MARCOS HENRIQUE FRANCO COSTA

Existência de elementos primitivos k-normais em corpos finitos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
2026

MARCOS HENRIQUE FRANCO COSTA

Existência de elementos primitivos k-normais em corpos finitos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica

Orientador: Prof. Dr. Josimar Joao Ramirez Aguirre.

UBERLÂNDIA - MG
2026

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

C837 Costa, Marcos Henrique Franco, 1993-
2026 Existência de elementos primitivos k-normais em Corpos Finitos [recurso eletrônico] / Marcos Henrique Franco Costa. - 2026.

Orientador: Josimar Joao Ramirez Aguirre.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2026.210
Inclui bibliografia.

1. Matemática. I. Aguirre, Josimar Joao Ramirez ,1989-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - pgmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 135, PPGMAT				
Data:	27/02/2026	Hora de início:	15:30	Hora de encerramento:	17:30
Matrícula do Discente:	12412MAT012				
Nome do Discente:	Marcos Henrique Franco Costa				
Título do Trabalho:	Existência de elementos primitivos k-normais em Corpos Finitos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Densidade de Elementos k-normais e completamente normais em Corpos Finitos				

Reuniu-se por videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Jean Carlos de Aguiar Lelis -Universidade de Brasília/UNB, Sávio Ribas - Universidade Federal de Ouro Preto/UFOP e Josimar Joao Ramirez Aguirre - IME/UFU orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Josimar Joao Ramirez Aguirre, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra para a exposição do seu trabalho.

A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do Programa. A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Josimar João Ramirez Aguirre**, **Professor(a) do Magistério Superior**, em 27/02/2026, às 17:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jean Carlos de Aguiar Lelis**, **Usuário Externo**, em 28/02/2026, às 08:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Sávio Ribas**, **Usuário Externo**, em 28/02/2026, às 11:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7084044** e o código CRC **99C13935**.

Referência: Processo nº 23117.010856/2026-29 SEI nº 7084044

Dedicatória

Dedico esta dissertação à minha família, amigos, e a todos que me apoiaram durante esta jornada.

Agradecimentos

Gostaria de expressar meus sinceros agradecimentos a todos que, de alguma forma, contribuíram para a conclusão de mais uma etapa acadêmica.

Agradeço a Deus pela oportunidade de obter uma formação tão importante na minha carreira, mesmo com todas as dificuldades enfrentadas ao me mudar para uma cidade muito distante da minha, sem bolsa de estudos, e conseguir chegar até aqui.

À minha família e amigos, agradeço o apoio à minha decisão de dar este passo na minha carreira, e todo o suporte que forneceram durante este período.

À todos meus colegas de mestrado, agradeço a disponibilidade e boa vontade ao me ajudar bastante em todas as disciplinas com seu conhecimento, quando tive dificuldades com os conteúdos, especialmente Carlos Daniel, José Armando e Mônica Madeira, sem os quais definitivamente eu não estaria aqui.

À todos os professoras com quem tive o prazer de conviver e trabalhar: Victor Neumann, Geraldo Botelho, Cícero Carvalho, Rosana Jafelice, Daniel Cariello e Rodolfo Collegari, agradeço o suporte e a compreensão de um caso atípico que enfrentamos a partir do segundo semestre, quando minha presença não foi possível em muitos dias letivos; e cada aprendizado nesta etapa que enriqueceu enormemente a minha bagagem.

E finalmente, ao meu orientador Josimar Aguirre, agradeço imensamente por sua dedicação, sua boa vontade ao precisar fazer reuniões de forma remota, e principalmente pela compreensão e apoio ao aceitar trabalhar com um mestrando que em uma situação como a minha: trabalhando durante toda a segunda metade do curso e à distância.

COSTA, M. H. F. *Existência de elementos primitivos k-normais em corpos finitos.* 2026. xi + 61 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Esta dissertação investiga as condições de existência de elementos que sejam simultaneamente primitivos e k-normais em extensões de corpos finitos. O estudo da existência de tais elementos é um problema central na Álgebra moderna, com implicações diretas na eficiência de sistemas criptográficos e na construção de códigos corretores de erros. Para abordar este problema, utilizamos uma fundamentação teórica que combina métodos combinatórios e analíticos. As principais ferramentas empregadas são a Função de Euler (ϕ) e a Função de Möbius (μ). No âmbito da Álgebra Linear sobre corpos finitos, exploramos as propriedades dos polinômios linearizados, que permitem caracterizar a independência linear dos conjugados de um elemento sob a ação dos automorfismos de Frobenius. Para a demonstração dos resultados principais, utilizamos ferramentas como caracteres aditivos e multiplicativos, um tipo particular de homomorfismos, integrando-os ao o estudo das somas de Gauss, que fornecem as estimativas para somas exponenciais necessárias para garantir que a quantidade de elementos desejados é estritamente positiva.

Palavras-chave: corpos finitos; elementos primitivos; elementos normais; elementos k-normais.

COSTA, M. H. F. *Existence of primitive k-normal elements in finite fields.* 2026. xi + 61 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

This dissertation investigates conditions for the existence of elements that are simultaneously primitive and k-normal in finite field extensions. The study of the existence of such elements is a central problem in modern Algebra, with direct implications on the efficiency of cryptographic systems and the construction of error-correcting codes. To approach this problem, we employ a theoretical framework that combines combinatorial and analytical methods. The primary tools utilized are the Euler totient function (ϕ) and the Möbius function (μ). Within the scope of Linear Algebra over finite fields, we explore the properties of linearized polynomials, which allow the characterization of the linear independence of an element's conjugates under the action of Frobenius automorphisms. To prove the main results, we use tools such as additive and multiplicative characters, a particular type of homomorphism, integrating them with the study of Gaussian sums, which provide the estimates for exponential sums needed to guarantee that the number of desired elements is strictly positive.

Keywords: finite fields; primitive elements; normal elements; k-normal elements.

Lista de Tabelas

1.1 Lista dos Elementos de $\mathbb{F}_{16}$ em Função de α. 11

3.1 Quantidade de elementos k-normais de $\mathbb{F}_{19^3}$ sobre $\mathbb{F}_{19}$. 52
3.2 Quantidade de elementos k-normais de $\mathbb{F}_{5^8}$ sobre $\mathbb{F}_5$. 52
3.3 Quantidade de elementos k-normais de $\mathbb{F}_{9^8}$ sobre $\mathbb{F}_9$. 52
3.4 Quantidade de elementos k-normais de $\mathbb{F}_{7^8}$ sobre $\mathbb{F}_7$. 52
3.5 Quantidade de elementos k-normais de $\mathbb{F}_{3^{16}}$ sobre $\mathbb{F}_3$. 52

4.1 Elementos k-normais e primitivos k-normais de $\mathbb{F}_{2^6}$ sobre $\mathbb{F}_2$. 58
4.2 Elementos k-normais e primitivos k-normais de $\mathbb{F}_{5^6}$ sobre $\mathbb{F}_5$. 58
4.3 Elementos k-normais e primitivos k-normais de $\mathbb{F}_{5^7}$ sobre $\mathbb{F}_5$. 59

Sumário

Resumo **viii**

Abstract **ix**

Lista de tabelas **x**

Introdução **1**

1 Estrutura dos Corpos Finitos **3**
1.1 Preliminares 3
1.2 Caracterização dos Corpos Finitos 8
1.3 Raízes de polinômios irredutíveis 13
1.4 Traço, Norma e Base 17

2 Ferramentas úteis em Corpos Finitos **27**
2.1 Polinômios linearizados 27
2.2 Caracteres 31
2.3 Soma de Gauss 34

3 Elementos especiais em Corpos Finitos **37**
3.1 Elementos m-livres 38
3.2 Elementos M-livres 41
3.3 Elementos k-normais 46

4 Elementos primitivos k-normais **53**
4.1 Condições para existência de elementos primitivos k-normais 53
4.2 Exemplos 58

Referências Bibliográficas **60**

Introdução

A teoria dos corpos finitos possui raízes que remontam aos séculos XVII e XVIII através da Teoria dos Números. O ponto de partida pode ser atribuído a Pierre de Fermat (1601-1665), cujo "Pequeno Teorema" estabeleceu as bases para entender a estrutura multiplicativa dos restos modulares. Posteriormente, Leonhard Euler (1707-1783) generalizou esses resultados através da função phi (ϕ), introduzindo a noção de ordens e índices que hoje são ferramentas essenciais para quantificar geradores em grupos cíclicos. Essa fundação aritmética foi a base para o surgimento das primeiras investigações sobre as propriedades de divisibilidade e resíduos que caracterizam os corpos de característica prima.

A transição da Aritmética para uma estrutura algébrica mais robusta ocorreu com o desenvolvimento da Teoria de Grupos e da Teoria de Anéis. Joseph-Louis Lagrange (1736-1813) demonstrou o teorema fundamental que relaciona a ordem de um subgrupo à ordem do grupo, um resultado que permite restringir os possíveis valores das ordens de elementos em extensões de corpos. Simultaneamente, Adrien-Marie Legendre (1752-1833) contribuiu com o estudo dos resíduos quadráticos e o símbolo que leva seu nome, fornecendo métodos para determinar a solubilidade de equações em domínios finitos.

O marco para a formalização da teoria ocorreu com Carl Friedrich Gauss (1777-1855) e Évariste Galois (1811-1832). Gauss, em sua obra *Disquisitiones Arithmeticae* [5], sistematizou a aritmética modular e provou a existência de raízes primitivas, o que equivale a demonstrar que o grupo multiplicativo de um corpo primo é cíclico. Contudo, foi Galois quem estendeu esses conceitos para além dos corpos de ordem prima, concebendo as extensões de corpos de ordem p^n. Ao introduzir o que hoje chamamos de Teoria de Galois, ele conectou a solubilidade de polinômios às propriedades estruturais de seus grupos de automorfismos, estabelecendo os fundamentos para o estudo das bases e da independência linear em corpos finitos.

