_j)$. Daí,

$$x = r_i e_i = \sum_{j \neq i} r_j e_j \Longrightarrow x = r_i e_i = r_i e_i e_i = \sum_{j \neq i} r_j e_j e_i = 0.$$

Logo $L_i \cap (\sum_{j \neq i} L_j) = \{0\}$. Portanto $R = \oplus_{i=1}^t L_i$. ■

Definição 2.2.16. Seja R um anel. Uma família de idempotentes $\{e_1, e_2, \ldots, e_t\}$ satisfazendo as condições $(i), (ii)$ e (iii) do Teorema 2.2.4 é chamada **família completa de idempotentes ortogonais**. Um idempotente satisfazendo as condições anteriores e a condição (iv) do mesmo teorema é chamado **idempotente primitivo**.

Lema 2.2.1. *Sejam L um ideal minimal à esquerda de um anel semissimples R e M um R-módulo simples. Então $LM \neq \langle 0 \rangle$ se, e somente se, $L \cong M$ como R-módulos; neste caso $LM = M$.*

Proposição 2.2.3. *Seja $R = \oplus_{i=1}^{t} L_i$ uma decomposição de um anel semissimples R como soma direta de ideais minimais à esquerda. Então todo R-módulo simples é isomorfo a um dos ideais L_i dados na decomposição.*

2.3 O TEOREMA DE WEDDERBURN-ARTIN

Um dos principais resultados que servem de base para a teoria dos códigos de grupo é o Teorema de Wedderburn-Artin. Veremos ao longo desta dissertação que este teorema pode ser considerado um ponto de interseção entre as diferentes teorias empregadas na determinação de códigos de p-grupo, tornando-o uma peça fundamental na construção de pontes entre tais teorias.

Lema 2.3.1. *Seja L um ideal minimal à esquerda de um anel semissimples R. Então a soma de todos os ideais à esquerda de R isomorfos a L é um ideal bilateral de R.*

Demonstração. Defina a soma $A = \sum_{J \cong L} J$, em que cada J é um ideal à esquerda de R. Como a soma de ideais à esquerda é também um ideal à esquerda, então A é um ideal à esquerda de R. Resta provar que A é também um ideal à direita de R. Pelo Teorema 2.2.2 podemos escrever $R = \oplus_{i=1}^{t} L_i$, com L_i um ideal minimal à esquerda, para cada $1 \leq i \leq t$. Assim, $AR = \sum_{J \cong L} JR = \sum_{J \cong L} \sum_{i=1}^{t} JL_i$, donde $JL_i = \langle 0 \rangle$ ou $JL_i = L_i$. Pelo Lema 2.2.1, a última igualdade ocorre se, e somente se, $J \cong L_i$. Daí, $L_i \cong L$ implica em $L_i \subset A$, assim $AR = \sum_{J \cong L} \sum_{i=1}^{t} JL_i \subset A$, logo A é também um ideal à direita de R. Portanto, $A = \sum_{J \cong L} J$ é um ideal bilateral de R. ■

Lema 2.3.2. *Seja I um ideal bilateral de um anel semissimples contendo um ideal minimal à esquerda L. Então I contém todos os ideais à esquerda isomorfos a L.*

Proposição 2.3.1. *Sejam L um ideal minimal à esquerda de um anel semissimples R e B a soma direta de todos os ideais à esquerda de R isomorfos a L. Então B é um ideal minimal bilateral de R.*

Demonstração. Por hipótese e pelo Lema 2.3.1, B é um ideal bilateral de R. Mostremos que B é minimal. Sejam B_1 um ideal bilateral de R contido em B e L_1 um ideal minimal à esquerda de R contido em B_1. Suponha $L_1 \ncong L$. Temos, pelo Lema 2.2.1, $L_1L = \langle 0 \rangle$, assim $L_iJ = \langle 0 \rangle$, para todo $J \cong L$, consequentemente, $L_1B = \langle 0 \rangle$. Como $L_1 \subset B$, segue $L_1L_1 = \langle 0 \rangle$. Por outro lado, o fato de L_1 ser um ideal minimal à esquerda de R implica, pelo Teorema 2.2.3, na existência de um elemento idempotente de R em L_1, contradizendo $L_1 = \langle 0 \rangle$, logo $B_1 \neq \langle 0 \rangle$ e $L_1 \cong L$.

Agora observe que $L_1 \subset B_1$ implica, pelo Lema 2.3.2, que B_1 contém todos os ideais à esquerda de R. Logo $B_1 \supset \sum_{J \cong L} J = B$. Portanto B é minimal. ■

Dada a decomposição de R como soma direta de ideais minimais à esquerda, podemos reagrupar os ideais minimais dessa soma de modo a obter classes de isomorfismos desses ideais, ou seja,

$$\begin{aligned} R &= L_1 \oplus \ldots \oplus L_t \\ &= (L_{11} \oplus \ldots \oplus L_{1r_1}) \oplus (L_{21} \oplus \ldots \oplus L_{2r_2}) \oplus \ldots \oplus (L_{s1} \oplus \ldots \oplus L_{sr_s}), \end{aligned} \tag{2.6}$$

com $r_1 + r_2 + \ldots + r_s = t$, em que $L_{in} \cong L_{im}$ e $L_{ik}L_{jh} = \langle 0 \rangle$ se $i \neq j$, de acordo com o Lema 2.2.1. Além disso, da Proposição 2.2.3, todo ideal minimal à esquerda de R é isomorfo a algum dos ideais de R dados na decomposição (2.6).

Teorema 2.3.1. *Com a notação acima, seja A_i a soma de todos os ideais à esquerda de R isomorfos a L_{i1}, com $1 \leq i \leq s$. Então:*

(i) cada A_i é um ideal minimal bilateral de R.

(ii) $A_iA_j = \langle 0 \rangle$, se $i \neq j$.

(iii) $R = \oplus_{i=1}^{s} A_i$ como anéis, em que s é o número de classes de isomorfismos de ideais minimais à esquerda de R.

Demonstração. (i) Da observação acima, L_{i1}, $1 \leq i \leq s$, é um ideal minimal de R. Logo, pela Proposição 2.3.1, A_i é um ideal minimal bilateral de R, para todo $1 \leq i \leq s$.

(ii) Escreva $R = (L_{11} \oplus \ldots \oplus L_{1r_1}) \oplus (L_{21} \oplus \ldots \oplus L_{2r_2}) \oplus \ldots \oplus (L_{s1} \oplus \ldots \oplus L_{sr_s})$ como na observação anterior. Dado $x \in R$, temos $x = x_{11} + \ldots + x_{1r_1} + x_{21} + \ldots + x_{2r_2} + \ldots + x_{s1} + \ldots + x_{sr_s}$, com $x_{ij} \in L_{ij}$, para $1 \leq i \leq s$ e $1 \leq j \leq t$. Tome $y_i = x_{i1} + \ldots + x_{ir_i}$, com $1 \leq i \leq s$. Como $L_{i1} + \ldots + L_{ir_i} \subset A_i$, então $y_i \in A_i$, para cada $1 \leq i \leq s$, e $x = y_1 + y_2 + \ldots + y_s$. Logo $R = A_1 + A_2 + \ldots + A_s = \sum_{J_1 \cong L_{11}} J_1 + \ldots + \sum_{J_s \cong L_{s1}} J_s$. Daí,

$A_iA_j = \left(\sum_{J_i\cong L_{i1}} J_i \sum_{J_j\cong L_{j1}} J_j\right)$. Como $L_{ik} \subset A_i,\ 1 \leq k \leq r_i;\ L_{jh} \subset A_j,\ 1 \leq h \leq r_j$ e $J_i \cong L_{ik},\ J_j \cong L_{jh}$, então $L_{ik}L_{jh} = \langle 0\rangle$ implica em $J_iJ_j = \langle 0\rangle$ para todo $i \neq j$. Portanto, $A_iA_j = \langle 0\rangle$ se $i \neq j$.

(iii) Suponha que exista $x = y_1 + y_2 + \ldots + y_s \in A_i \bigcap \sum_{j\neq i} A_j$. Daí, $y_i \in A_i$ e $y_i \in A_j$, para todo $i \neq j$. Assim, $y_i = x_{i1} + \ldots + x_{ir_i} \in L_{j1} \oplus \ldots \oplus L_{jr_j}$ e, consequentemente, $x_{ik} \in L_{ik} \cap L_{jh},\ 1 \leq k \leq r_i,\ 1 \leq h \leq r_j$. Como $L_n \cap L_m = \{0\}$, para todo $n \neq m$ e $1 \leq n, m \leq t$, então $L_{ik} \cap L_{jh} = \{0\}$, para todo $i \neq j$. Logo $x_{ik} = 0$ se $i \neq j$, e daí $y_i = 0$, para todo $1 \leq i \leq s$. Portanto, $x = 0$ e a soma é direta.

■

Definição 2.3.1. Um anel R é dito **simples** se seus únicos ideais bilaterais são $\langle 0\rangle$ e R.

Proposição 2.3.2. *Seja D um anel de divisão e seja n um inteiro positivo. Então o anel de matrizes completo $M_n(D)$ não contém ideais próprios.*

Pela Proposição 2.3.2 e a Definição 2.3.1, $M_n(D)$ é um anel simples.

Corolário 2.3.1. *Os ideais A_i, com $1 \leq i \leq s$, definidos no Teorema 2.3.1 são anéis simples.*

Observação 2.3.1. Os ideais bilaterais construídos no Teorema 2.3.1 determinam completamente todos os ideais bilaterais de R.

Proposição 2.3.3. *Seja $R = \oplus_{i=1}^{s} A_i$ uma decomposição de um anel semissimples R como soma direta de ideais minimais bilaterais. Então*

(i) Todo ideal bilateral I de R pode ser escrito da forma

$$I = A_{i1} \oplus \ldots \oplus A_{it},\ \text{com } 1 \leq i_1 \leq \ldots \leq i_t \leq s.$$

(ii) Se $R = \oplus_{i=1}^{r} B_i$ é uma outra decomposição de R como soma direta de ideais minimais bilaterais, então $s = r$ e, com um ajuste nos índices, $A_i = B_i$, para todo i.

Demonstração. (i) Seja I um ideal bilateral de R. Temos $I \subset R = A_1 \oplus \ldots \oplus A_s$, assim $I = (A_1 \cap I) \oplus \ldots \oplus (A_s \cap I)$. Como A_i é minimal e $A_i \cap I$ é um ideal de A_i, para cada $1 \leq i \leq s$, então $A_i \cap I = \langle 0\rangle$ ou $A_i \cap I = A_i$. Logo, $I = \langle 0\rangle$ ou $I = A_{i1} \oplus \ldots \oplus A_{it}$.

(ii) Por hipótese $R = A_1 \oplus \ldots \oplus A_s$. Daí, $B_1 \oplus \ldots \oplus B_r = A_1 \oplus \ldots \oplus A_s$, para todo $1 \leq j \leq r$. Assim, temos $B_j = B_j \cap A_1 \oplus \ldots \oplus B_j \cap A_s$. A_i é minimal, para todo $1 \leq i \leq s$, e a soma é direta, logo $B_j \cap A_i = \langle 0\rangle$ ou $B_j \cap A_i = A_i$, para cada

$1 \leq j \leq r$ e $1 \leq i \leq s$. Como B_j também é minimal e soma é direta, então, para cada $1 \leq j \leq r$, $B_j \cap A_i = B_j$, para algum $1 \leq i \leq s$, e $B_j \cap A_k = \langle 0 \rangle$, para todo $k \neq i$. Logo, para cada $1 \leq j \leq r$, temos $B_j = A_i$, para algum $1 \leq i \leq s$. Portanto $r = s$ e, reorganizando os índices, temos $A_i = B_i$, para cada $1 \leq i \leq s$.

■

Definição 2.3.2. Os ideais minimais bilaterais de um anel semissimples R são chamados **componentes simples** de R.

Definição 2.3.3. O conjunto

$$\mathcal{Z}(R) := \{r \in R;\ rx = xr,\ \forall\ x \in R\}$$

é chamado **centro de** R e seus elementos são ditos **centrais**.

Teorema 2.3.2. *Seja $R = \oplus_{i=1}^{s} A_i$ uma decomposição de um anel semissimples de R como soma direta de ideais minimais bilaterais. Então existe uma família $\{e_1, \ldots, e_s\}$ de elementos de R tais que:*

(i) $e_i \neq 0$ *é um idempotente central, para* $1 \leq i \leq s$.

(ii) Se $i \neq j$, *então* $e_i e_j = 0$.

(iii) $1 = e_1 + \ldots + e_s$.

(iv) e_i *não pode ser escrito como* $e_i = e_i' + e_i''$, *em que* e_i' *e* e_i'' *são idempotentes tais que* $e_i', e_i'' \neq 0$ *e* $e_i' e_i'' = 0, 1 \leq i \leq s$.

Demonstração. A demonstração deste resultado é idêntica à do Teorema 2.2.4, exceto pelo fato de termos que provar que os idempotentes são centrais, ou seja, pertencem ao centro de R. Para tanto, tome $x \in R$. Temos, por (iii), $x = xe_1 + \ldots + xe_s = e_1x + \ldots + e_sx$. Como A_i é um ideal bilateral, para todo $1 \leq i \leq s$, e os idempotentes são ortogonais, então

$$\begin{aligned} xe_i &= e_ixe_i + (e_1x + \ldots + e_{i-1}x + e_{i+1}x + \ldots + e_sx)e_i \\ &= e_i^2x + e_i(e_1x + \ldots + e_{i-1}x + e_{i+1}x + \ldots + e_sx) \\ &= e_ix + e_ie_1x + \ldots + e_ie_{i-1}x + \ldots + e_ie_{i-1}x + e_ie_{i+1}x + \ldots + e_ie_sx \\ &= e_ix, \text{ para todo } 1 \leq i \leq s. \end{aligned}$$

Portanto, os idempotentes e_i, para $1 \leq i \leq s$, são centrais. ■

Definição 2.3.4. Os elementos $\{e_1, \ldots, e_s\}$ do Teorema 2.3.2 são chamados **idempotentes centrais primitivos** de R.

Teorema 2.3.3 (Teorema de Wedderburn-Artin)**.** *Um anel R é semissimples se, e somente se, é isomorfo a uma soma direta de álgebras de matrizes sobre anéis de divisão:*

$$R \cong M_{n_1}(D) \oplus \ldots \oplus M_{n_s}(D).$$

2.4 ANÉIS DE POLINÔMIOS

Nesta seção apresentamos alguns resultados da teoria de anéis de polinômios que utilizaremos nos próximos capítulos. A principal referência base desta seção é [13].

Seja $\mathbb{F}_q$ um corpo finito. Ao longo de todo o texto, denotamos por $\mathbb{F}_q[x]$ o anel de polinômios sobre o corpo $\mathbb{F}_q$. Em alguns momentos omitimos a indeterminada de um polinômio $f(x)$ em $\mathbb{F}_q[x]$ e o denotamos apenas por f, a fim de não sobrecarregar a notação.

Teorema 2.4.1. *Todo ideal de $\mathbb{F}_q[x]$ é principal, ou seja, é da forma $I = \langle g(x)\rangle$, com $g(x) \in \mathbb{F}_q[x]$.*

Demonstração. Seja I um ideal de $\mathbb{F}_q[x]$. Se $I = \{0\}$, então $I = \langle 0\rangle$. Se $I \neq \{0\}$, considere $g(x) \in I$ não nulo, de modo que $g(x)$ tenha o menor grau possível em I, (o que é possível, pois o conjunto formado pelos graus dos polinômios de I é não vazio, logo, pelo princípio da boa ordenação, I possui um menor elemento), assim, $\langle g(x)\rangle \subset I$.

Seja $f(x) \in I$. Pelo algoritmo da divisão polinomial, existem únicos $q(x), r(x) \in \mathbb{F}_q[x]$, tais que

$$f(x) = g(x)q(x) + r(x), \quad \text{com } r(x) = 0 \ \text{ ou } \ \partial(r(x)) < \partial(g(x)).$$

Então

$$r(x) = f(x) + g(x)(-q(x)) \in I.$$

Se $r(x) \neq 0$, então teríamos um polinômio de I com grau menor do que o grau de $g(x)$, contradizendo a minimalidade do grau de $g(x)$. Logo, $r(x) = 0$ e $f(x) = g(x)q(x) \in \langle g(x)\rangle$, donde segue $I \subset \langle g(x)\rangle$. Portanto, $I = \langle g(x)\rangle$. ■

Corolário 2.4.1. *Seja $I \neq \{0\}$ um ideal de $\mathbb{F}_q[x]$. Então existe um único polinômio mônico $g(x)$ em I (de grau mínimo) tal que $I = \langle g(x)\rangle$.*

Demonstração. Desde que $I \neq \{0\}$, segue, do Teorema 2.4.1, $I = \langle f(x)\rangle$, com $f(x) \in \mathbb{F}_q[x]$. Como todo polinômio é associado a apenas um único polinômio mônico, existem únicos $g(x) \in \mathbb{F}_q[x]$ e $a \in \mathbb{F}_q^*$, com $g(x)$ mônico, tais que $f(x) = ag(x)$. Logo, $\langle f(x)\rangle \subset \langle g(x)\rangle$. Por outro lado, temos

$$g(x) = a^{-1}f(x) \iff g(x) \in \langle f(x)\rangle \iff \langle g(x)\rangle \subset \langle f(x)\rangle.$$

Portanto $I = \langle g(x)\rangle = \langle f(x)\rangle$. ■

Seja o anel quociente

$$\frac{\mathbb{F}_q[x]}{\langle p(x)\rangle} = \{\overline{r(x)};\ r(x) \in \mathbb{F}[x],\ \text{com } r(x) = 0,\ \text{ou } \partial(r(x)) < n\}, \tag{2.7}$$

em que $\overline{r(x)} = \{r(x) + t(x)p(x);\ t(x) \in \mathbb{F}_q[x]\}$ denota a classe de $r(x)$ em $\dfrac{\mathbb{F}_q[x]}{\langle p(x)\rangle}$. Neste anel quociente, a adição e a multiplicação são dados por

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)};$$

$$\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)},$$

para todos $\overline{f(x)},\ \overline{g(x)} \in \dfrac{\mathbb{F}_q[x]}{\langle p(x)\rangle}$. Além disso, dados $\lambda \in \mathbb{F}_q$ e $\overline{f(x)} \in \dfrac{\mathbb{F}_q[x]}{\langle p(x)\rangle}$, temos $\lambda\overline{f(x)} = \overline{\lambda f(x)} \in \dfrac{\mathbb{F}_q[x]}{\langle p(x)\rangle}$. Com essas operações, $\dfrac{\mathbb{F}_q[x]}{\langle p(x)\rangle}$ é um espaço vetorial de dimensão $n = \partial(p(x))$ sobre o corpo $\mathbb{F}_q$, sendo $\{1, \bar{x}, \ldots, \overline{x^{n-1}}\}$ uma base para este espaço vetorial.

Observação 2.4.1. Se $r_1(x), r_2(x) \in \mathbb{F}_q[x]$, com $\partial(r_1(x)) < n$ e $\partial(r_2(x)) < n$, são tais que $r_1(x) \neq r_2(x)$, então $\overline{r_1(x)} \neq \overline{r_2(x)}$. De fato, suponha (por contradição) $\overline{r_1(x)} = \overline{r_2(x)}$, com $r_1(x) \neq r_2(x)$. Temos

$$\begin{aligned} \overline{r_1(x)} = \overline{r_2(x)} &\implies \overline{r_1(x)} - \overline{r_2(x)} = \bar{0} \implies \overline{r_1(x) - r_2(x)} = \overline{p(x)} \implies \\ &\implies r_1(x) - r_2(x) = p(x)q(x) \implies \\ &\implies n > \partial(r_1(x) - r_2(x)) = \partial(p(x)q(x)) \geq n, \end{aligned}$$

o que é uma contradição. Logo $r_1(x) = r_2(x)$.

Seja $\mathbb{F}_q$ um corpo finito. Definimos o anel $\mathcal{R}_n$ por

$$\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}. \tag{2.8}$$

Pelas Observação 2.4.1, o anel quociente $\mathcal{R}_n$ é um espaço vetorial de dimensão $n = \partial(p(x))$ sobre o corpo $\mathbb{F}_q$, sendo $\{1, \bar{x}, \ldots, \overline{x^{n-1}}\}$ uma base de $\mathcal{R}_n$.

Teorema 2.4.2. *Todo ideal de $\mathcal{R}_n$ é da forma $I = \langle\overline{f(x)}\rangle$, em que $f(x)$ é um divisor de $p(x)$.*

Demonstração. Seja I um ideal de $\mathcal{R}_n$. Defina o conjunto

$$J = \{g(x) \in \mathbb{F}_q[x];\ \overline{g(x)} \in I\}.$$

Temos $\overline{p(x)} \in I$, logo J é um conjunto não-vazio por definição. Sejam $g_1(x), g_2(x) \in J$, mostremos que $g_1(x) - g_2(x) \in J$. De fato, temos

$$g_1(x), g_2(x) \in J \iff \overline{g(x)}, \overline{g_2(x)} \in I.$$

Logo,

$$\overline{g_1(x) - g_2(x)} = \overline{g_1(x)} - \overline{g_2(x)} \in I,$$

consequentemente, $g_1(x) - g_2(x) \in J$.

Mostremos agora que, para $g(x) \in J$ e $h(x) \in \mathbb{F}_q[x]$, temos $g(x)h(x) \in J$. Com efeito,

$$\begin{aligned} g(x) \in J,\ h(x) \in \mathbb{F}_q[x] &\implies \overline{g(x)} \in I \quad \text{e} \quad \overline{h(x)} \in \mathcal{R}_n \\ &\implies \overline{g(x)h(x)} \in I \\ &\implies g(x)h(x) \in J. \end{aligned}$$

Portanto, J é um ideal de $\mathbb{F}_q[x]$.

Falta mostrarmos que I é um ideal principal. Pelo Teorema 2.4.1, existe $f(x) \in \mathbb{F}_q^*[x]$ tal que $J = \langle f(x) \rangle$. Como $p(x) \in J$, existe $q(x) \in \mathbb{F}_q[x]$ tal que $p(x) = f(x)q(x)$. Além disso, $J = \langle f(x) \rangle$ implica em $\overline{g(x)} = \overline{h(x)f(x)} = \overline{f(x)h(x)}$. Logo,

$$I = \left\{ \overline{f(x)h(x)};\ \overline{h(x)} \in \mathcal{R}_n \right\} = \langle \overline{f(x)} \rangle,$$

como queríamos. ■

Suponha $mdc(n, q) = 1$ e seja $x^n - 1 = f_1 f_2 \cdots f_t$ a decomposição de $x^n - 1$ como um produto de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$. Como $mdc(n, q) = 1$, o polinômio $x^n - 1$ é separável sobre $\mathbb{F}_q$ e temos $f_i \neq f_j$, se $i \neq j$. Ao longo de toda esta seção, os polinômios denotados por f_i, para $1 \leq i \leq t$, são os polinômio irredutíveis dados na decomposição de $x^n - 1$ sobre $\mathbb{F}_q$.

Teorema 2.4.3. *Seja $I = \langle \overline{g(x)} \rangle$ um ideal de $\mathcal{R}_n$, com $g(x)$ um divisor de $x^n - 1$, e seja $h(x) = \dfrac{x^n - 1}{g(x)}$. Então $g(x)$ e $h(x)$ são coprimos e existem $r(x), s(x)$ em $\mathbb{F}_q[x]$ tais que*

$$r(x)g(x) + s(x)h(x) = 1.$$

Além disso, $e(x) = r(x)g(x)$ e temos $\langle \overline{e(x)} \rangle = \mathcal{R}_n \overline{e(x)}$ e $\overline{e(x)}^2 = \overline{e(x)}$, donde $\overline{c(x)}\ \overline{e(x)} = \overline{c(x)}$, para todo $\overline{c(x)} \in R_n$, isto é, todo ideal I de $\mathcal{R}_n$ é gerado por um idempotente $\overline{e(x)}$ que é a identidade de I.

Demonstração. Seja $I = \langle \overline{g} \rangle$ em $\mathcal{R}_n$. Daí, $g(x) \mid (x^n - 1)$ e, consequentemente, $g(x) = f_1^{m_1}(x) f_2^{m_2}(x) \dots f_t^{m_t}(x)$, com $m_j = 0$ ou $m_j = 1$, para $1 \leq j \leq t$. Seja $h = \dfrac{x^n - 1}{g}$. Temos $mdc(g(x), h(x)) = 1$. Dessa forma, existem $r(x), s(x) \in \mathbb{F}_q[x]$ tais que

$$r(x)g(x) + s(x)h(x) = 1 \text{ em } \mathbb{F}_q[x].$$

Considere $e(x) = r(x)g(x)$. Então,

$$\begin{aligned} r(x)g(x)[r(x)g(x) + s(x)h(x)] = r(x)g(x) &\implies e(x)^2 + r(x)s(x)g(x)h(x) = e(x) \\ &\implies e(x)^2 + r(x)s(x)\,(x^n - 1) = e(x) \\ &\implies \overline{e(x)^2} = \overline{e(x)} \text{ em } \mathcal{R}_n. \end{aligned}$$

Logo $\overline{e(x)}$ é um idempotente de R_n. Como $mdc(r(x), h(x)) = 1$, temos

$$\begin{aligned} g(x)r(x)g(x) + s(x)(x^n - 1) = g(x) &\implies \overline{g(x)r(x)g(x)} = \overline{g(x)} \\ &\implies \overline{g(x)e(x)} = \overline{g(x)} \\ &\implies \overline{g(x)} \in \mathcal{R}_n\overline{e(x)} = \langle \overline{e(x)} \rangle \\ &\implies \langle \overline{g(x)} \rangle \subset \langle \overline{e(x)} \rangle. \end{aligned}$$

Como $e(x) = r(x)g(x)$, então $\langle \overline{e(x)} \rangle \subset \langle \overline{g(x)} \rangle$. Logo, $I = \langle \overline{g(x)} \rangle = \langle \overline{e(x)} \rangle$. Além disso, dado $\overline{c(x)} \in \langle \overline{e(x)} \rangle$, temos $\overline{c(x)e(x)} = \overline{a(x)e(x)}^2 = \overline{a(x)c(x)}$, para todo $\overline{c(x)} \in I$. Em razão disso, se existir $\overline{f(x)} \in \mathcal{R}_n$ tal que $\langle \overline{f(x)} \rangle = I$, então $\overline{e(x)} = \overline{f(x)e(x)} = \overline{f(x)}$. Logo, $\overline{e(x)} \in \mathcal{R}_n$ e é único. Portanto, $\overline{e(x)}$ é a identidade em I. ■

Teorema 2.4.4. *Se $\overline{e(x)} \in \mathcal{R}_n$ é tal que $\overline{e(x)}^2 = \overline{e(x)}$ e $I = \langle \overline{e(x)} \rangle$, então I é gerado por $\overline{g(x)} \in \mathcal{R}_n$, tal que*

$$g(x) = mdc(e(x), x^n - 1). \tag{2.9}$$

Demonstração. Pelo Teorema 2.4.3, temos $x^n - 1 = h(x)g(x)$ e $e(x) = r(x)g(x)$, com $h(x)$ e $g(x)$ primos entre si. Logo, $mdc(r(x)g(x), h(x)g(x)) = mdc(e(x), x^n - 1) = g(x)$. ■

Proposição 2.4.1. *O ideal $\mathcal{N}_i = \langle \overline{f_i(x)} \rangle$ é um ideal maximal de $\mathcal{R}_n$, para cada $1 \leq i \leq t$.*

Demonstração. Suponha que exista um ideal $J = \langle \overline{g(x)} \rangle$ de $\mathcal{R}_n$ contendo $\mathcal{N}_i = \langle \overline{f_i(x)} \rangle$, para cada $1 \leq i \leq t$. Como $\mathcal{N}_i \subset J$, temos $\overline{f_i(x)} \in \langle \overline{g(x)} \rangle$, assim, existe $s(x) \in \mathcal{R}_n$ tal que

$$\begin{aligned} \overline{f_i(x)} = \overline{s(x)g(x)} &\implies f_i(x) - s(x)g(x) \in \langle x^n - 1 \rangle \\ &\implies x^n - 1 \mid [f_i(x) - s(x)g(x)] \\ &\implies f_i(x) - s(x)g(x) = t(x)(x^n - 1); \text{ com } t(x) \in \mathbb{F}_q[x] \\ &\implies f_i(x) = g(x)\left[t(x)\frac{(x^n - 1)}{g(x)} + s(x)\right] \end{aligned}$$

$$\implies \quad g(x) \mid f_i(x) \text{ em } \mathbb{F}_q[x].$$

Como $f_i(x)$ é irredutível em $\mathbb{F}_q[x]$, então $g(x) = 1$ ou $g(x) = f_i(x)$. Logo, $J = \mathcal{R}_n$ ou $J = \mathcal{N}_i$ e, portanto, $\mathcal{N}_i$ é maximal. ■

Proposição 2.4.2. *O ideal $\mathcal{M}_i$ gerado pela classe módulo $x^n - 1$ do polinômio $\widehat{f}_i(x) = \dfrac{x^n - 1}{f_i(x)}$ é um ideal minimal de $\mathcal{R}_n$, para $1 \leq i \leq t$.*

Demonstração. Seja J um ideal de $\mathcal{R}_n$ gerado pelo elemento $\overline{g(x)}$ tal que $0 \subset J \subset \mathcal{M}_i$. Como $g(x) \mid (x^n - 1)$, então $g(x) = f_1^{m_1}(x) f_2^{m_2}(x) \dots f_t^{m_t}(x)$, com $m_j = 0$ ou $m_j = 1$, para $1 \leq j \leq t$. Além disso, $J \subset \mathcal{M}_i$ implica em $\overline{g(x)} \in \mathcal{M}_i = \langle \overline{\widehat{f}_i(x)} \rangle$, assim, existe $k(x) \in \mathbb{F}_q[x]$ tal que

$$\begin{aligned}
\overline{g(x)} = \overline{k(x)}\,\overline{\widehat{f}_i(x)} \quad &\implies \quad g(x) - k(x)\widehat{f}_i(x) \in \langle x^n - 1 \rangle \\
&\implies \quad x^n - 1 \mid [g(x) - k(x)\widehat{f}_i(x)] \\
&\implies \quad g(x) - k(x)\widehat{f}_i(x) = c(x)(x^n - 1);\ c(x) \in \mathbb{F}_q[x] \\
&\implies \quad g(x) = \widehat{f}_i(x)\,[c(x) f_i(x) + k(x)] \\
&\implies \quad \widehat{f}_i(x) \mid g(x) \text{ em } \mathbb{F}_q[x] \\
&\implies \quad f_j(x) \mid g(x), \text{ para todo } j \neq i.
\end{aligned}$$

Logo, $g(x) = f_1(x) f_2(x) \dots f_i^{m_i}(x) \dots f_t(x)$, com $m_i = 0$ ou $m_i = 1$. Se $m_i = 0$, então $g(x) = \widehat{f}_i(x)$, donde segue $J = \mathcal{M}_i$. Se $m_i = 1$, então $g(x) = x^n - 1$, donde segue $J = \langle 0 \rangle$. Portanto, $\mathcal{M}_i$ é minimal. ■

Sejam $\mathcal{M}_i = \langle \widehat{f}_i \rangle$ um ideal minimal de $\mathcal{R}_n$ e $h_i(x) = \dfrac{x^n - 1}{\widehat{f}_i(x)}$. Pelo Teorema 2.4.3, existem polinômios $r_i(x)$ e $s_i(x)$, tais que $r_i(x)\widehat{f}_i(x) + s_i(x) f_i(x) = 1$ e $\bar{e}(x)_i = \bar{r}_i(x)\overline{\widehat{f}_i}$ é um idempotente primitivo em $\mathcal{R}_n$, para $1 \leq i \leq t$.

Teorema 2.4.5. *Seja $\mathcal{R}_n$ o anel quociente $\dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$. Então*

$$\mathcal{R}_n = \mathcal{M}_1 \oplus \mathcal{M}_2 \oplus \cdots \oplus \mathcal{M}_t,$$

com $\mathcal{M}_i$ um ideal minimal de $\mathcal{R}_n$, para $1 \leq i \leq t$.

Demonstração. Considere os polinômios $\widehat{f}_i$, com $1 \leq i \leq t$, definidos na Proposição 2.4.2. Temos $mdc(\widehat{f}_1, \widehat{f}_2, \dots, \widehat{f}_t) = 1$, assim, pelo algoritmo de Euclides, existem $r_1, r_2, \dots, r_t \in \mathbb{F}_q[x]$, tais que

$$1 = r_1\widehat{f}_1 + r_2\widehat{f}_2 + \cdots + r_t\widehat{f}_t.$$

Logo, para todo elemento, não nulo, u pertencente a $\mathbb{F}_q[x]$, temos

$$u = ur_1\widehat{f_1} + ur_2\widehat{f_2} + \cdots + ur_t\widehat{f_t}$$

Tomando classes módulo $x^n - 1$, segue

$$\bar{u} = \overline{ur_1}\overline{\widehat{f_1}} + \overline{ur_2}\overline{\widehat{f_2}} + \cdots + \overline{ur_t}\overline{\widehat{f_t}} \in \mathcal{M}_1 + \mathcal{M}_2 + \cdots + \mathcal{M}_t.$$

Portanto, $\mathcal{R}_n$ é soma dos ideais minimais $\mathcal{M}_i$, para $1 \leq i \leq t$.

Seja $v \in \mathbb{F}_q[x]$, de modo que $\bar{v} \in \mathcal{M}_i \cap \left(\sum_{i \neq j} \mathcal{M}_j\right)$. Como $\bar{v} \in \mathcal{M}_i$, temos $\bar{v} = v_i\widehat{f_i} + \langle x^n - 1\rangle$, para algum $v_i \in \mathbb{F}_q[x]$. Dessa forma, existe $\varphi_i \in \mathbb{F}_q[x]$, tal que $v = v_i\widehat{f_i} + \varphi_i\left(x^n - 1\right) = f_j(v_i\dfrac{\widehat{f_i}}{f_j} + \varphi_i\widehat{f_j})$, para todo $j \neq i$, donde segue $f_j \mid v$, para todo $j \neq i$. De modo similar ao caso anterior, segue $f_i \mid v$, para todo $i \neq j$. Logo, $f_i \mid v$, para todo $1 \leq i \leq t$, consequentemente, $(x^n - 1) \mid v$ e isso implica em $\bar{v} = 0$.

Portanto, $\mathcal{R}_n$ é soma direta de ideais minimais $\mathcal{M}_i$, para $1 \leq i \leq t$. ■

O Corolário a seguir é uma consequência imediata dos Teorema 2.2.2 e 2.4.5

Corolário 2.4.2. *$\mathcal{R}_n$ é um anel semisimples.*

Corolário 2.4.3. *Seja t um inteiro positivo.* Sejam $\{i_1, \ldots, i_s\}, \{j_1, \ldots, j_{t-s}\}$ *uma partição do anel $\mathbb{Z}_t$. Então o ideal gerado por*

$$f_{i_1} \cdots f_{i_2} = \frac{x^n - 1}{f_{j_1} \cdots f_{j_{t-s}}}$$

é

$$\bigoplus_{k=1}^{t-s} \mathcal{M}_{j_k}$$

e o idempotente gerador deste ideal é

$$e_{j_1} + \cdots + e_{j_{t-s}} = 1 - \left(e_{i_1} + \cdots + e_{i_s}\right).$$

Proposição 2.4.3. *Seja $n_i = \partial\left(f_i\right)$. Então*

$$\mathcal{M}_i \cong \frac{\mathbb{F}_q[x]}{\langle f_i\rangle} \cong \mathbb{F}_{q^{n_i}}.$$

3 ANÉIS DE GRUPO

Neste capítulo, introduzimos o conceito de álgebras de grupo e alguns resultados dessa estrutura que serão bastante utilizados ao longo desta dissertação. Esse estudo foi baseado, principalmente, em [21]. Para maiores detalhes e demonstrações de resultados que optamos por omitir aqui, sugerimos as referências , [1], [17] e [21].