Dentro desta estrutura, os elementos primitivos desempenham um papel protagonista. Um elemento é primitivo se for um gerador de um grupo cíclico. A importância desses elementos reside na sua capacidade de representar todos os elementos não nulos do corpo como potências de uma única base. A garantia da existência de tais elementos permitiu simplificar cálculos complexos, transformando a multiplicação em uma operação aditiva sobre os expoentes. Em termos teóricos, a busca por elementos primitivos com propriedades adicionais é um dos problemas mais persistentes e férteis da Álgebra moderna, exigindo estimativas refinadas de somas de caracteres.

Complementarmente, a teoria explora os elementos normais, que são fundamentais para o entendimento das extensões de corpos como espaços vetoriais. Um elemento é normal se gera um tipo específico de base do espaço vetorial (base normal), conceito que otimiza operações de potenciação, uma vez que, em tal base, elevar um elemento à q (ordem do corpo base) resulta em um simples deslocamento cíclico de suas coordenadas, propriedade que torna os elementos normais objetos de desejo tanto na Matemática quanto na Computação. Recentemente a literatura viu o surgimento e a expansão dos elementos k-normais, introduzidos por Huczynska et al. [10], que são uma generalização elegante da normalidade. Um elemento é k-normal se o subespaço gerado por seus conjugados possui dimensão igual a k sobre o corpo base. Essa definição permite uma classificação mais refinada dos elementos do corpo.

A motivação para o estudo desses elementos transcende a estética matemática, encontrando aplicação direta na Criptografia e na Teoria de Códigos. Na criptografia de chave pública, como nos protocolos baseados no Problema do Logaritmo Discreto [8], elementos primitivos garantem o maior período possível para geradores de sequências. Por outro lado, a estrutura de elementos normais e k-normais é explorada na Teoria de Códigos para a construção de códigos corretores de erros eficientes, onde a aritmética rápida em corpos finitos é essencial para o processamento de grandes volumes de dados em tempo real.

É importante salientar que, embora as aplicações referenciadas justifiquem o interesse contemporâneo pelo tema, esta dissertação vincula-se estritamente ao domínio da Matemática. Por conseguinte, tais aplicações não são detalhadas de forma explícita ao longo do texto, uma vez que o escopo do trabalho prioriza o desenvolvimento teórico e a demonstração de condições que garantem a existência de tais elementos.

Desta forma, esta dissertação propõe-se a investigar as condições de existência de elementos que sejam simultaneamente primitivos e k-normais em corpos finitos, resultado publicado originalmente por Reis [15]. Os Capítulos 1 e 2 são baseados no livro *Finite Fields* [12]. No Capítulo 1, apresentamos as preliminares básicas para o trabalho, além da estrutura fundamental dos corpos finitos. O Capítulo 2 é dedicado às ferramentas analíticas necessárias, como polinômios linearizados; um tipo particular de homomorfismos de grupos chamados de Caracteres; e somas exponenciais envolvendo as imagens destas aplicações, chamadas de Somas de Gauss. O Capítulo 3, baseado em [10], traz o conceito de *liberdade*, usado para definir e caracterizar os elementos m-livres e M-livres, que são fundamentais para objetivo final do trabalho, além de introduzir os elementos k-normais. Por fim, o Capítulo 4 consolida a pesquisa ao provar as condições teóricas estabelecidas em [15] para a existência de elementos que sejam simultaneamente primitivos e k-normais, apresentando exemplos numéricos que ilustram e validam os resultados obtidos.

Marcos Henrique Franco Costa
Uberlândia-MG, 27 de fevereiro de 2026.

Capítulo 1

Estrutura dos Corpos Finitos

Este capítulo inicial é fortemente baseado na obra *Finite Fields*, de Rudolf Lidl e Harald Niederreiter [12]. Na primeira seção, apresentamos rapidamente conceitos e propriedades básicas sobre estruturas algébricas que serão usados no restante do capítulo, e ao longo de toda a dissertação. A partir da Seção 1.2 apresentamos caracterizações e propriedades fundamentais de corpos finitos.

1.1 Preliminares

Definição 1.1.1. *(Grupo) Um conjunto G munido de uma operação binária $(\cdot)$ é chamado um* ***grupo*** *$(G, \cdot)$ se possui as seguintes propriedades:*

- *A operação $\cdot$ é associativa, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall a, b, c \in G$;*
- *G possui elemento identidade (ou unidade), isto é, $\exists e \in G \ / \ a \cdot e = a, \ \forall a \in G$;*
- *todo elemento de G possui um inverso, isto é, $\forall a \in G, \ \exists b \in G \ / \ a \cdot b = e$.*

Se $a \cdot b = b \cdot a \ \ \forall a, b \in G$, então G é um ***grupo abeliano****.*

O conjunto dos números inteiros é grupo sob a adição, denotado por $\mathbb{Z}$. Dado um número natural n, o conjunto $\{0, 1, 2, \ldots, n-1\}$ é grupo onde a operação é dada pelo resto da soma de dois elementos a e b deste grupo por n. Além disso, dizemos que a é *congruente* a b módulo n se $a-b$ é um múltiplo de n, e escrevemos $a \equiv b \pmod{n}$.

Definição 1.1.2. *(Ordem de um grupo) O número de elementos de um grupo finito G é chamado de* ***ordem*** *do grupo G, e é denotado por $|G|$.*

Definição 1.1.3. *(Ordem de um elemento) Seja G um grupo munido com a multiplicação. A* ***ordem*** *de um elemento $g \in G$ é o menor inteiro positivo n tal que $g^n = 1$, e escrevemos $|g| = n$.*

Definição 1.1.4. *(Grupo cíclico) Um grupo G sob a multiplicação é um* ***grupo cíclico*** *se existe um elemento $a \in G$ tal que todo elemento de G é uma potência de a, isto é, $\forall b \in G,\ \exists j \in \mathbb{Z}\ /\ b = a^j$. Neste caso, podemos escrever $G = \langle a \rangle$. Além disso, a é um* ***gerador*** *de G, e a ordem do elemento a é igual à ordem de G, ou seja $|G| = |a|$.*

Definição 1.1.5. *(Subgrupo) Um subconjunto H de G é um* ***subgrupo*** *de G se H por si só é um grupo com a mesma operação de G.*

Definição 1.1.6. *(Subgrupo normal) O subgrupo H do grupo G é chamado de* ***subgrupo normal*** *de G se $aha^{-1} \in H,\ \forall a \in G,\ h \in H$.*

Teorema 1.1.7. *[12, Teorema 1.15] Seja G um grupo de ordem m.*

(i) Se $G = \langle a \rangle$ é cíclico, o elemento a^k gera um subgrupo de ordem $\frac{m}{mdc(k,m)}$.

(ii) Se s divide m, G possui $\phi(s)$ elementos de ordem s, onde ϕ é a Função phi de Euler, e $\phi(s)$ indica o número de inteiros j tais que $1 \leq j \leq s$ e $mdc(s, j) = 1$.

(iii) Se $G = \langle a \rangle$ é cíclico, G possui $\phi(m)$ geradores, isto é, elementos a^r tais que $\langle a^r \rangle = \langle a \rangle$, e $mdc(r, m) = 1$.

Quando comparamos a estrtura de dois grupos, aplicações entre grupos que preservam suas operações são de grande importância. Este conceito é formalizado na definição a seguir.

Definição 1.1.8. *(Homomorfismo) Uma aplicação $f\colon G \to H$ do grupo $(G, *)$ no grupo $(H, \cdot)$ é um* ***homomorfismo*** *de grupos se preserva a operação de G, isto é, $f(a * b) = f(a) \cdot f(b),\ \forall a, b \in G$. Além disso, se f é bijetora, f é chamada de* ***isomorfismo****. Um isomorfismo de G em G é chamado de* ***automorfismo****.*

Definição 1.1.9. *(Kernel) Dado um homomorfismo $f\colon G \to H$, o kernel (ou núcleo) de f é o conjunto $ker(f) = \{a \in G\ /\ f(a) = e'\}$, onde e' é o elemento identidade em H.*

Definição 1.1.10. *(Classe lateral) Seja H um subgrupo de G. Para um elemento $g \in G$, o conjunto $gH = \{gh\ /\ h \in H\}$ é chamado de* ***classe lateral*** *à esquerda de G módulo H, e o conjunto $Hg = \{hg\ /\ h \in H\}$ é chamado de classe lateral à direita de G módulo H. Se G é um grupo abeliano, a distinção entre classes laterais à esquerda e à direita módulo H torna-se desnecessária.*

Definição 1.1.11. *(Grupo quociente) Para um subgrupo normal H de G, o grupo formado pelas classes laterais de G módulo H é chamado de* ***grupo quociente*** *de G módulo H e é denotado por G/H.*

Teorema 1.1.12. *[12, Teorema 1.23] (Teorema do Homomorfismo). Seja a função $f\colon G \to f(G) = G_1$ um homomorfismo de grupos sobrejetor. Então $ker(f)$ é um subgrupo normal de G, e G_1 é isomorfo a $G/ker(f)$. Reciprocamente, se H é qualquer subgrupo normal de G, então a aplicação $\psi\colon G \to G/H$ definida por $\psi(a) = aH$ com $a \in G$ é um homomorfismo de G sobre G/H com $ker(\psi) = H$.*

Como vimos, grupos são estruturas algébricas munidas de uma operação. No entanto, se fornecemos a estas estruturas uma operação a mais satisfazendo certas propriedades, podemos ter uma estrutura algébrica mais complexa, definida a seguir.