3.1 CONCEITOS BÁSICOS

Seja G um grupo finito e R um anel. Denotamos por RG o conjunto de todas as combinações lineares formais

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

em que $a_g \in R$ e $a_g = 0$, para quase todo $a_g \in R$, ou seja, apenas um número finito de coeficientes é diferente de zero em cada uma dessas somas. Quando conveniente, também podemos escrever α na forma:

$$\alpha = \sum_{g \in G} a(g) g.$$

Sejam $\alpha = \sum_{g \in G} \alpha_g g,\ \beta = \sum_{g \in G} \beta_g g \in RG$ e $c \in \mathbb{F}$, definimos as operações de adição e multiplicação em RG como segue

$$\begin{array}{rccc} + : & RG \times RG & \to & RG \\ & (\alpha, \beta) & \mapsto & \alpha + \beta \end{array} \qquad \begin{array}{rccc} \cdot : & RG \times RG & \to & RG \\ & (\alpha, \beta) & \mapsto & \alpha \cdot \beta, \end{array}$$

por

$$\alpha + \beta = \sum_{g \in G} (\alpha_g + \beta_g) g; \qquad \alpha \cdot \beta = \sum_{g,h \in G} \sum_{g,h \in G} (\alpha_g \beta_h) gh. \tag{3.1}$$

Além disso, definimos a multiplicação de um elemento de RG por um escalar de R da seguinte maneira

$$\begin{array}{rccc} * : & R \times RG & \to & RG \\ & (c, \alpha) & \mapsto & c * \alpha = c\alpha = \sum_{g \in G} (c\alpha_g) g. \end{array} \tag{3.2}$$

Para um elemento arbitrário $\alpha = \sum_{g \in G} a_g g$ em RG, definimos o **suporte** de α pelo conjunto dos elementos de G que aparecem efetivamente na expressão de α, ou seja,

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

Pela definição que demos para o elemento α de RG, dados $\alpha = \sum_{g \in G} a_g g$ e $\beta = \sum_{g \in G} b_g g \in RG$, temos $\alpha = \beta$ se, e somente se, $a_g = b_g$, para todo $g \in G$.

Definição 3.1.1. O conjunto RG, com as operações definidas em (3.1) e (3.2), é chamado **anel de grupo** de G sobre R. No caso em que R é comutativo, RG também é chamado **álgebra de grupo** de G sobre R.

A função $i : G \longrightarrow RG$ definida por $i(x) = \sum_{g \in G} a(g)g$, em que $a(x) = 1$ e $a(g) = 0$ se $g \neq x$, é injetora. Assim, a restrição $i : G \longrightarrow i(G)$ nos dá um isomorfismo de grupos multiplicativos. Deste modo, RG é um módulo livre e G é uma base para RG sobre R.

Proposição 3.1.1. *Sejam R um anel comutativo e G, H grupos. Então $R(G \times H) \cong (RG)H$ (o anel de grupo de H sobre o anel RG).*

Proposição 3.1.2. *Sejam $\{R_i\}_{i \in I}$ uma família de anéis e $R = \oplus_{i \in I} R_i$. Então, para qualquer grupo G, $RG \cong \oplus_{i \in I} R_i G$.*

Proposição 3.1.3. *Sejam $G = \langle a \rangle$ um grupo cíclico de ordem n e $\mathbb{F}$ um corpo finito. Todo ideal de $\mathbb{F}G$ é da forma $\mathbb{F}Gf(a)$, em que $f(x)$ é um divisor de $x^n - 1$.*

3.2 SEMISSIMPLICIDADE DE ANÉIS DE GRUPOS

O Teorema 2.3.2 estabelece condições necessárias e suficientes para que uma família de elementos $\{e_1, \ldots, e_s\}$ de um anel semissimples R seja composta de idempotentes primitivos. Em [21, Seção 3.3], são determinadas condições sobre R e G que permitem decompor RG como soma direta de certos subanéis. Em particular, são determinadas condições para que RG seja um anel semissimples e, consequentemente, possa ser escrito como soma direta de ideais minimais, conforme o Teorema 2.3.2. Além disso, é feita uma descrição do centro de uma álgebra de grupo, a fim de determinar a estrutura de uma álgebra de grupo semissimples. Para essas álgebras, é determinado o número de todas as componentes simples, o que possibilita determinar sua estrutura a partir de exemplos concretos em [21, Seção 3.6].

Nesta dissertação, vamos nos restringir a enunciar e discutir os principais resultados e definições aqui utilizados. Alguns destes resultados são demonstrados aqui; aqueles cuja demonstração é omitida, podem ser encontrados demonstrados na referência supracitada.

Definição 3.2.1. A aplicação $\varepsilon : RG \longrightarrow R$ dada por

$$\varepsilon\left(\sum_{g \in G} \alpha(g)g\right) = \sum_{g \in G} \alpha(g)$$

é um homomorfismo de anéis chamado **função de aumento** de RG e seu núcleo, que denotamos por $\Delta(G)$, é dito **ideal de aumento** de RG.

Seja H um subgrupo normal em G e seja $\omega : G \longrightarrow G/H$ o epimorfismo canônico. Podemos definir um homomorfismo $\varepsilon_H : RG \longrightarrow R(G/H)$ por

$$\varepsilon_H \left(\sum_{g \in G} \alpha(g) g \right) = \sum_{g \in G} \alpha(g) \omega(g).$$

Com as notações acima denotamos $Ker\,(\varepsilon_H)$ por $\triangle(G, H)$.

Teorema 3.2.1. *(Maschke) Seja G um grupo. Então o anel de grupo RG é semissimples se, e somente se, as seguintes condições são válidas:*

(i) R é um anel semissimples.

(ii) G é finito.

(iii) $|G|$ é invertível em R.

Corolário 3.2.1. *Seja G um grupo finito e $\mathbb{F}$ um corpo. Então $\mathbb{F}G$ é semisimples se, e somente se, $car(\mathbb{F}) \nmid |G|$.*

A fim de obter mais informações sobre a estrutura das álgebras de grupo, podemos enunciar o Teorema de Wedderburn-Artin como segue:

Teorema 3.2.2. *Sejam G um grupo finito e $\mathbb{F}$ um corpo tal que $car\,(\mathbb{F}) \nmid |G|$. Então:*

(i) $\mathbb{F}G$ 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.

(ii) Qualquer ideal bilateral de $\mathbb{F}G$ é uma soma direta de alguns dos membros da família $\{B_i\}_{1 \leq i \leq r}$.

(iii) Cada componente simples B_i é isomorfa a um anel de matrizes completo da forma $M_{n_i}(D_i)$, em que D_i é um anel de divisão contendo uma cópia de $\mathbb{F}$ em seu centro, e o isomorfismo

$$\mathbb{F}G \overset{\phi}{\cong} \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de $\mathbb{F}$-álgebras.

(iv) Em cada matriz $M_{n_i}(D_i)$, o conjunto

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ & & \cdots & \\ x_{n_i} & 0 & \cdots & 0 \end{bmatrix} ; x_1, x_2, \cdots, x_{n_i} \in D_i \right\} \cong D_i^{n_i}$$

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.

(v) $I_i \ncong I_j$, *se* $i \neq j$.

(vi) Qualquer $\mathbb{F}G$-módulo simples é isomorfo a algum I_i, para $1 \leq i \leq r$.

Corolário 3.2.2. *Sejam G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado tal que* $\text{car}(\mathbb{F}) \nmid |G|$. *Então*

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

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

Demonstração. Como $car(\mathbb{F}) \nmid |G|$, as hipóteses do Teorema 3.2.2 são satisfeitas, assim,

$$\mathbb{F}G \cong \oplus_{i=1}^{r} M_{n_i}(D_i), \tag{3.3}$$

em que D_i é um anel de divisão contendo uma cópia de $\mathbb{F}$ em seu centro. Daí, calculando as dimensões sobre $\mathbb{F}$ em ambos os lados da equação (3.3), temos

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : \mathbb{F}],$$

donde cada anel de divisão é finitamente dimensional sobre $\mathbb{F}$. Como $\mathbb{F}$ é um corpo algebricamente fechado, temos $D_i = \mathbb{F}$, para $1 \leq i \leq r$, e o resultado segue. ■

Na definição a seguir, adotamos a definição de **classe de conjugação** de um grupo G, conforme [21, p. 22].

Definição 3.2.2. Sejam G um grupo, R um anel comutativo e $\{C_i\}_{i \in I}$ o conjunto de classes de conjugação de G contendo apenas um número finito de elementos. Para cada índice $i \in I$, definimos $\gamma_i = \widetilde{C_i} = \sum_{x \in C_i} x$. Esses elementos são chamados **soma de classe** de G sobre R.

Teorema 3.2.3. *Seja G um grupo e R um anel comutativo. Então o conjunto $\{\gamma_i\}_{i \in I}$ de todas as somas de classe de G sobre R forma uma base para $\mathcal{Z}(RG)$, o centro de RG, sobre R.*

Demonstração. Dado um elemento arbitrário $g \in G$, temos $g^{-1}\gamma_i g = \sum_{x \in C_i} g^{-1}xg$. Como a conjugação por g é um automorfismo de G que fixa as somas de classe (ou seja, $C_i^g = C_i$,

para todo índice $i \in I$), então $\sum_{x \in C_i} g^{-1}xg = \sum_{y \in C_i} y = \gamma_i$. Logo, $\gamma_i g = g\gamma_i$, para todo $g \in G$, isto é, $\gamma_i \in \mathcal{Z}(RG)$, para todo $i \in I$.

Para mostrar que esses elementos são linearmente independentes, seja $\sum_{i \in I} r_i\gamma_i = 0$ uma soma finita. Podemos escrever essa equação como $\sum_{i \in I} r_i \sum_{x \in C_i} x = 0$ e, como as diferentes somas de classe têm suportes disjuntos (pois classes diferentes implicam em classes disjuntas), a independência linear dos elementos de G em R mostra que devemos ter $r_i = 0$, para todo $i \in I$.

Para concluir a demonstração, resta provar que $\{\gamma_i\}_{i \in I}$ é um conjunto gerador de $\mathcal{Z}(RG)$. Para tanto, suponha $\alpha = \sum_{g \in G} a_g g \in \mathcal{Z}(RG)$. Afirmamos que se $g \in supp(\alpha)$, então qualquer outro elemento h na classe de conjugação de g também pertence a $supp(\alpha)$ e $a_g = a_h$. De fato, se $h = x^{-1}gx$, para algum $x \in G$, como α é central, então $\alpha = x^{-1}\alpha x$, ou seja,

$$\sum_{g \in G} a_g g = \sum_{g \in G} a_g x^{-1}gx.$$

Logo, $h \in supp(\alpha)$, para todo h na classe de conjugação de g e, ao comparar o coeficiente de h em ambos os lados dessa equação, obtemos $a_h = a_g$, para todo h na classe de conjugação de g. Como as classes de conjugação distintas de G são duas a duas disjuntas, então podemos escrever G como união disjunta dessas classes. Daí, para $i \in I$,

$$\begin{aligned}
\alpha = \sum_{g \in G} a_g g &= \sum_{h_1 \in C_1} a_1 h_1 + \sum_{h_2 \in C_2} a_2 h_2 + \ldots + \sum_{h_i \in C_i} a_i h_i \\
&= a_1 \sum_{h_1 \in C_1} h_1 + a_2 \sum_{h_2 \in C_2} h_2 + \ldots + a_i \sum_{h_i \in C_i} h_i \\
&= a_1\gamma_1 + a_2\gamma_2 + \ldots + a_i\gamma_i \\
&= \sum_i a_i\gamma_i.
\end{aligned}$$

Portanto, $\{\gamma_i\}_{i \in I}$ também é um conjunto de geradores para $\mathcal{Z}(RG)$ e isto conclui a prova do resultado. ■

Proposição 3.2.1. *Sejam G um grupo finito e $\mathbb{F}$ um corpo algebricamente fechado tal que $car(\mathbb{F}) \nmid |G|$. Então o número de componentes simples de $\mathbb{F}G$ é igual ao número de classes de conjugação de G.*

Demonstração. Pelo Teorema 3.2.3, o conjunto de todas as somas de classe de $\{\gamma_i\}_{i \in I}$ de G sobre $\mathbb{F}$ forma uma base para $\mathcal{Z}(\mathbb{F}G)$ sobre $\mathbb{F}$. Como G é um grupo finito, então o número de somas de classe é igual ao número de classes de conjugação de G. Logo, basta mostrar que a dimensão de $\mathcal{Z}(\mathbb{F}G)$ sobre $\mathbb{F}$ é igual ao número de componentes simples de

$\mathbb{F}G$. Pelo Corolário 3.2.2,

$$\mathbb{F}G \cong \oplus_{i=1}^{r} M_{n_i}(\mathbb{F}),$$

daí,

$$\mathcal{Z}(\mathbb{F}G) \cong \oplus_{i=1}^{r} \mathcal{Z}(M_{n_i}(\mathbb{F})).$$

Para um anel de matrizes $M_n(\mathbb{F})$, é fácil provar que

$$\mathcal{Z}(M_n(\mathbb{F})) = \{\alpha I : \alpha \in \mathbb{F}\},$$

assim, $\mathcal{Z}(M_n(\mathbb{F})) \cong \mathbb{F}$. Logo,

$$\mathcal{Z}(\mathbb{F}G) \cong \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{r \text{ vezes}}.$$

Portanto, $[\mathcal{Z}(\mathbb{F}G) : \mathbb{F}] = r$. ■

Lema 3.2.1. *Sejam R um anel com unidade e H um subgrupo de um grupo G. Se $|H|$ é invertível em R, então $\widehat{H} = \frac{1}{|H|}\sum_{h\in H} h$ é um idempotente de RG. Além disso, se $H \triangleleft G$ então $\widehat{H}$ é central.*

Demonstração. Primeiro, provamos que $\widehat{H}$ é um idempotente. De fato, pelo isomorfismo $\varphi_h : H \longrightarrow H$, definido por $x \longmapsto hx$,

$$\begin{aligned}\widehat{H}\widehat{H} &= \frac{1}{|H|^2}(\sum_{h\in H} h)(\sum_{h\in H} h) = \frac{1}{|H|^2}\sum_{h\in H} h(\sum_{h\in H} h) \overset{\varphi_h}{=} \frac{1}{|H|^2}\sum_{h\in H}\sum_{h\in H} h = \\ &= \frac{1}{|H|^2}|H|\sum_{h\in H} h = \frac{1}{|H|}\sum_{h\in H} h.\end{aligned}$$

Finalmente, se $H \triangleleft G$, para qualquer $g \in G$, temos $g^{-1}Hg = H$; portanto,

$$g^{-1}(\sum_{h\in H} h)g = \sum_{h\in H} g^{-1}hg = \sum_{h\in H} h.$$

Assim, $(\sum_{h\in H} h)g = g(\sum_{h\in H} h)$, para todo $g \in G$, isto mostra que $\sum_{h\in H} h$ é central em G. Portanto, $\widehat{H}$ é central em G.

■

Proposição 3.2.2. *Sejam R um anel com unidade e H um subgrupo normal do grupo G. Se $|H|$ é invertível em R, então*

$$RG = RG\widehat{H} \oplus RG(1 - \widehat{H}),$$

como soma direta de anéis. Além disso,

$$RG\widehat{H} \cong R(G/H) \quad e \quad RG(1 - \widehat{H}) = \Delta(G, H).$$

3.3 ÁLGEBRAS DE GRUPO ABELIANAS

Sejam $G = \left\{1, a, \ldots, a^{n-1}\right\}$, com $a^n = 1$, um grupo cíclico de ordem n e $\mathbb{F}$ um corpo finito com q elementos tal que $\text{car}(\mathbb{F}) \nmid |G|$. Defina a função $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}G$ por $\varphi(f) = f(a) \in \mathbb{F}G$. Sejam $f, h \in \mathbb{F}[x]$. Da definição de adição e multiplicação em $\mathbb{F}G$, segue

$$\varphi(f+h) = (f+h)(a) = f(a) + h(a);$$
$$\varphi(fh) = (fh)a = f(a)h(a); \text{ para todo } f, h \in \mathbb{F}[x].$$

Assim, φ é um homomorfismo de anéis. Além disso, dado $\alpha = \sum_{i=0}^{n} \alpha_i a^i \in \mathbb{F}G$, arbitrário, existe $f = f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in \mathbb{F}[x]$, de grau n, tal que

$$\varphi(f) = \sum_{i=0}^{n} \alpha_i a^i = \alpha \in \mathbb{F}G.$$

Portanto, φ é um epimorfismo de anéis.

Pelo Corolário 2.4.1, existe um único polinômio de grau mínimo f_0 em $\mathbb{F}[x]$ tal que $Ker(\varphi) = \langle f_0 \rangle$. Como $a^n = 1$, então $x^n - 1 \in Ker(\varphi)$. Seja $g = \sum_{i=0}^{r} k_i x^i \in F[x]$ um polinômio não nulo de grau $r < n$, assim, $\varphi(g) = \sum_{i=0}^{r} k_i a^i$ em $\mathbb{F}G$. Como G é uma base para $\mathbb{F}G$ sobre $\mathbb{F}$, então $\{1, a, a^2, \ldots, a^r\}$ é um conjunto linearmente independente, assim, $g(a) \neq 0$. Logo, $x^n - 1$ é o polinômio de menor grau em $\mathbb{F}[x]$ cuja imagem pela aplicação φ se anula no elemento a em $\mathbb{F}G$. Portanto, $Ker(\varphi) = \langle x^n - 1 \rangle$, donde segue, pelo 1º Teorema do Isomorfismo de anéis,

$$\mathbb{F}G \overset{\overline{\varphi}}{\cong} \frac{\mathbb{F}[x]}{\langle x^n - 1 \rangle}. \tag{3.4}$$

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, por hipótese, $car(\mathbb{F}) \nmid n$, esse polinômio é separável e, portanto, $f_i \neq f_j$, se $i \neq j$. Pelo Teorema Chinês dos Restos, podemos escrever:

$$\mathbb{F}G \cong \frac{\mathbb{F}[x]}{\langle f_1 \rangle} \oplus \frac{\mathbb{F}[x]}{\langle f_2 \rangle} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{\langle f_t \rangle}. \tag{3.5}$$

Sob esse isomorfismo, o gerador a corresponde ao elemento

$$(x + \langle f_1 \rangle, \ldots, x + \langle f_t \rangle).$$

Seja ζ_i uma raiz de f_i, para $1 \leq i \leq t$. Então $\dfrac{\mathbb{F}[x]}{\langle f_i \rangle} \cong \mathbb{F}(\zeta_i)$ e, consequentemente,

$$\mathbb{F}G \cong \mathbb{F}(\zeta_1) \oplus \mathbb{F}(\zeta_2) \oplus \cdots \oplus \mathbb{F}(\zeta_t). \tag{3.6}$$

Uma vez que todos os elementos ζ_i, para $1 \leq i \leq t$, são raízes de $x^n - 1$, mostramos que $\mathbb{F}G$ é isomorfo a uma soma direta de extensões ciclotômicas de $\mathbb{F}$. Sob o isomorfismo (3.6), o elemento $a \in G$ corresponde à n-upla $(\zeta_1, \zeta_2, \ldots, \zeta_t) \in \mathbb{F}(\zeta_1) \oplus \mathbb{F}(\zeta_2) \oplus \cdots \oplus \mathbb{F}(\zeta_t)$.

Pelos Teoremas 2.1.6 e 2.1.7, $\Phi_d(x) = \prod_{i=1}^{\frac{\phi(d)}{t}} f_{d_i}$, com f_{d_i} irredutível e de grau t sobre $\mathbb{F}$, para cada $1 \leq i \leq \dfrac{\phi(d)}{t}$. Assim, a decomposição de $\mathbb{F}G$ pode ser reescrita na forma:

$$\mathbb{F}G \cong \bigoplus_{d|n} \bigoplus_{i=1}^{\frac{\phi(d)}{t}} \frac{\mathbb{F}[x]}{\langle f_{d_i} \rangle} \cong \bigoplus_{d|n} \bigoplus_{i=1}^{\frac{\phi(d)}{t}} \mathbb{F}(\zeta_{d_i}),$$

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

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

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

Note que o fato de G ser um grupo cíclico de ordem n implica na existência de um único subgrupo de ordem d, para cada d que divide a ordem n de G. Além disso, cada um desses subgrupos possui exatamente $\phi(d)$ geradores, isto é, $\phi(d)$ elementos de ordem d. No entanto, isto não se verifica quando G é um grupo abeliano não cíclico, uma vez que a unicidade de um subgrupo de ordem d em G não é garantida. Em vista disso, passamos a denotar a quantidade de subcorpos isomorfos a $\mathbb{F}(\zeta_d)$ por

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

em que n_d denota o número de elementos de ordem d em G.

O Teorema seguinte garante a decomposição de $\mathbb{F}G$ como produto direto de a_d cópias de $\mathbb{F}(\zeta_d)$, para cada d que divide n, no caso em que G é um grupo abeliano, não necessariamente cíclico.

Teorema 3.3.1. *(Perlis-Walker) Seja G um grupo abeliano finito de ordem n, e seja $\mathbb{F}$ um corpo tal que $car(\mathbb{F}) \nmid |G|$. Então*

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

em que ζ_d denota uma raiz primitiva da unidade de ordem d e $a_d = \dfrac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}$. 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. É fácil ver que o resultado vale para grupos de ordem menor ou igual a 3, visto que grupos dessa ordem são cíclicos e já provamos o resultado para estes tipos de grupos. Assumimos como hipótese de indução 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. Se G é abeliano e não cíclico, pelo Teorema Fundamental dos Grupos Abelianos Finitos, podemos escrever $G = G_1 \times H$, em que H é cíclico e G_1 é um produto direto de grupos cíclicos, com $|G_1| = n_1 < n$. Pela hipótese de indução, podemos escrever $\mathbb{F}G_1 \cong \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})$, em que $a_{d_1} = \dfrac{n_{d_1}}{[\mathbb{F}(\zeta_{d_1}) : \mathbb{F}]}$ e n_{d_1} denota o número de elementos de ordem d_1 em G_1. Assim, pelos Teoremas 3.1.1 e 3.1.3,

$$\mathbb{F}G = \mathbb{F}(G_1 \times H) \cong (\mathbb{F}G_1)H \cong \left(\bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})\right) H \cong \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})H. \tag{3.7}$$

Como o resultado vale para grupos cíclicos, temos

$$\begin{aligned}
\bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})H &\cong \bigoplus_{d_1|n_1} a_{d_1} \bigoplus_{d_2||H|} a_{d_2}\mathbb{F}(\zeta_{d_1})\mathbb{F}(\zeta_{d_2}) \\
&\cong \bigoplus_{d_1|n_1} a_{d_1} \bigoplus_{d_2||H|} a_{d_2}\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}) \\
&= \bigoplus_{d_1|n_1} \bigoplus_{d_2||H|} a_{d_1}a_{d_2}\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}),
\end{aligned}$$

em que $a_{d_2} = \dfrac{n_{d_2}}{[\mathbb{F}(\zeta_{d_1}\zeta_{d_2}) : \mathbb{F}(\zeta_{d_1})]}$ e n_{d_2} denota o número de elementos de ordem d_2 em H. Seja $d = mmc(d_1, d_2)$, temos $\mathbb{F}(\zeta_{d_1}\zeta_{d_2}) = \mathbb{F}(\zeta_d)$, assim,

$$\mathbb{F}G \cong \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})H \cong \bigoplus_{d_1|n_1} \bigoplus_{d_2||H|} a_{d_1}a_{d_2}\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}) \cong \bigoplus_{d|n} a_d\mathbb{F}(\zeta_d),$$

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

$$a_d[\mathbb{F}(\zeta_d) : \mathbb{F}] = \sum_{d_1,d_2} a_{d_1}[\mathbb{F}(\zeta_{d_1}\zeta_{d_2}) : \mathbb{F}(\zeta_{d_1})]a_{d_2}[\mathbb{F}(\zeta_{d_1}) : \mathbb{F}] = \sum_{d_1,d_2} n_{d_1}n_{d_2}. \tag{3.8}$$

Finalmente, por hipótese, cada elemento $g \in G$ pode ser escrito na forma $g = g_1h$, 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 (3.8), concluímos

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

■

Corolário 3.3.1. *Seja G um grupo abeliano finito de ordem n. Então*

$$\mathbb{Q}G \cong \oplus_{d|n} a_d \mathbb{Q}(\zeta_d) \tag{3.9}$$

em que ζ_d denota uma raiz primitiva da unidade de ordem d, e a_d o número de subgrupos cíclicos (ou quocientes cíclicos) de G.

Demonstração. Pelo Teorema 3.3.1, $a_d = \dfrac{n_d}{[\mathbb{Q}(\zeta_d) : \mathbb{Q}]}$, no qual n_d é o número de elementos de ordem d em G.

Pelo Teorema 2.1.7, $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \phi(d)$, em que ϕ denota a função de Euler. Observamos que o número de geradores de um grupo cíclico de ordem d é precisamente $o(d)$, então $\dfrac{n_d}{\phi(d)}$ é o número de subgrupos cíclicos de ordem d em G e, consequentemente, isso também é igual ao número de quocientes cíclicos de G. ■

3.4 IDEMPOTENTES DE $\mathbb{F}G$

Considerando $\mathbb{F}$ um corpo finito e G um grupo cíclico finito de ordem n, vamos agora determinar os idempotentes da álgebra de grupo $\mathbb{F}G$.

Por (3.4), (3.5) e a Proposição 2.4.3,

$$\mathbb{F}G \cong \frac{\mathbb{F}[x]}{\langle x^n - 1\rangle} \cong \frac{\mathbb{F}[x]}{\langle f_1\rangle} \oplus \frac{\mathbb{F}[x]}{\langle f_2\rangle} \oplus \cdots \oplus \frac{\mathbb{F}[x]}{\langle f_t\rangle} \cong \mathcal{R}_n e_1 \oplus \cdots \oplus \mathcal{R}_n e_t.$$

Portanto,

$$\mathbb{F}G = \overline{\varphi}(\mathcal{R}_n) = \mathbb{F}G\overline{\varphi}(e_1) \oplus \cdots \oplus \mathbb{F}G\overline{\varphi}(e_t).$$

Note que $\overline{e_i(x)} = r_i(\bar{x})\hat{f}_i(\bar{x})$, donde $\overline{\varphi}(\overline{e_i(x)}) = r_i(a)\widehat{f}_i(a)$. Com isso, os idempotentes de $\mathbb{F}G$ são da forma

$$e_i(a) = r_i(a)\widehat{f}_i(a), \text{ para } 1 \leq i \leq t.$$

Exemplo 3.4.1. Sejam $\mathbb{F} = \mathbb{F}_2$ e $G = \langle a : \ a^7 = 1\rangle$ um corpo finito com 2 elementos e um grupo cíclico de ordem 7, respectivamente. Temos

$$x^7 - 1 = \underbrace{(x-1)}_{f_1(x)}\underbrace{(x^3+x^2+1)}_{f_2(x)}\underbrace{(x^3+x+1)}_{f_3(x)} \quad \text{sobre } \mathbb{F}_2.$$

Assim,

(i) $\mathcal{M}_1 = \langle \widehat{f_1}(\bar{x})\rangle = \langle \overline{x^6+x^5+x^4+x^3+x^2+x+1}\rangle = \langle g_0(\bar{x})\rangle$.

(ii) $\mathcal{M}_2 = \langle \widehat{f_2}(\bar{x})\rangle = \langle \overline{x^4+x^3+x^2+1}\rangle = \langle g_1(\bar{x})\rangle$.

(iii) $\mathcal{M}_3 = \langle \widehat{f_3}(\bar{x})\rangle = \langle \overline{x^4+x^2+x+1}\rangle = \langle g_2(\bar{x})\rangle$,

em que cada $\mathcal{M}_i$ é um ideal minimal em $F[x]/\langle x^7-1\rangle, i=1,2,3$. Logo, pelo Teorema 2.4.5,

$$\frac{\mathbb{F}[x]}{\langle x^7-1\rangle} = \mathcal{R}_7 \cong \mathcal{M}_1 \oplus \mathcal{M}_2 \oplus \mathcal{M}_3.$$

Pelo Teorema 2.4.3, temos

$$\begin{aligned} g_0(x) = x^6+x^5+x^4+x^3+x^2+x+1 &\implies h_0(x) = x+1; \\ g_1(x) = x^4+x^3+x^2+1 &\implies h_1(x) = x^3+x^2+1; \\ g_2(x) = x^4+x^2+x+1 &\implies h_2(x) = x^3+x+1; \end{aligned}$$

donde

$$\begin{aligned} &r_0(x)(x^6+x^5+x^4+x^3+x^2+x+1)+s_0(x)(x+1)=1; \\ &r_1(x)(x^4+x^3+x^2+1)+s_1(x)(x^3+x^2+1)=1; \\ &r_2(x)(x^4+x^2+x+1)+s_2(x)(x^3+x+1)=1; \end{aligned}$$

Para determinar $r_i(x)$ e $s_i(x)$, para $i=1,2,3$, aplicamos o algoritmo da divisão de Euclides como segue:

(i) Para $i=0$,

$$\begin{aligned} x^6+x^5+x^4+x^3+x^2+x+1 &= (x^5+x^3+x)(x+1)+1 \\ g_0(x)+(x^5+x^3+x)h_0(x) &= 1. \end{aligned}$$

Então $r_0(x)=1$ e $s_0(x)=x^5+x^3+x$.

(ii) Para $i=1$,

$$1=(1+x^2)(x^4+x^3+x^2+1)+x^3(x^3+x^2+1).$$

Logo,

$$(1+x^2)g_1(x)+x^3h_1(x)=1,$$

donde segue $r_1(x)=1+x^2$ e $s_1(x)=x^3$.

(iii) Para $i=2$,

$$\begin{aligned} x^4+x^2+x+1 &= x(x^3+x+1)+1 \\ g_2(x)+xh_2(x) &= 1. \end{aligned}$$

Então $r_2(x)=1$ e $s_1(x)=x$.

Portanto, os idempotentes primitivos de $\mathbb{F}G$ são

$$\begin{aligned} &e_0(a)=g_0(a)=a^6+a^5+a^4+a^3+a^2+a+1; \\ &e_1(a)=(1+a^2)g_1(a)=a^6+a^5+a^3+1; \\ &e_2(a)=g_2(a)=a^4+a^2+a+1. \end{aligned}$$

3.5 O NÚMERO DE COMPONENTES SIMPLES

Vimos no Teorema 3.2.3 que o conjunto formado pelas somas de classe de G sobre R forma uma base para o centro $\mathcal{Z}(G)$ de RG. Consequentemente, as componentes simples de RG são geradas por essas classes. Em particular, quando G é um grupo finito, vimos na Proposição 3.2.1 que cada componente simples de RG corresponde a uma classe de conjugação de G e concluímos, portanto, que o número de idempotentes primitivos de RG é igual ao número de classes de conjugação de G. Além disso, construímos, no Lema 3.2.1, um idempotente de RG a partir de subgrupos G.

Os resultados que apresentamos até aqui indicam que, para encontrar os idempotentes primitivos de uma álgebra de grupo $\mathbb{F}G$, devemos, primeiro, determinar as componentes simples desta álgebra. Por essa razão, vamos descrever, nesta seção, uma maneira de encontrar as componentes simples de $\mathbb{F}G$ para o caso dos grupos abelianos, dada em [7]. Trata-se de um cálculo que usa apenas a estrutura algébrica de $\mathbb{F}G$.

3.5.1 Fatos Básicos

Sejam $\mathbb{F}$ um corpo finito com q elementos e G um grupo abeliano finito tal que $mdc(q, |G|) = 1$. Então $\mathbb{F}G$ é semissimples e, se $\{e_1, e_2, \ldots, e_r\}$ é o conjunto de idempotentes primitivos de $\mathbb{F}G$, temos

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

em que $\mathbb{F}_i \cong (\mathbb{F}G)e_i$, com $1 \leq i \leq r$, são corpos que são extensões finitas de $\mathbb{F}$. Seja

$$\mathcal{D} = \bigoplus_{i=1}^{r} \mathbb{F}e_i. \tag{3.10}$$

Observe que $\mathbb{F}e_i \cong \mathbb{F}$ como corpos na forma natural e, portanto, o número r de componentes simples é também a dimensão de $\mathcal{D}$ como espaço vetorial sobre $\mathbb{F}$.

Lema 3.5.1. *Seja α um elemento de $\mathbb{F}G$. Então $\alpha \in \mathcal{D}$ se, e somente se, $\alpha^q = \alpha$.*

Demonstração. Dado $\alpha \in \mathbb{F}G$, podemos escrever

$$\alpha = \sum_{i=1}^{r} \alpha_i, \quad \text{com} \quad \alpha_i = \alpha e_i \in (\mathbb{F}G)e_i, \quad \text{para } 1 \leq i \leq r.$$

Temos $\alpha \in \mathcal{D}$ se, e somente se, cada $\alpha_i \in \mathbb{F}e_i$, para todo índice i. Pelo Teorema 2.1.1, $\mathbb{F}e_i \cong \mathbb{F}$ é o corpo de decomposição do polinômio $x^q - x$, daí, $\alpha_i \in \mathbb{F}e_i$ se, e somente se, $\alpha_i^q = \alpha_i$, para todo índice i. Assim,

$$\begin{aligned} \alpha^q &= (\alpha_1 + \alpha_2 + \cdots + \alpha_r)^q \\ &= \alpha_1^q + \alpha_2^q + \cdots + \alpha_r^q. \end{aligned}$$

Portanto, $\alpha_i^q = \alpha_i$, para todo índice i, se, e somente se, $\alpha^q = \alpha$. ■

Definição 3.5.1. Seja g um elemento no grupo abeliano finito G. Definimos a q-**classe ciclotômica de** g em G por

$$\mathcal{C}_g = \left\{ g^{q^j};\ 0 \leq j \leq t_g - 1 \right\},$$

em que t_g é o menor inteiro positivo tal que

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

e $o(g)$ denota a ordem de g em G. Como $mdc(q, o(g)) = 1$, a existência do número t_g é garantida.

Lema 3.5.2. *Se $\mathcal{C}_g \neq \mathcal{C}_h$, então $\mathcal{C}_g \cap \mathcal{S}_h = \emptyset$.*

Demonstração. Se $x \in \mathcal{C}_g \cap \mathcal{C}_h$, então $x = g^{q^j}$, para algum inteiro j. Logo, é imediato que $\mathcal{C}_x \subset \mathcal{C}_g$. Como $mdc(q,\ o(g)) = 1$, então $o(x) = o(g)$. Queremos encontrar o menor inteiro positivo s tal que $(g^{q^j})^{q^s} = g^{q^j}$. Assim,

$$g^{q^j(q^s-1)} = 1 \Longleftrightarrow o(x) \mid (q^s - 1) \Longleftrightarrow q^s \equiv 1 \pmod{o(x)}.$$

Como $o(x) = o(g)$ e t_g é o menor inteiro positivo tal que

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

segue $s = t_g$. Logo, $\mathcal{C}_x = \mathcal{C}_g$. Da mesma forma, segue $\mathcal{C}_x = \mathcal{C}_h$. Portanto, $\mathcal{C}_g = \mathcal{C}_h$. ■

Lema 3.5.3. *Seja α um elemento de $\mathcal{D}$. Se $\alpha = \sum_{g \in G} \alpha_g g$, então $\alpha_g = \alpha_{g^q} = \cdots = \alpha_{g^{q^{t_g-1}}}$, para cada $g \in G$.*

Demonstração. Seja $\alpha \in \mathbb{F}G$ tal que $\alpha \in \mathcal{D}$. Pelo Lema 3.5.1, $\alpha^q = \alpha$. Se $\alpha = \sum_{g \in G} \alpha_g g$, então

$$\alpha = \sum_{g \in G} \alpha_g g = \left(\sum_{g \in G} \alpha_g g \right)^q = \sum_{g \in G} \alpha_g^q g^q.$$

Como $\alpha_g \in \mathbb{F}$, segue $\alpha_g^q = \alpha_g$, assim,

$$\alpha = \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g g^q. \tag{3.11}$$

Como $g \in supp(\alpha)$, então g comparece em um dos termos do primeiro membro da igualdade (3.11). Logo, $g^q \in supp(\alpha)$ e deve comparecer com o mesmo coeficiente nos dois membros dessa igualdade. Assim, $\alpha_{g^q} = \alpha_g$. Repetindo essa construção obtemos, para cada $g \in G$,

$$\alpha_g = \alpha_{g^q} = \ldots = \alpha_{g^{q g-1}}.$$

■

3.5.2 O números de componentes simples de $\mathbb{F}G$

Seja $\mathcal{T} = \{g_1, g_2, \ldots, g_r\}$ um conjunto de representantes das q-classes ciclotômicas de G.

Teorema 3.5.1. *Sejam $\mathbb{F}$ um corpo finito com q elementos e G um grupo abeliano finito tal que $mdc(q, |G|) = 1$. Então o número de componentes simples de $\mathbb{F}G$ é igual ao número de q-classes ciclotômicas de G.*

Demonstração. Por (3.10), o número de componentes simples de $\mathbb{F}G$ é igual a dimensão de $\mathcal{D}$ sobre $\mathbb{F}$. Exibimos uma base desta subálgebra. Dado uma q-classe ciclotômica $\mathcal{C}_g$, definimos

$$\eta_g = \sum_{x \in \mathcal{C}_g} x \in \mathbb{F}G.$$

Afirmamos que $\mathcal{B} = \{\eta_{g_i} \mid 1 \leq i \leq r\}$ é uma $\mathbb{F}$-base de $\mathcal{D}$. Como os suportes de $\eta_{g_1}, \ldots, \eta_{g_r}$ são dois a dois disjuntos, $\mathcal{B}$ é um conjunto linearmente independente. Assim, precisamos apenas mostrar que $\mathcal{B}$ é também gerador de $\mathcal{D}$. Como

$$\begin{aligned}
\eta_{g_i}^q &= (\sum_{x \in \mathcal{C}_{g_i}} x)^q \\
&= (x + x^q + \cdots + x^{q^{t_{g_i}-1}})^q \\
&= x^q + x^{q^2} + \cdots + x^{q^{t_{g_i}}} \\
&= (\sum_{x \in \mathcal{C}_{g_i}} x) \\
&= \eta_{g_i}, \quad 1 \leq i \leq r,
\end{aligned}$$

então, pelo Lema 3.5.1, $\eta_{g_i} \in \mathcal{D}$. Logo, $\mathcal{D} \subset \mathcal{B}$. Seja $\alpha \in \mathcal{D} = \oplus_{i=1}^{r} \mathbb{F}e_i$. Se $\alpha = \sum_{g \in G} \alpha_g g$, então, pelo Lema 3.5.3, temos

$$\alpha_g = \alpha_{g^q} = \ldots = \alpha_{g^{t_g - 1}},$$

para cada $g \in G$ e, consequentemente,

$$\alpha = \sum_{g \in \mathcal{T}} \alpha_g \eta_g.$$

■

Pelo Teorema de Perlis-Walker 3.3.1, o número de componentes simples da álgebra de grupo $\mathbb{Q}G$, de um grupo abeliano finito G, é igual ao número de subgrupos cíclicos de G e também o número de seus fatores cíclicos. Se $x \in \mathcal{C}_g$, então $x = g^{q^j}$, para algum j. Como $mdc(q, o(g)) = 1$, então $\langle x \rangle = \langle g \rangle$. Portanto, cada q-classe ciclotômica $\mathcal{C}_g$ é um subconjunto do conjunto $\mathcal{G}_g$ de todos os geradores do grupo cíclico $\langle g \rangle$. Assim, é claro que

o número de subgrupos cíclicos de G é uma cota inferior para o número de componentes simples, e que esta cota é obtida se, e somente se, $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$.

Para os inteiros r e m, denotamos por $\bar{r} \in \mathbb{Z}_m$ a imagem de r no anel dos inteiros módulo m. Então

$$\mathcal{G}_g = \{g^r;\ mdc(r, o(g)) = 1\} = \{g^r;\ \bar{r} \in U(\mathbb{Z}_{o(g)})\}$$

Além disso, para um grupo finito G, o **expoente** $\exp(G)$ é o menor inteiro positivo t tal que $g^t = 1$, para todo $g \in G$.

Teorema 3.5.2. *Sejam $\mathbb{F}$ um corpo finito com q elementos e G um grupo abeliano finito de expoente e, tal que $mdc(q, |G|) = 1$. Então $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, $U(\mathbb{Z}_e)$ é um grupo cíclico gerado por $\bar{q} \in \mathbb{Z}_e$.*

Demonstração. Assuma que $U(\mathbb{Z}_\epsilon)$ é um grupo cíclico gerado por $\bar{q} \in \mathbb{Z}_e$. Para um elemento $g \in G$, temos $o(g) \mid e$.

Seja π o epimorfismo natural de $\mathbb{Z}_e$ em $\mathbb{Z}_{o(g)}$. Como $\bar{q} \in \mathbb{Z}_e$ é um gerador do grupo cíclico $U(\mathbb{Z}_e)$, então $\pi(\bar{q}) \in \mathbb{Z}_{o(g)}$ é um gerador do grupo cíclico $U(\mathbb{Z}_{o(g)})$

Para cada elemento $x \in \mathcal{G}_g$, temos $x = g^r$, para algum inteiro positivo r tal que $\bar{r} \in U(\mathbb{Z}_{o(g)})$. Então $\bar{r} = \pi(\bar{q})^j$, para algum j, e $x = g^{\pi(\bar{q})^j} \in \mathcal{C}_g$. Daí, $\mathcal{G}_g \subset \mathcal{C}_g$ e, portanto, $\mathcal{C}_g = \mathcal{G}_g$.

Reciprocamente, suponha $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$. Se G é um grupo abeliano de expoente e, então existe um elemento $g_0 \in G$ de ordem e, em particular, $\mathcal{C}_{g_0} = \mathcal{G}_{g_0}$.

Daí, para cada inteiro positivo r tal que $\bar{r} \in U(\mathbb{Z}_e)$, temos $g_0^r \in \mathcal{G}_{g_0} = \mathcal{C}_{g_0}$, logo existe algum inteiro j tal que $r = q^j$. Portanto, $\bar{q}$ gera $U(\mathbb{Z}_e)$. ■

Corolário 3.5.1. *Sejam $\mathbb{F}$ um corpo finito com q elementos, G um grupo abeliano finito de expoente e, tal que $mdc(q, |G|) = 1$. Então $\mathcal{C}_g = \mathcal{G}_g$, para todo $g \in G$ se, e somente se, uma das seguintes afirmações acontece.*

(i) $e = 2$ *e* q *é ímpar;*

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

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

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

Demonstração. (i) Sejam $e = 2$. Um gerador do grupo cíclico $U(\mathbb{Z}_2)$ é um elemento $t \in \mathbb{Z}_+$ tal que $mdc(t, 2) = 1$, isto é, todo inteiro positivo ímpar satisfaz essa condição. Logo, se q é ímpar então $\bar{q}$ é um gerador do grupo cíclico $U(\mathbb{Z}_2)$

(ii) Considere o grupo cíclico $U(\mathbb{Z}_4)$. O único gerador de $U(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$ é $\bar{q} = \overline{3}$. Logo, $\bar{q}$ gera $U(\mathbb{Z}_4)$ se, e somente se, $q \equiv 3 \pmod 4$.

(iii) Considere o grupo cíclico $U(\mathbb{Z}_{p^n})$. Então $\bar{q}$ gera $U(\mathbb{Z}_{p^n})$ se, e somente se, $mdc(q, p^n) = 1$. Pelo Teorema de Euler, $q^{\phi(p^n)} \equiv 1 \pmod{p^n}$, isto é, $o(\bar{q}) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$.

(iv) Considere o grupo cíclico $U(\mathbb{Z}_{2p^n})$. Então $\bar{q}$ gera $U(\mathbb{Z}_{2p^n})$ se, e somente se, $mdc(q, 2p^n) = 1$. Pelo Teorema de Euler, $q^{\phi(2p^n)} \equiv 1 \pmod{2p^n}$. Como $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$, segue $q^{\phi(p^n)} \equiv 1 \pmod{2p^n}$, isto é, $\bar{q} = \phi(p^n)$ em $U(\mathbb{Z}_{2p^n})$.

■

4 IDEMPOTENTES PRIMITIVOS

Neste capítulo descrevemos os idempotentes primitivos de uma álgebra de grupo de um grupo abeliano finito. Num primeiro momento, determinamos esses elementos para o caso particular de um grupo cíclico. Num segundo momento, determinamos esses elementos para um caso mais geral, no qual consideramos um grupo abeliano não cíclico.

Para encontrar os idempotentes primitivos nos baseamos em dois artigos principais: [9] e [15]. Calculamos esses elementos a partir da técnica estabelecida em [15], a qual se baseia na teoria de corpos finitos, e também os calculamos a partir da técnica estabelecida em [9], a qual se baseia na teoria de grupos. Cabe observar, no entanto, que optamos por apresentar cada técnica (com seus respectivos cálculos) de modo intercalado, respeitando, primeiro, a estrutura do grupo subjacente à álgebra de grupo, a qual nos referimos em cada seção.

Para maiores detalhes e demonstrações de resultados que apresentamos aqui, sugerimos as referências supracitadas e [5], [8] e [14], como complementares.

Como hipóteses gerais para todo o capítulo, consideramos $\mathbb{F}_q$ um corpo finito e p um primo inteiro positivo tal que $mdc(p, q) = 1$. Além disso, definimos um grupo G por p-**grupo** se seu expoente for uma potência de um primo dado p. Em particular, isso significa que a ordem de cada elemento de G é em si uma potência de p.

Uma consideração importante a se fazer, relativa a abordagem adotada por [15], é que os isomorfismos (4.5) e (4.8) (apresentados neste capítulo) nos permitem transitar com naturalidade entre as estruturas algébricas isomorfas em cada caso, por isso, optamos por não denotar os seus elementos idempotentes de maneiras diferentes

4.1 IDEMPOTENTES PRIMITIVOS EM ÁLGEBRAS DE GRUPO CÍCLICAS

Nesta primeira abordagem, a fatoração de polinômios sobre corpos finitos é bastante utilizada, bem como a função traço definida em 2.1.3, a qual, neste contexto, é denotada por $\mathrm{Tr}_{q^t/q}$, e representa a função traço de $\mathbb{F}_{q^t}$ sobre $\mathbb{F}_q$.

Sejam $G = C_{p^m}$ um p-grupo cíclico gerado por um elemento x de ordem p^m e t a ordem multiplicativa de q módulo p. Usamos a notação $p^s \| (q^t - 1)$ para indicar que s é a maior potência de p tal que $p^s \mid (q^t - 1)$. Adotaremos estas hipóteses ao longo de toda esta seção.

Os Lemas 4.1.2, 4.1.3 e 4.1.4, a seguir, dão uma maneira de fatorar o polinômio ciclotômico $x^{p^m} - 1$ sobre $\mathbb{F}_q$.

Definição 4.1.1. Seja um polinômio mônico $f(x) = \sum_{i=0}^{t} a_i x^i \in \mathbb{F}_q[x]$ (com $a_0 \neq 0$) de grau t sobre $\mathbb{F}_q$. O polinômio $f^*(x)$, dado por

$$f^*(x) = a_0^{-1} x^t f(x^{-1}) = a_0^{-1} \sum_{i=0}^{t} a_{t-i} x^i$$

é o **polinômio recíproco** de $f(x)$. Se $f(x) = f^*(x)$, então dizemos que $f(x)$ é **auto-recíproco** sobre $\mathbb{F}_q$. Para um fator irredutível mônico $f(x) \in \mathbb{F}_q[x]$ de $x^n - 1$, $f^*(x)$ também é um fator irredutível mônico de $x^n - 1$.

Lema 4.1.1. *O polinômio $f(x)$ é auto-recíproco se, e somente se, α^{-1} é uma raiz de $f(x)$ para cada raiz α de $f(x)$ sobre o corpo de decomposição de $f(x)$.*

Lema 4.1.2. *Seja $n \geq 2$ um número inteiro positivo. Para qualquer $\gamma \in \mathbb{F}_q^*$ com $o(\gamma) = e$, $x^n - \gamma$ é irredutível sobre $\mathbb{F}_q$ se, e somente se, as seguintes condições são satisfeitas:*

(i) Todo divisor primo de n divide e, mas não divide $\dfrac{(q-1)}{e}$;

(ii) Se $4 \mid n$, então $4 \mid (q-1)$.

O Lema 4.1.2 pode ser encontrado em [5].

Lema 4.1.3. *Seja $q - 1 = p^s c$ tal que $mdc(c, p) = 1$, $s > 0$ e p é um primo ímpar. Então a fatoração irredutível do polinômio $x^{p^m} - 1$ sobre $\mathbb{F}_q$ é*

$$x^{p^m} - 1 = \begin{cases} \prod_{u=0}^{p^s-1} (x - \zeta_{p^s}^u) \prod_{h=s+1}^{m} \prod_{k=1, p\nmid k}^{p^s-1} (x^{p^{h-s}} - \zeta_{p^s}^k), & se \quad m > s; \\ \prod_{u=0}^{p^m-1} (x - \zeta_{p^m}^u), & se \quad m \leq s; \end{cases}$$

em que ζ_{p^s} e ζ_{p^m} são raízes p^s-ésima e p^m-ésima primitiva da unidade em $\mathbb{F}_q$, respectivamente.

Demonstração. Pelo Teorema 2.1.4, o grupo multiplicativo $\mathbb{F}_q^*$ do corpo finito $\mathbb{F}_q$ é cíclico e de ordem $q - 1 = p^s c$, com $mdc(p, c) = 1$, logo $\mathbb{F}_q^* = \langle \xi \rangle$, em que ξ é uma raiz $(q-1)$-ésima primitiva da unidade em $\mathbb{F}_q$. Além disso, como $p^s \mid (q-1)$, existe um único subgrupo em $\mathbb{F}_q^*$ de ordem p^s. Se $m \leq s$, então existe uma raiz p^m-ésima primitiva da unidade ζ_{p^m} no subgrupo de ordem p^s de $\mathbb{F}_q^*$. Logo, $\zeta_{p^m} \in \mathbb{F}_q$ e, portanto, $x^{p^m} - 1$ é separável sobre $\mathbb{F}_q$.

Agora, investigamos o caso $m > s$. Seja $\zeta = \xi^c$. Então ζ é uma raiz p^s-ésima primitiva da unidade, que denotamos por ζ_{p^s}. Para $1 \leq k \leq p^s - 1$ e $mdc(p, k) = 1$,

temos $o(\zeta_{p^s}^k) = p^s$. Assim, $p \mid o(\zeta_{p^s})$ e $mdc\left(p, \dfrac{q-1}{o(\zeta_{p^m}^k)}\right) = 1$. Pelo Lema 4.1.2, o polinômio $x^{p^j} - \zeta_{p^s}^k$ é irredutível em $\mathbb{F}_q[x]$. Além disso, $x - \zeta_{p^s}^u$ e $x^{p^j} - \zeta_{p^s}^k$ são divisores de $x^{p^m} - 1$, para $1 \leq j \leq m-s$ e $1 \leq u \leq p^s - 1$, com $mdc(p, j) = 1$. Como os fatores irredutíveis $x - \zeta_{p^s}^u$ e $x^{p^j} - \zeta_{p^s}^k$ são distintos entre si, então

$$\prod_{u=0}^{p^s-1}(x - \zeta_{p^s}^k) \cdot \prod_{j=1}^{m-s}\prod_{\substack{k=1 \\ p\nmid k}}^{p^s-1}(x^{p^j} - \zeta_{p^s}^k) \mid (x^{p^m} - 1). \tag{4.1}$$

Por outro lado, o grau de $\displaystyle\prod_{k=1\ p\nmid k}^{p^{s-1}}(x^{p^j} - \zeta_{p^s}^j)$ é $p^j(p^s - p^{s-1})$. Logo, o grau do produtório de fatores que dividem $x^{p^m} - 1$ em (4.1) é

$$p^s + (p + p^2 + \ldots + p^{m-s})(p^s - p^{s-1}) = p^s + \frac{p^{m-s+1} - p}{p-1}(p^s - p^{s-1}) = p^m.$$

Portanto, vale a igualdade entre o polinômio $x^{p^m} - 1$ e o polinômio formado pelo produtório de fatores irredutíveis dados em (4.1). Isto prova o resultado. ■

Lema 4.1.4. *Sejam p um primo tal que $mdc(p, q) = 1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t - 1)$. Temos,*

(i) se t é par e $1 \leq m \leq s$, então a fatoração irredutível de $x^{p^m} - 1$ sobre $\mathbb{F}_q$ é

$$x^{p^m} - 1 = (x-1)\prod_{\delta=1}^{m}\Phi_{p^\delta}(x) = (x-1)\prod_{\delta=1}^{m}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(x), \tag{4.2}$$

em que cada $f_{\delta,i}(x) = \displaystyle\prod_{\mu=0}^{t-1}(x - \zeta_{p^\delta}^{l_i q^\mu})$, com $mdc(l_i, p) = 1$, é irredutível sobre $\mathbb{F}_q$.

(ii) se t é par e $m > s$, então a fatoração irredutível de $x^{p^m} - 1$ sobre $\mathbb{F}_q$ é

$$x^{p^m} - 1 = (x-1)\prod_{h=1}^{m}\Phi_{p^h}(x) = (x-1)\prod_{\delta=1}^{s}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(x)\prod_{\varepsilon=s+1}^{m}\prod_{i=1}^{\frac{\phi(p^s)}{t}} f_{\varepsilon,i}(x), \tag{4.3}$$

em que cada $f_{\delta,i}(x) = \displaystyle\prod_{\mu=0}^{t-1}(x - \zeta_{p^\delta}^{l_i q^\mu})$, com $1 \leq \delta \leq s$, é irredutível sobre $\mathbb{F}_q$, e cada $f_{\varepsilon,i}(x) = \displaystyle\prod_{\mu=0}^{t-1}(x^{p^{\varepsilon-s}} - \zeta_{p^s}^{l_i q^\mu})$, com $s+1 \leq \varepsilon \leq m$, é irredutível sobre $\mathbb{F}_q$.

Demonstração. Se $1 \leq m \leq s$, temos, por (2.3) e a Definição 2.1.8,

$$x^{p^m} - 1 = \prod_{h=1}^{m}(x - \zeta_{p^m}^j) = \prod_{h=1}^{m}\prod_{j\in S_h}(\zeta_{p^m}^j).$$

Logo, por (2.4) e (2.5), $f_{h,i}(x) = \prod_{\mu=0}^{t-1}(x - \zeta_{p^h}^{l_i q^\mu})$, com $mdc(l_i, p) = 1$, é irredutível sobre $\mathbb{F}_q$, para $1 \leq h \leq m$, $1 \leq i \leq \dfrac{\phi(p^h)}{t}$. Além disso, t par implica em $q^t - 1 = (q^{\frac{t}{2}} - 1)(q^{\frac{t}{2}} + 1)$, donde segue $p \nmid q^{\frac{t}{2}-1}$ e $p^s \mid q^{\frac{t}{2}+1}$, consequentemente, $q^{\frac{t}{2}} \equiv -1 \pmod{p^s}$. Como $\dfrac{\mathbb{F}_q[x]}{\langle f_{h,i}(x)\rangle} \cong \mathbb{F}_{q^t}$ e $f_{h,i}(\bar{x}) = \bar{0}$, temos, pelo automorfismo (de Frobenius) $\sigma : \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_{q^t}$, definido por $\sigma(x) = x^q$, com $Gal(\mathbb{F}_{q^t}, \mathbb{F}_q) = \langle\sigma\rangle$. Logo,

$$0 = \sigma^{\frac{t}{2}}(f_{h,i}(\bar{x})) = f_{h,i}(\sigma^{\frac{t}{2}}(\bar{x})) = \bar{x}^{q^{\frac{t}{2}}}.$$

É claro que $\bar{x}^{q^{\frac{t}{2}}}$ é uma raiz de $f_{h,i}(x)$ e, como $\bar{x} = \zeta_{p^h}^{l_i}$, para algum l_i tal que $mdc(l_i, p) = 1$, segue $\bar{x}^{q^{\frac{t}{2}}} = (\zeta_{p^h}^{l_i})^{q^{\frac{t}{2}}} = (\zeta_{p^h}^{q^{\frac{t}{2}}})^{l_i}$. Como $\zeta_{p^n} \in \langle\zeta_{p^s}\rangle \subset \mathbb{F}_{q^t}^*$ e $q^{\frac{t}{2}} \equiv -1 \pmod{p^s}$, então $\bar{x}^{q^{\frac{t}{2}}} = \zeta_{p^h}^{-l_i}$. Logo, $f_{h,i}(\zeta_{p^h}^{l_i}) = 0 = f_{h,i}(\zeta_{p^h}^{-l_i})$. Portanto, pelo Lema 4.1.1, $f_{h,i}$ é auto-recíproco. Isto prova o resultado para o caso $1 \leq m \leq s$.

Se $m > s$, sejam $S = \{j, 1 \leq j \leq p^s\}$ e $S_h = \{j = p^{m-h} l_i \in S, mdc(l_i, p) = 1\}$, com $h = 0, 1, \ldots, m$, em que $S_0 = \{p^s\}$. Para $1 \leq h \leq m$, defina

$$\Psi_h(x) = \begin{cases} \displaystyle\prod_{j \in S_\delta} (x - \zeta_{p^s}^j), & \text{se } \ 1 \leq \delta \leq s; \\ \displaystyle\prod_{j \in S_m} (x^{p^{\varepsilon - s}} - \zeta_{p^s}^j), & \text{se } s+1 \leq \varepsilon \leq m. \end{cases} \tag{4.4}$$

Por (4.4) e o Lema 4.1.2, temos a seguinte fatoração do polinômio $x^{p^m} - 1$ sobre $\mathbb{F}_{q^t}$:

$$x^{p^m} - 1 = x^{p^m} - 1 = \Psi_0(x) \ldots \Psi_s(x) \Psi_{s+1}(x) \ldots \Psi_m(x).$$

Com isso, de modo similar ao caso anterior, obtemos $f_{\delta,i}(x) = \prod_{\mu=0}^{t-1}(x - \zeta_{p^\delta}^{l_i q^\mu})$, com $mdc(l_i, p) = 1$, irredutível sobre $\mathbb{F}_q$, para $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$; $f_{\varepsilon,i}(x) = \prod_{\mu=0}^{t-1}(x^{p^{\varepsilon-s}} - \zeta_{p^s}^{l_i q^\mu})$, com $mdc(l_i, p) = 1$, irredutível sobre $\mathbb{F}_q$, para $s+1 \leq \varepsilon \leq m$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$. Quanto à auto-reciprocidade de $f_{\varepsilon,i}$, fazendo $z = x^{p^{\varepsilon-s}}$, o resultado segue de forma análoga ao caso anterior. ■

Note que, no Lema 4.1.4, $0 \leq h \leq m$. Pelo item (ii), podemos ter $m > s$ e, neste caso, adotamos $h = \delta$, se $1 \leq \delta \leq s$, e $h = \varepsilon$, se $s+1 \leq h \leq m$, como visto na demonstração. A partir daqui, adotaremos esse padrão em todo texto.

Considere as hipóteses adotadas no início da seção. Por (3.4), temos

$$\mathbb{F}_q G \cong \frac{\mathbb{F}_q[x]}{\langle x^{p^m} - 1\rangle} = \mathcal{R}_{p^m}. \tag{4.5}$$

Convém observar que, quando o grau do polinômio $x^{p^m}-1$ é tal que $m \leq s$, a hipótese $p^s \| (q^t-1)$ garante que todas as raízes deste polinômio estejam na extensão $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$. Por outro lado, quando $m > s$, nem todas as raízes de $x^{p^m}-1$ estão em $\mathbb{F}_{q^t}$, isso quer dizer que existem fatores do polinômio que são irredutíveis sobre $\mathbb{F}_{q^t}$, como foi abordado na demonstração do Lema 4.1.3.

A seguir, obtemos um resultado, com as hipóteses mencionadas anteriormente, que nos permitirá calcular todos os idempotentes primitivos da álgebra de grupos $\mathbb{F}_qG$.

Teorema 4.1.1. *Sejam p um primo inteiro tal que $mdc(p,q)=1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t-1)$. Sejam*

$$S=\{j : 1 \leq j \leq p^m\} \quad e \quad S_h=\{j=p^{m-h}l \in S : 1 \leq l \leq p^\delta, mdc(l,p)=1\}.$$

Então os idempotentes primitivos do anel $\dfrac{\mathbb{F}_q[x]}{\langle x^{p^m}-1\rangle}$ são dados como segue:

(i) O idempotente primitivo

$$e_0(x)=\frac{1}{p^m}\sum_{u=0}^{p^m-1}x^u$$

corresponde ao polinômio irredutível $x-1$ sobre $\mathbb{F}_q$.

(ii) Se $1 \leq \delta \leq s$ $(h=\delta)$, então os idempotentes primitivos

$$e_{\delta,i}(x)=\frac{1}{p^m}\frac{x^{p^m}-1}{x^{p^\delta}-1}\sum_{u=0}^{p^\delta-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_iu})x^u, \text{ para } 1 \leq i \leq \frac{\phi(p^\delta)}{t},$$

correspondem aos polinômios irredutíveis $f_{\delta,i}(x)$ sobre $\mathbb{F}_q$ dados em (4.2).

(iii) Se $s+1 \leq h \leq m$ $(h=\varepsilon)$, então os idempotentes primitivos

$$e_{\varepsilon,i}(x)=\frac{1}{p^{m+s-\varepsilon}}\frac{x^{p^m}-1}{x^{p^\varepsilon}-1}\sum_{u=0}^{p^s-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_iu})x^{up^{\varepsilon-s}}, \text{ para } 1 \leq i \leq \frac{\phi(p^s)}{t},$$

correspondem aos polinômios irredutíveis $f_{\varepsilon,i}(x)$ sobre $\mathbb{F}_q$ dados em (4.3).

Além disso, se $m \leq s$, então existem $1+\dfrac{p^m-1}{t}$ idempotentes primitivos em $\dfrac{\mathbb{F}_q[x]}{\langle x^{p^m}-1\rangle}$; se $m > s$, então existem $1+\dfrac{p^s-1}{t}+\dfrac{(m-s)\,(p^s-p^{s-1})}{t}$ idempotentes primitivos em $\dfrac{\mathbb{F}_q[x]}{\langle x^{p^m}-1\rangle}$.

Exemplo 4.1.1. Sejam $p=3, q=17$. Então $t=2$ é a ordem multiplicativa de 17 módulo 3, e $3^2\|(17^2-1)$, isto é, $s=2$ é a maior potência de 3 que divide 17^2-1. Para $1 \leq m \leq s$, temos dois casos:

(i) Se $m = 1$, temos a seguinte fatoração do polinômio $x^3 - 1$ sobre $\mathbb{F}_{17}$:

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

em que $f_{1,1}(x) = (x - \zeta_3)(x - \zeta_3^2) = x^2 + x + 1$, com $l_i = 1$. Assim, $\mathrm{Tr}_{q^2/q}(\zeta_3^{-1}) = \mathrm{Tr}_{q^2/q}(\zeta_3^{-2}) = -1$. Logo, existem 2 idempotentes primitivos em $\mathbb{F}_{17}(C_3)$:

$$\begin{aligned} e_0(x) &= \frac{1}{3}\sum_{u=0}^{2} x^u = \frac{1}{3}(1 + x + x^2); \\ e_{1,1}(x) &= \frac{1}{3}\frac{x^3-1}{x^3-1}\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u = \frac{1}{3}(2 - x - x^2). \end{aligned} \tag{4.6}$$

(ii) Se $m = 2$, temos a seguinte fatoração do polinômio $x^9 - 1$ sobre $\mathbb{F}_{17}$:

$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^2 - 7x + 1)(x^2 - 13x + 1)(x^2 - 14x + 1),$$

em que

$$\begin{aligned} f_{1,1}(x) &= (x - \zeta_3)(x - \zeta_3^2) = x^2 + x + 1; \\ f_{2,1}(x) &= (x - \zeta_9)(x - \zeta_9^8) = x^2 - 7x + 1; \\ f_{2,2}(x) &= (x - \zeta_9^2)(x - \zeta_9^7) = x^2 - 13x + 1; \\ f_{2,3}(x) &= (x - \zeta_9^4)(x - \zeta_9^5) = x^2 - 14x + 1, \end{aligned}$$

com $l_1 = 1, l_2 = 2, l_3 = 4$. Daí,

$$\begin{aligned} \mathrm{Tr}_{q^2/q}(\zeta_3^{-1}) &= \mathrm{Tr}_{q^2/q}(\zeta_3^{-2}) = -1; \\ \mathrm{Tr}_{q^2/q}(\zeta_9^{-1}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-8}) = 7; \\ \mathrm{Tr}_{q^2/q}(\zeta_9^{-2}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-7}) = 13; \\ \mathrm{Tr}_{q^2/q}(\zeta_9^{-4}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-5}) = 14. \end{aligned}$$

Logo, existem 5 idempotentes primitivos em $\mathbb{F}_{17}(C_9)$:

$$\begin{aligned} e_0(x) &= \frac{1}{9}\sum_{u=0}^{8} x^u = \frac{1}{3}(1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8); \\ e_{1,1}(x) &= \frac{1}{9}\frac{x^9-1}{x^3-1}\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u \\ &= \frac{1}{9}(x^6 + x^3 + 1)(2 - x - x^2); \\ e_{2,1}(x) &= \frac{1}{9}\frac{x^9-1}{x^9-1}\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u \\ &= \frac{1}{9}(2 + 7x + 13x^2 - x^3 + 14x^4 + 14x^5 - x^6 + 13x^7 + 7x^8); \\ e_{2,2}(x) &= \frac{1}{9}\frac{x^9-1}{x^9-1}\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u \end{aligned} \tag{4.7}$$

$$= \frac{1}{9}(2 + 13x + 14x^2 - x^3 + 7x^4 + 7x^5 - x^6 + 14x^7 + 13x^8);$$

$$e_{2,3}(x) = \frac{1}{9}\frac{x^9 - 1}{x^9 - 1}\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u$$

$$= \frac{1}{9}(2 + 14x + 7x^2 - x^3 + 13x^4 + 14x^5 - x^6 + 7x^7 + 14x^8).$$

Para $1 \leq s < m$, podemos tomar $m = 3$ como exemplo. Neste caso, temos a seguinte fatoração do polinômio $x^{27} - 1$ sobre $\mathbb{F}_{17}$:

$$x^{27} - 1 = (x-1)(x^2 + x + 1)(x^2 - 7x + 1)(x^2 - 13x + 1)(x^2 - 14x + 1)(x^6 - 7x^3 + 1)$$
$$(x^6 - 13x^3 + 1)(x^6 - 14x^3 + 1),$$

em que

$$\begin{aligned}
f_{1,1}(x) &= (x - \zeta_3)(x - \zeta_3^2) = x^2 + x + 1;\\
f_{2,1}(x) &= (x - \zeta_9)(x - \zeta_9^8) = x^2 - 7x + 1;\\
f_{2,2}(x) &= (x - \zeta_9^2)(x - \zeta_9^7) = x^2 - 13x + 1;\\
f_{2,3}(x) &= (x - \zeta_9^4)(x - \zeta_9^5) = x^2 - 14x + 1;\\
f_{3,1}(x) &= (x^3 - \zeta_9)(x^3 - \zeta_9^8) = x^6 - 7x^3 + 1;\\
f_{3,2}(x) &= (x^3 - \zeta_9^2)(x^3 - \zeta_9^7) = x^6 - 13x^3 + 1;\\
f_{3,3}(x) &= (x^3 - \zeta_9^4)(x^3 - \zeta_9^5) = x^6 - 14x^3 + 1.
\end{aligned}$$

com $l_1 = 1, l_2 = 2, l_3 = 4$. Daí,

$$\begin{aligned}
\mathrm{Tr}_{q^2/q}(\zeta_3^{-1}) &= \mathrm{Tr}_{q^2/q}(\zeta_3^{-2}) = -1;\\
\mathrm{Tr}_{q^2/q}(\zeta_9^{-1}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-8}) = 7;\\
\mathrm{Tr}_{q^2/q}(\zeta_9^{-2}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-7}) = 13;\\
\mathrm{Tr}_{q^2/q}(\zeta_9^{-4}) &= \mathrm{Tr}_{q^2/q}(\zeta_9^{-5}) = 14.
\end{aligned}$$

Logo, existem 8 idempotentes primitivos em $\mathbb{F}_{17}(C_{27})$:

$$\begin{aligned}
e_0(x) &= \frac{1}{27}\sum_{u=0}^{26} x^u = \frac{1}{27}(1 + x + x^2 + \ldots + x^{26});\\
e_{1,1}(x) &= \frac{1}{27}\frac{x^{27} - 1}{x^3 - 1}\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\\
&= \frac{1}{27}(1 + x^3 + x^6 + x^9 + x^{12} + x^{15} + x^{18} + x^{21} + x^{24})(2 - x - x^2);\\
e_{2,1}(x) &= \frac{1}{27}\frac{x^{27} - 1}{x^9 - 1}\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\\
&= \frac{1}{27}(1 + x^9 + x^{18})(2 + 7x + 13x^2 - x^3 + 14x^4 + 14x^5 - x^6 + 13x^7 + 7x^8);\\
e_{2,2}(x) &= \frac{1}{27}\frac{x^{27} - 1}{x^9 - 1}\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{27}(1+x^9+x^{18})(2+13x+14x^2-x^3+7x^4+7x^5-x^6+14x^7+13x^8);\\
e_{2,3}(x) &= \frac{1}{27}\frac{x^{27}-1}{x^9-1}\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\\
&= \frac{1}{27}(1+x^9+x^{18})(2+14x+7x^2-x^3+13x^4+14x^5-x^6+7x^7+14x^8);\\
e_{3,1}(x) &= \frac{1}{27}\frac{x^{27}-1}{x^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\\
&= \frac{1}{27}(6+7x+13x^2-x^3+\ldots+14x^{23}-x^{24}+13x^{25}+7x^{26});\\
e_{3,2}(x) &= \frac{1}{27}\frac{x^{27}-1}{x^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\\
&= \frac{1}{27}(6+13x+14x^2-x^3+\ldots+7x^{23}-x^{24}+14x^{25}+13x^{26});\\
e_{3,3}(x) &= \frac{1}{27}\frac{x^{27}-1}{x^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\\
&= \frac{1}{27}(6+14x+7x^2-x^3+\ldots+14x^{23}-x^{24}+7x^{25}+14x^{26}).
\end{aligned}
$$

Agora, vamos apresentar os idempotentes primitivos calculados a partir da teoria de grupos. A ideia central nesta outra abordagem é estabelecer uma relação entre os idempotentes primitivos da álgebra de grupo $\mathbb{F}_qG$ e os subgrupos do grupo cíclico G subjacentes a esta álgebra de grupo. Para isso, apresentamos algumas definições e resultados dados em [9].

Lema 4.1.5. *Sejam p um número primo e $G=\langle a\rangle$ um grupo cíclico de ordem p^m, $m\geq 1$. Considere*

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

a cadeia descendente de todos os subgrupo cíclicos de G, em que $G_i=\langle a^{p^i}\rangle$. Então os elementos

$$e_0=\widehat{G}=\frac{1}{|G|}\sum_{g\in G} g \quad e \quad e_i=\widehat{G_i}-\widehat{G_{i-1}}=\frac{1}{|G_i|}\sum_{g\in G_i} g-\frac{1}{|G_{i-1}|}\sum_{g\in G_{i-1}},\quad 1\leq i\leq m,$$

formam um conjunto de idempotentes primitivos na álgebra de grupo $\mathbb{Q}G$ tal que

$$e_0+e_1+\cdots+e_m=1.$$

Demonstração. Pelo Corolário 3.3.1, do Teorema de Perlis-Walker,

$$\mathbb{Q}G\cong\bigoplus_{p^i|p^m} a_{p^i}\mathbb{Q}(\zeta_{p^i})=\bigoplus_{p^i|p^m}\mathbb{Q}(\zeta_{p^i}),\quad \text{com } 0\leq i\leq m,$$

em que ζ_{p^i} denota uma raiz primitiva da unidade de ordem p^i e temos, precisamente, $m+1$ idempotentes primitivos na álgebra de grupo $\mathbb{Q}G$. Como $\widehat{G_i}\widehat{G_j}=\widehat{G_i}$, para todos

$0 \leq i < j \leq m$, segue

$$e_0 e_i = \widehat{G}(\widehat{G_i} - \widehat{G_{i-1}}) = 0 \quad \text{e}$$
$$e_i e_j = (\widehat{G_i} - \widehat{G_{i-1}})(\widehat{G_j} - \widehat{G_{j-1}}) = \widehat{G_i}\widehat{G_j} - \widehat{G_i}\widehat{G_{j-1}} - \widehat{G_{i-1}}\widehat{G_j} + \widehat{G_{i-1}}\widehat{G_{j-1}} = 0,$$

para $1 \leq i < j \leq m$. Assim, os idempotentes e_i, e_j, com $j \neq i$, são dois a dois ortogonais. Além disso, temos

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

Logo, $\{e_0, e_1, \ldots, e_m\}$ é o conjunto dos $m+1$ idempotentes de $\mathbb{Q}G$.