Definição 1.1.13. *(Anel) Um conjunto A munido de duas operações binárias $(+)$ e $(\cdot)$ é chamado um* ***anel*** *$(A, +, \cdot)$ se possui as seguintes propriedades:*

- *A é um grupo abeliano com respeito a operação $+$;*
- *A operação $\cdot$ é associativa, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c,\ \forall a, b, c \in A$;*
- *A preserva a distributividade, isto é, $a \cdot (b + c) = a \cdot b + a \cdot c$, e $(b + c) \cdot a = b \cdot a + c \cdot a,\ \forall a, b, c \in A$.*

Definição 1.1.14. *Seja $(A, +, \cdot)$ um anel.*

(i) *A é um* ***anel com identidade*** *se possui identidade multiplicativa, isto é, $\exists e \in A\ /\ a \cdot e = e \cdot a = a,\ \forall a \in A$.*

(ii) *A é um* ***anel comutativo*** *se $\cdot$ é comutativa.*

(iii) *A é um* ***domínio de integridade*** *se for um anel comutativo, com $e \neq 0$, onde $a \cdot b = 0$ implica $a = 0$ ou $b = 0$.*

(iv) *A é um* ***anel de divisão*** *se A^* é um grupo com a operação $(\cdot)$.*

(v) *A é um* ***corpo*** *se for um anel comutativo de divisão.*

Definição 1.1.15. *(Ideal) Seja I um subconjunto do anel $(A, +, \cdot)$. I é um* ***ideal*** *se*

- *$(I, +, \cdot)$ é um anel;*
- *I é fechado para as operações $+$ e $\cdot$;*
- *$a \cdot b \in I,\ \forall a, b \in I$.*

Se $\exists j \in I$ tal que $I = \langle j \rangle$, então I é um ***ideal principal****.*

Teorema 1.1.16. *[12, Teorema 1.38] O anel quociente $\mathbb{Z}/\langle p\rangle$, onde p é um número primo, é um corpo.*

Definição 1.1.17. *(Corpo de Galois) Sejam $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, com p primo, $\psi\colon \mathbb{Z}/\langle p\rangle \to \mathbb{F}_p$ uma aplicação definida por $\psi([a]) = a$. O conjunto $\mathbb{F}_p$ munido com a estrutura de corpo induzida por ψ, é um corpo finito, chamado de* ***Corpo de Galois*** *de ordem p.*

Os corpos de Galois é a base do nosso ambiente de trabalho, onde esta pesquisa se desenvolve. Vejamos, agora, propriedades importantes relacionadas aos corpos.

Definição 1.1.18. *(Característica) Dado um anel A, se existe $n \in \mathbb{N}$ tal que $na = 0$ para todo $a \in A$, o menor n com tal propriedade é a* ***característica*** *do anel A.*

Teorema 1.1.19. *[12, Teorema 1.46] Seja A um anel comutativo de característica prima p. Então, para todo $a, b \in A, n \in \mathbb{N}$, temos*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad e \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

Definição 1.1.20. *(Corpo primo) Um corpo F que não contém nenhum subcorpo próprio (subconjunto próprio de F que é um corpo por si só com as operações de F) é chamado de* ***corpo primo****.*

Teorema 1.1.21. *[12, Teorema 1.78] O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou $\mathbb{Q}$, caso sua característica seja, respectivamente, um primo p ou 0.*

Definição 1.1.22. *(Extensão de corpos) Sejam K um subcorpo de F, e M um subconjunto qualquer de F. A interseção de todos subcorpos de F que contém K e M é chamada de* ***extensão*** *do corpo K obtida ao adjuntar o conjunto M, e denotada por $K(M)$. Se M contém apenas 1 elemento θ, então $K(\theta)$ é uma* ***extensão simples*** *de K, e θ é um* ***elemento definidor*** *de $K(\theta)$ sobre K.*

Definição 1.1.23. *(Extensão algébrica) Sejam K um subcorpo de F, $\theta \in F$. Se θ é raiz de um polinômio não nulo com coeficientes em K, θ é um* ***elemento algébrico*** *sobre K. Para uma extensão L de K, se todo elemento de L é algébrico sobre K, então $L|K$ é uma* ***extensão algébrica****.*

Definição 1.1.24. *(Polinômio minimal) Seja $F|K$ uma extensão de corpos. Se $\theta \in F$ é algébrico sobre K, então o polinômio mônico único que gera o ideal $\{f \in K[X] \ / \ f(\theta) = 0\}$ é chamado de* ***polinômio minimal*** *de θ sobre K. Dizemos que o grau de θ é o grau do seu polinômio minimal.*

Teorema 1.1.25. *[12, Teorema 1.82] Sejam F uma extensão do corpo K, $f \in K[X]$. Se $\theta \in F$ é algébrico sobre K, então o polinômio minimal de θ sobre K é irredutível sobre K.*

Definição 1.1.26. *(Grau da extensão) Seja F uma extensão do corpo K. Se F é um corpo finito, a dimensão de F como espaço vetorial sobre K é chamada de* ***grau*** *de F sobre K, e denotada por $[F : K]$.*

Teorema 1.1.27. *[12, Teorema 1.84] Sejam F uma extensão finita do corpo K e L uma extensão finita de F. Então $[L : K] = [L : F][F : K]$.*

Teorema 1.1.28. *[12, Teorema 1.85] Toda extensão finita de um corpo K é algébrica sobre K.*

Teorema 1.1.29. *[12, Teorema 1.86] Sejam $F|K$ uma extensão de corpos e $\theta \in F$ um elemento algébrico sobre K de grau n. Então $[K(\theta) : K] = n$ e $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K.*

Os resultados e propriedades acima mostram que toda extensão de corpos finitos é gerada a partir de uma raiz de um polinômio irredutível sobre o corpo base. Agora, o objetivo é encontrar uma extensão que possua todas as raízes de tal polinômio, que leva à definição e ao teorema seguintes, fundamentais para a Teoria de Corpos.

Definição 1.1.30. *(Corpo de decomposição) Dados $f \in K[X]$ de grau n e F uma extensão do corpo K, dizemos que f se decompõe em F se f pode ser escrito como produto de fatores lineares de $F[X]$, isto é, se existem $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tais que*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

onde a é o coeficiente líder de f. Neste caso F é chamado de ***corpo de decomposição*** *de f sobre K se podemos escrever $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Teorema 1.1.31. *[12, Teorema 1.91] (Teorema da Existência e Unicidade dos Corpos de Decomposição) Se K é um corpo e $f \in K[X]$ é um polinômio de grau positivo, então existe um corpo de decomposição de f sobre K. Quaisquer corpos de decomposição de f sobre K são isomorfos um ao outro, onde este isomorfismo mantém os elementos de K fixos e leva as raízes de f umas nas outras.*

1.2 Caracterização dos Corpos Finitos

Pelo Teorema 1.1.16 e Definição 1.1.17, sabemos que para todo p primo, existe o *Corpo de Galois* $\mathbb{F}_p$ de ordem p, que consiste no anel quociente $\mathbb{Z}/\langle p\rangle$. Este é o exemplo mais comum de corpo finito, mas algumas de suas propriedades se extendem para corpos finitos arbitrários, como veremos a seguir.

A característica de um corpo é sempre igual a característica de seu subcorpo primo. Portanto, os Corpos de Galois tem um papel importante na Teoria de Corpos, pois todo corpo de característica p, com p primo, é isomorfo a $\mathbb{F}_p$ (Teorema 1.1.21), e todo corpo finito pode ser visto como uma extensão de $\mathbb{F}_p$ para algum p, como veremos nesta seção.

Apresentamos agora importantes propriedades relacionadas à existência e construção de corpos finitos. Vejamos uma condição necessária para estabelecermos o número de elementos de um corpo finito.

Lema 1.2.1. *Seja F um corpo finito, K um subcorpo de F com q elementos. Então F tem q^n elementos, onde $n = [F : K]$.*

Demonstração. Como F é um corpo finito, é um espaço vetorial de dimensão finita sobre K. Então, F é uma extensão finita de K, de grau n (por hipótese), e assim, por definição, F tem uma base de n elementos sobre K, ou seja, um conjunto de n elementos que gera todo o corpo F. Isto significa que qualquer elemento de F pode ser escrito como uma combinação linear de elementos dessa base com coeficientes em K. Seja essa base o conjunto $\{b_1, b_2, ..., b_n\}$. Dado $d \in F$, $d = a_1b_1 + a_2b_2 + \cdots + a_nb_n$ com $a_1, a_2, ..., a_n \in K$. Como K tem q elementos, existem q possibilidades de valor para cada $a_i, 1 \leq i \leq n$, e assim, q^n possibilidades de valor para d. Como d é um elemento arbitrário de F, F possui q^n elementos.

□

Teorema 1.2.2. *Sejam F um corpo finito de característica p e n o grau da extensão de F sobre seu subcorpo primo. Então F tem p^n elementos.*

Demonstração. Seja P subcorpo primo de F, isto é, a interseção de todos os subcorpos de F. Então P é isomorfo a $\mathbb{F}_p$, pois F tem característica p (Teorema 1.1.21). Portanto, como $n = [F : P]$, pelo lema anterior F tem p^n elementos.

□

A partir dos corpos $\mathbb{F}_p$ podemos construir outros corpos finitos através do processo de adjuntar raízes. Se $f \in \mathbb{F}_p[X]$ é um polinômio de grau n irredutível sobre $\mathbb{F}_p$, então, ao adjuntar uma raiz de f a $\mathbb{F}_p$, obtemos um corpo finito com p^n elementos. Entretanto, até este ponto ainda não é claro que para todo n positivo inteiro existe um polinômio de grau n irredutível sobre $\mathbb{F}_p$. Para estabelecer a existência de um corpo finito com p^n elementos para todo p primo e n positivo inteiro, usamos dois resultados a seguir.