Suponha que exista e_i, para algum $0 \leq i \leq m$, tal que $e_i = e_i' + e_i''$, com $e_i', e_i'' \neq 0$ e $e_i' e_i'' = 0$. Assim, $e_i' + e_i'' + \sum_{\substack{j=0 \\ j \neq i}}^{m} e_j = 1$ e $(e_i' + e_i'')e_j = 0$, para todo $0 \leq j \leq m$, com $j \neq i$. Logo, o conjunto $\{e_i', e_i''\} \cup \{e_j\}_{\substack{0 \leq j \leq m \\ j \neq i}}$ é um conjunto com $m+2$ idempotentes em $\mathbb{Q}G$, o que é uma contradição. Portanto, $\{e_0, e_1, \ldots, e_m\}$ é o conjunto dos idempotentes primitivos de $\mathbb{Q}G$. ■

O Corolário a seguir estabelece condições necessárias e suficientes para que o conjunto formado pelos idempotentes primitivos da álgebra de grupo $\mathbb{F}_q G$ seja dado da mesma maneira que o conjunto de idempotentes primitivos da álgebra de grupo $\mathbb{Q}G$. Tais condições são firmadas de modo a garantir que o número de componentes simples de $\mathbb{F}_q G$ seja igual ao de $\mathbb{Q}G$. Dizemos que este número de componentes é minimal.

Corolário 4.1.1. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos, G um grupo cíclico de ordem p^m, tal que $mdc\,(q, p^m) = 1$. Então o conjunto de idempotentes primitivos dados no Lema 4.1.5 é o conjunto de idempotentes primitivos de $\mathbb{F}_q G$ se, e somente se, vale uma das seguintes afirmações.*

(i) $p = 2$, $m = 1$ e q é ímpar ou $m = 2$ e $q \equiv (3 \bmod 4)$;

(ii) p é um primo ímpar e $o(\bar{q}) = \phi(p^m)$ em $U(\mathbb{Z}_{p^m})$.

Como consequência imediata do Corolário 4.1.1 temos o seguinte resultado.

Teorema 4.1.2. *Sejam $\mathbb{F}_q$ um corpo finito com q elementos e G um grupo cíclico de ordem p^m tal que $o(\bar{q}) = \phi(p^m)$ em $U(\mathbb{Z}_{p^m})$. Seja*

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

a cadeia descendente de todos os subgrupos cíclicos de G, em que $G_i = \langle a^{p^i} \rangle$. Então o conjunto dos idempotentes primitivos de $\mathbb{F}_q G$ é dado por

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

O Lema 4.1.5, o Corolário 4.1.1 e o Teorema 4.1.2 deixam claro que os idempotentes da álgebra de grupo $\mathbb{F}_qG$, construída a partir das hipóteses gerais estabelecidas no início deste capítulo, são primitivos se, e somente se, o número de componentes simples desta álgebra de grupo for minimal. Quando as hipóteses não são satisfeitas, pode-se construir os idempotentes primitivos utilizando a teoria de corpos finitos, como vimos no Exemplo 4.1.1 — no qual os polinômios x^6+x^3+1 e $x^{18}+x^9+1$ são redutíveis sobre $\mathbb{F}_{17}$, mas são irredutíveis sobre $\mathbb{Q}$. Para enriquecer essa discussão, considere o exemplo a seguir.

Exemplo 4.1.2. Sejam $\mathbb{F}_{11}$ um corpo finito com 11 elementos e $p=3$ um primo ímpar. Seja $G=\langle a\rangle$ um grupo cíclico finito de ordem 3^m. Daí,

(i) para $m=1$, como $mdc(11,3)=1$ e $o(\overline{11})=2=\phi(3)$ em $U(\mathbb{Z}_3)$, temos, pelo Teorema 4.1.2,

$$\langle a\rangle = G_0 \supset G_1 = \{1\}.$$

Logo, o conjunto de idempotentes primitivos de $\mathbb{F}_qG$ é dado por

$$\begin{aligned} e_0 &= \frac{1}{3}\sum_{g\in G} g = \frac{1}{3}(1+a+a^2)\\ e_1 &= \widehat{G_1}-\widehat{G_0} = 1-\frac{1}{3}(1+a+a^2) = \left(1-\frac{1}{3}\right)-\frac{1}{3}(a+a^2) = \frac{1}{3}(2-a-a^2); \end{aligned}$$

(ii) para $m=2$, como $mdc(11,9)=1$ e $o(\overline{11})=6=\phi(9)$ em $U(\mathbb{Z}_9)$, temos, pelo Teorema 4.1.2,

$$\langle a\rangle = G_0 \supset \langle a^3\rangle = G_1 \supset G_2 = \{1\}.$$

Logo, o conjunto de idempotentes primitivos de $\mathbb{F}_qG$ é dado por

$$\begin{aligned} e_0 &= \frac{1}{9}\sum_{g\in G} g = \frac{1}{9}(1+a+a^2+a^3+a^4+a^5+a^6+a^7+a^8);\\ e_1 &= \widehat{G_1}-\widehat{G_0} = \frac{1}{3}(1+a^3+a^6)-\frac{1}{9}(1+a+a^2+a^3+a^4+a^5+a^6+a^7+a^8)\\ &= \left(\frac{1}{3}-\frac{1}{9}\right)(1+a^3+a^6)+\frac{1}{9}(a+a^2+a^4+a^5+a^7+a^8);\\ e_2 &= \widehat{G_2}-\widehat{G_1} = 1-\frac{1}{3}(1+a^3+a^6) = \left(1-\frac{1}{3}\right)-\frac{1}{3}(a^3+a^6); \end{aligned}$$

(iii) para $m=3$, como $mdc(11,27)=1$ e $o(\overline{11})=18=\phi(27)$ em $U(\mathbb{Z}_{27})$, temos, pelo Teorema 4.1.2,

$$\langle a\rangle = G_0 \supset \langle a^3\rangle = G_1 \supset \langle a^9\rangle = G_2 \supset G_3 = \{1\}.$$

Logo, o conjunto de idempotentes primitivos de $\mathbb{F}_qG$ é dado por

$$e_0 = \frac{1}{27}\sum_{g\in G} g = \frac{1}{27}(1+a+a^2+\ldots+a^{26});$$

$$
\begin{aligned}
e_1 &= \widehat{G_1} - \widehat{G_0} = \frac{1}{9}(1 + a^3 + \ldots + a^{21} + a^{24}) - \frac{1}{27}(1 + a + a^2 \ldots + a^{26}) \\
&= \left(\frac{1}{9} - \frac{1}{27}\right)(1 + a^3 + \ldots + a^{21} + a^{24}) + \frac{1}{27}(a + a^2 + a^4 + \ldots + a^{23} + a^{25} + a^{26}); \\
e_2 &= \widehat{G_2} - \widehat{G_1} = \frac{1}{3}(1 + a^9 + a^{18}) - \frac{1}{9}(1 + a^3 + \ldots + a^{21} + a^{24}) \\
&= \left(\frac{1}{3} - \frac{1}{9}\right) - \frac{1}{3}(1 + a^9 + a^{18}) - \frac{1}{9}(1 + a^3 + \ldots + a^8 + a^{10} + \ldots + a^{21} + a^{24}); \\
e_3 &= \widehat{G_3} - \widehat{G_2} = 1 - \frac{1}{3}(1 + a^9 + a^{18}) = \left(1 - \frac{1}{3}\right)(a^9 + a^{18}).
\end{aligned}
$$

Note que as hipóteses do Teorema 4.1.2 são satisfeitas no Exemplo 4.1.1 para o caso em que $m = 1$, pois $o(17) = 2 = \phi(3)$ em $U(\mathbb{Z}_3)$. Portanto, os idempotentes primitivos encontrados nos Exemplos 4.1.1 e 4.1.2 são iguais neste caso, independente da teoria aplicada nos cálculos. No entanto, para os casos em que $m = 2$ e $m = 3$, $o(17) = 2 < 6 = \phi(9)$ em $U(\mathbb{Z}_9)$ e $o(17) = 2 < 18 = \phi(27)$ em $U(\mathbb{Z}_{27})$. Assim, no caso em que as hipóteses do Teorema 4.1.2 não são satisfeitas, existem mais idempotentes primitivos, uma vez que cada um deles corresponde aos fatores irredutíveis do polinômio $x^{p^m} - 1$.

4.2 IDEMPOTENTES PRIMITIVOS EM ÁLGEBRAS DE GRUPO ABELIANAS

É razoável pensar no que acontece quando se adotam hipóteses mais gerais para o grupo G. Motivados por isso, apresentamos como se determina os idempotentes primitivos de uma álgebra de grupo $\mathbb{F}_qG$, com G um p-grupo abeliano finito e não cíclico. Primeiramente, fizemos um estudo acerca dos subgrupos de alguns p-grupos abelianos específicos que nos serão úteis adiante. Por conseguinte, calculamos os idempotentes primitivos dessa álgebra de grupo a partir das técnicas estabelecidas em [8] e [15].

4.2.1 Subgrupos dos grupos abelianos $C_{p^2} \times C_p$ e $C_{p^2} \times C_{p^2}$

Nesta seção será feito um estudo sobre os grupos abelianos finitos da forma $C_{p^2} \times C_p$ e $C_{p^2} \times C_{p^2}$, com C_p e C_{p^2} p-grupos cíclicos de ordem p e p^2, respectivamente. Como os códigos que serão abordados nesta dissertação são construídos como ideais de uma álgebra de p-grupo abeliano finito da forma $\mathbb{F}_q(C_{p^m} \times C_{p^n})$, com p um primo ímpar e $\mathbb{F}_q$ um corpo finito com q elementos, é importante conhecer a estrutura de subgrupos do grupo subjacente.

4.2.1.1 Subgrupos de $C_{p^2} \times C_p$

Seja $G = C_{3^2} \times C_3$ o grupo abeliano produto direto dos grupos cíclicos $C_{3^2} = \langle a \rangle$ e $C_3 = \langle b \rangle$, em que $o(a) = 3^2$ e $o(b) = 3$. Temos $\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$,

$\langle b\rangle = \{e, b, b^2\}$ e $\langle a^3\rangle = \{e, a^3, a^6\} = \langle a^6\rangle$, com $o(a^3) = o(a^6) = 3$. Como o subgrupo gerado por a é cíclico de ordem 3^2, então os elementos de $\langle a\rangle$ cuja potência é prima com 3^2 são também geradores de $\langle a\rangle$, ou seja, $\langle a\rangle = \langle a^2\rangle = \langle a^4\rangle = \langle a^5\rangle = \langle a^7\rangle = \langle a^8\rangle$. Pelo mesmo argumento conclui-se $\langle b\rangle = \langle b^2\rangle$.

Note que $\langle ab\rangle = \{e, ab, a^2b^2, a^3b^3, a^4b^4, a^5b^5, a^6b^6, a^7b^7, a^8b^8\}$ e verifica-se que os únicos elementos de ordem 3 em $\langle ab\rangle$ são a^3 e a^6. Como o subgrupo gerado por ab é cíclico de ordem 3^2, então os elementos de ordem 3^2 em $\langle ab\rangle$ também são geradores de $\langle ab\rangle$. Logo $\langle ab\rangle = \langle a^2b^2\rangle, \langle a^4b\rangle = \langle a^5b^2\rangle = \langle a^7b\rangle = \langle a^8b^2\rangle$. Já os elementos a^3 e a^6 em $\langle ab\rangle$ são de ordem 3 e, portanto, geradores de um mesmo subgrupo de ordem 3 em $\langle ab\rangle$.

O grupo $G = C_{3^2} \times C_3 = \langle a\rangle \times \langle b\rangle$ é um produto direto interno, por esta razão, o subgrupo gerado por $\langle a^3\rangle \times \langle b\rangle$ é um produto direto interno e é dado por $\langle a^3\rangle \times \langle b\rangle = \{e, a^3, a^6, b, b^2, a^3b, a^3b^2, a^6b, a^6b^2\}$ de ordem 3^2, no qual todos os seus elementos diferentes do neutro têm ordem 3. Assim, o produto direto entre quaisquer dois elementos distintos e não neutros de $\langle a^3\rangle \times \langle b\rangle$ que geram subgrupos também distintos são geradores de $\langle a^3\rangle \times \langle b\rangle$, ou seja, $\langle a^3\rangle \times \langle b\rangle = \langle a^3\rangle \times \langle b^2\rangle = \langle a^3b\rangle \times \langle b\rangle = \langle a^3\rangle \times \langle b^2\rangle = \ldots = \langle a^6b\rangle \times \langle a^6b^2\rangle$. No entanto, os elementos distintos e não neutros de $\langle a^3\rangle \times \langle b\rangle$ que geram o mesmo subgrupo não são geradores de $\langle a^3\rangle \times \langle b\rangle$, como por exemplo, $\langle a^3b\rangle = \{e, a^3b, a^6b^2\} = \langle a^6b^2\rangle$ e $\langle a^3b\rangle \times \langle a^6b^2\rangle = \{e, a^3b, a^6b^2\}$, que é o mesmo subgrupo gerado por cada um dos grupos cíclicos deste produto direto. Também temos $\langle ab^2\rangle = \{e, ab^2, a^2b, a^3, a^4b^2, a^5b, a^6, a^7b^2, a^8b\}$, logo $\langle ab^2\rangle = \langle a^2b\rangle = \langle a^4b^2\rangle = \langle a^5b\rangle = \langle a^2b^2\rangle = \langle a^8b\rangle$, todos de ordem 3^2.

Desta forma, ficam determinados todos os subgrupos não triviais de $C_{3^2} \times C_3$.

i) Subgrupos de ordem 3:
$\langle b\rangle = \langle b^2\rangle$; $\langle a^3\rangle = \langle a^6\rangle$; $\langle a^3b\rangle = \langle a^6b^2\rangle = \langle a^3b\rangle \times \langle a^6b^2\rangle$; $\langle a^3b^2\rangle = \langle a^6b\rangle = \langle a^3b^2\rangle \times \langle a^6b\rangle$.

ii) Subgrupos de ordem 3^2:
$\langle a\rangle = \langle a^2\rangle = \langle a^4\rangle = \langle a^5\rangle = \langle a^7\rangle = \langle a^8\rangle$; $\langle ab\rangle = \langle a^2b^2\rangle = \langle a^4b\rangle = \langle a^5b^2\rangle = \langle a^7b\rangle = \langle a^8b^2\rangle$; $\langle ab^2\rangle = \langle a^2b\rangle = \langle a^4b^2\rangle = \langle a^5b\rangle = \langle a^7b^2\rangle = \langle a^8b\rangle$; $\langle a^3\rangle \times \langle b\rangle = \langle a^3\rangle \times \langle b^2\rangle = \ldots = \langle a^6b\rangle \times \langle a^6b^2\rangle$.

Portanto, $G = C_{3^2} \times C_3$ tem 4 subgrupos distintos de ordem 3^2, com 3 destes subgrupos cíclicos; 4 subgrupos de ordem 3, sendo todos eles cíclicos, totalizando 8 subgrupos não triviais.

4.2.1.2 Subgrupos de $C_{p^2} \times C_{p^2}$

Seja $G = C_{3^2} \times C_{3^2}$ o grupo abeliano produto direto dos grupos cíclicos $C_{3^2} = \langle a \rangle$ e $C_{3^2} = \langle b \rangle$, em que $o(a) = 3^2$ e $o(b) = 3^2$ Temos $\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$, $\langle b \rangle = \{e, b, b^2, b^3, b^4, b^5, b^6, b^7, b^8\}$, $\langle a^3 \rangle = \{e, a^3, a^6\} = \langle a^6 \rangle$ e $\langle b^3 \rangle = \{e, b^3, b^6\} = \langle b^6 \rangle$. Como o subgrupo gerado por a é cíclico de ordem 3^2, então os elementos de $\langle a \rangle$ cuja potência é prima com 3^2 são também geradores de $\langle a \rangle$, ou seja, $\langle a \rangle = \langle a^i \rangle$, para $i \in U(\mathbb{Z}_{3^2})$. Analogamente, temos $\langle b \rangle = \langle b^i \rangle$, para $i \in U(\mathbb{Z}_{3^2})$. Além disso, temos

$$\begin{aligned}
\langle ab \rangle &= \{e, ab, a^2b^2, a^3b^3, a^4b^4, a^5b^5, a^6b^6, a^7b^7, a^8b^8\}.\\
\langle a^2b \rangle &= \{e, a^2b, a^4b^2, a^6b^3, a^8b^4, ab^5, a^3b^6, a^5b^7, a^7b^8\}.\\
\langle a^3b \rangle &= \{e, a^3b, a^6b^2, b^3, a^3b^4, a^6b^5, b^6, a^3b^7, a^6b^8\}.\\
\langle a^4b \rangle &= \{e, a^4b, a^8b^2, a^3b^3, a^7b^4, a^2b^5, a^6b^6, ab^7, a^5b^8\}.\\
\langle a^5b \rangle &= \{e, a^5b, a^6b^2, a^6b^3, a^2b^4, a^7b^5, a^3b^6, a^8b^7, a^4b^8\}.\\
\langle a^6b \rangle &= \{e, a^6b, a^3b^2, b^3, a^6b^4, a^3b^5, b^6, a^6b^7, a^3b^8\}.\\
\langle a^7b \rangle &= \{e, a^7b, a^5b^2, a^3b^3, ab^4, a^8b^5, a^6b^6, a^4b^7, a^2b^8\}.\\
\langle a^8b \rangle &= \{e, a^8b, a^7b^2, a^6b^3, a^5b^4, a^4b^5, a^3b^6, a^2b^7, ab^8\}.
\end{aligned}$$

Note que os únicos elementos de ordem 3 nos subgrupos gerados por ab, a^4b e a^7b são a^3b^3 e a^6b^6. Deste modo, os subgrupos gerados pelos elementos de ordem 3^2 em $\langle ab \rangle$, $\langle a^4b \rangle$ e $\langle a^7b \rangle$ também os geram, isto é

$$\begin{aligned}
\langle ab \rangle &= \langle a^2b^2 \rangle = \langle a^4b^4 \rangle = \langle a^5b^5 \rangle = \langle a^7b^7 \rangle = \langle a^8b^8 \rangle;\\
\langle a^4b \rangle &= \langle a^8b^2 \rangle = \langle a^7b^4 \rangle = \langle a^2b^5 \rangle = \langle ab^7 \rangle = \langle a^5b^8 \rangle;\\
\langle a^7b \rangle &= \langle a^5b^2 \rangle = \langle ab^4 \rangle = \langle a^8b^5 \rangle = \langle a^4b^7 \rangle = \langle a^3b^8 \rangle.
\end{aligned}$$

Similarmente, como os únicos elementos de ordem 3 nos subgrupos gerados por a^3b e a^6b (respectivamente a^2b, a^5b e a^8b) são b^3 e b^6 (respectivamente a^3b^6 e a^6b^3), temos

$$\begin{aligned}
\langle a^3b \rangle &= \langle a^6b^2 \rangle = \langle a^3b^4 \rangle = \langle a^6b^5 \rangle = \langle a^3b^7 \rangle = \langle a^6b^8 \rangle;\\
\langle a^6b \rangle &= \langle a^3b^2 \rangle = \langle a^6b^4 \rangle = \langle a^3b^5 \rangle = \langle a^6b^7 \rangle = \langle a^3b^8 \rangle.
\end{aligned}$$

Respectivamente,

$$\begin{aligned}
\langle a^2b \rangle &= \langle a^4b^2 \rangle = \langle a^8b^4 \rangle = \langle ab^5 \rangle = \langle a^5b^7 \rangle = \langle a^7b^8 \rangle;\\
\langle a^5b \rangle &= \langle ab^2 \rangle = \langle a^2b^4 \rangle = \langle a^7b^5 \rangle = \langle a^8b^7 \rangle = \langle a^4b^8 \rangle;\\
\langle a^8b \rangle &= \langle a^7b^2 \rangle = \langle a^5b^4 \rangle = \langle a^4b^5 \rangle = \langle a^2b^7 \rangle = \langle ab^8 \rangle.
\end{aligned}$$

Os únicos subgrupos da forma $\langle ab^j \rangle$, com $j = 1, \ldots, 8$, que não são iguais a nenhum dos subgrupos da forma $\langle a^ib \rangle$, com $i = 1, \ldots, 8$, são os gerados por ab^3 e ab^6, pois

$\langle ab^2\rangle = \langle a^5b\rangle$; $\langle ab^4\rangle = \langle a^7b\rangle$; $\langle ab^4\rangle = \langle a^2b\rangle$; $\langle ab^7\rangle = \langle a^4b\rangle$ e $\langle ab^8\rangle = \langle a^8b\rangle$. Logo $\langle ab^3\rangle = \{e, ab^3, a^2b^6, a^3, a^4b^3, a^5b^6, a^6, a^7b^3, a^8b^6\}$ e $\langle ab^6\rangle = \{e, ab^6, a^2b^3, a^3, a^4b^6, a^5b^3, a^6, a^7b^6, a^8b^3\}$. Como os únicos elementos de ordem 3 nestes subgrupos são a^3 e a^6, temos

$$\begin{array}{ccccccccccc} \langle ab^3\rangle & = & \langle a^2b^6\rangle & = & \langle a^4b^3\rangle & = & \langle a^5b^6\rangle & = & \langle a^7b^3\rangle & = & \langle a^8b^6\rangle; \\ \langle ab^6\rangle & = & \langle a^2b^3\rangle & = & \langle a^4b^6\rangle & = & \langle a^5b^3\rangle & = & \langle a^7b^6\rangle & = & \langle a^8b^3\rangle. \end{array}$$

O produto direto entre os subgrupos $\langle a^3\rangle$ e $\langle b^3\rangle$ de G, ambos de ordem 3, é o subgrupo $\langle a^3\rangle \times \langle b^3\rangle = \{e, a^3, a^6, b^3, b^6, a^3b^3, a^6b^3, a^3b^6, a^6b^3\}$ de ordem 3^2, cujos elementos de ordem 3 são $a^3, a^6, b^3, b^6, a^3b^3, a^6b^6, a^3b^6$ e a^6b^3 e tais que $\langle a^3\rangle = \langle a^6\rangle$; $\langle b^3\rangle = \langle b^6\rangle$; $\langle a^3b^3\rangle = \langle a^6b^6\rangle$ e $\langle a^3b^6\rangle = \langle a^6b^3\rangle$. Observe que o produto direto entre quaisquer dois elementos de $\langle a^3\rangle \times \langle b^3\rangle$ não neutros, e que não são geradores do mesmo subgrupo, também é $\langle a^3\rangle \times \langle b^3\rangle$, ou seja, $\langle a^3\rangle \times \langle b^3\rangle = \langle a^3\rangle \times \langle b^6\rangle = \ldots = \langle b^6\rangle \times \langle a^6b^6\rangle$. Já o produto direto entre dois geradores de um mesmo subgrupo resulta nele próprio, como por exemplo, $\langle a^6b^3\rangle \times \langle a^3b^6\rangle = \{e, a^3b^6, a^6b^3\}$.

O produto direto entre os subgrupos $\langle a\rangle$ e $\langle b^3\rangle$ de ordem 3^2 e ordem 3, respectivamente, é o subgrupo $\langle a\rangle \times \langle b^3\rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, b^3, b^6, ab^3, ab^6, a^2b^3, a^2b^6, a^3b^3, a^3b^6, a^4b^3, a^4b^6, a^5b^3, a^5b^6, a^6b^4, a^6b^6, a^7b^3, a^7b^6, a^8b^3, a^8b^6\}$ de ordem 3^3. Os elementos de ordem 3 (respectivamente ordem 9) deste subgrupo são $a^3, a^6, b^3, b^6, a^3b^3, a^3b^6, a^6b^3$ e a^6b^6, (respectivamente ordem 9) $a, a^2, a^4, a^5, a^7, a^8, ab^3, ab^6, a^2b^3, a^2b^6, a^4b^3, a^4b^6, a^5b^3, a^5b^6, a^7b^3, a^7b^6, a^8b^3, a^8b^6$. O produto direto entre quaisquer dois elementos de ordem 3^2 de $\langle a^3\rangle \times \langle b\rangle$ resulta no grupo todo $G = \langle a\rangle \times \langle b\rangle$ quando estes dois elementos não forem geradores de um mesmo subgrupo, como por exemplo, $\langle ab^3\rangle \times \langle a^4b^6\rangle = \langle a\rangle \times \langle b\rangle = G$. Já o produto direto entre quaisquer dois elementos, um de ordem 3^2 e outro de ordem 3 resulta no próprio $\langle a\rangle \times \langle b^3\rangle$, desde que estes dois elementos sejam tais que o de ordem 3 não esteja contido no subgrupo gerado pelo de ordem 3^2, como por exemplo, $\langle ab^6\rangle \times \langle a^3b^3\rangle = \langle a\rangle \times \langle b^3\rangle$.

O mesmo raciocínio pode ser aplicado para $\langle a^i\rangle \times \langle b^{3j}\rangle$ e para $\langle b\rangle \times \langle a^3\rangle$, $\langle b^i\rangle \times \langle a^{3j}\rangle$, com $i \in U(\mathbb{Z}_{3^2})$ e $j = 1, 2$. Além disso, os subgrupos cíclicos de ordem 3^2 de G diferentes de $\langle a\rangle$ e $\langle b\rangle$ resultam em um novo subgrupo de ordem 3^3 quando realiza-se o produto direto dele com outro subgrupo cíclico de ordem 3 de G, como por exemplo,

$$\begin{array}{rcl} \langle a^3\rangle \times \langle ab\rangle & = & \{e, a^3, a^6, ab, a^2b^2, a^3b^3, a^4b^4, a^5b^5, a^6b^6, a^7b^7, a^8b^8, a^4b, a^5b, a^6b, a^7b^4, a^8b^5, b^6, \\ & & ab^7, a^2b^8, a^7b, a^8b^2, b^3, ab^4, a^2b^5, a^3b^6, a^4b^7, a^5b^8\} \end{array}$$

e

$$\begin{array}{rcl} \langle b^3\rangle \times \langle a^2b\rangle & = & \{e, b^3, b^6, a^2b, a^4b^2, a^6b^3, a^8b^4, ab^5, a^3b^6, a^5b^7, a^7b^8, a^2b^4, a^4b^5, a^6b^6, a^8b^7, ab^8, \\ & & a^3, a^5b, a^7b^2, a^2b^7, a^4b^8, a^6, a^8b, ab^2, a^3b^3, a^5b^4, a^7b^5\}. \end{array}$$

De modo similar ao que foi feito para $\langle a\rangle$ e $\langle b^3\rangle$, encontramos todos os subgrupos de ordem 3 e ordem 9 dos exemplos supracitados, consequentemente, todos os produtos diretos de subgrupos gerados por elementos de $\langle a\rangle$ e $\langle b^3\rangle$ que geram o grupo G.

Logo, os subgrupos distintos e não triviais de $G = C_{3^2} \times C_{3^2}$ e suas respectivas ordens são:

i) Subgrupos de ordem 3:
$\langle a^3\rangle = \langle a^6\rangle;\ \langle b^3\rangle = \langle b^6\rangle;\ \langle a^3b^3\rangle = \langle a^6b^6\rangle;\ \langle a^3b^6\rangle = \langle a^6b^3\rangle.$

ii) Subgrupos de ordem 3^2:
$\langle a\rangle = \langle a^i\rangle,\ \langle b\rangle = \langle b^i\rangle,\ \langle ab\rangle = \langle a^ib^i\rangle,\ i \in U(\mathbb{Z}_{3^2});$
$\langle a^2b\rangle = \langle a^4b^2\rangle = \langle a^8b^4\rangle = \langle ab^5\rangle = \langle a^5b^7\rangle = \langle a^7b^8\rangle;$
$\langle a^3b\rangle = \langle a^6b^2\rangle = \langle a^3b^4\rangle = \langle a^6b^5\rangle = \langle a^3b^7\rangle = \langle a^6b^8\rangle;$
$\langle a^4b\rangle = \langle a^8b^2\rangle = \langle a^7b^4\rangle = \langle a^2b^5\rangle = \langle ab^7\rangle = \langle a^5b^8\rangle;$
$\langle a^5b\rangle = \langle ab^2\rangle = \langle a^2b^4\rangle = \langle a^7b^5\rangle = \langle a^8b^7\rangle = \langle a^4b^8\rangle;$
$\langle a^6b\rangle = \langle a^3b^2\rangle = \langle a^6b^4\rangle = \langle a^3b^5\rangle = \langle a^6b^7\rangle = \langle a^3b^8\rangle;$
$\langle a^7b\rangle = \langle a^5b^2\rangle = \langle ab^4\rangle = \langle a^8b^5\rangle = \langle a^4b^7\rangle = \langle a^3b^8\rangle;$
$\langle a^8b\rangle = \langle a^7b^2\rangle = \langle a^5b^4\rangle = \langle a^4b^5\rangle = \langle a^2b^7\rangle = \langle ab^8\rangle;$
$\langle ab^3\rangle = \langle a^2b^6\rangle = \langle a^4b^3\rangle = \langle a^5b^6\rangle = \langle a^7b^3\rangle = \langle a^8b^6\rangle;$
$\langle ab^6\rangle = \langle a^2b^3\rangle = \langle a^4b^6\rangle = \langle a^5b^3\rangle = \langle a^7b^6\rangle = \langle a^8b^3\rangle;$
$\langle a^3\rangle \times \langle b^3\rangle = \langle a^3\rangle \times \langle a^3b^3\rangle = \ldots = \langle a^6\rangle \times \langle a^6b^6\rangle.$

iii) Subgrupos de ordem 3^3:
$\langle a\rangle \times \langle b^3\rangle = \langle a^i\rangle \times \langle b^3\rangle = \ldots = \langle a^i\rangle \times \langle a^6b^3\rangle,\ i \in U(Z_{3^2});$
$\langle b\rangle \times \langle a^3\rangle = \langle b^i\rangle \times \langle a^3\rangle = \ldots = \langle b^i\rangle \times \langle a^6b^3\rangle,\ i \in U(Z_{3^2});$
$\langle a^3\rangle \times \langle ab\rangle = \langle a^3\rangle \times \langle a^ib^i\rangle = \ldots = \langle a^3\rangle \times \langle a^4b\rangle = \ldots = \langle a^3\rangle \times \langle a^6b^8\rangle,\ i \in U(Z_{3^2});$
$\langle b^3\rangle \times \langle a^2b\rangle = \langle b^3\rangle \times \langle a^7b^5\rangle = \ldots = \langle a^6b^3\rangle \times \langle a^2b\rangle.$

Portanto, G possui 21 subgrupos distintos próprios, dentre os quais 16 são cíclicos.

Agora, seja $p = 5$. Temos o grupo $G = C_{5^2} \times C_{5^2}$. Utilizando o mesmo raciocínio empregado na determinação dos subgrupos de $C_{3^2} \times C_{3^2}$ e o auxílio do software *Sublime Text*, temos todos os subgrupos de todas as ordens de G, são eles

i) Subgrupos de ordem 5:
$\langle a^5\rangle;\ \langle a^{5j}b^5\rangle,\ 1 \leq i \leq 4;\ \langle b\rangle.$

ii) Subgrupos de ordem 5^2:
$\langle ab^j\rangle,\ 0 \leq j \leq 5^2 - 1;\ \langle a^{5i}b\rangle,\ 1 \leq i \leq 4;\ \langle a^5\rangle \times \langle b^5\rangle.$

iii) Subgrupos de ordem 5^3:
$\langle a\rangle \times \langle b^5\rangle;\ \langle a^5\rangle \times \langle ab^j\rangle,\ 0 \leq j \leq 4;\ \langle b\rangle \times \langle a^5\rangle.$

Portanto G, possui 43 subgrupos distintos próprios, dentre os quais 36 são cíclicos.

Considere $p = 7$. Temos o grupo $G = C_{7^2} \times C_{7^2}$. Utilizando o mesmo raciocínio empregado na determinação dos subgrupos anteriores e o auxílio do software *Sublime Text* temos todos os subgrupos de todas as ordens de G, são eles

i) Subgrupos de ordem 7:
$\langle a^7\rangle;\ \langle a^{7j}b^7\rangle,\ 1 \leq i \leq 6;\ \langle b\rangle.$

ii) Subgrupos de ordem 7^2:
$\langle ab^j\rangle,\ 0 \leq j \leq 7^2 - 1;\ \langle a^{7i}b\rangle,\ 1 \leq i \leq 6;\ \langle a^7\rangle \times \langle b^7\rangle.$

iii) Subgrupos de ordem 7^3:
$\langle a\rangle \times \langle b^7\rangle;\ \langle a^7\rangle \times \langle ab^j\rangle,\ 0 \leq j \leq 6;\ \langle b\rangle \times \langle a^7\rangle.$

Portanto, G possui 73 subgrupos distintos próprios, dentre os quais 56 são cíclicos.

Estendendo esta argumentação para um primo p qualquer, podemos conjecturar sobre o grupo $G = C_{p^2} \times C_{p^2}$ que seus subgrupos distintos próprios e suas respectivas ordens são:

i) Subgrupos de ordem p:
$\langle a^p\rangle;\ \langle a^{jp}b^p\rangle,\ 1 \leq i \leq p - 1;\ \langle b\rangle.$

ii) Subgrupos de ordem p^2:
$\langle ab^j\rangle,\ 0 \leq j \leq p^2 - 1;\ \langle a^{pi}b\rangle,\ 1 \leq i \leq p - 1;\ \langle a^p\rangle \times \langle b^p\rangle.$

iii) Subgrupos de ordem p^3:
$\langle a\rangle \times \langle b^p\rangle;\ \langle a^p\rangle \times \langle ab^j\rangle,\ 0 \leq j \leq p - 1;\ \langle b\rangle \times \langle a^p\rangle.$

Logo, $C_{p^2} \times C_{p^2}$ possui $p^2 + 3p + 3$ subgrupos próprios, o que pode ser verificado pelo artigo [23], pois nele o grupo $G = C_{p^2} \times C_{p^2}$ possui $(p^3((p-1)+2) - 7(p-1) - 2) \cdot \dfrac{1}{(p-1)^2}$ subgrupos, consequentemente, $(p^3(p+1) - 7(p-1) - 2) \cdot \dfrac{1}{(p-1)^2} - 2$ subgrupos próprios. Isto verifica-se, porque

$$\begin{aligned}(p^3((p-1)+2) - 7(p-1) - 2) \cdot \frac{1}{(p-1)^2} &= ((p-1)(p^3-7) + 2(p-1)(p^3-1)) \cdot \frac{1}{(p-1)^2} \\ &= (p-1)((p^3-7) + 2(p^2+p+1)) \cdot \frac{1}{(p-1)^2} \\ &= (p^3 + 2p^2 + 2p - 5) \cdot \frac{1}{(p-1)}\end{aligned}$$

$$= ((p-1)(p^2+3p+5)) \cdot \frac{1}{(p-1)}$$
$$= p^2+3p+5.$$

Portanto, G possui p^2+3p+3 subgrupos próprios.

4.2.2 Idempotentes primitivos em $\mathbb{F}_q(C_{p^m} \times C_{p^n})$

Considere as hipóteses adotadas, na página 53, em relação ao corpo $\mathbb{F}_q$ e seja $G = C_{p^m} \times C_{p^n}$ um p-grupo abeliano finito, em que $C_{p^m} = \langle x \rangle$ e $C_{p^n} = \langle y \rangle$ são grupos cíclicos tais que $o(x) = p^m$ e $o(y) = p^n$. Adotaremos essas hipóteses ao longo de toda esta seção. Além disso, quando tivermos $1 \leq h \leq n$, adotaremos $h = \delta$, se $1 \leq \delta \leq s$, e $s+1 \leq \lambda \leq n$, quando $n > s$.

Com as hipóteses mencionadas acima, temos

$$\mathbb{F}_q(G) \cong \frac{\mathbb{F}_q[x,y]}{\langle x^{p^m}-1, y^{p^n}-1 \rangle}. \tag{4.8}$$

A seguir, encontramos todos os idempotentes primitivos da álgebra de grupo $\mathbb{F}_qG$.

Lema 4.2.1. *Sejam p um primo inteiro, tal que $mdc(p,q) = 1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t-1)$. Seja m, n inteiros positivos com $m \leq s$ e $n \leq s$. Então, na extensão $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x) \rangle} \cong \mathbb{F}_{q^t}$ sobre $\mathbb{F}_q$, existe um polinômio $g_{\delta,i}(x) \in \mathbb{F}_q[x]$, tal que*

$$g_{\delta,i}(\bar{x}) = \zeta_{p^n},$$

em que $\bar{x} = x + \langle f_{\delta,i}(x) \rangle \in F_{\delta,i}$. Além disso, seja $f^*_{\delta,i}(x)$ o polinômio recíproco de $f_{\delta,i}(x)$, então na extensão $F^*_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f^*_{\delta,i}(x) \rangle}$,

$$g_{\delta,i}\left(\frac{1}{\bar{x}}\right) = \zeta^{-1}_{p^n}.$$

Demonstração. Desde que $p^s \| (q^t-1)$, $\zeta_{p^n} \in F_{\delta,i} \cong \mathbb{F}_{q^t}$. Como $[F_{q^t} : \mathbb{F}_q] = t$, existe um polinômio $g_{\delta,i}(x) \in \mathbb{F}_q[x]$, tal que $g_{\delta,i}(\bar{x}) = \zeta_{p^n}$ em $F_{\delta,i}$.

Seja $g_{\delta,i}(\bar{x})$ uma raiz p^n-ésima primitiva da unidade em $F_{\delta,i}$. Então, em $\mathbb{F}_q[x]$, $g_{\delta,i}(x)^{p^n} \equiv 1 \,(\mathrm{mod}\, f_{\delta,i}(x))$. Logo, existe um polinômio $k[x] \in \mathbb{F}_q[x]$, tal que $g_{\delta,i}(x)^{p^n} + k(x)f_{\delta,i}(x) = 1$. Por outro lado, na extensão $F^*_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f^*_{\delta,i}(x) \rangle}$, $f_{\delta,i}\left(\dfrac{1}{\bar{x}}\right) = 0$ (como vimos na demonstração do Lema 4.1.4), assim, $g_{\delta,i}\left(\dfrac{1}{\bar{x}}\right)^{p^n} = 1$. Reciprocamente, o resultado também vale. Portanto, $g_{\delta,i}\left(\dfrac{1}{\bar{x}}\right)$ é também uma p^n-ésima raiz da unidade em $F^*_{\delta,i}$.

Além disso, se $f_{\delta,i}(x) = f^*_{\delta,i}(x)$, então, pelo Lema 4.1.4, $\dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} \cong \mathbb{F}_{q^t}$, com $Gal(\mathbb{F}_{q^t}/\mathbb{F}_q) = \langle\sigma\rangle$. Logo $\sigma^{\frac{t}{2}}(g_{\delta,i}(\bar{x})) = g_{\delta,i}(\sigma^{\frac{t}{2}}(\bar{x}))$. Portanto $g_{\delta,i}\left(\dfrac{1}{\bar{x}}\right) = \zeta_{p^n}^{-1}$. ■

No Lema 4.2.1 podemos tomar $g_{\delta,i}(x) = x$, quando $h = s$.

Teorema 4.2.1. *Sejam p um número primo tal que $mdc(p,q) = 1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t - 1)$. Seja $G = A \times B$ um p-grupo abeliano finito, em que $A = \langle x\rangle$ e $B = \langle y\rangle$ são grupos cíclicos, tais que $o(x) = p^m$ e $o(y) = p^n$.*

Sejam $1 \leq m, n \leq s$. Então existem $1 + \dfrac{p^{m+n}-1}{t}$ idempotentes primitivos na álgebra de grupo $\mathbb{F}_q(G)$ como segue:

1. se $1 \leq \delta \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, então

$$E_{0;0} = \frac{1}{p^{m+n}}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^n-1} y^v\right);$$

$$E_{0;\delta,i} = \frac{1}{p^{m+n}}\frac{y^{p^n}-1}{y^{p^\delta}-1}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v})y^v\right);$$

2. se $1 \leq \delta \leq m$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ e $0 \leq k \leq p^n - 1$, então

$$E_{\delta,i;k} = \frac{1}{p^{m+n}}\frac{x^{p^m}-1}{x^{p^\delta}-1}\left(\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u})x^u\right)\left(\sum_{v=0}^{p^n-1} g_{\delta,i}(x)^{-kv}y^v\right),$$

em que $g_{\delta,i}(x) \in \mathbb{F}_q[x]$ e $g_{\delta,i}(\bar{x}) = \zeta_{p^n}$, com $\bar{x} \in \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}$.

Demonstração. Seja ζ_{p^m} a p^m-ésima raiz primitiva da unidade de $\mathbb{F}_{q^t}$. Como t é o menor inteiro positivo tal que $q^t \equiv 1 \pmod{p}$, $p^s \| (q^t - 1)$, com $m \leq s$, segue de (4.2)

$$x^{p^m} - 1 = (x-1)\prod_{\delta=1}^{m}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(x),$$

em que cada $f_{\delta,i}(x) = \prod_{\mu=0}^{t-1}(x - \zeta_{p^\delta}^{l_i q^\mu})$, com $mdc\,(l_i, p) = 1$, é irredutível sobre $\mathbb{F}_q$. Daí, pelo Teorema Chinês dos Restos, temos

$$\mathbb{F}_q(A) \cong \frac{\mathbb{F}_q[x]}{\langle x-1\rangle} \oplus \left(\bigoplus_{\delta=1}^{m}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} \frac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}\right) = F_0 \oplus \left(\bigoplus_{\delta=1}^{m}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i}\right), \tag{4.9}$$

com $F_0 = \mathbb{F}_q$ e cada $\dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} = F_{\delta,i} \cong \mathbb{F}_{q^t}$, para $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$. Assim, pelo Teorema 4.1.1, existem $1 + \dfrac{p^m - 1}{t}$ idempotentes primitivos em $\mathbb{F}_q(A)$:

$$\begin{aligned} e_0(x) &= \frac{1}{p^m} \sum_{u=0}^{p^m-1} x^u; \\ e_{\delta,i}(x) &= \frac{1}{p^m} \frac{x^{p^m} - 1}{x^{p^\delta} - 1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^u, \end{aligned} \tag{4.10}$$

para $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$.

Agora, vamos investigar todos os idempotentes primitivos do anel $\mathbb{F}_q(A \times B)$. Pela Proposição 3.1.1 e o isomorfismo (4.9), existe um isomorfismo sobre $\mathbb{F}_q$

$$\mathbb{F}_q(A \times B) \cong (\mathbb{F}_q A)B \cong \left(F_0 \oplus \left(\bigoplus_{\delta=1}^{m} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i} \right) \right) B \cong F_0(B) \oplus \left(\bigoplus_{\delta=1}^{m} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i}(B) \right) \tag{4.11}$$

Primeiramente, vamos investigar o somando direto $F_0(B)$ em (4.11). Por $n \leq s$ e (4.2), existe um isomorfismo sobre $\mathbb{F}_q$

$$F_0(B) \cong \frac{F_0[y]}{\langle y - 1\rangle} \oplus \left(\bigoplus_{\delta=1}^{n} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} \frac{F_0[y]}{\langle f_{\delta,i}(y)\rangle} \right) = F_{0;0} \oplus \left(\bigoplus_{\delta=1}^{n} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{0;\delta,i} \right), \tag{4.12}$$

com $F_{0;0} = \mathbb{F}_q$ e $F_{0;\delta,i} = \dfrac{\mathbb{F}_q[y]}{\langle f_{\delta,i}(y)\rangle}$, para $1 \leq \delta \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$. Daí, substituindo x por y e n por m em (4.10), obtemos $1 + \dfrac{p^n - 1}{t}$ idempotentes primitivos em $F_0(B)$:

$$\begin{aligned} \theta_{0;0}(y) &= \frac{1}{p^n} \sum_{v=0}^{p^n-1} y^v; \\ \theta_{0;\delta,i}(y) &= \frac{1}{p^n} \frac{y^{p^n} - 1}{y^{p^\delta} - 1} \sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v}) y^v. \end{aligned} \tag{4.13}$$

Logo, por (4.10) e (4.13), os idempotentes primitivos em $\mathbb{F}_q(G)$ correspondentes a $F_0(B)$ são:

$$\begin{aligned} E_{0;0} &= \theta_{0;0}(y) e_0(x) = \frac{1}{p^{m+n}} \left(\sum_{u=0}^{p^m-1} x^u \right) \left(\sum_{v=0}^{p^n-1} y^v \right); \\ E_{0;\delta,i} &= \theta_{0;\delta,i}(y) e_0(x) = \frac{1}{p^{m+n}} \frac{y^{p^n} - 1}{y^{p^\delta} - 1} \left(\sum_{u=0}^{p^m-1} x^u \right) \left(\sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v}) y^v \right), \end{aligned} \tag{4.14}$$

para $1 \leq \delta \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$.

Por conseguinte, vamos investigar cada somando direto $F_{\delta,i}(B)$, para cada $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ em (4.11). Por $n \leq s$ e o Lema 4.1.3, temos a seguinte fatoração para o polinômio $y^{p^n} - 1$ sobre $F_{\delta,i} \cong \mathbb{F}_{q^t}$:

$$y^{p^n} - 1 = \prod_{k=0}^{p^n-1} (y - \zeta_{p^n}^k).$$

Assim,

$$F_{\delta,i}(B) \cong \frac{F_{\delta,i}[y]}{\langle y^{p^n} - 1 \rangle} \cong \bigoplus_{k=0}^{p^n-1} \frac{F_{\delta,i}[y]}{\langle y - \zeta_{p^n}^k \rangle} = \bigoplus_{k=0}^{p^n-1} F_{\delta,i;k}, \tag{4.15}$$

em que $F_{\delta,i;k} = \dfrac{F_{\delta,i}[y]}{\langle y - \zeta_{p^n}^k \rangle}$, para $1 \leq k \leq p^n - 1$. Pelo item (i) do Teorema 4.1.1, existem p^n idempotentes primitivos em $F_{\delta,i}(B)$:

$$\theta_{\delta,i;k}(y) = \frac{1}{p^n} \sum_{v=0}^{p^n-1} \zeta_{p^n}^{-kv} y^v, \ 0 \leq k \leq p^n - 1. \tag{4.16}$$

Por outro lado, existe, pelo Lema 4.2.1 e $n \leq s$, um polinômio $g_{\delta,i}(x) \in \mathbb{F}_q[x]$ tal que

$$g_{\delta,i}(\bar{x}) = \zeta_{p^n}, \tag{4.17}$$

em que $\dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x) \rangle} = F_{\delta,i} \cong \mathbb{F}_{q^t}$. Por (4.10), (4.16), e (4.17), os idempotentes primitivos em $\mathbb{F}_q(G)$ correspondentes a $F_{\delta,i}(B)$ são:

$$\begin{aligned} E_{\delta,i;k} =& \frac{1}{p^n} \sum_{v=0}^{p^n-1} (g_{\delta,i}(x)^{-k} y)^v e_{\delta,i}(x) \\ =& \frac{1}{p^{m+n}} \frac{x^{p^m} - 1}{x^{p^\delta} - 1} \left(\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^u \right) \left(\sum_{v=0}^{p^n-1} g_{\delta,i}(x)^{-kv} y^v \right), \end{aligned}$$

para $0 \leq k \leq p^n - 1$. Deste modo, para o somando direto $F_0(B)$ existem $1 + \dfrac{p^n - 1}{t}$ idempotentes primitivos: $E_{0;0}$ e $E_{0;\delta,i}$, para $1 \leq \delta \leq n$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$. Para cada somando direto $F_{\delta,i}(B)$, com $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, existem p^n idempotentes primitivos: $E_{\delta,i;k}$, para $0 \leq k \leq p^n - 1$. Portanto, existem

$$1 + \frac{p^n - 1}{t} + \left(\frac{p^m - 1}{t} \right) p^n = 1 + \frac{p^n - 1 + p^{m+n} - p^n}{t} = 1 + \frac{p^{m+n} - 1}{t} \tag{4.18}$$

idempotentes primitivos em $\mathbb{F}_q(G)$. ■

A seguir, encontraremos os idempotentes primitivos em de $\mathbb{F}_q(G)$ no caso $s < n \leq m$.

Teorema 4.2.2. *Sejam p um primo tal que $mdc(p,q)=1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t-1)$. Seja $G=A\times B$ uma álgebra de p-grupo abeliano finito, em que $A=\langle x\rangle$ e $B=\langle y\rangle$ são grupos cíclicos, tais que, $o(x)=p^m$ e $o(y)=p^n$. Sejam $1\leq n\leq s<m$. Então existem $1+\dfrac{p^{n+s-1}(p-1)(m-s)+p^{n+s}-1}{t}$ idempotentes primitivos na álgebra de grupo $\mathbb{F}_q(G)$ como segue:*

1. se $1\leq\delta\leq n$ e $1\leq i\leq\dfrac{\phi(p^\delta)}{t}$, então

$$E_{0;0}=\frac{1}{p^{m+n}}\left(\sum_{u=0}^{p^m-1}x^u\right)\left(\sum_{v=0}^{p^n-1}y^v\right);$$

$$E_{0;\delta,i}=\frac{1}{p^{m+n}}\frac{y^{p^n}-1}{y^{p^\delta}-1}\left(\sum_{u=0}^{p^m-1}x^u\right)\left(\sum_{v=0}^{p^\delta-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_iv})y^v\right);$$

2. se $1\leq\delta\leq s$, $1\leq i\leq\dfrac{\phi(p^\delta)}{t}$ e $0\leq k\leq p^n-1$, então

$$E_{\delta,i;k}=\frac{1}{p^{m+n}}\frac{x^{p^m}-1}{x^{p^\delta}-1}\left(\sum_{u=0}^{p^\delta-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_iu})x^u\right)\left(\sum_{v=0}^{p^n-1}g_{\delta,i}(x)^{-kv}y^v\right);$$

3. se $s+1\leq\varepsilon\leq m$, $1\leq i\leq\dfrac{\phi(p^s)}{t}$ e $0\leq k\leq p^n-1$, então

$$E_{\varepsilon,i;k}=\frac{1}{p^{m+n+s-\varepsilon}}\frac{x^{p^m}-1}{x^{p^\varepsilon}-1}\left(\sum_{u=0}^{p^s-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_iu})x^{p^{\varepsilon-s}u}\right)\left(\sum_{v=0}^{p^n-1}g_{\varepsilon,i}(x)^{-kv}y^v\right),$$

em que $g_{\varepsilon,i}(x)\in\mathbb{F}_q[x]$ e $g_{\varepsilon,i}(\bar{x})=\zeta_{p^n}$, com $\bar{x}\in\dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}\cong\mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}\supset\mathbb{F}_{q^t}$.

Demonstração. Desde que $A=\langle x\rangle$, $o(x)=p^m$ e $m>s$, pelo Lema 4.1.4, o polinômio $x^{p^m}-1$ se fatora sobre $\mathbb{F}_q$ como segue:

$$x^{p^m}-1=(x-1)\left(\prod_{\delta=1}^{s}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}}f_{\delta,i}(x)\right)\left(\prod_{\varepsilon=s+1}^{m}\prod_{i=1}^{\frac{\phi(p^s)}{t}}f_{\varepsilon,i}(x)\right),$$

em que $f_{\delta,i}(x)=\prod_{\mu=0}^{t-1}(x-\zeta_{p^\delta}^{l_iq^\mu})$, se $1\leq\delta\leq s$, e $f_{\varepsilon,i}(x)=\prod_{\mu=0}^{t-1}(x^{p^{\varepsilon-s}}-\zeta_{p^s}^{l_iq^\mu})$, se $s+1\leq\varepsilon\leq m$. Assim, existe um isomorfismo de anéis:

$$\begin{aligned}\mathbb{F}_q(A)&\cong\frac{\mathbb{F}_q[x]}{\langle x-1\rangle}\oplus\left(\bigoplus_{\delta=1}^{s}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}}\frac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}\right)\oplus\left(\bigoplus_{\varepsilon=s+1}^{m}\bigoplus_{i=1}^{\frac{\phi(p^s)}{t}}\frac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}\right)\\&=F_0\oplus\left(\bigoplus_{\delta=1}^{s}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}}F_{\delta,i}\right)\oplus\left(\bigoplus_{\varepsilon=s+1}^{m}\bigoplus_{i=1}^{\frac{\phi(p^s)}{t}}F_{\varepsilon,i}\right),\end{aligned}\tag{4.19}$$

em que $F_0 = \mathbb{F}_q$; para cada $1 \leq \delta \leq s$, $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}$ e, para cada $s+1 \leq \varepsilon \leq m$, $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}$. Pelo Teorema 4.1.1, existem $1 + \dfrac{p^s-1}{t} + \dfrac{(m-s)\,(p^s-p^s-1)}{t}$ idempotentes primitivos em $\mathbb{F}_q(A)$:

$$\begin{aligned}
e_0(x) =& \frac{1}{p^m}\sum_{u=0}^{p^m-1} x^u;\\
e_{\delta,i}(x) =& \frac{1}{p^m}\frac{x^{p^m}-1}{x^{p^\delta}-1}\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u})x^u, \text{ para } 1 \leq \delta \leq s \text{ e } 1 \leq i \leq \frac{\phi(p^\delta)}{t};\\
e_{\varepsilon,i}(x) =& \frac{1}{p^{m+s-\varepsilon}}\frac{x^{p^m}-1}{x^{p^\varepsilon}-1}\sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u})x^{up^{\varepsilon-s}}, \text{ para } s+1 \leq \varepsilon \leq m \text{ e } 1 \leq i \leq \frac{\phi(p^s)}{t}.
\end{aligned} \tag{4.20}$$

Agora, vamos investigar os idempotentes primitivos no anel $\mathbb{F}_q(A \times B)$. Pela Proposição 3.1.1 e o isomorfismo (4.19), existe um isomorfismo sobre $\mathbb{F}_q$

$$\mathbb{F}_q(A \times B) \cong F_0(B) \oplus \left(\bigoplus_{\delta=1}^{s}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i}(B)\right) \oplus \left(\bigoplus_{\varepsilon=s+1}^{m}\bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} F_{\varepsilon,i}(B)\right). \tag{4.21}$$

Primeiramente, vamos investigar o somando direto $F_0(B)$. Pelo Lema 4.1.4 e $n \leq s$, temos a seguinte fatoração do polinômio $y^{p^n}-1$ sobre $\mathbb{F}_q$:

$$y^{p^n}-1 = (y-1)\prod_{\delta=1}^{n}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(y),$$

em que $f_{\delta,i}(y) = \prod_{\mu=0}^{t-1}(y - \zeta_{p^\delta}^{l_i q^\mu})$. Assim, existe um isomorfismos de anéis tal que

$$F_0(B) \cong \frac{F_0[y]}{\langle y-1\rangle} \oplus \left(\bigoplus_{\delta=1}^{n}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} \frac{F_0[y]}{\langle f_{\delta,i}(y)\rangle}\right) = F_{0;0} \oplus \left(\bigoplus_{\delta=1}^{n}\bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{0;\delta,i}\right), \tag{4.22}$$

em que $F_{0;0} = \mathbb{F}_q$ e cada $F_{0;\delta,i} = \dfrac{\mathbb{F}_q[y]}{\langle f_{\delta,i}(y)\rangle}$. Portanto, existem $1 + \dfrac{p^n-1}{t}$ idempotentes primitivos em $\mathbb{F}_q(A \times B)$ correspondentes a $F_0(B)$ em (4.21): $E_{0;0}, E_{0;\delta,i}$, para $1 \leq h \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, dados no Teorema 4.2.1.

Por conseguinte, investigaremos cada somando direto $F_{\delta,i}(B)$ e $F_{\varepsilon,i}(B)$. Note que, $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} \cong \mathbb{F}_{q^t}$, para $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$; $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}$, para $s+1 \leq \varepsilon \leq m$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$. Pelo Lema 4.1.3, temos a seguinte fatoração para o polinômio $y^{p^n}-1$ sobre $\mathbb{F}_{q^t}$:

$$y^{p^n}-1 = \prod_{k=0}^{p^n-1}(y - \zeta_{p^n}^k).$$

Daí, existem isomorfismos de anéis tais que

$$F_{\delta,i}(B) \cong \frac{F_{\delta,i}[y]}{\langle y^{p^n}-1\rangle} \cong \bigoplus_{k=0}^{p^n-1} \frac{F_{\delta,i}[y]}{\langle y-\zeta_{p^n}^k\rangle} = \bigoplus_{k=0}^{p^n-1} F_{\delta,i;k}, \text{ para } 1 \le \delta \le s;$$
$$F_{\varepsilon,i}(B) \cong \frac{F_{\varepsilon,i}[y]}{\langle y^{p^n}-1\rangle} \cong \bigoplus_{k=0}^{p^n-1} \frac{F_{\varepsilon,i}[y]}{\langle y-\zeta_{p^n}^k\rangle} = \bigoplus_{k=0}^{p^n-1} F_{\varepsilon,i;k}, \text{ para } s+1 \le \varepsilon \le m,$$

em que $F_{\delta,i;k} = \dfrac{F_{\delta,i}[y]}{\langle y-\zeta_{p^n}^k\rangle} \cong \mathbb{F}_{q^t}$, para $1 \le \delta \le s$ e $1 \le i \le \dfrac{\phi(p^\delta)}{t}$; $F_{\varepsilon,i;k} = \dfrac{F_{\varepsilon,i}[y]}{\langle y-\zeta_{p^n}^k\rangle} \cong \mathbb{F}_{q^t\cdot p^{\varepsilon-s}}$, para $s+1 \le \varepsilon \le m$ e $1 \le i \le \dfrac{\phi(p^s)}{t}$. Pelo Teorema 4.1.1, existem p^n idempotentes primitivos em $F_{\delta,i}(B)$ correspondentes a $F_{\delta,i;k}$ e p^n idempotentes primitivos em $F_{\varepsilon,i}(B)$ correspondentes a $F_{\varepsilon,i;k}$

$$\begin{aligned}\theta_{\delta,i;k}(y) &= \frac{1}{p^n}\sum_{v=0}^{p^n-1} \zeta_{p^n}^{-kv} y^v, \ 0 \le k \le p^n-1;\\ \theta_{\varepsilon,i;k}(y) &= \frac{1}{p^n}\sum_{v=0}^{p^n-1} \zeta_{p^n}^{-kv} y^v, \ 0 \le k \le p^n-1\end{aligned} \tag{4.23}$$

Por outro lado, pelo Lema 4.2.1 e $n \le s$, existe um polinômio $g_{\delta,i}(x)$ em $\mathbb{F}_q[x]$, tal que em $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} \cong \mathbb{F}_{q^t}$,

$$g_{\delta,i}(\bar{x}) = \zeta_{p^n}, \tag{4.24}$$

Além disso, o Lema 4.2.1 pode ser estendido para os casos $m > s$ e $n \le s$. Neste caso, basta observar que pelo isomorfismo $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}} \supset \mathbb{F}_{q^t}$, existe um polinômio $g_{\varepsilon,i}(x)$ em $\mathbb{F}_q[x]$ tal que em $F_{\varepsilon,i}$,

$$g_{\varepsilon,i}(\bar{x}) = \zeta_{p^n}. \tag{4.25}$$

Logo, por (4.20), (4.23), (4.24) e (4.25), os idempotentes primitivos de $\mathbb{F}_q(A\times B)$ correspondentes a $F_{\delta,i}(B)$ e $F_{\varepsilon,i}(B)$ são:

1. se $1 \le \delta \le s$ e $1 \le i \le \dfrac{\phi(p^\delta)}{t}$, então

$$\begin{aligned}E_{\delta,i;k} &= \frac{1}{p^n}\sum_{v=0}^{p^n-1} (g_{\delta,i}(x)^{-k}y)^v e_{\delta,i}(x)\\ &= \frac{1}{p^{m+n}}\frac{x^{p^m}-1}{x^{p^\delta}-1}\left(\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u})x^u\right)\left(\sum_{v=0}^{p^n-1} g_{\delta,i}(x)^{-kv}y^v\right),\end{aligned} \tag{4.26}$$

para $0 \le k \le p^n-1$;

2. se $s+1 \le \varepsilon \le m$ e $1 \le i \le \dfrac{\phi(p^s)}{t}$, então

$$\begin{aligned}E_{\varepsilon,i;k} &= \frac{1}{p^n}\sum_{v=0}^{p^n-1} (g_{\varepsilon,i}(x)^{-k}y)^v e_{\varepsilon,i}(x)\\ &= \frac{1}{p^{m+n+s-\varepsilon}}\frac{x^{p^m}-1}{x^{p^\varepsilon}-1}\left(\sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u})x^{p^{\varepsilon-s}u}\right)\left(\sum_{v=0}^{p^n-1} g_{\varepsilon,i}(x)^{-kv}y^v\right),\end{aligned} \tag{4.27}$$

para $0 \leq k \leq p^n - 1$.

Dessa forma, para o somando direto $F_0(B)$, existem $1 + \dfrac{p^n - 1}{t}$ idempotentes primitivos: $E_{0;0}$ e $E_{0;\delta,i}$, para $1 \leq \delta \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$. Para cada somando direto $F_{\delta,i}(B)$, com $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, existem p^n idempotentes primitivos: $E_{\varepsilon,i;k}$, para $0 \leq k \leq p^n - 1$. Para cada somando direto $F_{\varepsilon,i}(B)$, com $s+1 \leq \varepsilon \leq m$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, existem p^n idempotentes primitivos: $E_{\varepsilon,i;k}$, para $0 \leq k \leq p^n - 1$. Portanto, existem

$$\begin{aligned} 1 + \frac{p^n - 1}{t} + \left(\frac{p^s - 1}{t}\right) p^n + (m-s)\frac{\phi(p^s)}{t}p^n &= 1 + \frac{p^n(p^s + (m-s)(p^s - p^{s-1})) - 1}{t} \\ &= 1 + \frac{p^n(p^{s-1}(p + (m-s)(p-1)) - 1}{t} \\ &= 1 + \frac{p^{n+s-1}(m-s)(p-1) + p^{n+s} - 1}{t} \end{aligned} \tag{4.28}$$

idempotentes primitivos em $\mathbb{F}_q G$. ■

A seguir, encontraremos os idempotentes primitivos em de $\mathbb{F}_q(G)$ no caso $s < m \leq n$.

Teorema 4.2.3. *Sejam p um primo tal que $mdc(p,q) = 1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t - 1)$. Seja $G = A \times B$ uma álgebra de p-grupo abeliano finito, em que $A = \langle x \rangle$ e $B = \langle y \rangle$ são grupos cíclicos, tais que, $o(x) = p^m$ e $o(y) = p^n$. Seja $1 \leq s < m \leq n$. Então existem $1 + \dfrac{p^{2s} - 1}{t} + \dfrac{p^s - p^{s-1}}{t}\left(p^s + (n - m + 1)p^m + \dfrac{2\left(p^m - p^{s+1}\right)}{p-1}\right)$ idempotentes primitivos na álgebra de grupo $\mathbb{F}_q(G)$ como segue:*

1. *se $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, então*

$$E_{0;0} = \frac{1}{p^{m+n}}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^n-1} y^v\right);$$

$$E_{0;\delta,i} = \frac{1}{p^{m+n}}\frac{y^{p^n} - 1}{y^{p^\delta} - 1}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v})y^v\right);$$

$$E_{0;\delta,i} = \frac{1}{p^{m+s+n-\delta}}\frac{y^{p^m} - 1}{y^{p^\delta} - 1}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i v})y^{vp^{\lambda-s}}\right),$$

   para $s+1 \leq \lambda \leq n$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$;

2. *se $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ e $0 \leq k \leq p^s - 1$, então*

$$E_{\delta,i;k} = \frac{1}{p^{m+n}}\frac{x^{p^m} - 1}{x^{p^\delta} - 1}\frac{y^{p^n} - 1}{y^{p^s} - 1}\left(\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u})x^u\right)\left(\sum_{v=0}^{p^s-1} g_{\delta,i}(x)^{-kv}y^v\right),$$

em que $g_{\delta,i}(x) \in \mathbb{F}_q[x]$ *e* $g_{\delta,i}(\bar{x}) = \zeta_{p^s}$, *com* $\bar{x} \in \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}$;

3. *se* $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, $s+1 \leq \lambda \leq n$ *e* $1 \leq r \leq p^s - 1$, *com* $p \nmid r$, *então*

$$E_{\delta,i;\lambda,r} = \frac{1}{p^{m+n+s-\lambda}} \frac{x^{p^m}-1}{x^{p^\delta}-1} \frac{y^{p^n}-1}{y^{p^\lambda}-1} \left(\sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^u \right) \left(\sum_{v=0}^{p^s-1} g_{\delta,i}(x)^{-rv} y^{p^{\lambda-s}v} \right),$$

em que $g_{\delta,i}(x) \in \mathbb{F}_q[x]$ *e* $g_{\delta,i}(\bar{x}) = \zeta_{p^s}$, *com* $\bar{x} \in \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}$;

4. *se* $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$ *e* $0 \leq k \leq p^\varepsilon - 1$, *então*

$$E_{\varepsilon,i;k} = \frac{1}{p^{m+n}} \frac{x^{p^m}-1}{x^{p^\varepsilon}-1} \frac{y^{p^n}-1}{y^{p^\varepsilon}-1} \left(\sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{up^{\varepsilon-s}} \right) \left(\sum_{v=0}^{p^\varepsilon-1} x^{-kv} y^v \right),$$

em que $g_{\varepsilon,i}(x) \in \mathbb{F}_q[x]$ *e* $g_{\varepsilon,i}(\bar{x}) = \bar{x} = \zeta_{p^\varepsilon}$, *com* $\bar{x} \in \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}$;

5. *se* $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, $\varepsilon+1 \leq \lambda \leq n$ *e* $1 \leq r \leq p^\varepsilon - 1$, *com* $p \nmid r$, *então*

$$E_{\varepsilon,i;\lambda,r} = \frac{1}{p^{m+n+\varepsilon-\lambda}} \frac{x^{p^m}-1}{x^{p^\varepsilon}-1} \frac{y^{p^n}-1}{y^{p^\lambda-1}} \left(\sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{up^{\varepsilon-s}} \right) \left(\sum_{v=0}^{p^\varepsilon-1} x^{-rv} y^{p^{\lambda-\varepsilon}v} \right),$$

em que $g_{\varepsilon,i}(x) \in \mathbb{F}_q[x]$ *e* $g_{\varepsilon,i}(\bar{x}) = \zeta_{p^\varepsilon}$, *com* $\bar{x} \in \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}$.

Demonstração. Desde que $A = \langle x\rangle$, $o(x) = p^m$ e $m > s$, pelo Lema 4.1.4, o polinômio $x^{p^m} - 1$ se fatora sobre $\mathbb{F}_q$ como segue:

$$x^{p^m} - 1 = (x-1) \left(\prod_{\delta=1}^{s} \prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(x) \right) \left(\prod_{\varepsilon=s+1}^{m} \prod_{i=1}^{\frac{\phi(p^s)}{t}} f_{\varepsilon,i}(x) \right),$$

em que $f_{\delta,i}(x) = \prod_{\mu=0}^{t-1} (x - \zeta_{p^\delta}^{l_i q^\mu})$, se $1 \leq \delta \leq s$, e $f_{\varepsilon,i}(x) = \prod_{\mu=0}^{t-1} \left(y^{p^{\varepsilon-s}} - \zeta_{p^s}^{l_i q^\mu} \right)$, se $s+1 \leq \varepsilon \leq m$. Assim, existe um isomorfismo de anéis:

$$\begin{aligned} \mathbb{F}_q(A) &\cong \frac{\mathbb{F}_q[x]}{\langle x-1\rangle} \oplus \left(\bigoplus_{\delta=1}^{s} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} \frac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} \right) \oplus \left(\bigoplus_{\varepsilon=s+1}^{m} \bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} \frac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle} \right) \\ &= F_0 \oplus \left(\bigoplus_{\delta=1}^{s} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i} \right) \oplus \left(\bigoplus_{\varepsilon=s+1}^{m} \bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} F_{\varepsilon,i} \right), \end{aligned} \tag{4.29}$$

em que $F_0 = \mathbb{F}_q$; para cada $1 \leq \delta \leq s$, $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle}$ e, para cada $s+1 \leq \varepsilon \leq m$, $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle}$. Pelo Teorema 4.1.1, existem $1 + \dfrac{p^s-1}{t} + \dfrac{(m-s)\,(p^s-p^s-1)}{t}$ idempotentes primitivos em $\mathbb{F}_q(A)$ conforme (4.20).