Lema 1.2.3. *Se F é um corpo finito com q elementos, então $a^q = a,\ \forall a \in F$.*

Demonstração. Se $a = 0$, então $a^q = 0^q = 0 = a$. Já os elementos não nulos de F formam um grupo multiplicativo de ordem $q-1$, pois herdam de F o fechamento e a associatividade da multiplicação, o elemento neutro, e o inverso de todos os elementos. Pelo Teorema 1.1.7, a ordem de todo elemento $a \in F^*$ divide a ordem do grupo, ou seja, se $a^n = 1$ então $n|(q-1)$, e assim temos que $a^{q-1} = 1,\ \forall a \in F^*$. Logo, $a^q = a^{q-1} \cdot a = 1 \cdot a = a,\ \forall a \in F^*$.

□

Lema 1.2.4. *Se F é um corpo finito com q elementos e K é subcorpo de F, então $x^q - x \in K[X]$ se fatora em $F[X]$ como $\prod_{a \in F}(x-a)$ e F é corpo de decomposição de $x^q - x$ sobre K.*

Demonstração. Seja $f(x) = x^q - x$. Como $\deg(f) = q$, f tem no máximo q raízes distintas. Se $a^q = a$, então a é raiz de f. Logo, pelo lema anterior, todos os elementos de F são exatamente as q raízes de f, e portanto f se fatora em $F[X]$ como $\prod_{a \in F}(x-a)$, e por definição, F é corpo de decomposição de f sobre K, já que f não pode se decompor em um corpo de menor ordem.

□

Teorema 1.2.5. *(Teorema da Existência e Unicidade de Corpos Finitos) Para todo p primo, n positivo inteiro, existe corpo finito de ordem $q = p^n$, e qualquer corpo finito com q elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. Sejam $f(x) = x^q - x \in \mathbb{F}_p[X]$ e F seu corpo de decomposição sobre $\mathbb{F}_p[X]$. Como $f'(x) = qx^{q-1} - 1$, $f'(a) = -1,\ \forall a \in F$, e f não tem raízes múltiplas (pois não tem raízes em comum com f'). Portanto, f tem exatamente q raízes distintas em F. Seja $S = \{a \in F \ / \ a^q - a = 0\}$. Então S é subcorpo de F pois:

- $0, 1 \in S$ (já que $0^q - 0 = 0 - 0 = 0 \ \ e \ \ 1^q - 1 = 1 - 1 = 0$);
- Dados $a, b \in S$, temos $(a-b)^q = a^q - b^q = a - b$. Assim, $(a-b) \in S$
- Dados $a, b \neq 0 \in S$, temos, $(ab^{-1})^q = a^q \cdot b^{q(-1)} = ab^{-1}$. Assim, $(ab^{-1}) \in S$

Mas como S contém todas as raízes de f, S é corpo de decomposição de f. Pela unicidade dos corpos de decomposição (Teorema 1.1.31), $F = S$, e como S tem q elementos (as q raízes de f em F), F tem q elementos. Ou seja F é corpo finito de ordem q.

Vejamos agora a unicidade de F. Se $|F| = q = p^n$, F tem característica p, e assim, $\mathbb{F}_p$ é subcorpo primo de F. Pelo Lema 1.2.4, F é corpo de decomposição de f sobre $\mathbb{F}_p$. Novamente, pela unicidade dos corpos de decomposição, temos a unicidade de F.

□

A prova da unicidade no Teorema 1.2.5 nos dá uma justificativa para falar sobre *o corpo finito* (ou o corpo de Galois) com q elementos, ou seja, de ordem q. Vamos nos referir a este corpo como $\mathbb{F}_q$, onde entende-se que q é uma potência da característica p de $\mathbb{F}_q$, com p primo.

Exemplo 1.2.6. *Considere o corpo $\mathbb{F}_3$ e o polinômio x^2+1. Como este polinômio é irredutível sobre $\mathbb{F}_3$ (já que não possui raízes em $\mathbb{F}_3$), o conjunto*

$$\begin{aligned}\mathbb{F}_3[X]/\langle x^2+1\rangle &= \{g(x)+\langle x^2+1\rangle \ / \ g(x)\in\mathbb{F}_3[x]\}\\ &= \{ax+b+\langle x^2+1\rangle \ / \ a,b\in\mathbb{F}_3\}\end{aligned}$$

é um corpo. Logo,

$$\begin{array}{c}\mathbb{F}_3[X]/\langle x^2+1\rangle\\ \Big|2\\ \mathbb{F}_3\end{array}$$

é uma extensão de corpos finitos. Seja α uma raiz de x^2+1. Temos $\alpha^2+1=0$ que implica $\alpha^2=-1\equiv 2$. Existe um isomofismo entre $\mathbb{F}_3[X]/\langle x^2+1\rangle$ e $\mathbb{F}_9$, e podemos ver a seguinte correspondência

$$\begin{array}{ccc}\underline{\mathbb{F}_3/\langle x^2+1\rangle} & & \underline{\mathbb{F}_9}\\ \langle x^2+1\rangle & \to & \alpha^2+1=0\\ \langle x^2+1\rangle+1 & \to & \alpha^2+2=1\\ \langle x^2+1\rangle+2 & \to & \alpha^2=2\\ \langle x^2+1\rangle+x & \to & \alpha^2+\alpha+1=\alpha\\ \langle x^2+1\rangle+x+1 & \to & \alpha^2+\alpha+2=\alpha+1\\ \langle x^2+1\rangle+x+2 & \to & \alpha^2+\alpha=\alpha+2\\ \langle x^2+1\rangle+2x & \to & \alpha^2+2\alpha+1=2\alpha\\ \langle x^2+1\rangle+2x+1 & \to & \alpha^2+2\alpha+2=2\alpha+1\\ \langle x^2+1\rangle+2x+2 & \to & \alpha^2+2\alpha=2\alpha+2\end{array}$$

e escrever

$$\begin{aligned}\mathbb{F}_3[x]/\langle x^2+1\rangle &= \{a\alpha+b \ / \ a,b\in\mathbb{F}_3\}\\ &= \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}.\end{aligned}$$

Portanto, $\mathbb{F}_3[X]/\langle x^2+1\rangle$ é isomorfo a $\mathbb{F}_9$, e $\{1,\alpha\}$ é uma base de $\mathbb{F}_9$ sobre $\mathbb{F}_3$.

Exemplo 1.2.7. *No Exemplo 1.2.6 mostramos como construir um corpo a partir de um polinômio. A Tabela abaixo mostra o corpo $\mathbb{F}_{16}$ construído usando o polinômio irredutível x^4+x+1 sobre $\mathbb{F}_2$. Os elementos são representados como combinações lineares de $\{1,\alpha,\alpha^2,\alpha^3\}$ com coeficientes em $\{0,1\}$, onde α é uma raiz de x^4+x+1.*

k	Potência de α (α^k)	Forma Polinomial	Forma Vetorial ($a_3a_2a_1a_0$)
0	$\alpha^{\mathbf{0}}$	1	0001
1	$\alpha^{\mathbf{1}}$	α	0010
2	$\alpha^{\mathbf{2}}$	α^2	0100
3	$\alpha^{\mathbf{3}}$	α^3	1000
4	$\alpha^{\mathbf{4}}$	$\alpha + 1$	0011
5	$\alpha^{\mathbf{5}}$	$\alpha^2 + \alpha$	0110
6	$\alpha^{\mathbf{6}}$	$\alpha^3 + \alpha^2$	1100
7	$\alpha^{\mathbf{7}}$	$\alpha^3 + \alpha + 1$	1011
8	$\alpha^{\mathbf{8}}$	$\alpha^2 + 1$	0101
9	$\alpha^{\mathbf{9}}$	$\alpha^3 + \alpha$	1010
10	$\alpha^{\mathbf{10}}$	$\alpha^2 + \alpha + 1$	0111
11	$\alpha^{\mathbf{11}}$	$\alpha^3 + \alpha^2 + \alpha$	1110
12	$\alpha^{\mathbf{12}}$	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
13	$\alpha^{\mathbf{13}}$	$\alpha^3 + \alpha^2 + 1$	1101
14	$\alpha^{\mathbf{14}}$	$\alpha^3 + 1$	1001
15	$\alpha^{\mathbf{15}}$	1	0001

Tabela 1.1: Lista dos Elementos de $\mathbb{F}_{16}$ em Função de α.

Teorema 1.2.8. *(Caracterização de subcorpos) Seja $\mathbb{F}_q$ o corpo finito com $q = p^n$ elementos. Todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, onde m é um divisor positivo de n. Por outro lado, se m é um divisor positivo de n, então existe um único subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. Seja K um subcorpo de $\mathbb{F}_q$. Como p é um número primo e a ordem de K divide a ordem de F, $|K| = p^m$ com $m \leq n$. Pelo Lema 1.2.1, p^n é uma potência de p^m, ou seja, $\exists r \in \mathbb{N}$ tal que $(p^m)^r = p^n \Rightarrow m|n$. Por outro lado,

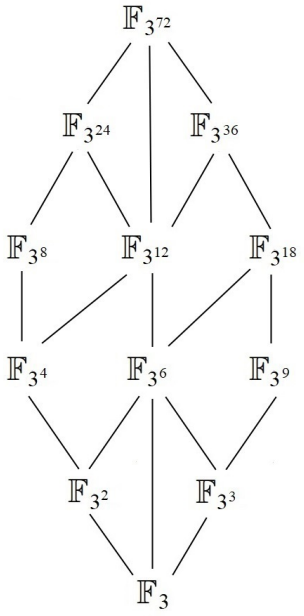
$$\begin{aligned} m|n &\implies (p^m - 1) \mid (p^n - 1) \implies (x^{p^m-1} - 1) \mid (x^{p^n-1} - 1) \\ &\implies (x^{p^m} - x) \mid (x^{p^n} - x) \text{ em } \mathbb{F}_p[X] \end{aligned}$$

o que implica que cada raiz de $x^{p^m} - x$ também é raiz de $x^q - x$. Então, pelo Teorema 1.2.5, o corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$, de ordem p^m, está contido em $\mathbb{F}_q$. Suponha que haja mais de um subcorpo de ordem p^m contido em $\mathbb{F}_q$. Então a união deles contém mais de p^m raízes de $x^{p^m} - x$. Absurdo. Logo, existe um único subcorpo de $\mathbb{F}_q$ de ordem p^m.