Agora, vamos investigar os idempotentes primitivos no anel $\mathbb{F}_q(A \times B)$. Pela Proposição 3.1.1 e o isomorfismo (4.19), existe um isomorfismo sobre $\mathbb{F}_q$

$$\mathbb{F}_q(A \times B) \cong F_0(B) \oplus \left(\bigoplus_{\delta=1}^{s} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{\delta,i}(B) \right) \oplus \left(\bigoplus_{\varepsilon=s+1}^{m} \bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} F_{\varepsilon,i}(B) \right). \tag{4.30}$$

Primeiramente, vamos investigar o somando direto $F_0(B)$. Pelo Lema 4.1.4 e $n > s$, temos a seguinte fatoração do polinômio $y^{p^n}-1$ sobre $\mathbb{F}_q$:

$$y^{p^n}-1 = (y-1)\prod_{h=1}^{n}\Phi_{p^h}(y) = (y-1)\left(\prod_{\delta=1}^{s}\prod_{i=1}^{\frac{\phi(p^\delta)}{t}} f_{\delta,i}(y)\right)\left(\prod_{\lambda=s+1}^{n}\prod_{i=1}^{\frac{\phi(p^s)}{t}} f_{\lambda,i}(y)\right),$$

em que $f_{\delta,i}(y) = \prod_{\mu=0}^{t-1}(y-\zeta_{p^\delta}^{l_i q^\mu})$, se $1 \leq \delta \leq s$, e $f_{\lambda,i}(y) = \prod_{\mu=0}^{t-1}(y^{p^{\lambda-s}}-\zeta_{p^s}^{l_i q^\mu})$, se $s+1 \leq \lambda \leq n$. Assim, existe um isomorfismo de anéis tal que

$$\begin{aligned}\mathbb{F}_0(B) = \mathbb{F}_q(B) &\cong \frac{\mathbb{F}_q[y]}{\langle y-1\rangle} \oplus \left(\bigoplus_{\delta=1}^{s} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} \frac{\mathbb{F}_q[y]}{\langle f_{\delta,i}(y)\rangle} \right) \oplus \left(\bigoplus_{\lambda=s+1}^{n} \bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} \frac{\mathbb{F}_q[y]}{\langle f_{\lambda,i}(y)\rangle} \right) \\ &= F_{0;0} \oplus \left(\bigoplus_{\delta=1}^{s} \bigoplus_{i=1}^{\frac{\phi(p^\delta)}{t}} F_{0;\delta,i} \right) \oplus \left(\bigoplus_{\lambda=s+1}^{n} \bigoplus_{i=1}^{\frac{\phi(p^s)}{t}} F_{0;\lambda,i} \right),\end{aligned} \tag{4.31}$$

em que $F_{0;0} = \mathbb{F}_q$; para cada $1 \leq \delta \leq s$, $F_{0;\delta,i} = \dfrac{\mathbb{F}_q[y]}{\langle f_{\delta,i}(y)\rangle}$ e, para cada $s+1 \leq \lambda \leq n$, $F_{0;\lambda,i} = \dfrac{\mathbb{F}_q[y]}{\langle f_{\lambda,i}(y)\rangle}$. Pelo Teorema 4.1.1, existem $1 + \dfrac{p^s-1}{t} + \dfrac{(n-s)\,(p^s-p^s-1)}{t}$ idempotentes primitivos em $F_0(B)$ dados por (4.20) substituindo x por y e m por n. Portanto, os idempotentes primitivos em $\mathbb{F}_q(A \times B)$ correspondentes a $F_0(B)$ são: $E_{0;0}$; $E_{0;\delta,i}$, com $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, dados pelo Teorema 4.2.2; para $s+1 \leq \lambda \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\lambda)}{t}$, os idempotentes primitivos são

$$\begin{aligned}E_{0;\lambda,i} &= \theta_{0;\lambda,i}(y)e_0(x) \\ &= \frac{1}{p^{m+s+n-\lambda}}\frac{y^{p^m}-1}{y^{p^\lambda}-1}\left(\sum_{u=0}^{p^m-1} x^u\right)\left(\sum_{v=0}^{p^s-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i v})y^{vp^{\lambda-s}}\right).\end{aligned} \tag{4.32}$$

Por conseguinte, vamos investigar o somando direto $F_{\delta,i}(B)$. Para $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, $F_{\delta,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\delta,i}(x)\rangle} \cong \mathbb{F}_{q^t}$. Pelo Lema 4.1.3, temos a seguinte fatoração para o

polinômio $y^{p^n}-1$ sobre $\mathbb{F}_{q^t}$:

$$y^{p^n}-1=\prod_{k=0}^{p^s-1}(y-\zeta_{p^s}^k)\prod_{\lambda=s+1}^{n}\prod_{\substack{r=1\\ p\nmid r}}^{p^s-1}(y^{p^{\lambda-s}}-\zeta_{p^s}^r).$$

Daí, existe um isomorfismo de anéis tal que

$$\begin{aligned}F_{\delta,i}(B)\cong\frac{F_{\delta,i}[y]}{\langle y^{p^n}-1\rangle} &\cong \left(\bigoplus_{k=0}^{p^s-1}\frac{F_{\delta,i}[y]}{\langle y-\zeta_{p^s}^k\rangle}\right)\oplus\left(\bigoplus_{\lambda=s+1}^{n}\bigoplus_{\substack{r=1\\ p\nmid r}}^{p^s-1}\frac{F_{\delta,i}[y]}{\langle y^{p^{\lambda-s}}-\zeta_{p^s}^r\rangle}\right)\\ &= \left(\bigoplus_{k=0}^{p^s-1}F_{\delta,i;k}\right)\oplus\left(\bigoplus_{\lambda=s+1}^{n}\bigoplus_{\substack{r=1\\ p\nmid r}}^{p^s-1}F_{\delta,i;\lambda,r}\right),\ \text{para } 1\le\delta\le s;\end{aligned}$$

em que cada $F_{\delta,i;k}=\dfrac{F_{\delta,i}[y]}{\langle y-\zeta_{p^s}^k\rangle}$, e cada $F_{\delta,i;\lambda,r}=\dfrac{F_{\delta,i}[y]}{\langle y^{p^{\lambda-s}}-\zeta_{p^s}^r\rangle}$, se $s+1\le\lambda\le n$. Pelo Teorema 4.1.1, existem p^s idempotentes primitivos em $F_{\delta,i}(B)$ correspondente a $F_{\delta,i;k}$:

$$\theta_{\delta,i;k}(y)=\frac{1}{p^n}\frac{y^{p^n}-1}{y^{p^s}-1}\sum_{v=0}^{p^s-1}\zeta_{p^s}^{-kv}y^v,\ \text{para } 0\le k\le p^s-1,$$

e existem $(n-s)(p^s-p^{s-1})$ idempotentes primitivos em $F_{\delta,i}(B)$ correspondentes a $F_{\delta,i;\lambda,r}$:

$$\theta_{\delta,i;\lambda,r}(y)=\frac{1}{p^{n+s-\delta}}\frac{y^{p^n}-1}{y^{p^\lambda}-1}\sum_{v=0}^{p^s-1}\zeta_{p^s}^{-rv}y^{p^{\lambda-s}v},\ \text{para } s+1\le\lambda\le n \text{ e } 1\le r\le p^s-1,\ \text{com } p\nmid r$$

Note que $g_{\delta,i}(\bar{x})=\zeta_{p^s}$ é uma p^s-ésima raiz primitiva da unidade em $F_{\delta,i}$ (como observamos na demonstração do Teorema 4.2.2). Dessa forma, os idempotentes primitivos de $\mathbb{F}_q(A\times B)$ correspondentes a cada $F_{\delta,i}(B)$ são:

1. se $1\le\delta\le s$ e $1\le i\le\dfrac{\phi(p^\delta)}{t}$, então

$$\begin{aligned}E_{\delta,i;k}&=\frac{1}{p^n}\frac{y^{p^n}-1}{y^{p^s}-1}\sum_{v=0}^{p^s-1}(g_{\delta,i}(x)^{-k}y)^v e_{\delta,i}(x)\\ &=\frac{1}{p^{m+n}}\frac{x^{p^m}-1}{x^{p^\delta}-1}\frac{y^{p^n}-1}{y^{p^s}-1}\left(\sum_{u=0}^{p^\delta-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_iu})x^u\right)\left(\sum_{v=0}^{p^s-1}g_{\delta,i}(x)^{-kv}y^v\right),\end{aligned}\tag{4.33}$$

   para $0\le k\le p^s-1$;

2. se $1\le\delta\le s$, $1\le i\le\dfrac{\phi(p^\delta)}{t}$ e $s+1\le\lambda\le n$, então

$$\begin{aligned}E_{\delta,i;\lambda,r}&=\frac{1}{p^{n+s-\lambda}}\frac{y^{p^n}-1}{y^{p^\lambda}-1}\sum_{v=0}^{p^s-1}\left(g_{\delta,i}(x)^r y^{p^{\lambda-s}}\right)^v e_{\delta,i}(x)\\ &=\frac{1}{p^{m+n+s-\lambda}}\frac{x^{p^m}-1}{x^{p^\delta}-1}\frac{y^{p^n}-1}{y^{p^\lambda}-1}\left(\sum_{u=0}^{p^\delta-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_iu})x^u\right)\left(\sum_{v=0}^{p^s-1}g_{\delta,i}(x)^{-rv}y^{p^{\lambda-s}v}\right)\end{aligned}\tag{4.34}$$

   para $1\le r\le p^s-1$, com $p\nmid r$.

Para $s+1 \leq \varepsilon \leq m \leq n$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}$. Da mesma maneira que observamos na demonstração do Teorema 4.2.2, o Lema 4.2.1 pode ser estendido para o caso $m > s$ e $n > s$ por meio do isomorfismo $F_{\varepsilon,i} = \dfrac{\mathbb{F}_q[x]}{\langle f_{\varepsilon,i}(x)\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}$, de modo a obtermos $g_{\varepsilon,i}(\bar{x}) = \bar{x} = \zeta_{p^\varepsilon}$ uma p^ε-ésima raiz primitiva da unidade em $F_{\varepsilon,i}$. Pelo Lema 4.1.3, temos a seguinte fatoração para o polinômio $y^{p^n}-1$ sobre $\mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}$:

$$y^{p^n}-1 = \prod_{k=0}^{p^\varepsilon-1}(y-\zeta_{p^\varepsilon}^k)\prod_{\lambda=\varepsilon+1}^{n}\prod_{\substack{r=1\\ p\nmid r}}^{p^\varepsilon-1}(y^{p^{\lambda-\varepsilon}}-\zeta_{p^\varepsilon}^r).$$

Daí, existe um isomorfismo de anéis tal que

$$\begin{aligned} F_{\varepsilon,i}(B) \cong \frac{F_{\varepsilon,i}[y]}{\langle y^{p^n}-1\rangle} &\cong \left(\bigoplus_{k=0}^{p^\varepsilon-1}\frac{F_{\varepsilon,i}[y]}{\langle y-\zeta_{p^\varepsilon}^k\rangle}\right)\oplus\left(\bigoplus_{\lambda=\varepsilon+1}^{n}\bigoplus_{\substack{r=1\\ p\nmid r}}^{p^\varepsilon-1}\frac{F_{\varepsilon,i}[y]}{\langle y^{p^{\lambda-\varepsilon}}-\zeta_{p^\varepsilon}^r\rangle}\right)\\ &= \left(\bigoplus_{k=0}^{p^\varepsilon-1}F_{\varepsilon,i;k}\right)\oplus\left(\bigoplus_{\lambda=\varepsilon+1}^{n}\bigoplus_{\substack{r=1\\ p\nmid r}}^{p^\varepsilon-1}F_{\varepsilon,i;\lambda,r}\right), \end{aligned}$$

em que cada $F_{\varepsilon,i;k} = \dfrac{F_{\varepsilon,i}[y]}{\langle y-\zeta_{p^\varepsilon}^k\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}}}$ e $F_{\varepsilon,i;\lambda,r} = \dfrac{F_{\varepsilon,i}[y]}{\langle y^{p^{\lambda-\varepsilon}}-\zeta_{p^\varepsilon}^r\rangle} \cong \mathbb{F}_{q^{t\cdot p^{\varepsilon-s}\cdot p^{\lambda-\varepsilon}}} = \mathbb{F}_{q^{t\cdot p^{\lambda-s}}}$. Pelo Teorema 4.1.1, existem p^ε idempotentes primitivos em $F_{\varepsilon,i}(B)$ correspondentes a $F_{\varepsilon,i;k}$:

$$\theta_{\varepsilon,i;k}(y) = \frac{1}{p^n}\frac{y^{p^n}-1}{y^{p^\varepsilon}-1}\sum_{v=0}^{p^\varepsilon-1}\zeta_{p^\varepsilon}^{-kv}y^v, \text{ com } 0\leq k\leq p^\varepsilon-1,$$

e existem $(n-\varepsilon)(p^\varepsilon-p^{\varepsilon-1})$ idempotentes primitivos em $F_{\varepsilon,i}(B)$ correspondentes a $F_{\varepsilon,i;\lambda,r}$:

$$\theta_{\varepsilon,i;\lambda,r}(y) = \frac{1}{p^{n+\varepsilon-\lambda}}\frac{y^{p^n}-1}{y^{p^\lambda}-1}\sum_{v=0}^{p^\varepsilon-1}\zeta_{p^\varepsilon}^{-rv}y^{p^{\lambda-\varepsilon}v}, \text{ para } \varepsilon+1\leq\lambda\leq n \text{ e } 1\leq r\leq p^\varepsilon-1, \text{ com } p\nmid r.$$

Assim, os idempotentes primitivos em $\mathbb{F}_q(A\times B)$ correspondentes a cada $F_{\varepsilon,i}(B)$ são:

1. se $s+1\leq\varepsilon\leq m$ e $1\leq i\leq\dfrac{\phi(p^\varepsilon)}{t}$

$$\begin{aligned} E_{\varepsilon,i;k} =& \frac{1}{p^n}\frac{y^{p^n}-1}{y^{p^\varepsilon}-1}\sum_{v=0}^{p^\varepsilon-1}(x^{-k}y)^v e_{\varepsilon,i}(x)\\ =& \frac{1}{p^{m+n}}\frac{x^{p^m}-1}{x^{p^\varepsilon}-1}\frac{y^{p^n}-1}{y^{p^\varepsilon}-1}\left(\sum_{u=0}^{p^s-1}\mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_iu})x^{up^{\varepsilon-s}}\right)\left(\sum_{v=0}^{p^\varepsilon-1}x^{-kv}y^v\right), \end{aligned} \tag{4.35}$$

   para $0\leq k\leq p^\varepsilon-1$;

2. se $s+1 \leq \varepsilon \leq m$ e $1 \leq i \leq \dfrac{\phi(p^{\varepsilon})}{t}$

$$\begin{aligned} E_{\varepsilon,i;\lambda,r} =& \frac{1}{p^{n+\varepsilon-\lambda}} \frac{y^{p^n}-1}{y^{p^\lambda}-1} \sum_{v=0}^{p^{\varepsilon}-1} (x^{-r}y^{p^{\lambda-\varepsilon}})^v e_{\varepsilon,i}(x) \\ =& \frac{1}{p^{m+n+\varepsilon-\lambda}} \frac{x^{p^m}-1}{x^{p^\varepsilon}-1} \frac{y^{p^n}-1}{y^{p^\lambda}-1} \left(\sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{up^{\varepsilon-s}} \right) \left(\sum_{v=0}^{p^{\varepsilon}-1} x^{-rv} y^{p^{\lambda-\varepsilon}v} \right), \end{aligned} \tag{4.36}$$

para $\varepsilon+1 < \lambda < n$ e $1 < r < p^{\varepsilon}-1$, com $p \nmid r$.

Logo, para o somando direto $F_0(B)$, existem $1 + \dfrac{p^s-1}{t} + \dfrac{(n-s)\,(p^s-p^{s-1})}{t}$ idempotentes primitivos: $E_{0;0}, E_{0;\delta,i}$, para $1 \leq \delta \leq s,\ 1 \leq i \leq \dfrac{\phi(p^{\delta})}{t}$, conforme o Teorema 4.2.2; $E_{0;\lambda,i}$, para $s+1 \leq \lambda \leq n,\ 1 \leq i \leq \dfrac{\phi(p^s)}{t}$, segundo (4.32). Para cada somando direto $F_{\delta,i}(B)$, com $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^{\delta})}{t}$, existem $p^s + (n-s)(p^s - p^{s-1})$ idempotentes primitivos: $E_{\delta,i;k}$, para $0 \leq k \leq p^s - 1$, dados em (4.33); $E_{\delta,i;\lambda,r}$, para $s+1 \leq \lambda \leq n$ e $1 \leq r \leq p^s-1$, com $p \nmid r$, em (4.34). Para cada somando direto $F_{\varepsilon,i}(B)$, com $s+1 \leq \varepsilon \leq m$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, existem $p^{\delta} + (n-\varepsilon)(p^{\varepsilon} - p^{\varepsilon-1})$ idempotentes primitivos: $E_{\varepsilon,i;k}$, para $0 \leq k \leq p^{\varepsilon}-1$, em (4.35); $E_{\varepsilon,i;\lambda,r}$, para $\varepsilon+1 \leq \lambda \leq n$ e $1 \leq r \leq p^{\varepsilon}-1$, com $p \nmid r$, em (4.36). Com isso, temos

$$\begin{aligned} & 1 + \frac{p^s-1}{t} + \frac{(n-s)(p^s-p^{s-1})}{t} + \frac{p^s-1}{t}(p^s + (n-s)(p^s-p^{s-1})) + \\ & + \frac{p^s-p^{s-1}}{t}(p^{\varepsilon} + (n-\varepsilon)(p^{\varepsilon}-p^{\varepsilon-1})), \end{aligned}$$

para $s+1 \leq \varepsilon \leq m$. Assim,

$$\begin{aligned} & 1 + \frac{p^{2s}-1}{t} + \frac{p^s-p^{s-1}}{t}((p^s-1)(n-s) + (n-s) + p^{\varepsilon} + (n-\varepsilon)(p^{\varepsilon}-p^{\varepsilon-1})) \\ = \ & 1 + \frac{p^{2s}-1}{t} + \frac{p^s-p^{s-1}}{t} \underbrace{(p^s(n-s) + p^{\varepsilon} + (n-\varepsilon)(p^{\varepsilon}-p^{\varepsilon-1}))}_{(I)}, \end{aligned}$$

para $s+1 \leq \varepsilon \leq m$. Como ocorre a variação de ε, vamos investigar o que acontece em (I), fazendo ε percorrer $s+1 \leq \varepsilon \leq m$. Temos

$$\begin{aligned} & p^s(n-s) + p^m + (n-m)(p^m - p^{m-1}) + p^{m-1} + (n-(m-1))(p^{m-1}-p^{m-2}) + \ldots \\ & \ldots + p^{s+1} + (n-(s+1))(p^{s+1}-p^s) \\ =& p^s(n-s) + p^m + (n-m)p^m - (n-m)p^{m-1} + p^{m-1} + (n-(m-1))p^{m-1} - \\ & - (n-(m-1))p^{m-2} + \ldots + p^{s+1} + (n-(s+1))p^{s+1} - (n-(s-1))p^s \\ =& p^s(n-s) + (n-m+1)p^m + 2p^{m-1} + 2p^{m-2} + \ldots + +2p^{s+1} + (s-n+1)p^s \\ =& p^s + (n-m+1)p^m + \frac{2(p^m - p^{s+1})}{p-1}. \end{aligned}$$

Portanto, existem $1+\dfrac{p^{2s}-1}{t}+\dfrac{p^s-p^{s-1}}{t}\left(p^s+(n-m+1)p^m+\dfrac{2\,(p^m-p^{s+1})}{p-1}\right)$ idempotentes primitivos em $\mathbb{F}_q(G)$. ■

Exemplo 4.2.1. Sejam $p=3, q=17$. Então $t=2$ é a ordem multiplicativa de 17 módulo 3, e $3^2\|(17^2-1)$. Para $1\leq m,n\leq s$, temos três casos:

i) Se $m=n=1$, então $\mathbb{F}_{17}(A\times B)=\mathbb{F}_{17}(C_3\times C_3)$, em que $A=\langle x\rangle$ e $B=\langle y\rangle$, com $o(x)=3=o(y)$. Assim, os idempotentes primitivos de $\mathbb{F}_{17}(A)$ são os mesmos do caso $m=1$ no Exemplo 4.1.1, consequentemente, a decomposição do polinômio x^3-1 sobre $\mathbb{F}_{17}$ e os traços também são os mesmos encontrados naquele exemplo.

Como $n=1$, substituindo x por y e m por n em (4.6), obtemos 2 idempotentes primitivos em $F_0(B)$:

$$\begin{aligned}\theta_{0;0}(y)&=\frac{1}{3}\sum_{v=0}^{2}y^v=\frac{1}{3}(1+y+y^2);\\ \theta_{0;1,1}(y)&=\frac{1}{3}\frac{y^3-1}{y^3-1}\sum_{v=0}^{2}\mathrm{Tr}_{q^t/q}(\zeta_3^{-v})y^v=\frac{1}{3}(2-y-y^2).\end{aligned}\tag{4.37}$$

Pelo Lema 4.2.1, existe $g_{1,1}(\bar{x})=\bar{x}$ em $F_{1,1}\cong\dfrac{\mathbb{F}_{17}[x]}{\langle x^2+x+1\rangle}$. Logo, existem 5 idempotentes primitivos em $\mathbb{F}_{17}(C_3\times C_3)$:

$$\begin{aligned}E_{0;0}&=\frac{1}{9}\left(\sum_{u=0}^{2}x^u\right)\left(\sum_{v=0}^{2}y^v\right)=\frac{1}{9}(1+x+x^2)(1+y+y^2)\\&=\frac{1}{9}(1+x+x^2+y+y^2+xy+x^2y+xy^2+x^2y^2);\\ E_{0;1,1}&=\frac{1}{p^{m+n}}\frac{y^3-1}{y^3-1}\left(\sum_{u=0}^{2}x^u\right)\left(\sum_{v=0}^{2}\mathrm{Tr}_{q^t/q}(\zeta_3^{-v})y^v\right)=\frac{1}{9}(1+x+x^2)(2-y-y^2)\\&=\frac{1}{9}(2-y-y^2+2x+2x^2-xy-xy^2-x^2y-x^2y^2);\\ E_{1,1;0}&=\frac{1}{9}\frac{x^3-1}{x^3-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{2}x^0y^v\right)=\frac{1}{9}(2-x-x^2)(1+y+y^2)\\&=\frac{1}{9}(2-x-x^2+2y+2y^2-xy-xy^2-x^2y-x^2y^2);\\ E_{1,1;1}&=\frac{1}{9}\frac{x^3-1}{x^3-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{2}xy^v\right)=\frac{1}{9}(2-x-x^2)(x+xy+xy^2)\\&=\frac{1}{9}(-1+2x-x^2-y-y^2+2xy+2xy^2-x^2y-x^2y^2);\\ E_{1,1;2}&=\frac{1}{9}\frac{x^3-1}{x^3-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{2}xy^v\right)=\frac{1}{9}(2-x-x^2)(x^2+x^2y+x^2y^2)\\&=\frac{1}{9}(-1-y-y^2-x+2x^2-xy-xy^2+2x^2y+2x^2y^2).\end{aligned}$$

ii) Se $m=2$ e $n=1$, então $\mathbb{F}_{17}(A\times B)=\mathbb{F}_{17}(C_9\times C_3)$, em que $A=\langle x\rangle$ e $B=\langle y\rangle$, com $o(x)=9$ e $o(y)=3$. Assim, os idempotentes primitivos de $\mathbb{F}_{17}(A)$ são os mesmos do

caso $m = 2$ no Exemplo 4.1.1, consequentemente, a decomposição do polinômio $x^9 - 1$ sobre $\mathbb{F}_{17}$ e os traços também são os mesmos encontrados naquele exemplo. Além disso, como $n = 1$, os idempotentes primitivos em $F_0(B)$ são os mesmos do caso anterior.

Pelo Lema 4.2.1, existem $g_{1,1}(\bar{x}) = 9 + 11\bar{x}$ em $F_{1,1} \cong \dfrac{\mathbb{F}_{17}[x]}{\langle x^2 + x + 1\rangle}$ e $g_{2,i}(\bar{x}) = \bar{x}$ em $F_{2,i}$ para $1 \leq i \leq 3$. Logo, existem 14 idempotentes primitivos em $\mathbb{F}_{17}(C_9 \times C_3)$:

$$
\begin{aligned}
E_{0;0} &= \frac{1}{27}\left(\sum_{u=0}^{8} x^u\right)\left(\sum_{v=0}^{2} y^v\right) = \sum_{u,v=0}^{8,2} x^u y^v;\\
E_{0;1,1} &= \frac{1}{27}\frac{y^3-1}{y^3-1}\left(\sum_{u=0}^{2} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right) = \frac{1}{27}\left(\sum_{u=0}^{2} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right);\\
E_{1,1;k} &= \frac{1}{27}\frac{x^9-1}{x^3-1}\left(\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8} y^v(9+11x)^{-kv}\right)\\
&= \frac{1}{27}(x^6+x^3+1)\left(\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8} y^v(9+11x)^{-kv}\right), 0 \leq k \leq 2\\
E_{2,1;k} &= \frac{1}{27}\frac{x^9-1}{x^9-1}\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum^{8} x^{-kv}y^v\right)\\
&= \frac{1}{27}\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum^{8} x^{-kv}y^v\right), 0 \leq k \leq 2;\\
E_{2,2;k} &= \frac{1}{27}\frac{x^9-1}{x^9-1}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{8} x^{-kv}y^v\right)\\
&= \frac{1}{27}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{8} x^{-kv}y^v\right), 0 \leq k \leq 2;\\
E_{2,3;k} &= \frac{1}{27}\frac{x^9-1}{x^9-1}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{8} x^{-kv}y^v\right)\\
&= \frac{1}{27}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{8} x^{-kv}y^v\right), 0 \leq k \leq 2.
\end{aligned}
$$

iii) Se $m = 2$ e $n = 2$, então $\mathbb{F}_{17}(A \times B) = \mathbb{F}_{17}(C_9 \times C_9)$, em que $A = \langle x\rangle$ e $B = \langle y\rangle$, com $o(x) = 9 = o(y)$. Assim, os idempotentes primitivos de $\mathbb{F}_{17}(A)$ são os mesmos do caso $m = 2$ no Exemplo 4.1.1, consequentemente, a decomposição do polinômio $x^9 - 1$ sobre $\mathbb{F}_{17}$ e os traços também são os mesmos encontrados naquele exemplo. Como $n = 2$, substituindo x por y e m por n em (4.7), obtemos 5 idempotentes primitivos em $F_0(B)$

$$
\begin{aligned}
\theta_{0;0}(y) &= \frac{1}{9}\sum_{v=0}^{8} y^v = \frac{1}{3}(1+y+y^2+y^3+y^4+y^5+y^6+y^7+y^8);\\
\theta_{0;1,1}(y) &= \frac{1}{9}\frac{y^9-1}{y^3-1}\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v = \frac{1}{9}(y^6+y^3+1)(2-y-y^2);\\
\theta_{0;2,1}(y) &= \frac{1}{9}\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^v = \frac{1}{9}(2+7y+13y^2-y^3+14y^4+14y^5-y^6+13y^7+7y^8);\\
\theta_{0;2,2}(y) &= \frac{1}{9}\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^v = \frac{1}{9}(2+13y+14y^2-y^3+7y^4+7y^5-y^6+14y^7+13y^8);
\end{aligned}
$$

$$\theta_{0;2,3}(y) = \frac{1}{9}\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^v = \frac{1}{9}(2+14y+7y^2-y^3+13y^4+14y^5-y^6+7y^7+14y^8).$$

Pelo Lema 4.2.1, existe $g_{1,1}(\bar{x}) = 9+11\bar{x}$ em $F_{1,1} \cong \dfrac{\mathbb{F}_{17}[x]}{\langle x^2+x+1\rangle}$ e $g_{2,i}(\bar{x}) = \bar{x}$ em $F_{2,i}$ para $1 \leq i \leq 3$. Logo, existem 41 idempotentes primitivos em $\mathbb{F}_{17}(C_9 \times C_9)$:

$$\begin{aligned}
E_{0;0} &= \frac{1}{81}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}y^v\right)\sum_{u,v=0}^{8,8}x^uy^v;\\
E_{0;1,1} &= \frac{1}{81}\frac{y^9-1}{y^3-1}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right)\\
&= \frac{1}{81}(y^6+y^3+1)\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right);\\
E_{0;2,1} &= \frac{1}{81}\frac{y^9-1}{y^9-1}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^v\right);\\
E_{0;2,2} &= \frac{1}{81}\frac{y^9-1}{y^9-1}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^v\right);\\
E_{0;2,3} &= \frac{1}{81}\frac{y^9-1}{y^9-1}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}x^u\right)\left(\sum_{v=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^v\right);\\
E_{1,1;k} &= \frac{1}{81}\frac{x^9-1}{x^3-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8}y^v(9+11x)^{-kv}\right)\\
&= \frac{1}{81}(x^6+x^3+1)\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8}y^v(9+11x)^{-kv}\right);\\
E_{2,1;k} &= \frac{1}{81}\frac{x^9-1}{x^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0 \leq k \leq 8;\\
E_{2,2;k} &= \frac{1}{81}\frac{x^9-1}{x^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0 \leq k \leq 8;\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0 \leq k \leq 8;\\
E_{2,3;k} &= \frac{1}{81}\frac{x^9-1}{x^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0 \leq k \leq 8.
\end{aligned}$$

Para o caso em que $1 \leq n \leq s < m$, digamos $n = 1$ e $m = 3$, então $\mathbb{F}_{17}(A \times B) = \mathbb{F}_{17}(C_{27} \times C_3)$, em que $A = \langle x \rangle$ e $B = \langle y \rangle$, com $o(x) = 27$ e $o(y) = 3$. Assim, os idempotentes primitivos de $\mathbb{F}_{17}(A)$ são os mesmos do caso $m = 3$ no Exemplo 4.1.1, consequentemente, a decomposição do polinômio $x^{27}-1$ sobre $\mathbb{F}_{17}$ e os traços também são os mesmos encontrados naquele exemplo. Além disso, como $n = 1$, os idempotentes primitivos em $F_0(B)$ são os mesmos do primeiro caso deste exemplo. Pelo Lema 4.2.1, existem $g_{1,1}(\bar{x}) = 9 + 11\bar{x}$ em $F_{1,1} \cong \dfrac{\mathbb{F}_{17}[x]}{\langle x^2 + x + 1 \rangle}$; $g_{2,i}(\bar{x}) = \bar{x}^3$ em $F_{2,i}$, para $1 \leq i \leq 3$; $g_{3,i}(\bar{x}) = \bar{x}^9$ em $F_{3,i}$, para $1 \leq i \leq 3$. Logo, existem 23 idempotentes primitivos em $\mathbb{F}_{17}(C_{27} \times C_3)$:

$$
\begin{aligned}
E_{0;0} &= \frac{1}{81}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{2} y^v\right) = \sum_{u,v=0}^{26,2} x^u y^v;\\
E_{0;1,1} &= \frac{1}{81}\frac{y^3-1}{y^3-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v}) y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{2} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v}) y^v\right);\\
E_{1,1;k} &= \frac{1}{81}\frac{x^{27}-1}{x^3-1}\left(\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u}) x^u\right)\left(\sum_{v=0}^{2} y^v (9+11x)^{-kv}\right)\\
&= \frac{1}{81}(x^{24}+x^{21}+x^{18}+x^{15}+x^{12}+x^9+x^6+x^3+1)\cdot\\
&\quad \cdot\left(\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u}) x^u\right)\left(\sum_{v=0}^{2} y^v (9+11x)^{-kv}\right), 0 \leq k \leq 2;\\
E_{2,1;k} &= \frac{1}{81}\frac{x^{27}-1}{x^9-1}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u}) x^u\right)\left(\sum_{v=0}^{2} x^{-3kv} y^v\right)\\
&= \frac{1}{81}(x^{18}+x^9+1)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u}) x^u\right)\left(\sum^{2} x^{-3kv} y^v\right), 0 \leq k \leq 2;\\
E_{2,2;k} &= \frac{1}{81}\frac{x^{27}-1}{x^9-1}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u}) x^u\right)\left(\sum_{v=0}^{2} x^{-3kv} y^v\right)\\
&= \frac{1}{81}(x^{18}+x^9+1)\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u}) x^u\right)\left(\sum_{v=0}^{2} x^{-3kv} y^v\right), 0 \leq k \leq 2;\\
E_{2,3;k} &= \frac{1}{81}\frac{x^{27}-1}{x^9-1}\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4u}) x^u\right)\left(\sum_{v=0}^{2} x^{-3kv} y^v\right)\\
&= \frac{1}{81}(x^{18}+x^9+1)\left(\sum_{u=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4u}) x^u\right)\left(\sum_{v=0}^{2} x^{-3kv} y^v\right), 0 \leq k \leq 2;\\
E_{3,1;k} &= \frac{1}{81}\frac{x^{27}-1}{x^{27}-1}\left(\sum_{v=0}^{26} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u}) x^{3u}\right)\left(\sum_{v=0}^{2} x^{-9kv} y^v\right)\\
&= \frac{1}{81}\left(\sum_{v=0}^{26} \mathrm{Tr}_{q^2/q}(\zeta_9^{-u}) x^{3u}\right)\left(\sum_{v=0}^{2} x^{-9kv} y^v\right), 0 \leq k \leq 2;\\
E_{3,2;k} &= \frac{1}{81}\frac{x^{27}-1}{x^{26}-1}\left(\sum_{u=0}^{26} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2u}) x^{3u}\right)\left(\sum_{v=0}^{2} x^{-9kv} y^v\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{81}\left(\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^{3u}\right)\left(\sum_{v=0}^{2}x^{-9kv}y^v\right), 0\leq k\leq 2;\\
E_{3,3;k} &= \frac{1}{81}\frac{x^{27}-1}{x^{27}-1}\left(\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^{3u}\right)\left(\sum_{v=0}^{2}x^{-9kv}y^v\right)\\
&= \frac{1}{81}\left(\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^{3u}\right)\left(\sum_{v=0}^{2}x^{-9kv}y^v\right), 0\leq k\leq 2.
\end{aligned}
$$

Para o caso em que $1 \leq s < m \leq n$, digamos $m = 3$ e $n = 3$, então $\mathbb{F}_{17}(A \times B) = \mathbb{F}_{17}(C_{27} \times C_{27})$, em que $A = \langle x\rangle$ e $B = \langle y\rangle$, com $o(x) = 27$ e $o(y) = 27$. Assim, os idempotentes primitivos de $\mathbb{F}_{17}(A)$ são os mesmos do caso $m = 3$ no Exemplo 4.1.1, consequentemente, a decomposição do polinômio $x^{27} - 1$ sobre $\mathbb{F}_{17}$ e os traços também são os mesmos encontrados naquele exemplo. Como $n = 3$, substituindo x por y e m por n no terceiro caso do Exemplo (4.1.1), obtemos 8 idempotentes primitivos em $F_0(B)$:

$$
\begin{aligned}
\theta_{0;0}(y) &= \frac{1}{27}\sum_{u=0}^{26}y^u = \frac{1}{27}(1+y+y^2+\ldots+y^{26});\\
\theta_{0;1,1}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^3-1}\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})y^u\\
&= \frac{1}{27}(1+y^3+y^6+y^9+y^{12}+y^{15}+y^{18}+y^{21}+y^{24})(2-y-y^2);\\
\theta_{0;2,1}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^9-1}\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})y^u\\
&= \frac{1}{27}(1+y^9+y^{18})(2+7y+13y^2-y^3+14y^4+14y^5-y^6+13y^7+7y^8);\\
\theta_{0;2,2}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^9-1}\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})y^u\\
&= \frac{1}{27}(1+y^9+y^{18})(2+13y+14y^2-y^3+7y^4+7y^5-y^6+14y^7+13y^8);\\
\theta_{0;2,3}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^9-1}\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})y^u\\
&= \frac{1}{27}(1+y^9+y^{18})(2+14y+7y^2-y^3+13y^4+14y^5-y^6+7y^7+14y^8);\\
\theta_{0;3,1}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})y^u\\
&= \frac{1}{27}(6+7y+13y^2-y^3+\ldots+14y^{23}-y^{24}+13y^{25}+7y^{26});\\
\theta_{0;3,2}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})y^u\\
&= \frac{1}{27}(6+13y+14y^2-y^3+\ldots+7y^{23}-y^{24}+14y^{25}+13y^{26});\\
\theta_{0;3,3}(y) &= \frac{1}{27}\frac{y^{27}-1}{y^{27}-1}\sum_{u=0}^{26}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})y^u
\end{aligned}
$$

$$= \frac{1}{27}(6 + 14y + 7y^2 - y^3 + \ldots + 14y^{23} - y^{24} + 7y^{25} + 14y^{26}).$$

Pelo Lema 4.2.1, existem $g_{1,1}(\bar{x}) = 9 + 11\bar{x}$ em $F_{1,1} \cong \dfrac{\mathbb{F}_{17}[x]}{\langle x^2 + x + 1\rangle}$; $g_{2,i}(\bar{x}) = \bar{x}^3$ em $F_{2,i}$, para $1 \leq i \leq 3$; $g_{3,i}(\bar{x}) = \bar{x}^9$ em $F_{3,i}$, para $1 \leq i \leq 3$. Logo, pelo Teorema 4.2.3, existem 149 idempotentes primitivos em $\mathbb{F}_{17}(C_{27} \times C_{27})$:

$$E_{0;0} = \frac{1}{729}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{36} y^v\right) = \sum_{u,v=0}^{26,26} x^u y^v;$$

$$E_{0;1,1} = \frac{1}{729}\frac{y^{27}-1}{y^3-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right)$$
$$= \frac{1}{729}(y^{24} + y^{21} + y^{18} + y^{15} + y^{12} + y^9 + y^6 + y^3 + 1)\left(\sum_{u=0}^{2} x^u\right)\left(\sum_{v=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-v})y^v\right);$$

$$E_{0;2,1} = \frac{1}{729}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^v\right)$$
$$= \frac{1}{729}(y^{18} + y^9 + 1)\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^v\right);$$

$$E_{0;2,2} = \frac{1}{729}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^v\right)$$
$$= \frac{1}{729}(y^{18} + y^9 + 1)\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^v\right);$$

$$E_{0;2,3} = \frac{1}{729}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^v\right)$$
$$= \frac{1}{729}(y^{18} + y^9 + 1)\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^v\right);$$

$$E_{0;3,1} = \frac{1}{243}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^{3v}\right)$$
$$= \frac{1}{243}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-v})y^{3v}\right);$$

$$E_{0;3,2} = \frac{1}{243}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^{3v}\right)$$
$$= \frac{1}{243}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-2v})y^{3v}\right);$$

$$E_{0;3,3} = \frac{1}{243}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^{3v}\right)$$
$$= \frac{1}{243}\left(\sum_{u=0}^{26} x^u\right)\left(\sum_{v=0}^{8} \mathrm{Tr}_{q^2/q}(\zeta_9^{-4v})y^{3v}\right);$$

$$E_{1,1;k} = \frac{1}{729}\frac{x^{27}-1}{x^3-1}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{2} \mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8} y^v(9+11x)^{-kv}\right)$$

$$= \frac{1}{729}(x^{24}+x^{21}+x^{18}+x^{15}+x^{12}+x^9+x^6+x^3+1)(y^{18}+y^9+1)\cdot$$
$$\cdot\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8}y^v(9+11x)^{-kv}\right), 0\le k\le 8;$$

$$E_{2,1;k} = \frac{1}{729}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right)$$
$$= \frac{1}{729}(x^{18}+x^9+1)(y^{18}+y^9+1)\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0\le k\le 8;$$

$$E_{2,2;k} = \frac{1}{729}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{2}x^{-kv}y^v\right)$$
$$= \frac{1}{729}(x^{18}+x^9+1)(y^{18}+y^9+1)\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^u\right)\left(\sum_{v=0}^{8}x^{-kv}y^v\right), 0\le k\le 8;$$

$$E_{2,3;k} = \frac{1}{729}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^9-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{2}x^{-3kv}y^v\right)$$
$$= \frac{1}{729}(x^{18}+x^9+1)(y^{18}+y^9+1)\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^u\right)\left(\sum_{v=0}^{2}x^{-kv}y^v\right), 0\le k\le 8;$$

$$E_{1,1;3,r} = \frac{1}{243}\frac{x^{27}-1}{x^3-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8}(9+11x)^{-3v}y^v\right)$$
$$= \frac{1}{243}(x^{24}+x^{21}+x^{18}+x^{15}+x^{12}+x^9+x^6+x^3+1)\cdot$$
$$\cdot\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-u})x^u\right)\left(\sum_{v=0}^{8}(9+11x)^{-3v}y^v\right),\ 1\le r\le 8,\ k\ne 3,\ k\ne 6;$$

$$E_{2,1;3,r} = \frac{1}{243}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-2u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^v\right)$$
$$= \frac{1}{243}(x^{18}+x^9+1)\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-2u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^v\right),\ 1\le r\le 8,\ k\ne 3,\ k\ne 6;$$

$$E_{2,2;3,r} = \frac{1}{243}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^{3v}\right)$$
$$= \frac{1}{243}(x^{18}+x^9+1)\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^{3v}\right),\ 1\le r\le 8,\ k\ne 3,\ k\ne 6;$$

$$E_{2,3;3,r} = \frac{1}{243}\frac{x^{27}-1}{x^9-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^{3v}\right)$$
$$= \frac{1}{243}(x^{18}+x^9+1)\left(\sum_{u=0}^{2}\mathrm{Tr}_{q^2/q}(\zeta_3^{-4u})x^u\right)\left(\sum_{v=0}^{8}x^{-3v}y^{3v}\right),\ 1\le r\le 8,\ k\ne 3,\ k\ne 6;$$

$$E_{3,1;k} = \frac{1}{729}\frac{x^{27}-1}{x^{27}-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^v\right)$$
$$= \frac{1}{729}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^v\right), 0\le k\le 26;$$

$$E_{3,2;k} = \frac{1}{729}\frac{x^{27}-1}{x^{27}-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^v\right)$$

$$= \frac{1}{729}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-2u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^{v}\right), 0 \leq k \leq 26;$$

$$E_{3,3;k} = \frac{1}{729}\frac{x^{27}-1}{x^{27}-1}\frac{y^{27}-1}{y^{27}-1}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^{v}\right)$$

$$= \frac{1}{729}\left(\sum_{u=0}^{8}\mathrm{Tr}_{q^2/q}(\zeta_9^{-4u})x^{3u}\right)\left(\sum_{v=0}^{26}x^{-kv}y^{v}\right), 0 \leq k \leq 26;$$

Os idempotentes primitivos encontrados no Exemplo 4.2.1 foram determinados a partir da teoria de corpos finitos, conforme [15], no caso em que o grupo da álgebra de grupo $\mathbb{F}_qG$ é um p-grupo abeliano finito. Vamos agora apresentar algumas definições e resultados estabelecidos em [8] para determinar os idempotentes primitivos de uma álgebra de grupo cujo grupo tem a mesma estrutura do caso anterior.

Definição 4.2.1. Seja G um grupo abeliano. Um subgrupo H de G é chamado de **subgrupo cocíclico** se o grupo quociente G/H é cíclico e não isomorfo a $\{1\}$. Usamos a notação

$$\mathcal{S}_{\mathrm{cc}}(G) = \{H \mid H \text{ é um subgrupo cocíclico de } G\}.$$

Sejam $\mathbb{F}_q$ um corpo finito com q elementos e G um p-grupo abeliano finito. Para cada subgrupo cocíclico H de G, podemos construir um idempotente de $\mathbb{F}_qG$. Se G/H é um p-grupo cíclico e não isomorfo a $\{1\}$, existe um único subgrupo $H^{\#}$ de G contendo H tal que $|H^{\#}/H| = p$ e o elemento $e_H = \widehat{H} - \widehat{H^{\#}} = \dfrac{1}{|H|}\displaystyle\sum_{h\in H} h - \dfrac{1}{|H^{\#}|}\sum_{h\in H^{\#}} h$ é um idempotente de $\mathbb{F}_qG$. Dessa forma, o conjunto abaixo é formado pelos idempotentes de $\mathbb{F}_qG$.

$$\{\widehat{G}\} \cup \left\{e_H = \widehat{H} - \widehat{H^{\#}} \mid H \in \mathcal{S}_{cc}(G)\right\}. \tag{4.38}$$

A partir dos resultados seguintes, vamos mostrar que os elementos do conjunto (4.38) são idempotentes primitivos.

Lema 4.2.2. *Sejam G um p-grupo abeliano finito e H um subgrupo arbitrário de G. Então, $G/H \neq \{1\}$ é um grupo cíclico se, e somente se, existe um único subgrupo L tal que $H < L \leq G$ e $[L : H] = p$.*

Demonstração. Suponha, sem perda de generalidade, $|G| = p^n$. Seja $H \leq G$, temos $|H| = p^i$, para algum $i \leq n$, logo $|G/H| = p^{n-i}$. Suponha $G/H \neq \{1\}$ um grupo cíclico, assim, existe um único subgrupo em G/H de cada ordem que divide a ordem de G/H. Daí, para cada subgrupo K de ordem $p^j \geq p^i$ de G, $H \leq K$ e o subgrupo quociente G/K é o único de sua ordem em G/H e tal que $[G/H : G/K] = p^{j-i}$. Em particular, existe um subgrupo $K = L$ de ordem p^{i+1} de G contendo H, donde segue $G/L \leq G/H$ e

$|G/K| = p^{n-i-1}$. Além disso, $[G/H : G/L] = p$ e isso implica em $p \cdot |G/L| = |G/H|$, logo $p \cdot |H| = |L|$. Portanto, existe um único L, tal que $H < L \leq G$ e $[L : H] = p$.

Reciprocamente, suponha $G/H \neq \{1\}$ não cíclico. Como G/H é p-grupo, então existem pelo menos dois elementos $\bar{a}, \bar{b} \in G/H$ tais que $o(\bar{a}) = o(\bar{b}) = p$ e $\langle \bar{a} \rangle \neq \langle \bar{b} \rangle$. Pelo Teorema da Correspondência, existem dois subgrupos distintos K_1 e K_2 em G tais que $\overline{K_1} = \langle \bar{a} \rangle$, $\overline{K_2} = \langle \bar{b} \rangle$ e $[K_i : H] = p$, para $i = 1, 2$, o que contradiz a hipótese. Isto prova o resultado. ■

Teorema 4.2.4. *Sejam p um número primo, G um grupo abeliano finito de expoente p^n e $\mathbb{F}_q$ um corpo finito com q elementos tal que $p \neq q$. Então (4.38) é um conjunto de idempotentes ortogonais dois a dois de $\mathbb{F}_qG$ cuja soma é igual a 1, ou seja,*

$$1 = \widehat{G} + \sum_{H \in \mathcal{S}_{cc}(G)} e_H, \tag{4.39}$$

em que 1 denota o elemento identidade em $\mathbb{F}_qG$.

Demonstração. Vimos acima que o conjunto (4.38) é formado por elementos idempotentes. Vamos mostrar que estes elementos são ortogonais.

Sejam H e K subgrupos cocíclicos distintos de G. Logo existem H^* e K^*, subgrupos de G tais que $[H^* : H] = [K^* : K] = p$. Se $H \subsetneq K$, então K/H é cíclico, com $|K/H| = p^j$, para $j \geq 1$. Daí, existe $H_1 \leqslant G$, tal que $|H_1/H| = p$. Pela unicidade, $H^* = H_1$. Assim,

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

Se H e K não estão contidos um no outro, então H e K estão contidos propriamente em $HK := \{hk;\ h \in H \text{ e } k \in K\}$ e, consequentemente, H^* e K^* também estão contidos propriamente em HK, logo $H^*K^* \subset HK$. Por outro lado, da definição de subgrupo cocíclico, temos $HK \subset H^*K^*$. Portanto, $HK = H^*K^*$. Além disso, $HK \subset H^*K \subset H^*K^* \subset HK$, logo $H^*K = HK$. Analogamente, segue $HK^* = HK$. Assim,

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

Resta mostrar que a soma destes idempotentes é igual a 1. Para cada subgrupo cíclico $C = \langle c \rangle$ de G, denote por $G(C)$ o conjunto de todos os geradores de C, isto é,

$$G(C) = \{c^j \in C;\ mdc(j, |C|) = 1\}.$$

Se $\mathcal{C}$ denota a família de todos os subgrupos cíclicos de G, então $|G| = \sum_{C \in \mathcal{C}} |G(C)|$ e, como G é um p-grupo,

$$|G(C)| = \phi(p^i) = p^i - p^{i-1} = |C| - \frac{|C|}{p}.$$

Denote por $\mathcal{S}_{cc}(G)$ o conjunto de todos os subgrupos cocíclicos de G. Seja $e = \sum_{H\in\mathcal{S}_{cc}} e_H$. Afirmamos que $e = 1$. Para provar este fato, basta mostrar que $(\mathbb{F}_qG)e = \mathbb{F}_qG$. Com efeito, visto que esses idempotentes são dois a dois ortogonais, como mostramos anteriormente, a união dos ideais gerados por eles é disjunta, daí,

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

Assim,

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

como espaços vetoriais sobre $\mathbb{F}_q$. Por definição de e_H, $\widehat{H} = \widehat{H^*} + e_H$, donde $\widehat{H^*}e_H = \widehat{H^*}(\widehat{H} - \widehat{H^*}) = 0$. Deste modo, $(\mathbb{F}_qG)\widehat{H} = (\mathbb{F}_qG)\widehat{H^*} \oplus (\mathbb{F}_qG)e_H$, logo

$$\dim_{\mathbb{F}_q}(\mathbb{F}_qG)e_H = \dim_{\mathbb{F}_q}(\mathbb{F}_qG)\widehat{H} - \dim_{\mathbb{F}_q}(\mathbb{F}_qG)\widehat{H^*}.$$

Pela Proposição 3.2.2, $(\mathbb{F}_qG)\widehat{H} \cong \mathbb{F}_q(G/H)$ e $(\mathbb{F}_qG)\widehat{H^*} \cong \mathbb{F}_q(G/H^*)$, assim,

$$\dim_{\mathbb{F}_q}(\mathbb{F}_qG)e_H = \dim_{\mathbb{F}_q}\mathbb{F}_q(G/H) - \dim_{\mathbb{F}_q}\mathbb{F}_q(G/H^*),$$

donde

$$\dim_{\mathbb{F}_q}\mathbb{F}_q(G/H) = |G/H| \quad \text{e} \quad \dim_{\mathbb{F}_q}\mathbb{F}_q(G/H^*) = |G/H^*|.$$

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

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

Assim,

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

Logo,

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

Portanto, como $(\mathbb{F}_qG)e \subset \mathbb{F}_qG$, segue $(\mathbb{F}_qG)e = \mathbb{F}_qG$. ■

Teorema 4.2.5. *Sob as hipóteses do Teorema 4.2.4, o conjunto (4.38) é o conjunto dos idempotentes primitivos de $\mathbb{F}_qG$ se, e somente se, $o(\bar{q}) = \phi(p^n)$ em $U(\mathbb{Z}_{p^n})$, em que ϕ denota a função de Euler.*

A Definição 4.2.1, o Lema 4.2.2 e os Teoremas 4.2.4 e 4.2.5 podem ser estendidos para grupos ainda mais gerais, como grupos abelianos que não sejam p-grupos. Como em

um grupo abeliano finito G todos os seus subgrupos são normais, seus subgrupos de Sylow também o são. Dessa forma, o grupo G pode ser escrito como $G = G_{p_1} \times \cdots \times G_{p_t}$, em que G_{p_i} denota o p_i-subgrupo de Sylow de G, para os números primos distintos $p_1, \ldots, p_t$. A partir disso, tais resultados são estendidos conforme [8]. Nesta dissertação, entretanto, tratamos apenas de p-grupos abelianos finitos

No exemplo a seguir, denotamos por $[i]_k$ a classe do inteiro i módulo k. Além disso, utilizamos os subgrupos determinados na Subseção 4.2.1 para escrever os idempotentes primitivos.

Exemplo 4.2.2. Sejam $\mathbb{F}_{11}$ um corpo finito com 11 elementos e $p = 3$ um primo ímpar. Seja $G = \langle a \rangle \times \langle b \rangle$ um 3-grupo abeliano finito de ordem 3^{m+n}, como $mdc(11, 3) = 1$. Daí,

i) para $m = n = 1$, $\exp(G) = 3$, e $o(\overline{11}) = 6 = \phi(9)$ em $U(\mathbb{Z}_9)$. Assim, pelo Teorema 4.2.5, o conjunto de idempotentes primitivos de $\mathbb{F}_q G$ é dado por

$$\begin{aligned}
e_0 &= \frac{1}{3}\sum_{g\in G} g = \frac{1}{9}(1 + a + a^2 + b + b^2 + ab + a^2b + ab^2 + a^2b^2) \\
e_1 &= \widehat{\langle a \rangle} - \widehat{G} = \frac{1}{3}(1 + a + a^2) - \frac{1}{9}(1 + a + a^2 + b + b^2 + ab + a^2b + ab^2 + a^2b^2) \\
&= \left(\frac{1}{3} - \frac{1}{9}\right)(1 + a + a^2) - \frac{1}{9}(b + b^2 + ab + a^2b + ab^2 + a^2b^2); \\
e_2 &= \widehat{\langle b \rangle} - \widehat{G} = \frac{1}{3}(1 + b + b^2) - \frac{1}{9}(1 + a + a^2 + b + b^2 + ab + a^2b + ab^2 + a^2b^2) \\
&= \left(\frac{1}{3} - \frac{1}{9}\right)(1 + b + b^2) - \frac{1}{9}(a + a^2 + ab + a^2b + ab^2 + a^2b^2).
\end{aligned}$$

ii) Para $m = 2$ e $n = 1$, $\exp(G) = 9$ e $o(\overline{11}) = 18 = \phi(9)$ em $U(\mathbb{Z}_{27})$. Assim, o conjunto de idempotentes primitivos de $\mathbb{F}_q G$ é dado por

$$\begin{aligned}
e_0 &= \frac{1}{27}\sum_{g\in G} g = \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j; \\
e_1 &= \widehat{\langle a \rangle} - \widehat{G} = \frac{1}{9}\sum_{i=1}^{8} a^i - \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j = \left(\frac{1}{9} - \frac{1}{27}\right)\sum_{i=1}^{8} a^i - \frac{1}{27}\sum_{i=0,j=1}^{8,2} a^i b^j; \\
e_2 &= \widehat{\langle b \rangle} - \widehat{G} = \frac{1}{3}\sum_{j=0}^{2} b^j - \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j = \left(\frac{1}{3} - \frac{1}{27}\right)\sum_{j=0}^{2} b^j - \frac{1}{27}\sum_{i=1,j=0}^{8,2} a^i b^j; \\
e_3 &= \widehat{\langle ab \rangle} - \widehat{G} = \frac{1}{9}\sum_{i=0}^{8} a^i b^{[i]_3} - \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j; \\
e_4 &= \widehat{\langle ab^2 \rangle} - \widehat{G} = \frac{1}{9}\sum_{i=0}^{8} a^i b^{2[i]_3} - \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j; \\
e_5 &= \widehat{\langle a^3 \rangle \times \langle b \rangle} - \widehat{G} = \frac{1}{9}\sum_{i,j=0}^{2,2} a^{3i} b^j - \frac{1}{27}\sum_{i,j=0}^{8,2} a^i b^j;
\end{aligned}$$

$$e_6 = \widehat{\langle a^3b\rangle} - \widehat{\langle a^3\rangle \times \langle b\rangle} = \frac{1}{3}\sum_{i=0}^{2} a^{3i}b^i - \frac{1}{9}\sum_{i,j=0}^{2,2} a^{3i}b^j;$$

$$e_7 = \widehat{\langle a^6b\rangle} - \widehat{\langle a^3\rangle \times \langle b\rangle} = \frac{1}{3}\sum_{i=0}^{2} a^{[6i]_9}b^i - \frac{1}{9}\sum_{i,j=0}^{2,2} a^{3i}b^j.$$

iii) Para $m = 2$ e $n = 2$, $\exp(G) = 9$ e $o(\overline{11}) = 54 = \phi(81)$ em $U(\mathbb{Z}_{81})$. Assim, pelo Teorema 4.2.5, o conjunto de idempotentes primitivos de $\mathbb{F}_qG$ é dado por

$$e_0 = \frac{1}{81}\sum_{g\in G} g = \frac{1}{81}\sum_{g\in\langle a\rangle\times\langle b\rangle} g;$$

$$e_1 = \widehat{\langle a\rangle \times \langle b^3\rangle} - \widehat{G} = \frac{1}{27}\left(\sum_{h\in\langle a\rangle\times\langle b^3\rangle} h\right) - \frac{1}{81}\left(\sum_{g\in\langle a\rangle\times\langle b\rangle} g\right);$$

$$e_2 = \widehat{\langle a^3\rangle \times \langle ab\rangle} - \widehat{G} = \frac{1}{27}\left(\sum_{h\in\langle a^3\rangle\times\langle ab\rangle} h\right) - \frac{1}{81}\left(\sum_{g\in\langle a\rangle\times\langle b\rangle} g\right);$$

$$e_3 = \widehat{\langle a^3\rangle \times \langle ab^2\rangle} - \widehat{G} = \frac{1}{27}\left(\sum_{h\in\langle a^3\rangle\times\langle ab^2\rangle} h\right) - \frac{1}{81}\left(\sum_{g\in\langle a\rangle\times\langle b\rangle} g\right);$$

$$e_4 = \widehat{\langle b\rangle \times \langle a^3\rangle} - \widehat{G} = \frac{1}{27}\left(\sum_{h\in\langle b\rangle\times\langle a^3\rangle} h\right) - \frac{1}{81}\left(\sum_{g\in\langle a\rangle\times\langle b\rangle} g\right);$$

$$e_5 = \widehat{\langle a\rangle} - \widehat{\langle a\rangle \times \langle b^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle a\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a\rangle\times\langle b^3\rangle} h\right);$$

$$e_6 = \widehat{\langle ab^3\rangle} - \widehat{\langle a\rangle \times \langle b^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^3\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a\rangle\times\langle b^3\rangle} h\right);$$

$$e_7 = \widehat{\langle ab^6\rangle} - \widehat{\langle a\rangle \times \langle b^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^6\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a\rangle\times\langle b^3\rangle} h\right);$$

$$e_8 = \widehat{\langle ab\rangle} - \widehat{\langle a^3\rangle \times \langle ab\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a^3\rangle\times\langle ab\rangle} h\right);$$

$$e_9 = \widehat{\langle ab^2\rangle} - \widehat{\langle a^3\rangle \times \langle ab\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^2\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a^3\rangle\times\langle ab\rangle} h\right);$$

$$e_{10} = \widehat{\langle ab^5\rangle} - \widehat{\langle a^3\rangle \times \langle ab\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^5\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle a^3\rangle\times\langle ab\rangle} h\right);$$

$$e_{11} = \widehat{\langle ab^4\rangle} - \widehat{\langle b^3\rangle \times \langle a^2b\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^4\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b^3\rangle\times\langle a^2b\rangle} h\right);$$

$$e_{12} = \widehat{\langle ab^7\rangle} - \widehat{\langle b^3\rangle \times \langle a^2b\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^7\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b^3\rangle\times\langle a^2b\rangle} h\right);$$

$$e_{13} = \widehat{\langle ab^8\rangle} - \widehat{\langle b^3\rangle \times \langle a^2b\rangle} = \frac{1}{9}\left(\sum_{h\in\langle ab^8\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b^3\rangle\times\langle a^2b\rangle} h\right);$$

$$
\begin{aligned}
e_{14} &= \widehat{\langle a^6b\rangle} - \widehat{\langle b\rangle \times \langle a^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle a^6b\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b\rangle\times\langle a^3\rangle} h\right);\\
e_{15} &= \widehat{\langle a^3b\rangle} - \widehat{\langle b\rangle \times \langle a^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle a^3b\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b\rangle\times\langle a^3\rangle} h\right);\\
e_{16} &= \widehat{\langle b\rangle} - \widehat{\langle b\rangle \times \langle a^3\rangle} = \frac{1}{9}\left(\sum_{h\in\langle b\rangle} h\right) - \frac{1}{27}\left(\sum_{h\in\langle b\rangle\times\langle a^3\rangle} h\right).
\end{aligned}
$$

O próximo exemplo é uma generalização para o primo p no caso em que o grupo $G = C_{p^2} \times C_p$.

Exemplo 4.2.3. Considere o corpo $\mathbb{F}_2$ e seja p um primo ímpar. Seja $G = \langle a\rangle \times \langle b\rangle$ um grupo abeliano finito, com $o(a) = p^2$ e $o(b) = p$. Como $\bar{2}$ é um gerador de $U(\mathbb{Z}_{p^2})$, as hipóteses do Teorema 4.2.5 são satisfeitas, assim, os idempotentes primitivos da álgebra de grupo $\mathbb{F}_2(\langle a\rangle \times \langle b\rangle)$ são dados por:

$$
\begin{aligned}
&e_0 = \widehat{a}\widehat{b} = \widehat{G};\ e_1 = \widehat{b} - \widehat{\langle a^p\rangle \times \langle b\rangle};\ e_{1j} = \widehat{a^{jp}b} - \widehat{\langle a^p\rangle \times \langle b\rangle},\ j = 1,\ldots,p-1;\\
&e_2 = \widehat{a} - \widehat{G};\ e_{2i} = \widehat{ab^i} - \widehat{G},\ i = 1,\ldots,p-1; e_3 = \widehat{\langle a^p\rangle \times \langle b\rangle} - \widehat{G}.
\end{aligned}
$$

Os idempotentes primitivos que foram descritos usando a teoria de grupos são apresentados de maneira bem mais geral, do que a posta aqui, nos artigos [7], [8] e [10]. Além disso, Guerreiro, Milies e Ferraz [8] determinaram condições necessárias e suficientes para que os idempotentes primitivos dados desta forma fossem G-isomorfos, o que permite classificar alguns tipos de códigos. Para maiores detalhes sugerimos as referências supracitadas

Observe que, para o caso mais geral (no que se refere a grupos abelianos não cíclicos) chegamos a conclusões semelhantes às descritas nas páginas 62 e 63. Os Exemplos 4.2.1 e 4.2.2 mostram que, quando as hipóteses do Teorema 4.2.5 não são satisfeitas no Exemplo 4.2.1, existem mais idempotentes primitivos, uma vez que cada um deles corresponde às componentes simples de $\mathbb{F}_qG$ encontradas nos Teoremas 4.2.1, 4.2.2 e 4.2.3, e o número de componentes nestes casos são maiores do que o número de componentes de $\mathbb{Q}G$.

5 CÓDIGOS DE GRUPO

Neste capítulo, descrevemos todos os códigos abelianos lineares com complementar dual (LCD) e todos os códigos auto-ortogonais sobre uma álgebra de grupo. Iniciamos com alguns dos principais conceitos de códigos corretores de erros, especificamente, códigos lineares e códigos cíclicos, com base em [12] e [18]. Por conseguinte, abordamos estes mesmos códigos sobre álgebras de grupo e também introduzimos os códigos de grupo, precisamente, códigos abelianos e minimais, conforme [2], [3], [11], [15] e [19]. Além disso, apresentamos alguns conceitos, relativos a subespaços ortogonais de uma álgebra de grupo e algumas considerações, com base em [6]. Por fim, descrevemos os códigos abelianos LCD e auto-ortogonais em $\mathbb{F}_qG$, de acordo com [15].

5.1 PRELIMINARES

Sejam $\mathbb{F}_q$ um corpo finito e $n \in \mathbb{N}^*$. Um **código linear** $\mathcal{C}$ pode ser visto como um subespaço vetorial próprio de $\mathbb{F}_q^n$. Em particular, este código é dito um **código cíclico** se, para todo $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$, temos $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

É fácil ver que o espaço vetorial $\mathbb{F}_q^n$ é isomorfo ao anel quociente (visto como espaço vetorial sobre $\mathbb{F}_q$) $\mathcal{R}_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$ e, com isso, podemos definir $\mathcal{C}$ como um ideal de $\mathcal{R}_n$. Além disso, se G é um grupo cíclico finito gerado por um elemento a de ordem n, a álgebra de grupo $\mathbb{F}_qG$ é isomorfa ao anel $\mathcal{R}_n$ e, assim, podemos definir $\mathcal{C}$ como um ideal de $\mathbb{F}_qG$. Estas diferentes abordagens podem ser entendidas de maneira bem simples com o diagrama abaixo, dado por Guerreiro e Milies [11]:

$$\begin{array}{ccccc} \mathcal{C} \subset \mathbb{F}_q^n & \overset{\Psi}{\to} & \mathcal{R}_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} & \overset{\varphi}{\to} & \mathbb{F}_qG = \mathbb{F}_q\langle a\rangle \\ \pi \quad \downarrow & & \bar{x} \downarrow & & a \downarrow \\ \mathcal{C} \subset \mathbb{F}_q^n & \overset{\Psi}{\to} & \mathcal{R}_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} & \overset{\varphi}{\to} & \mathbb{F}_qG = \mathbb{F}_q\langle a\rangle, \end{array}$$

em que $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ é tal que $\pi(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2})$, chamado de operador troca cíclica, Ψ representa o isomorfismo linear entre os espaços vetoriais $\mathbb{F}_q^n$ e $\mathcal{R}_n$, e φ representa o isomorfismo entre os anéis $\mathcal{R}_n$ e $\mathbb{F}_qG$. Além disso, o operador π em $\mathbb{F}_q^n$ é equivalente à multiplicação por $\bar{x}$ em $\mathcal{R}_n$ que, por sua vez, é equivalente a multiplicação por a em $\mathbb{F}_qG$.

Estendendo essas ideias, Berman [2], [3] e, independentemente, MacWilliams [19] definiram **códigos abelianos** como ideais em álgebras de grupo abeliano finito e, mais geralmente, um **código de grupo à esquerda** foi definido como um ideal à esquerda

em uma álgebra de grupo finito [11]. Neste caso, denotamos um código abeliano por $\mathcal{C} = \mathbb{F}_q(G)E$, com $E^2 = E$.

Na Seção 3.4 e no Capítulo 4 discutimos extensivamente como se determinam os idempotentes primitivos de uma álgebra de grupo. A partir destes elementos e a definição de código abeliano, dizemos que um código é **minimal** se for um ideal minimal na álgebra de grupo. Em particular, se $mdc(q, |G|) = 1$, então pelo Corolário 3.2.1 do Teorema de Maschke, $\mathbb{F}_q(G)$ é semissimples. Neste caso, todo ideal desta álgebra de grupo é uma soma direta de alguns ideais minimais. Portanto, um código abeliano de $\mathbb{F}_qG$ é a soma direta de alguns códigos minimais em $\mathbb{F}_qG$.

Para $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{F}_q(G)$, o **peso de Hamming** $w(\alpha)$ é definido como o número de elementos não nulos α_g, ou seja, $w(\alpha) = supp(\alpha)$. A **distância mínima de Hamming** $d(\mathcal{C})$ de um código abeliano $\mathcal{C}$ é definida por $d(\mathcal{C}) := \min\{w(\alpha) \mid \alpha \in \mathcal{C}, \alpha \neq 0\}$, a dimensão refere-se à dimensão de $\mathbb{F}_q(G)$ como um espaço vetorial sobre $\mathbb{F}_q$ e é dita **dimensão de um código abeliano**. Um código abeliano $\mathcal{C}$ em $\mathbb{F}_q(G)$ de dimensão k e distância mínima de Hamming d será chamado **código** $[|G|, k, d]$ **sobre** $\mathbb{F}_q$.

O **produto interno euclidiano em** $\mathbb{F}_q(G)$ é definido da seguinte forma: para todos $\alpha = \sum_{g\in G} \alpha_g g,\ \beta = \sum_{g\in G} \beta_g g \in \mathbb{F}_q(G)$,

$$\langle \alpha, \beta \rangle = \sum_{g\in G} \alpha_g \beta_g.$$

Note que a álgebra de grupo $\mathbb{F}_qG$ possui uma forma bilinear simétrica não degenerada G-invariante natural $\langle ., . \rangle$, definida por

$$\langle g, h \rangle = \begin{cases} 1 \text{ se } g = h, \\ 0 \text{ caso contrário.} \end{cases} \tag{5.1}$$

Aqui, a G-invariância significa que $\langle \alpha g, \beta g \rangle = \langle \alpha, \beta \rangle$, para todos $\alpha, \beta \in \mathbb{F}_qG$ e todo $g \in G$.

Para cada $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{F}_q(G)$, $\hat{\alpha} = \sum_{g\in G} \alpha_g g^{-1}$ é chamada **involução adjunta** de α. Além disso, α é dito **auto-adjunto** se $\alpha = \hat{\alpha}$.

Observe que a aplicação $\hat{}\ : \mathbb{F}_qG \longrightarrow \mathbb{F}_qG$ define um anti-isomorfismo de $\mathbb{F}_qG$, segundo [21, Proposição 3.2.11], e para todo $\alpha, \beta \in \mathbb{F}_qG$, a forma bilinear definida em (5.1) satisfaz

$$\langle \alpha, \beta \rangle = \langle \alpha\hat{\beta}, 1 \rangle = \langle 1, \beta\hat{\alpha} \rangle.$$

5.2 CÓDIGOS ABELIANOS COM COMPLEMENTAR DUAL (LCD) E AUTO-ORTOGONAIS ABELIANOS

Definição 5.2.1. Um código linear $\mathcal{C}$ sobre $\mathbb{F}_q$ é chamado **código LCD (código linear com dual complementar)** se $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$, em que

$$\mathcal{C}^\perp = \{\beta \in \mathbb{F}_q G : \langle \alpha, \beta \rangle = 0, \text{ para todo } \alpha \in \mathcal{C}\}.$$

Se $\mathcal{C} \subseteq \mathcal{C}^\perp$, então $\mathcal{C}$ é chamado **código auto-ortogonal**.

Os idempotentes primitivos em $\mathbb{F}_q(G)$ são obtidos no Teorema 4.2.1, se $1 \leq n, m \leq s$, no Teorema 4.2.2, se $1 \leq n \leq s < m$, e no Teorema 4.2.3, se $1 \leq s < m \leq n$. Seja $\mathcal{C}$ um código abeliano em $\mathbb{F}_q(G)$. Então $\mathcal{C} = \mathbb{F}_q(G)E$, no qual E é a soma direta de alguns idempotentes primitivos em $\mathbb{F}_q(G)$ (veja p. 96). Nesta seção, investigamos todos os códigos abelianos LCD e auto-ortogonais em $\mathbb{F}_q(G)$. Primeiro, por conveniência, denotamos

$$N_1 = \frac{p^{n+s-1}(p-1)(m-s) + p^{n+s} - 1}{t}$$

e

$$N_2 = \frac{p^{2s}-1}{t} + \frac{p^s - p^{s-1}}{t}\left(p^s + (n-m+1)p^m + \frac{2\left(p^m - p^{s+1}\right)}{p-1}\right).$$

A seguir, apresentamos um Lema que caracteriza os códigos LCD e auto-ortogonais.

Lema 5.2.1. *Seja $\mathcal{C} = \mathbb{F}_q(G)E$, com $E^2 = E$, um código abeliano de uma álgebra de grupo abeliana $\mathbb{F}_q(G)$.*

(i) [6, Teorema 3.1] Então $\mathcal{C}$ é um código abeliano LCD se, e somente se, $E^2 = E = \hat{E}$.

(ii) Então $\mathcal{C}$ é um código auto-ortogonal se, e somente se, $E\hat{E} = 0$.

Demonstração. (i) Primeiro, suponha $\mathcal{C} = \mathbb{F}_q(G)E$ um código abeliano LCD. Seja $\mathbb{F}_q G = \mathcal{C} \oplus \mathcal{C}^\perp$ e escreva $1 = E + H$ com $E \in \mathcal{C}$ e $H \in \mathcal{C}^\perp$. Uma vez que $\mathcal{C}$ e $\mathcal{C}^\perp$ são ideais de $\mathbb{F}_q G$, segue

$$E = E^2 + EH \Longrightarrow E - E^2 = EH \in \langle H \rangle \subset \mathcal{C}^\perp \Longrightarrow E - E^2 \in \mathcal{C} \cap \mathcal{C}^\perp \Longrightarrow E = E^2,$$

e, de modo análogo, $H = H^2$. Além disso, $\mathbb{F}_q(G)E \oplus \mathbb{F}G(1-E)$, e isso implica em $\mathcal{C} = \mathbb{F}_q(G)E$ e $\mathcal{C}^\perp = \mathbb{F}_q(G)H$. Se $\alpha, \beta \in \mathbb{F}_q G$, então

$$0 = \langle \alpha E, \beta H \rangle = \langle \alpha, \beta H \hat{E} \rangle = \langle \alpha, \beta(1-E)\hat{E} \rangle.$$

Como a forma bilinear é não degenerada em $\mathbb{F}_q G$, segue $(1-E)\hat{E} = 0$ e, consequentemente, $\hat{E} = E\hat{E}$. Portanto,

$$E = \hat{\hat{E}} = \widehat{E\hat{E}} = \hat{E}.$$

Reciprocamente, suponha $E^2 = E = \hat{E}$. Como E é um idempotente, pelo Teorema 2.2.3, $\mathbb{F}_qG = \mathbb{F}_q(G)E \oplus \mathbb{F}G(1-E)$. Como $\langle \alpha\beta, \rho\rangle = \langle \alpha, \rho\hat{\beta}\rangle$, para todos $\alpha, \beta, \rho \in \mathbb{F}_qG$, então, para $\alpha, \beta \in \mathbb{F}_qG$, obtemos

$$\begin{aligned}\langle \alpha E, \beta(1-E)\rangle &= \langle \alpha, \beta(1-E)\hat{E}\rangle = \langle \alpha, \beta(1-E)E\rangle \\ &= \langle \alpha, 0\rangle = 0.\end{aligned}$$

Logo $\mathbb{F}_qG(1-E)$ é um ideal de $\mathcal{C}^{\perp}$. Como

$$\dim_{\mathbb{F}_q} \mathbb{F}_qG(1-E) = |G| - \dim_{\mathbb{F}_q} \mathcal{C} = \dim_{\mathbb{F}_q} \mathcal{C}^{\perp},$$

segue $\mathbb{F}_qG(1-E) = \mathcal{C}^{\perp}$. Portanto, $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. Isto prova o resultado.

(ii) Sejam $E = \sum_{h\in G} \rho_h h$ um idempotente em $\mathbb{F}_q(G)$ e sejam $a = \alpha E, b = \beta E \in \mathcal{C} \subset \mathbb{F}_q(G)$, com $\alpha = \sum_{g\in G} \alpha_g g$, $\beta = \sum_{h\in G} \beta_h h \in \mathbb{F}_q(G)$. Pela G-invariância da forma bilinear dada em (5.1), temos, para todo $g \in G$,

$$\langle gE, \beta\rangle = \langle E, \beta\rangle = \sum_{g\in G} \rho_h\beta_h \quad \text{e} \quad \langle g, \beta\hat{E}\rangle = \langle g, \sum_{g\in G} \beta_h\rho_h g\rangle = \sum_{g\in G} \rho_h\beta_h$$

Logo, $\langle gE, \beta\rangle = \langle g, \beta\hat{E}\rangle$, para todo $g \in G$. Além disso,

$$\langle a, b\rangle = \langle \alpha E, \beta E\rangle = \langle \alpha, \beta E\hat{E}\rangle = \langle \alpha, b\hat{E}\rangle, \quad \text{para todos } a, b \in \mathcal{C}$$

Como $\mathcal{C}$ é auto-ortogonal se, e somente se, $\langle a, b\rangle = 0$, para todo $a, b \in \mathcal{C}$, então

$$0 = \langle a, b\rangle = \langle \alpha E, \beta E\rangle = \langle \alpha, b\hat{E}\rangle$$

Pela arbitrariedade de a e b, podemos tomar $b = \hat{E}$ e, assim, $\langle \alpha, E\hat{E}\rangle = 0$. Portanto, $E\hat{E} = 0$.