□

O Teorema 1.2.8 mostra que o único subcorpo de $\mathbb{F}_{p^n}$ de ordem p^m, onde m é um divisor positivo de n, consiste exatamente das raízes do polinômio $x^{p^m} - x \in \mathbb{F}_p[X]$ em $\mathbb{F}_{p^n}$.

Exemplo 1.2.9. *Os subcorpos do corpo $\mathbb{F}_{3^{72}}$ podem ser determinados pelos divisores positivos de 72. As relações de continência entre estes subcorpos podem ser vistas através do seguinte diagrama:*



Pelo Teorema 1.2.8, estas continências são equivalentes à divisibilidade entre os divisores de 72.

Teorema 1.2.10. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $(\mathbb{F}_q{}^*, \cdot)$ é cíclico.*

Demonstração. Provemos que um subgrupo finito qualquer de um corpo finito é cíclico. Sejam G um subgrupo finito de um corpo finito F tal que $|G| = n$, d um divisor positivo de n e $\varphi(d)$ o número de elementos de ordem d em G. Se $\varphi(d) \neq 0$, seja $a \in G$ tal que $|a| = d$, e H subgrupo de G gerado por a. Como $H = \langle a \rangle$, $|H| = |a| = d$ e todo elemento de H é raiz de $x^d = 1$. Então, H é exatamente o conjunto das d raízes de $x^d = 1$. Dado $h \in H$, temos que $h = a^j$ com $0 \leq j \leq d-1$, e $|h| = \dfrac{|a|}{mdc(d,j)}$ (Teorema 1.1.7), o que implica que $|h| = |a| \Leftrightarrow mdc(d,j) = 1$. Como $0 \leq j \leq d-1$, a quantidade de elementos j tais que $mdc(d,j) = 1$ é igual a $\phi(d)$ (Função de Euler de d). Portanto, $\varphi(d) = 0$ ou $\phi(d)$, logo, $\varphi(d) \leq \phi(d)$. Daí,

$$n = \sum_{d|n} \varphi(d) \leq \sum_{d|n} \phi(d) = n \;\Rightarrow\; \sum_{d|n} \varphi(d) = \sum_{d|n} \phi(d) \;\Rightarrow\; \varphi(d) = \phi(d),\ \forall d|n$$

Em particular, $\varphi(n) = \phi(n) \;\Rightarrow\; \exists g \in G \;/\; |g| = n \;\Rightarrow\; G = \langle g \rangle$.

□

Definição 1.2.11. *(Elemento primitivo) O gerador do grupo cíclico $(\mathbb{F}_q{}^*, \cdot)$ é chamado de **elemento primitivo** de $\mathbb{F}_q$.*

Da demonstração do teorema anterior, sabemos que o número de elementos primitivos em $\mathbb{F}_q$ é dado por $\phi(q-1)$.

Teorema 1.2.12. *Se $\mathbb{F}_q$ é um corpo finito, $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$, então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ é um elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja α um elemento primitivo de $\mathbb{F}_r$. Como $\alpha \in \mathbb{F}_r$ e $\mathbb{F}_q \subset \mathbb{F}_r$, $\mathbb{F}_q(\alpha) \subset \mathbb{F}_r$. Por outro lado, ${\mathbb{F}_r}^* = \langle\alpha\rangle$, então $\mathbb{F}_q(\alpha)$ contém todos os elementos de ${\mathbb{F}_r}^*$, além do 0. Assim, $\mathbb{F}_r \subset \mathbb{F}_q(\alpha)$. Portanto, $\mathbb{F}_r = \mathbb{F}_q(\alpha)$, ou seja, $\mathbb{F}_r$ é uma extensão simples de $\mathbb{F}_q$ adjuntado de qualquer elemento primitivo de $\mathbb{F}_r$.

□

Corolário 1.2.13. *Para todo corpo finito $\mathbb{F}_q$ e todo n positivo inteiro, existe um polinômio irredutível de grau n em $\mathbb{F}_q[X]$.*

Demonstração. Seja $\mathbb{F}_r$ um corpo de ordem q^n. Temos $n = [\mathbb{F}_r : \mathbb{F}_q]$. Pelo lema anterior, $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ para algum α primitivo em $\mathbb{F}_r$. Então, o polinômio minimal de α sobre $\mathbb{F}_q$ é irredutível (Teorema 1.1.25), e tem grau n (Teorema 1.1.29).

□

1.3 Raízes de polinômios irredutíveis

Vejamos agora algumas propriedades sobre o conjunto de raízes de um polinômio irredutível sobre um corpo finito.

Lema 1.3.1. *Sejam $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ e α raiz de f numa extensão de $\mathbb{F}_q$. Então, dado $h \in \mathbb{F}_q[X]$, $h(\alpha) = 0$ se, e somente se, f divide h.*

Demonstração. Seja a o coeficiente líder de f. Defina $g(x) = a^{-1} \cdot f(x)$. Daí, g é um polinômio mônico, irredutível, e que tem α como raiz, ou seja, é o polinômio minimal de α sobre $\mathbb{F}_q$. Como estamos em um corpo, que é um domínio principal, o ideal $J = \{f \in \mathbb{F}_q[X] \ / \ f(\alpha) = 0\}$ possui um gerador. Como f é irredutível, este gerador é igual a g, e portanto $g|f$. Então, dado $h \in \mathbb{F}_q[X]$, se $h(\alpha) = 0$, então $g|h$ e consequentemente $f|h$ (pois f é irredutível); por outro lado, $f|h \Rightarrow h(\alpha) = 0$.

□

Lema 1.3.2. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então, $f(x)$ divide $x^{q^n} - x$ se, e somente se, m divide n.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Suponha que $f(x) \mid (x^{q^n} - x)$, e então α é raiz de $x^{q^n} - x$, o que implica que $\alpha \in \mathbb{F}_{q^n}$. Logo $\mathbb{F}_q(\alpha)$ é subcorpo de $\mathbb{F}_{q^n}$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, temos que $m|n$.

Por outro lado, se α é raiz de f, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, ou seja, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Como $m|n$, segue que $\mathbb{F}_{q^m}$ é subcorpo de $\mathbb{F}_{q^n}$, e então $\alpha \in \mathbb{F}_{q^n}$. Pelo Lema 1.3.1, $f(x) \mid (x^{q^n} - x)$.

□

Teorema 1.3.3. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau n. Então, f tem raiz α em $\mathbb{F}_{q^n}$ e todas as raízes de f são simples e iguais a $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Logo, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$ e $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Vejamos que se $\beta \in \mathbb{F}_{q^n}$ é raiz de f então β^q também é raiz de f. Escreva $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ com $a_i \in \mathbb{F}_q$, $0 \leq i \leq n$. Daí,

$$\begin{aligned} f(\beta^q) &= a_n\beta^{qn} + a_{n-1}\beta^{q(n-1)} + \cdots + a_1\beta^q + a_0 \\ &= a_n^q\beta^{qn} + a_{n-1}^q\beta^{q(n-1)} + \cdots + a_1{}^q\beta^q + (a_0)^q \\ &= (a_n\beta^n)^q + (a_{n-1}\beta^{n-1})^q + \cdots + (a_1\beta)^q + (a_0)^q \\ &= (a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0)^q \\ &= f(\beta)^q = 0^q = 0 \end{aligned}$$

Ou seja, β^q é raiz de f. Portanto $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ são raízes de f.

Agora suponha que nem todas as raízes de f são simples. Então, existem j, k inteiros tais que $0 \leq j < k \leq n-1$ e $\alpha^{q^j} = \alpha^{q^k}$. Elevando essa igualdade a q^{n-k} temos $\alpha^{q^{j+n-k}} = \alpha^{q^{k+n-k}} = \alpha^{q^n} = \alpha$, logo $f(x) \mid (x^{q^{j+n-k}} - x)$, e assim, pelo Lema 1.3.2, $n \mid (j+n-k)$. Mas $0 < j+n-k < n$ (pois $j < k$), gerando uma contradição. Ou seja, todas as raízes de f são simples.

□

Corolário 1.3.4. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau n. Então, o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^n}$.*

Demonstração. O teorema anterior mostra que todas as raízes de f estão em $\mathbb{F}_{q^n}$, logo f se decompõe em $\mathbb{F}_{q^n}$. Além disso, o Teorema 1.3.2 mostra que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, ou seja, $\mathbb{F}_{q^n}$ é o menor corpo com todas as raízes de f, logo, é o corpo de decomposição de f.

□

Corolário 1.3.5. *Quaisquer polinômios irredutíveis em $\mathbb{F}_q[X]$ de mesmo grau tem corpos de decomposição isomorfos.*

Demonstração. Sejam f e g polinômios irredutíveis de grau n. Pelo corolário anterior, o corpo de decomposição de ambos é dado por $\mathbb{F}_{q^n}$.

□

Exemplo 1.3.6. *No Exemplo 1.2.6 mostramos a construção de $\mathbb{F}_9$ a partir de $\mathbb{F}_3$ usando o polinômio x^2+1. Considere agora o polinômio x^2+x+2. Seja β uma raiz deste polinômio. Temos $\beta^2+\beta+2 = 0 \Rightarrow \beta^2 = 2\beta+1$. Então, o isomorfismo é tal que*

$$\begin{array}{ccc} \dfrac{\mathbb{F}_3/\langle x^2+x+2\rangle}{\langle x^2+x+2\rangle} & & \underline{\mathbb{F}_9} \\ \langle x^2+x+2\rangle + 1 & \to & \beta^2+1 = 2\beta+2 \\ \langle x^2+x+2\rangle + 2 & \to & \beta^2+2 = 2\beta \\ \langle x^2+x+2\rangle + x & \to & \beta^2 = 2\beta+1 \\ \langle x^2+x+2\rangle + x + 1 & \to & \beta^2+\beta+1 = 2 \\ \langle x^2+x+2\rangle + x + 2 & \to & \beta^2+\beta+2 = 0 \\ \langle x^2+x+2\rangle + 2x & \to & \beta^2+\beta = 1 \\ \langle x^2+x+2\rangle + 2x + 1 & \to & \beta^2+2\beta+1 = \beta+2 \\ \langle x^2+x+2\rangle + 2x + 2 & \to & \beta^2+2\beta+2 = \beta \\ \langle x^2+x+2\rangle + 2x + 2 & \to & \beta^2+2\beta = \beta+1. \end{array}$$

Ou seja, como x^2+x+2 também irredutível sobre $\mathbb{F}_3$ de grau 2, o corpo $\mathbb{F}_3/\langle x^2+x+2\rangle$ também é isomorfo a $\mathbb{F}_9$, e $\{1,\beta\}$ é uma base de $\mathbb{F}_9$ sobre $\mathbb{F}_3$.

Definição 1.3.7. *(Elemento conjugado) Seja $\alpha \in \mathbb{F}_{q^n}$. Os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ são **conjugados** de α com respeito a $\mathbb{F}_q$.*

Os conjugados de $\alpha \in \mathbb{F}_{q^n}$ com respeito a $\mathbb{F}_q$ são todos distintos se, e somente se, o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau n. Caso contrário, o grau d deste polinômio é um divisor próprio de n, e os conjugados de α com respeito a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^{q^{n/d}}, \alpha^{q^{2n/d}}, \ldots, \alpha^{q^{(d-1)n/d}}$ que se repetem $\frac{n}{d}$ vezes.

Teorema 1.3.8. *Os conjugados de $\alpha \in {\mathbb{F}_q}^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ tem a mesma ordem em $({\mathbb{F}_q}^*, \cdot)$.*

Demonstração. Sejam $\mathbb{F}_q$ um corpo finito tal que $q = p^n$ e $\alpha \in \mathbb{F}_q$. Dado um subcorpo $\mathbb{F}_r$ de $\mathbb{F}_q$, $r = p^m$ para algum m divisor de n, e os conjugados de α com respeito a $\mathbb{F}_r$ são $\alpha, \alpha^r, \alpha^{r^2}, \ldots, \alpha^{r^{k-1}}$, onde $k = \dfrac{n}{m}$, pois

$$\alpha^{r^k} = \alpha^{(p^m)^k} = \alpha^{p^{mk}} = \alpha^{p^n} = \alpha^q = \alpha.$$

Então, $\alpha^{r^k-1} = 1 \Rightarrow ord(\alpha) \mid (r^k - 1)$. Considerando $\langle\alpha\rangle$ um subgrupo finito de $({\mathbb{F}_q}^*, \cdot)$, para $0 \leq j \leq k-1$, α^{r^j} gera um subgrupo finito de $\langle\alpha\rangle$. Assim, $ord(\alpha^{r^j}) = \frac{ord(\alpha)}{\mathrm{mdc}(r^j, ord(\alpha))}$ (Teorema 1.1.7). Vejamos que $\mathrm{mdc}\big(r^j, ord(\alpha)\big) = 1$. Temos que $r^j = (p^m)^j = p^{mj}$ e $r^k = (p^m)^k = p^{mk}$. Se $\mathrm{mdc}\big(p^{mj}, ord(\alpha)\big) > 1$, então

$$p \mid ord(\alpha) \Rightarrow p \mid (r^k - 1) \Rightarrow p \mid (p^{mk} - 1) \Rightarrow p|1.$$

Absurdo. Logo, $ord(\alpha^{r^j}) = \dfrac{ord(\alpha)}{\mathrm{mdc}\big(r^j, ord(\alpha)\big)} = ord(\alpha)$.

□

Corolário 1.3.9. *Se α é um elemento primitivo de $\mathbb{F}_q$, então todos os seus conjugados com respeito a qualquer subcorpo de $\mathbb{F}_q$ também são.*

Demonstração. Pelo teorema anterior, eles tem a mesma ordem de α, ou seja, também geram $({\mathbb{F}_q}^*, \cdot)$.

□

Exemplo 1.3.10. *Seja $\alpha \in \mathbb{F}_{2^4}$ uma raiz do polinômio $f(x) = x^4 + x + 1 \in \mathbb{F}_2[X]$. Os conjugados de α com respeito a $\mathbb{F}_2$ são $\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \alpha^{2^3}$, ou seja, $\alpha, \alpha^2, \alpha^4, \alpha^8$, e todos são elementos primitivos de $\mathbb{F}_{2^4}$. Já os conjugados de α com respeito a $\mathbb{F}_{2^2}$ são $\alpha^{(2^2)^0}, \alpha^{(2^2)^1}$ ou seja α, α^4.*

Existe uma forte relação entre elementos conjugados e certos automorfismos de um corpo finito. Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$. Ao dizer um *automorfismo* σ de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, nos referimos ao automorfismo de $\mathbb{F}_{q^n}$ que fixa os elementos de $\mathbb{F}_q$, os chamados *Automorfismos de Frobenius*. Isto é, $\sigma\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ é uma aplicação bijetora com $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\cdot\sigma(\beta),\ \forall \alpha, \beta \in \mathbb{F}_{q^n}$; e $\sigma(a) = a,\ \forall a \in \mathbb{F}_q$.

Teorema 1.3.11. *Os automorfismos distintos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ são exatamente as aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ dadas por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^n},\ 0 \leq j \leq n-1$.*

Demonstração. Para cada σ_j e todo $\alpha, \beta \in \mathbb{F}_{q^n}$, como o contradomínio de σ_j é $\mathbb{F}_{q^n}$,

$$\sigma_j(\alpha+\beta) = (\alpha+\beta)^j = \alpha^j + \beta^j = \sigma_j(\alpha) + \sigma_j(\beta);$$

$$\sigma_j(\alpha\beta) = (\alpha\beta)^{q^j} = \alpha^{q^j} \cdot \beta^{q^j} = \sigma_j(\alpha) \cdot \sigma_j(\beta).$$

Logo, σ_j é um homomorfismo de $\mathbb{F}_{q^n}$ em $\mathbb{F}_{q^n}$ (endomorfismo de $\mathbb{F}_{q^n}$).

Temos que $\sigma_j(\alpha) = 0 \Leftrightarrow \alpha^{q^0} = 0 \Leftrightarrow \alpha = 0$. Então, $ker(\sigma_j) = \{0\} \Rightarrow \sigma_j$ é injetora. Como $\mathbb{F}_{q^n}$ é finito, segue que σ_j é sobrejetora. Logo, σ_j é um automorfismo de $\mathbb{F}_{q^n}$. Além disso, pelo Lema 1.2.3, $\sigma_j(\alpha) = \alpha^{q^j} = \alpha,\ \forall \alpha \in \mathbb{F}_q$. Logo, σ_j é um automorfismo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Sejam $0 < i, j < n$. Suponha que $\sigma_i = \sigma_j$. Então, $\alpha^{q^i} = \alpha^{q^j},\ \forall \alpha \in \mathbb{F}_{q^n}$. Suponha, sem perda de generalidade, $i > j$. Dividindo esta igualdade por α^{q^j}, temos $\alpha^{q^i - q^j} = 1$, logo, $ord(\alpha) \mid (q^i - q^j)$. Considere α um elemento primitivo. Então,

$$ord(\alpha) = q^n - 1 \implies (q^n-1) \mid (q^i - q^j) \implies (q^n-1) \mid q^j(q^{i-j}-1).$$

Como (q^n-1) e q^j não tem fatores primos em comum, (q^n-1) divide $(q^{i-j}-1)$, e então, $n < (i-j)$. Contradição. Logo, $\sigma_i \neq \sigma_j$.

Agora, sejam σ um automorfismo qualquer de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, β um elemento primitivo de $\mathbb{F}_{q^n}$ e $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[X]$ o polinômio minimal de β sobre $\mathbb{F}_q$. Daí,

$$\begin{aligned} 0 = \sigma(0) &= \sigma(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0) \\ &= \sigma(\beta)^n + a_{n-1}\sigma(\beta)^{n-1} + \cdots + a_1\sigma(\beta) + a_0 \end{aligned}$$

e então $\sigma(\beta)$ é raiz de $f(x)$, e pelo Teorema 1.3.3, $\sigma(\beta) = \beta^{q^j}$ para algum j tal que $0 \leq j \leq n-1$. Dado $\alpha \in \mathbb{F}_{q^n},\ \alpha = \beta^s$ para algum s. Como σ é um homomorfismo de grupos, $\sigma_j(\alpha) = \sigma_j(\beta^s) = \sigma_j(\beta)^s = (\beta^{q^j})^s = (\beta^s)^{q^j} = \alpha^{q^j}$.

□

Após este teorema podemos ver que os conjugados de α são obtidos aplicando todos os automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ ao elemento α. Estes automorfismos formam um grupo onde a operação é a composição de aplicações. Este grupo é cíclico, de ordem n e gerado por σ_1.