■

Lema 5.2.2. *Sejam p um primo tal que $mdc(p, q) = 1$, t a ordem multiplicativa de q módulo p e $p^s \| (q^t - 1)$. Então*

(i) se t é ímpar e $1 \leq m \leq s$, a fatoração irredutível de $x^{p^m} - 1$ sobre $\mathbb{F}_q$ pode ser reorganizada como

$$x^{p^m} - 1 = (x-1) \prod_{\delta=1}^{m} \prod_{i=1}^{\frac{\phi(p^\delta)}{2t}} (f_{\delta,i}(x) f^*_{\delta,i}(x)), \tag{5.2}$$

em que cada $f_{\delta,i}(x) = \prod_{\mu=0}^{t-1} (x - \zeta_{p^\delta}^{l_i q^\mu})$, com $mdc(l_i, p) = 1$, e $f^*_{\delta,i}(x)$ é o polinômio recíproco de $f_{\delta,i}(x)$.

(ii) se t é ímpar e $m > s$, a fatoração irredutível de $x^{p^m}-1$ sobre $\mathbb{F}_q$ pode ser reorganizada como

$$x^{p^m}-1=(x-1)\prod_{\delta=1}^{s}\prod_{i=1}^{\frac{\phi(p^\delta)}{2t}}(f_{\delta,i}(x)f^*_{\delta,i}(x))\prod_{\varepsilon=s+1}^{m}\prod_{i=1}^{\frac{\phi(p^s)}{2t}}(f_{\varepsilon,i}(x)f^*_{\varepsilon,i}(x)), \tag{5.3}$$

em que cada $f_{\delta,i}(x)=\prod_{\mu=0}^{t-1}(x-\zeta_{p^\delta}^{l_iq^\mu})$, com $1\le\delta\le s$, e $f^*_{\delta,i}(x)$ é o polinômio recíproco de $f_{\delta,i}(x)$; cada $f_{\varepsilon,i}(x)=\prod_{\mu=0}^{t-1}(x^{p^{\varepsilon-s}}-\zeta_{p^s}^{l_iq^\mu})$, com $s+1\le\varepsilon\le m$, e $f^*_{\varepsilon,i}(x)$ o polinômio recíproco de $f_{\varepsilon,i}(x)$.

Demonstração. Sejam $1\le\delta\le m$ e t ímpar. Suponha, por contradição, $f_{\delta,i}(x)=f^*_{\delta,i}(x)$. Daí, $f_{\delta,i}(\zeta_{p^\delta}^{l_i})=f_{\delta,i}(\zeta_{p^\delta}^{-l_i})=0$ e, assim, l_i e $-l_i$ pertencem a mesma q-classe ciclotômica, isto é, $q^jl_i\equiv -l_i \pmod p$, com $1\le j\le t-1$. Em particular, para $l_i=1$, temos $q^j\equiv -1\pmod p$, daí $p\mid(q^j+1)$ e, consequentemente, $p\mid(q^j+1)(q^j-1)=q^{2j}-1$. Como t é a ordem multiplicativa de q módulo p, então $t\mid 2j$, o que contradiz a hipótese t ímpar. Portanto, $f_{\delta_i}(x)$ não é auto-recíproco Isto prova o resultado para o caso $1\le m\le s$. Além disso, se $m>s$, fazendo $z=x^{p^{\varepsilon-s}}$, concluímos que $f_{\delta_i}(x)$ não é auto-recíproco. ■

Teorema 5.2.1. *Considerando os idempotentes primitivos determinados no Teorema 4.2.1, então a involução adjunta de cada um desses elementos é:*

1. *se $1\le\delta\le n$ e $1\le i\le\dfrac{\phi(p^\delta)}{t}$, então*

$$\widehat{E_{0;0}}=E_{0;0}\quad e\quad \widehat{E_{0;\delta,i}}=E_{0;\delta,\hat{i}},$$

em que cada $E_{0;\delta,i}$ corresponde a $f_{\delta,i}(y)$ e cada $E_{0;\delta,\hat{i}}$ corresponde a $f_{\delta,\hat{i}}(y)=f^*_{\delta,i}(y)$;

2. *se $1\le\delta\le m$, $1\le i\le\dfrac{\phi(p^\delta)}{t}$ e $0\le k\le p^n-1$, então*

$$\widehat{E_{\delta,i;k}}=E_{\delta,\hat{i};k},$$

em que cada $E_{\delta,i;k}$ corresponde a $f_{\delta,i}(x)$ e cada $E_{\delta,\hat{i};k}$ corresponde a $f_{\delta,\hat{i}}(y)=f^*_{\delta,i}(y)$.

Além disso, se t é par, existem $1+\dfrac{p^{m+n}-1}{t}$ idempotentes primitivos auto-adjuntos; se t é ímpar, existe apenas um idempotente primitivo auto-adjunto.

Demonstração. No Teorema 4.2.1, é fácil verificar que

1. se $1 \leq \delta \leq n$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, então

$$\begin{aligned}
\widehat{E_{0;0}} &= \frac{1}{p^{m+n}} \sum_{u=0}^{p^m-1} \sum_{v=0}^{p^n-1} x^{-u} y^{-v} = E_{0;0};\\
\widehat{E_{0;\delta,i}} &= \frac{1}{p^{m+n}} \frac{y^{-p^n}-1}{y^{-p^\delta}-1} \sum_{u=0}^{p^m-1} x^{-u} \sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v}) y^{-v}\\
&= \frac{1}{p^{m+n}} \frac{y^{p^n}-1}{y^{p^\delta}-1} \sum_{u=0}^{p^m-1} x^{u} \sum_{v=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i v}) y^{p^\delta-v}\\
&= E_{0;\delta,\hat{i}},
\end{aligned}$$

em que cada $E_{0;\delta,i}$ corresponde a $f_{\delta,i}(y)$ e cada $E_{0;\delta,\hat{i}}$ corresponde a $f_{\delta,\hat{i}}(y) = f^*_{\delta,i}(y)$;

2. se $1 \leq \delta \leq m$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ e $0 \leq k \leq p^n - 1$, então

$$\begin{aligned}
\widehat{E_{\delta,i;k}} &= \frac{1}{p^{m+n}} \frac{x^{-p^m}-1}{x^{-p^\delta}-1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^{-u} \sum_{v=0}^{p^n-1} y^{-v} g_{\delta,i}(x^{-1})^{-kv}\\
&= \frac{1}{p^{m+n}} \frac{x^{p^m}-1}{x^{p^\delta}-1} \sum_{v=0}^{p^n-1} y^{v} g_{\delta,i}(x^{-1})^{kv} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^{p^\delta-u}\\
&= E_{\delta,\hat{i};k},
\end{aligned}$$

em que cada $E_{\delta,i;k}$ corresponde a $f_{\delta,i}(x)$ e cada $E_{\delta,\hat{i};k}$ corresponde a $f_{\delta,\hat{i}}(y) = f^*_{\delta,i}(y)$.

Se t for par, pelo Lema 4.1.4, cada $E_{0;\delta,\hat{i}} = E_{0;\delta,i}$ e cada $E_{\delta,\hat{i};k} = E_{\delta,i;k}$, portanto existem $1 + \dfrac{p^{m+n}-1}{t}$ idempotentes primitivos auto-adjuntos; se t for ímpar, pelo Lema 5.2.2, existe um idempotente primitivo auto-adjunto $E_{0;0}$. ■

Corolário 5.2.1. *Sob as mesmas hipóteses do Teorema 5.2.1, se t for par, então existem $2^{1+\frac{p^{m+n}-1}{t}}$ códigos abelianos LCD em $\mathbb{F}_q(G)$ e não há códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$; se t for ímpar, então existem $2^{\frac{p^{m+n}-1}{2t}+1}$ códigos abelianos LCD e $3^{\frac{p^{m+n}-1}{2t}}$ códigos abelianos auto-ortogonais de $\mathbb{F}_q(G)$.*

Demonstração. Desde que $\mathbb{F}_q(G)$ é semissimples, cada idempotente E de $\mathbb{F}_q(G)$ é uma soma finita de idempotentes primitivos dados no Teorema 5.2.1. Daí, para todo $E \in \mathbb{F}_q G$, existem $\kappa_{0;0}$, $\kappa_{0;\delta,i}$ e $\kappa_{\delta,i;k}$, para $1 \leq \delta \leq n$, $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, tais que

$$E = \kappa_{0;0} E_{0;0} + \kappa_{0;\delta,i} \widehat{E_{0;\delta,i}} + \kappa_{\delta,i;k} \widehat{E_{\delta,i;k}}.$$

Como $E^2 = E$, então

$$E^2 = E \iff (\kappa_{0;0} E_{0;0} + \kappa_{0;\delta,i} E_{0;\delta,\hat{i}} + \kappa_{\delta,i;k} E_{\delta,\hat{i};k})^2 = \kappa_{0;0} E_{0;0} + \kappa_{0;\delta,i} E_{0;\delta,\hat{i}} + \kappa_{\delta,i;k} E_{\delta,\hat{i};k}$$

$$\begin{aligned}
&\iff \kappa_{0;0}^2 E_{0;0} + \kappa_{0;\delta,i}^2 E_{0;\delta,\hat{\imath}} + \kappa_{\delta,i;k}^2 E_{\delta,\hat{\imath};k} = \kappa_{0;0} E_{0;0} + \kappa_{0;\delta,i} E_{0;\delta,\hat{\imath}} + \kappa_{\delta,i;k} E_{\delta,\hat{\imath};k} \\
&\iff (\kappa_{0;0}^2 - \kappa_{0;0}) E_{0;0} + (\kappa_{0;\delta,i}^2 - \kappa_{0;\delta,i}) E_{0;\delta,\hat{\imath}} + (\kappa_{\delta,i;k}^2 - \kappa_{\delta,i;k}) E_{\delta,\hat{\imath};k} = 0 \\
&\iff \kappa_{0;0}(1-\kappa_{0;0}) = 0;\ \kappa_{0;\delta,i}(1-\kappa_{0;\delta,i}) = 0;\ \kappa_{\delta,i;k}(1-\kappa_{\delta,i;k}) = 0 \\
&\iff \kappa_{0;0} = 0 \text{ ou } 1;\ \kappa_{0;\delta,i} = 0 \text{ ou } 1;\ \kappa_{\delta,i;k} = 0 \text{ ou } 1,
\end{aligned}$$

para $1 \leq \delta \leq n$, $1 \leq \delta \leq m$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$. Logo, existem $2^{1+\frac{p^{m+n}-1}{t}}$ idempotentes em $\mathbb{F}_q G$.

Se t for par, então, pelo Teorema 5.2.1, todos os idempotentes primitivos E satisfazem $E^2 = E = \hat{E}$. De acordo com o Lema 5.2.1, não há códigos abelianos auto-ortogonais e existem $2^{1+\frac{p^{m+n}-1}{t}}$ códigos abelianos LCD de $\mathbb{F}_q(G)$.

Se t for ímpar, então, de acordo com o Teorema 5.2.1, existe ao menos um idempotente primitivo auto-adjunto em $\mathbb{F}_q G$, a saber, $E_{0;0}$. Pelo item (i) do Lema 5.2.1,

$$\begin{aligned}
E = \hat{E} &\iff \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{E_{0;\delta,i}} + \kappa_{\delta,i;k}\widehat{E_{\delta,i;k}} = \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{\widehat{E_{0;\delta,i}}} + \kappa_{\delta,i;k}\widehat{\widehat{E_{\delta,i;k}}} \\
&\iff \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{E_{0;\delta,i}} + \kappa_{\delta,i;k}\widehat{E_{\delta,i;k}} = \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}E_{0;\delta,i} + \kappa_{\delta,i;k}E_{\delta,i;k} \\
&\iff \kappa_{0;0}(E_{0;0} - E_{0;0}) + \kappa_{0;\delta,i}(\widehat{E_{0;\delta,i}} - E_{0;\delta,i}) + \kappa_{\delta,i;k}(\widehat{E_{\delta,i;k}} - E_{\delta,i;k}) = 0, \quad (5.4)
\end{aligned}$$

donde a igualdade (5.4) é verdadeira se, e somente se,

$$\begin{cases} E_{0;\delta,i} = \widehat{E_{0;\delta,i}}, & \text{se } \kappa_{0;\delta,i} = 1; \\ E_{\delta,i;k} = \widehat{E_{\delta,i;k}}, & \text{se } \kappa_{\delta,i;k} = 1. \end{cases} \quad \text{e} \quad \begin{cases} E_{0;\delta,i} \neq \widehat{E_{0;\delta,i}}, & \text{se } \kappa_{0;\delta,i} = 0; \\ E_{\delta,i;k} \neq \widehat{E_{\delta,i;k}}, & \text{se } \kappa_{\delta,i;k} = 0. \end{cases} \quad (5.5)$$

Agrupando em um conjunto $\mathcal{U}$ todos os idempotentes primitivos de $\mathbb{F}_q G$ que são diferentes de $E_{0;0}$, temos $\dfrac{p^{m+n}-1}{t}$ elementos em $\mathcal{U}$. Como toda involução adjunta de um idempotente primitivo é também um idempotente primitivo em $\mathbb{F}_q G$, então esses elementos aparecem em pares e podemos reagrupá-los em um conjunto $\mathcal{H} = \left\{ (E_j, \widehat{E_j}) : 1 \leq j \leq \dfrac{p^{m+n}-1}{2t} \right\}$. Assim, por (5.5),

$$E = \hat{E} \iff E = \kappa_0 E_{0;0} + \sum_{j \in I} \kappa_j (E_j + \widehat{E_j}), \quad (5.6)$$

com $I \subset \left\{1, \ldots, \dfrac{p^{m+n}-1}{2t}\right\}$, $\kappa_0, \kappa_j \in \{0,1\}$ e $\kappa_j = 0$, se $E_j \neq \widehat{E_j}$; $\kappa_j = 1$, se $E = \hat{E}$. Logo, pelo Lema 5.2.1, existem $2^{\frac{p^{m+n}-1}{2t}+1}$ códigos abelianos LCD.

Por outro lado, temos, pelo item (ii) do Lema 5.2.1,

$$\begin{aligned}
E\hat{E} = 0 &\iff (\kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{E_{0;\delta,i}} + \kappa_{\delta,i;k}\widehat{E_{\delta,i;k}})(\kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{\widehat{E_{0;\delta,i}}} + \kappa_{\delta,i;k}\widehat{\widehat{E_{\delta,i;k}}}) = 0 \\
&\iff \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}\widehat{E_{0;\delta,i}} + \kappa_{\delta,i;k}\widehat{E_{\delta,i;k}} = \kappa_{0;0}E_{0;0} + \kappa_{0;\delta,i}E_{0;\delta,i} + \kappa_{\delta,i;k}E_{\delta,i;k} = 0
\end{aligned}$$

$$
\begin{aligned}
\iff\ & \kappa_{0;0}E_{0;0}(\kappa_{0;0}E_{0;0}+\kappa_{0;\delta,i}E_{0;\delta,i}+\kappa_{\delta,i;k}E_{\delta,i;k})+\\
& +\kappa_{0;\delta,i}\widehat{E_{0;\delta,i}}(\kappa_{0;0}E_{0;0}+\kappa_{0;\delta,i}E_{0;\delta,i}+\kappa_{\delta,i;k}E_{\delta,i;k})+\\
& +\kappa_{\delta,i;k}\widehat{E_{\delta,i;k}}(\kappa_{0;0}E_{0;0}+\kappa_{0;\delta,i}E_{0;\delta,i}+\kappa_{\delta,i;k}E_{\delta,i;k})=0\\
\iff\ & \kappa_{0;0}^2E_{0;0}+\kappa_{0;\delta,i}^2\widehat{E_{0;\delta,i}}E_{0;\delta,i}+\kappa_{0;\delta,i}\kappa_{\delta,i;k}\widehat{E_{0;\delta,i}}E_{\delta,i;k}+\kappa_{\delta,i;k}^2\widehat{E_{\delta,i;k}}E_{\delta,i;k}+\\
& +\kappa_{\delta,i;k}\kappa_{0;\delta,i}\widehat{E_{\delta,i;k}}E_{0;\delta,i}=0\\
\iff\ & \kappa_{0;0}^2E_{0;0}+\kappa_{0;\delta,i}\kappa_{\delta,i;k}\widehat{E_{0;\delta,i}}E_{\delta,i;k}+\kappa_{\delta,i;k}\kappa_{0;\delta,i}\widehat{E_{\delta,i;k}}E_{0;\delta,i}=0\\
\iff\ & \kappa_{0;0}=0;\ \text{e}\ \kappa_{0;\delta,i}\kappa_{\delta,i;k}=0\\
\iff\ & \begin{cases}\kappa_{0;\delta,i}=0 & \text{e}\ \ \kappa_{\delta,i;k}=0;\\ \kappa_{0;\delta,i}=0 & \text{e}\ \ \kappa_{\delta,i;k}=1;\\ \kappa_{0;\delta,i}=1 & \text{e}\ \ \kappa_{\delta,i;k}=1.\end{cases}
\end{aligned}
\tag{5.7}
$$

Logo, por (5.7),

$$E\widehat{E}=0\iff\sum_{j\in I}\kappa_jE_j+\kappa_j'\widehat{E_j},\tag{5.8}$$

com $I\subset\left\{1,\ldots,\dfrac{p^{m+n}-1}{2t}\right\}$, $\kappa_j,\kappa_j'\in\{0,1\}$ e $\kappa_j+\kappa_j'\leq 1$. Portanto, pelo Lema 5.2.1, existem $3^{\frac{p^{m+n}-1}{2t}}$ códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$. ■

Teorema 5.2.2. *Considerando os idempotentes primitivos determinados no Teorema 4.2.2, então a involução adjunta de cada um desses elementos é:*

1. *se* $1\leq\delta\leq n$ *e* $1\leq i\leq\dfrac{\phi(p^\delta)}{t}$, *então*

$$\widehat{E_{0;0}}=E_{0;0}\ \text{e}\ \widehat{E_{0;\delta,i}}=E_{0;\delta,\hat{i}},$$

em que cada $E_{0;\delta,i}$ *corresponde a* $f_{\delta,i}(y)$ *e cada* $E_{0;\delta,\hat{i}}$ *corresponde a* $f_{\delta,\hat{i}}(y)=f_{\delta,i}^*(y)$;

2. *se* $1\leq\delta\leq s$, $1\leq i\leq\dfrac{\phi(p^\delta)}{t}$ *e* $0\leq k\leq p^n-1$, *então*

$$\widehat{E_{\delta,i;k}}=E_{\delta,\hat{i};k},$$

em que cada $E_{\delta,i;k}$ *corresponde a* $f_{\delta,i}(x)$ *e cada* $E_{\delta,\hat{i};k}$ *corresponde a* $f_{\delta,\hat{i}}(x)=f_{\delta,i}^*(x)$;

3. *se* $s+1\leq\varepsilon\leq m$, $1\leq i\leq\dfrac{\phi(p^s)}{t}$ *e* $0\leq k\leq p^n-1$, *então*

$$\widehat{E_{\varepsilon,i;k}}=E_{\varepsilon,\hat{i};k},$$

em que cada $E_{\varepsilon,i;k}$ *corresponde a* $f_{\varepsilon,i}(x)$ *e cada* $E_{\varepsilon,\hat{i};k}$ *corresponde a* $f_{\varepsilon,\hat{i}}(x)=f_{\varepsilon,i}^*(x)$.

Além disso, se t *for par, existem* $1+N_1$ *idempotentes primitivos auto-adjuntos; se* t *for ímpar, então existe um idempotente primitivo auto-adjunto.*

Demonstração. Os casos 1 e 2 estão provados no Teorema 5.2.1. Se $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$ e $\leq k \leq p^n - 1$, então

$$\begin{aligned}\widehat{E_{\varepsilon,i;k}} &= \frac{1}{p^{m+n+s-\varepsilon}} \frac{x^{-p^m}-1}{x^{-p^\delta}-1} \sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{-p^{\varepsilon-s}u} \sum_{v=0}^{p^n-1} g_{\delta,i}(x^{-1})^{-kv} y^{-v} \\ &= \frac{1}{p^{m+n+s-\varepsilon}} \frac{x^{p^m}-1}{x^{p^\delta}-1} \sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{p^{\varepsilon-s}(p^s-u)} \sum_{v=0}^{p^n-1} g_{\delta,i}(x^{-1})^{kv} y^{v} \\ &= E_{\varepsilon,\hat{i};k}.\end{aligned}$$

Pelo Lema 4.1.4, se t for par, existem $1+N_1$ idempotentes primitivos auto-adjuntos; se t for ímpar, então existe um único idempotente primitivo auto-adjunto. ■

Optamos por omitir as provas do Corolários 5.2.2 e 5.2.3 a seguir, uma vez que são análogas à prova do Corolário 5.2.1.

Corolário 5.2.2. *Sob as mesmas hipóteses do Teorema 5.2.2, se t for par, então existem 2^{1+N_1} códigos abelianos LCD em $\mathbb{F}_q(G)$ e não há códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$; se t for ímpar, então existem $2^{1+\frac{N_1}{2}}$ códigos abelianos LCD e $3^{\frac{N_1}{2}}$ códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$.*

Teorema 5.2.3. *Considerando os idempotentes primitivos determinados no Teorema 4.2.3, então a involução adjunta de cada um desses elementos é:*

1. *se $1 \leq \delta \leq s$ e $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, então*

$$\widehat{E_{0;0}} = E_{0;0}, \ \widehat{E_{0;\delta,i}} = E_{0;\delta,\hat{i}},$$

em que cada $E_{0;\delta,i}$ corresponde a $f_{\delta,i}(y)$ e cada $E_{0;\delta,\hat{i}}$ corresponde a $f_{\delta,\hat{i}}(y) = f^*_{\delta,i}(y)$. Além disso, se $s+1 \leq \lambda \leq n$ e $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, então

$$\widehat{E_{0;\lambda,i}} = E_{0;\lambda,\hat{i}},$$

em que cada $E_{0;\lambda,i}$ corresponde a $f_{\lambda,i}(y)$ e cada $E_{0;\lambda,\hat{i}}$ corresponde a $f_{\lambda,\hat{i}}(y) = f^*_{\lambda,i}(y)$;

2. *se $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ e $0 \leq k \leq p^\delta - 1$, então*

$$\widehat{E_{\delta,i;k}} = E_{\delta,\hat{i};k},$$

em que cada $E_{\delta,i;k}$ corresponde a $f_{\delta,i}(x)$ e cada $E_{\delta,\hat{i};k}$ corresponde a $f_{\delta,\hat{i}}(x) = f^*_{\delta,i}(x)$;

3. *se $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, $s+1 \leq \lambda \leq n$ e $1 \leq r \leq p^s - 1$, com $p \nmid r$, então*

$$\widehat{E_{\delta,i;\lambda,r}} = E_{\delta,\hat{i};\lambda,r},$$

4. se $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$ *e* $0 \leq k \leq p^\varepsilon - 1$, *então*

$$\widehat{E_{\varepsilon,i;k}} = E_{\varepsilon,\hat{i};k},$$

em que cada $E_{\varepsilon,i;k}$ *corresponde a* $f_{\varepsilon,i}(x)$ *e cada* $E_{\varepsilon,\hat{i};k}$ *corresponde a* $f_{\varepsilon,\hat{i}}(x) = f^*_{\varepsilon,i}(x)$;

5. se $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, $\varepsilon+1 \leq \lambda \leq n$ *e* $1 \leq r \leq p^\varepsilon - 1$, *com* $p \nmid r$, *então*

$$\widehat{E_{\varepsilon,i;\lambda,r}} = E_{\varepsilon,\hat{i};\lambda,r},$$

em que cada $E_{\varepsilon,i;\lambda,r}$ *corresponde a* $f_{\varepsilon,i}(x)$ *e cada* $E_{\varepsilon,\hat{i};k}$ *corresponde a* $f_{\varepsilon,\hat{i}}(x) = f^*_{\varepsilon,i}(x)$.

Além disso, se t *for par, existem* $1 + N_2$ *idempotentes primitivos auto-adjuntos; se* t *for ímpar, então existe um idempotente primitivo auto-adjunto.*

Demonstração. O caso 1 está provado no Teorema 5.2.2. Vamos provar os demais casos.

2. Se $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$ e $0 \leq k \leq p^\delta - 1$,

$$\begin{aligned}
\widehat{E_{\delta,i;k}} &= \frac{1}{p^{m+n}} \frac{x^{-p^m}-1}{x^{-p^\delta}-1} \frac{y^{-p^n}-1}{y^{-p^s}-1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^{-u} \sum_{v=0}^{p^s-1} g_{\delta,i}(x^{-1})^{-kv} y^{-v} \\
&= \frac{1}{p^{m+n}} \frac{x^{p^m}-1}{x^{p^\delta}-1} \frac{y^{p^n}-1}{y^{p^s}-1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{l_i u}) x^{p^\delta-u} \sum_{v=0}^{p^s-1} g_{\delta,i}(x^{-1})^{-kv} y^{p^s-v} \\
&= E_{\delta,\hat{i};k};
\end{aligned}$$

3. se $1 \leq \delta \leq s$, $1 \leq i \leq \dfrac{\phi(p^\delta)}{t}$, $s+1 \leq \lambda \leq n$ e $1 \leq r \leq p^s - 1$, com $p \nmid r$, então

$$\begin{aligned}
\widehat{E_{\delta,i;\lambda,r}} &= \frac{1}{p^{m+n+s-\lambda}} \frac{x^{-p^m}-1}{x^{-p^\delta}-1} \frac{y^{-p^n}-1}{y^{-p^\lambda}-1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^{-u} \sum_{v=0}^{p^s-1} g_{\delta,i}(x^{-1})^{-rv} y^{-p^{\lambda-s}v} \\
&= \frac{1}{p^{m+n+s-\lambda}} \frac{x^{p^m}-1}{x^{p^\delta}-1} \frac{y^{p^n}-1}{y^{p^\lambda}-1} \sum_{u=0}^{p^\delta-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\delta}^{-l_i u}) x^{p^\delta-u} \sum_{v=0}^{p^s-1} g_{\delta,i}(x^{-1})^{-rv} y^{p^{\lambda-s}(p^s-u)} \\
&= E_{\delta,\hat{i};\lambda,r};
\end{aligned}$$

4. se $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$ e $0 \leq k \leq p^\varepsilon - 1$, então

$$\begin{aligned}
\widehat{E_{\varepsilon,i;k}} &= \frac{1}{p^{m+n}} \frac{x^{-p^m}-1}{x^{-p^\varepsilon}-1} \frac{y^{-p^n}-1}{y^{-p^\delta}-1} \sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^i}^{-l_i u}) x^{-up^{\varepsilon-s}} \sum_{v=0}^{p^\varepsilon-1} x^{kv} y^{-v} \\
&= \frac{1}{p^{m+n}} \frac{x^{p^m}-1}{x^{p^\varepsilon}-1} \frac{y^{p^n}-1}{y^{p^\varepsilon}-1} \sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^i}^{-l_i u}) x^{p^{\varepsilon-s}(p^s-u)} \sum_{v=0}^{p^\varepsilon-1} x^{-kv} y^{p^\varepsilon-v} \\
&= E_{\varepsilon,\hat{i};k};
\end{aligned}$$

5. se $s+1 \leq \varepsilon \leq m$, $1 \leq i \leq \dfrac{\phi(p^s)}{t}$, $\varepsilon+1 \leq \lambda \leq n$ e $1 \leq r \leq p^\delta - 1$, com $p \nmid r$,

$$\begin{aligned}\widehat{E_{\varepsilon,i;\lambda,r}} &= \frac{1}{p^{m+n+\varepsilon-\lambda}} \frac{x^{-p^m}-1}{x^{-p^\varepsilon}-1} \frac{y^{-p^n}-1}{y^{-p^\lambda}-1} \sum_{u=0}^{p^\varepsilon-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^\varepsilon}^{-l_i u}) x^{-u} \sum_{v=0}^{p^\varepsilon-1} x^{rv} y^{-p^{\lambda-\varepsilon}v} \\ &= \frac{1}{p^{m+n+\varepsilon-\lambda}} \frac{x^{p^m}-1}{x^{p^\varepsilon}-1} \frac{y^{p^n}-1}{y^{p^\lambda}-1} \sum_{u=0}^{p^s-1} \mathrm{Tr}_{q^t/q}(\zeta_{p^s}^{-l_i u}) x^{p^{\varepsilon-s}(p^s-u)} \sum_{v=0}^{p^\varepsilon-1} x^{-rv} y^{p^{\lambda-\varepsilon}(p^\varepsilon-v)} \\ &= E_{\delta,\hat{i};\lambda,r}.\end{aligned}$$

Se t for par, pelo Lema 4.1.4, existem $1+N_2$ idempotentes primitivos auto-adjuntos; se t for ímpar, pelo Lema 5.2.2, então existe um idempotente primitivo auto-adjunto.

■

Corolário 5.2.3. *Sob as mesmas hipóteses do Teorema 5.2.3, se t for par, existem 2^{1+N_2} códigos abelianos LCD de $\mathbb{F}_q(G)$ e não há códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$; se t for ímpar, então existem $2^{1+\frac{N_2}{2}}$ códigos abelianos LCD e $3^{\frac{N_2}{2}}$ códigos abelianos auto-ortogonais em $\mathbb{F}_q(G)$.*

6 RESULTADOS E DISCUSSÕES

Primeiramente observamos que as hipóteses adotadas sobre a característica dos corpos e a ordem dos grupos em [8] e [15] são diferentes. Em [8], as hipóteses são mais restritivas e os resultados determinam que o número de componentes simples da álgebra de grupo $\mathbb{F}_qG$, com G um p-grupo abeliano finito, é o mesmo número de componentes simples da álgebra de grupo $\mathbb{Q}G$, em que $\mathbb{Q}$ é o corpo dos racionais. No entanto, sob essas hipóteses, é possível estabelecer uma relação dos idempotentes primitivos com alguns subgrupos do grupo G, o que permite utilizar a estrutura de grupo para determinação de alguns parâmetros dos códigos minimais correspondentes a esses idempotentes primitivos.

Em [15], as hipóteses são mais gerais e o número de idempotentes primitivos, logo, de componentes simples, é maior ou igual do que no caso $\mathbb{Q}G$, porém, não é possível estabelecer uma correspondência dos idempotentes primitivos com os subgrupos do grupo subjacentes à álgebra de grupo.

Os códigos gerados pelos idempotentes primitivos de $\mathbb{F}_qG$, calculados utilizando a teoria de grupos, foram classificados por meio de um critério de equivalência de códigos a menos de G-isomorfismos, conforme [8]. Já os idempotentes primitivos de $\mathbb{F}_qG$, calculados utilizando resultados da teoria de corpos finitos, foram completamente determinados em [15]. Entretanto, os códigos gerados por esses elementos não foram classificados por nenhum critério de equivalência em [15].

Além disso, percebemos, pela própria definição dos códigos abelianos LCD e auto-ortogonais abelianos, que a quantidade desses códigos está relacionada à quantidade de idempotentes primitivos da álgebra de grupo que consideramos. Por essa razão, é claro que se tivermos mais idempotentes primitivos, teremos mais códigos LCD e auto-ortogonais abelianos. Isto nos leva a pensar que a quantidade de códigos desses dois tipos será minimal, se o número de idempotentes primitivos também for minimal.

Uma questão levantada neste trabalho, que pode ser explorada futuramente, é a de qual critério de equivalência permite classificar os códigos encontrados em [15], visto que, nesse artigo, existem códigos que foram construídos sobre álgebras de grupo que não satisfazem as hipóteses do Teorema 4.2.5 e, portanto, não podem ser classificados a menos de G-equivalência.

REFERÊNCIAS

[1] BASTOS, G. T. **Comparação de técnicas para o cálculo de idempotentes geradores de códigos abelianos**. 2013. Dissertação de Mestrado. Universidade Federal de Viçosa.

[2] BERMAN, S. D. Semisimple cyclic and Abelian codes. II. **Cybernetics**, v. 3, n. 3, p. 17-23, 1967.

[3] BERMAN, S. D. On the theory of group codes. **Cybernetics**, v. 3, n. 1, p. 25-31, 1967.

[4] BERNAL, J. J.; DEL RÍO, Á.; SIMÓN, J. J.. An intrinsical description of group codes. **Designs, Codes and Cryptography**, v. 51, n. 3, p. 289-300, 2009.

[5] CHEN, B.; LIU, H.; ZHANG, G. A class of minimal cyclic codes over finite fields. **Designs, Codes and Cryptography**, v. 74, n. 2, p. 285-300, 2015.

[6] DE LA CRUZ, J.; WILLEMS, W. On group codes with complementary duals. **Designs, Codes and Cryptography**, v. 86, p. 2065-2073, 2018.

[7] FERRAZ, R. A. Simple components and central units in group algebras. **Journal of Algebra**, v. 279, n. 1, p. 191-203, 2004.

[8] FERRAZ, R. A.; GUERREIRO, M.; MILIES, C. P. G-Equivalence in Group Algebras and Minimal Abelian Codes. **IEEE Transactions on Information Theory**, v. 60, n. 1, p. 252-260, 2013.

[9] FERRAZ, R. A.; MILIES, C. P. Idempotents in group algebras and minimal abelian codes. **Finite Fields and Their Applications**, v. 13, n. 2, p. 382-393, 2007.

[10] GUERREIRO, M.; FERRAZ, R. A.; MILIES, C. P. Minimal codes in binary abelian group algebras. In: **2011 IEEE Information Theory Workshop**. IEEE, 2011. p. 225-228.

[11] GUERREIRO, M.; MILIES, C. P. Group algebras and coding theory. **São Paulo Journal of Mathematical Sciences**, v. 10, n. 2, p. 346-371, 2016.

[12] HEFEZ, A.; VILLELA, M. L. T. **Códigos corretores de erros**. Instituto de Matematica Pura e Aplicada, 2008.

[13] HUNGERFORD, T. W. **Algebra**. Springer Science & Business Media, 2012.

[14] LI, F.; YUE, Q. The primitive idempotents and weight distributions of irreducible constacyclic codes. **Designs, Codes and Cryptography**, v. 86, p. 771-784, 2018.

[15] LI, F.; YUE, Q.; WU, Y. LCD and Self-Orthogonal Group Codes in a Finite Abelian p-Group Algebra. **IEEE Transactions on Information Theory**, v. 66, n. 5, p. 2717-2728, 2019.

[16] LIDL, R.; NIEDERREITER, H. **Finite fields**. Cambridge university press, 1997.

[17] LUCHETTA, V. O. J. **Códigos cíclicos como ideais em álgebras de grupos**. 2005. Dissertação de Mestrado. Universidade de São Paulo.

[18] MACWILLIAMS, F. J.; SLOANE, N. J. A. **The theory of error-correcting codes**. Elsevier, 1977.

[19] MACWILLIAMS, M. F. J. Binary codes which are ideals in the group algebra of an abelian group. **Bell System Technical Journal**, v. 49, n. 6, p. 987-1011, 1970.

[20] MILIES, C. P. **Anéis e módulos**. 1972.

[21] MILIES, C. P.; SEHGAL, S. K. **An introduction to group rings**. Springer Science & Business Media, 2002.

[22] MILLER, R. L. Minimal codes in abelian group algebras. **Journal of Combinatorial Theory**, Series A, v. 26, n. 2, p. 166-178, 1979.

[23] PETRILLO, J. Counting subgroups in a direct product of finite cyclic groups. **The College Mathematics Journal**, v. 42, n. 3, p. 215-222, 2011.

[24] ROTMAN, J. J. **An introduction to the theory of groups**. Springer-Verlag, 1995.