1.4 Traço, Norma e Base

Nesta seção, adotaremos $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^n}$, a menos que seja especificado. Vejamos, novamente, a extensão finita F do corpo finito K como um espaço vetorial sobre K. Isso significa que F tem dimensão n sobre K, e se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de F sobre K, todo elemento $d \in F$ se escreve como

$$d = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n \text{ com } c_j \in K \text{ para } 1 \leq j \leq n.$$

Definição 1.4.1. *(Traço) Para todo $\alpha \in F$, o **traço** de α sobre K é definido por*

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}.$$

*Se P for o subcorpo primo de F, $Tr_{F/P}(\alpha)$ é o **traço absoluto** de α e escrevemos apenas $Tr_F(\alpha)$.*

Além de uma soma de conjugados, o traço também pode ser visto da seguinte forma: seja $f \in K[X]$ o polinômio minimal de α sobre K de grau d divisor de n. Então $g(x) = f(x)^{n/d} \in K[X]$ é chamado **polinômio característico** de α sobre K. Pelo Teorema 1.3.3 as raízes de f são $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$, e pelo parágrafo após a Definição 1.3.7, as raízes de g em F são os conjugados de α com respeito a K. Daí, g se escreve como

$$\begin{aligned} g(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \\ &= (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\ldots(x-\alpha^{q^{n-1}}) \end{aligned}$$

onde, pelas Fórmulas de Viète, $Tr_{F/K}(\alpha) = -a_{n-1}$. Em particular, $Tr_{F/K}(\alpha) \in K$.

Teorema 1.4.2. *A função traço satisfaz as seguintes propriedades:*

(i) $Tr_{F/K}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta),\ \forall \alpha, \beta \in F$;

(ii) $Tr_{F/K}(c\alpha) = c \cdot Tr_{F/K}(\alpha),\ \forall c \in K, \alpha \in F$;

(iii) $Tr_{F/K}$ *é transformação linear sobrejetora de F sobre K, onde F e K são vistos como espaços vetoriais sobre K;*

(iv) $Tr_{F/K}(a) = na,\ \forall a \in K$;

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha),\ \forall \alpha \in F$.

Demonstração. (i) Sejam $\alpha, \beta \in F$. De acordo com o Teorema 1.1.19,

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= \alpha + \beta + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{n-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} \\ &= Tr_{F/K}(\alpha) + Tr_{F/K}(\beta). \end{aligned}$$

(ii) Pelo Lema 1.2.3 $c^{q^j} = c,\ \forall c \in K, j \geq 0$. Logo,

$$\begin{aligned} Tr_{F/K}(c\alpha) &= c\alpha + (c\alpha)^q + \cdots + (c\alpha)^{q^{n-1}} = c\alpha + c\alpha^q + \cdots + c\alpha^{q^{n-1}} \\ &= c \cdot Tr_{F/K}(\alpha). \end{aligned}$$

(iii) Os ítens (i) e (ii) provam que $Tr_{F/K}$ é uma transformação linear de F sobre K. Como K é um espaço unidimensional seus únicos subcorpos são $\{0\}$ e K. Se $Tr_{F/K}$ não fosse sobrejetora, sua imagem seria $\{0\}$. Sabemos que $Tr_{F/K}(\alpha) = 0$ se, e somente se, α é raiz de $x^{q^{n-1}} + \cdots + x^q + x \in K[X]$. Mas este polinômio tem no máximo q^{n-1} raízes e K tem q^n elementos. Logo, existe $\alpha \in F$ tal que $Tr_{F/K}(\alpha) \neq 0$, o que implica que $Im\ (Tr_{F/K}) \neq \{0\}$. Ou seja, $Im\ (Tr_{F/K}) = K$ e $Tr_{F/K}$ é sobrejetora.

(iv) Seja $a \in K$. $Tr_{F/K}(a) = a + a^q + \cdots + a^{q^{n-1}} = \underbrace{a + a + \cdots + a}_{n \text{ vezes}} = na$.

(v) Seja $\alpha \in F$.

$$\begin{aligned} Tr_{F/K}(\alpha^q) &= \alpha^q + (\alpha^q)^q + \cdots + (\alpha^q)^{q^{n-1}} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^n} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha \\ &= Tr_{F/K}(\alpha). \end{aligned}$$

□

A função Traço $Tr_{F/K}$ é, não somente uma transformação linear sobrejetora de F em K, mas também um "modelo" de todas as transformações lineares de F sobre K com a vantagem de ser independente da escolha de uma determinada base.

Teorema 1.4.3. *Seja $F|K$ uma extensão de corpos finitos, ambos considerados espaços vetoriais sobre K. As transformações lineares de F sobre K são exatamente as aplicações T_β com $\beta \in F$, onde $T_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ para todo $\alpha \in F$. Além disso, $T_\beta \neq T_\gamma$ sempre que β e γ são distintos em F.*

Demonstração. Pelo Teorema 1.4.2(iii), T_β é transformação linear de F sobre K. Para $\beta, \gamma \in F,\ \beta \neq \gamma$, temos

$$T_\beta(\alpha) - T_\gamma(\alpha) = Tr_{F/K}(\beta\alpha) - Tr_{F/K}(\gamma\alpha) = Tr_{F/K}\big((\beta - \gamma) \cdot \alpha\big) \neq 0$$

para algum $\alpha \in F$. Logo, $T_\beta \neq T_\gamma$.

As aplicações T_β fornecem q^n transformações lineares de F sobre K diferentes (uma para cada $\beta \in F$). Por outro lado, podemos obter as transformações lineares de F sobre K, atribuindo um elemento arbitrário de K aos n elementos de uma base de F sobre K. Como K tem q elementos, são exatamente q^n possibilidades. Portanto, as aplicações T_β são exatamente estas q^n possíveis aplicações.

□

Teorema 1.4.4. *Seja F uma extensão finita de K. Dado $\alpha \in F$, $Tr_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q - \beta$ para algum $\beta \in F$.*

Demonstração. ($\Rightarrow$) Seja β raiz de $x^q - x - \alpha$ em alguma extensão de F. Temos $\alpha = \beta^q - \beta$. Daí,

$$\begin{aligned} 0 = Tr_{F/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{n-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^n} - \beta^{q^{n-1}}) \\ &= \beta^{q^n} - \beta. \end{aligned}$$

Ou seja, $\beta^{q^n} = \beta \Rightarrow \beta \in F$.
($\Leftarrow$) Se $\alpha = \beta^q - \beta$, então $Tr_{F/K}(\alpha) = Tr_{F/K}(\beta^q - \beta) = Tr_{F/K}(\beta^q) - Tr_{F/K}(\beta) = 0$, pois pelo Teorema 1.4.2(v), $Tr_{F/K}(\beta^q) = Tr_{F/K}(\beta)$.

□

Teorema 1.4.5. *(Transitividade do Traço) Sejam $E|F$ e $F|K$ extensões de corpos finitos. Então $Tr_{E/K}(\alpha) = Tr_{F/K}\left(Tr_{E/F}(\alpha)\right)$ para todo $\alpha \in E$.*

Demonstração. Se $n = [F : K]$ e $m = [E : F]$, então $[E : K] = nm$ (Teorema 1.1.27). Daí,

$$\begin{aligned} Tr_{F/K}\left(\left(Tr_{E/F}(\alpha)\right)\right) &= \sum_{i=0}^{n-1} \left(Tr_{E/F}(\alpha)\right)^{q^i} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{(q^n)^j}\right)^{q^i} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^{q^{nj+i}} = \sum_{k=0}^{nm-1} \alpha^{q^k} = Tr_{E/K}(\alpha). \end{aligned}$$

□

Definição 1.4.6. *(Norma) Para todo $\alpha \in F$, a **norma** de α sobre K é definida por*

$$N_{F/K}(\alpha) = \alpha.\alpha^q.\alpha^{q^2} \ldots \alpha^{q^{n-1}} = \alpha^{\frac{(q^n-1)}{(q-1)}}.$$

Comparando as constantes do polinômio g após a Definição 1.4.1, podemos notar que $N_{F/K}(\alpha) = (-1)^n a_0$. Em particular, $N_{F/K}(\alpha) \in K$.

Teorema 1.4.7. *A função norma satisfaz as seguintes propriedades:*

(i) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha) \cdot N_{F/K}(\beta),\ \forall \alpha, \beta \in F$;

(ii) $N_{F/K}$ *é sobrejetora de F sobre K, e de F^* sobre K^*;*

(iii) $N_{F/K}(a) = a^n,\ \forall a \in K$;

(iv) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha),\ \forall \alpha \in F$.

Demonstração. (i) Sejam $\alpha, \beta \in F$.

$$\begin{aligned} N_{F/K}(\alpha\beta) &= \alpha.\beta.(\alpha.\beta)^q \dots (\alpha.\beta)^{q^{n-1}} = \alpha.\alpha^q \dots \alpha^{q^{n-1}}.\beta.\beta^q \dots \beta^{q^{n-1}} \\ &= N_{F/K}(\alpha) \cdot N_{F/K}(\beta). \end{aligned}$$

(ii) Como $N_{F/K}(\alpha) \in K$, $\forall \alpha \in F$, $N_{F/K}$ é uma aplicação de F em K, e como $N_{F/K}(\alpha) = 0 \Leftrightarrow \alpha = 0$, também é uma aplicação de F^* em K^*. A propriedade (i) mostra que $N_{F/K}$ é um homomorfismo de grupos entre F^* e K^*, logo, os elementos do kernel de $N_{F/K}$ são as raízes de $x^{\frac{(q^n-1)}{(q-1)}} = 1$. Seja d a ordem do kernel. Temos que $d \leq \frac{(q^n-1)}{(q-1)}$, e de acordo com o Teorema 1.1.12,

$$|Im(N_{F/K})| = \frac{|F^*|}{|ker(N_{F/K})|} = \frac{q^n - 1}{d} \geq q - 1 = |K^*|$$

Portanto, $N_{F/K}$ é sobrejetora de F^* em K^*, logo, sobrejetora de F em K.

(iii) Seja $a \in K$. $N_{F/K}(a) = a.a^q \dots a^{q^{n-1}} = \underbrace{a.a \dots a}_{n \text{ vezes}} = a^n$.

(iv) Seja $\alpha \in F$.

$$\begin{aligned} N_{F/K}(\alpha^q) &= \alpha^q.(\alpha^q)^q \dots (\alpha^q)^{q^{n-1}} \\ &= \alpha^q.\alpha^{q^2} \dots \alpha^{q^n} \\ &= \alpha^q.\alpha^{q^2} \dots \alpha \\ &= N_{F/K}(\alpha). \end{aligned}$$

□

Teorema 1.4.8. *(Transitividade da Norma) Sejam $E|F$ e $F|K$ extensões de corpos finitos. Então $N_{E/K}(\alpha) = N_{F/K}\left(N_{E/F}(\alpha)\right)$ para todo $\alpha \in E$.*

Demonstração. Como $n = [F : K]$ e $m = [E : F]$, temos $[E : K] = nm$. Daí,

$$\begin{aligned} N_{F/K}\left(N_{E/F}(\alpha)\right) = N_{F/K}\left(\alpha^{\frac{(q^{nm}-1)}{(q^n-1)}}\right) &= \left(\alpha^{\frac{(q^{nm}-1)}{(q^n-1)}}\right)^{\frac{(q^n-1)}{(q-1)}} \\ = \alpha^{\frac{(q^{nm}-1)}{(q-1)}} &= N_{E/K}(\alpha) \end{aligned}$$

□

Seja $\{\alpha_1, \dots, \alpha_n\}$ uma base de F sobre K. Todo elemento α de F se escreve como $c_1\alpha_1 + \dots + c_n\alpha_n$, onde a função $c_j \colon \alpha \mapsto c_j(\alpha)$, com $c_j(\alpha) \in K$, $1 \leq j \leq n$, é transformação linear de F em K, e pelo Teorema 1.4.3, existe $\beta_j \in F$ tal que $c_j(\alpha) = Tr_{F/K}(\beta_j \cdot \alpha)$, $\forall \alpha \in F$. Fazendo $\alpha = \alpha_i$ para cada $i \in \{1, \dots, n\}$, encontramos $\alpha_i = 0.\alpha_1 + \dots + 1.\alpha_i + \dots + 0.\alpha_n = Tr_{F/K}(\beta_j \,.\, \alpha_1).\alpha_1 + \dots + Tr_{F/K}(\beta_j \cdot \alpha_i) \cdot \alpha_i + \dots + Tr_{F/K}(\beta_j \cdot \alpha_n) \cdot \alpha_n$. Isto implica que

$$Tr_{F/K}(\beta_j \cdot \alpha_i) = \begin{cases} 0, & \text{se } i \neq j; \\ 1, & \text{se } i = j. \end{cases}$$

Vejamos agora que $\{\beta_1, \ldots, \beta_n\}$ também é uma base de F sobre K. Como este conjunto possui n elementos, basta provar que é linearmente independente. Sejam $d_1, d_2, \ldots, d_n \in K$ tais que $d_1\beta_1 + \cdots + d_m\beta_n = 0$. Multiplicando ambos os lados por um α_i fixo, temos $d_1\beta_1\alpha_i + \cdots + d_i\beta_i\alpha_i + \cdots + d_n\beta_n\alpha_i = 0$. Daí,

$$\begin{aligned} 0 = Tr_{F/K}(0) &= Tr_{F/K}(d_1\beta_1\alpha_i + \cdots + d_i\beta_i\alpha_i + \cdots + d_n\beta_n\alpha_i) \\ &= d_1.Tr_{F/K}(\beta_1\alpha_i) + \cdots + d_i.Tr_{F/K}(\beta_i\alpha_i) + \cdots + d_n.Tr_{F/K}(\beta_n\alpha_i) \\ &= d_1.0 + \cdots + d_i.1 + \cdots + d_n.0 \\ &= d_i \end{aligned}$$

e como i é arbitrário, $d_i = 0,\ \forall i$. Logo, $\{\beta_1, \ldots, \beta_n\}$ também é base de F sobre K.

Definição 1.4.9. *(Base dual) Seja $F|K$ uma extensão de corpos finitos. As bases $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_n\}$ de F sobre K são* ***bases duais (ou bases complementares)*** *se para $1 \leq i, j \leq n$,*

$$Tr_{F/K}(\beta_j \cdot \alpha_i) = \begin{cases} 0, & \text{se } i = j; \\ 1, & \text{se } i \neq j. \end{cases}$$

Exemplo 1.4.10. *Sejam $\alpha \in \mathbb{F}_{2^3}$ uma raiz do polinômio x^3+x^2+1 irredutível sobre $\mathbb{F}_2[X]$ e $\alpha, \alpha^2, \alpha^4$ os seus conjugados com respeito a $\mathbb{F}_2$. Vejamos que $\{\alpha, \alpha^2, 1+\alpha+\alpha^2\}$ é uma base de $\mathbb{F}_{2^3}$ sobre $\mathbb{F}_2$. Como este conjunto tem 3 elementos, basta mostrar que é linearmente independente. Sabemos que $\{1, \alpha, \alpha^2\}$ é uma base de $\mathbb{F}_{2^3}$ sobre $\mathbb{F}_2$ (Teorema 1.1.29). Sejam $c_1, c_2, c_3 \in \mathbb{F}_2$ tais que $c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2) = 0$. Então,*

$$\begin{aligned} c_3.1 + (c_1 + c_3)\alpha + (c_2 + c_3)\alpha^2 = 0 &\Rightarrow c_1 = (c_1 + c_3) = (c_2 + c_3) = 0 \\ &\Rightarrow c_1 = c_2 = c_3 = 0 \end{aligned}$$

Ou seja, o conjunto $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ é uma base de $\mathbb{F}_{2^3}$ sobre $\mathbb{F}_2$.

A base dual (ou complementar) de $\{\alpha, \alpha^2, 1+\alpha+\alpha^2\}$ é exatamente $\{\alpha, \alpha^2, 1+\alpha+\alpha^2\}$. Tais bases são chamadas de ***bases autoduais****. O elemento α^5, por exemplo, pode ser representado unicamente como $\alpha^5 = c_1\alpha+c_2\alpha^2+c_3(1+\alpha+\alpha^2)$, e os coeficientes $c_1, c_2, c_3 \in \mathbb{F}_2$ são determinados por*

- $c_1 = Tr_{F/K}(\alpha\alpha^5) = 0$;
- $c_2 = Tr_{F/K}(\alpha^2\alpha^5) = 1$;
- $c_3 = Tr_{F/K}\left((1 + \alpha + \alpha^2).\alpha^5\right) = 1$.

Ou seja, $\alpha^5 = \alpha^2 + (1 + \alpha + \alpha^2) = 1 + \alpha$.

O número de bases distintas F sobre K pode ser grande, mas existem 2 tipos importantes: a **base polinomial** $\{1, \alpha, \ldots, \alpha^{n-1}\}$, dada pelas potências de um elemento α que define F sobre K, que normalmente é um elemento primitivo de F. Na continuação, veremos outro tipo de base.

Definição 1.4.11. *(Elemento normal) Uma base de F sobre K dada por $\alpha \in F$ e seus conjugados com respeito a K, da forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$, é chamada de* ***base normal*** *de F sobre K. Neste caso, $\alpha \in F$ é chamado de* ***elemento normal*** *sobre K.*

A base $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ de $\mathbb{F}_8$ sobre $\mathbb{F}_2$ é um exemplo de base normal, já que $\alpha^4 = 1 + \alpha + \alpha^2$. Antes de provar a existência para o caso geral, vejamos alguns lemas necessários.

Lema 1.4.12. *(Lema de Artin) Sejam G um grupo qualquer, F um corpo qualquer, $\psi_1, \ldots, \psi_m$ homomorfismos distintos de G em F^*, e $a_1, \ldots, a_n$ elementos de F com pelo menos um não nulo. Então existe $g \in G$ tal que $a_1\psi_1(g) + \cdots + a_n\psi_n(g) \neq 0$.*

Demonstração. Provemos por indução em n. Se $n = 1$, $a_1 \neq 0$ e como $\psi_1(g) \in F^*$, tem-se o resultado. Assuma que $n > 1$ e que o resultado é válido para $n - 1$. Se $a_1 = 0$, voltamos ao caso $n - 1$ e tem-se o resultado.

Agora considere $a_1 \neq 0$ e suponha, por absurdo, que

$$a_1\psi_1(g) + \cdots + a_n\psi_n(g) = 0, \ \forall g \in G \ (*)$$

Como $\psi_1 \neq \psi_n$, existe $h \in G$ tal que $\psi_1(h) \neq \psi_n(h)$. Substituindo g por gh em $(*)$, e posteriormente multiplicando por $\psi_n(h)^{-1}$, temos

$$\begin{aligned} 0 &= a_1\psi_1(gh) + \cdots + a_n\psi_n(gh) \\ &= a_1\psi_1(g)\psi_1(h)\psi_n(h)^{-1} + \cdots + a_{n-1}\psi_{n-1}(g)\psi_{n-1}(h)\psi_n(h)^{-1} + a_n\psi_n(g), \end{aligned}$$

e considerando $b_i = a_i\psi_i(h)\psi_n(h)^{-1}$ para $1 \leq i \leq n - 1$ obtemos

$$0 = b_1\psi_1(g) + \cdots + b_{n-1}\psi_{n-1}(g) + a_n\psi_n(g) \ (**)$$

Subtraindo $(*)$ de $(**)$ temos $c_1\psi_1(g) + \cdots + c_{n-1}\psi_{n-1}(g) = 0$, $\forall g \in G$, onde $c_i = a_i - b_i$ para $1 \leq i \leq n-1$. Em particular, $c_1 = a_1 - b_1 = a_1 - a_1\psi_1(h)\psi_n(h)^{-1} \neq 0$, pois $\psi_1(h) \neq \psi_n(h)$, contrariando a hipótese de indução.

□

Vejamos alguns conceitos de Álgebra Linear que serão utilizados no lema a seguir. Seja F um espaço vetorial de dimensão n sobre um corpo K. Dizemos que um polinômio $f \in K[x]$ anula a transformação linear $T\colon F \to F$ se $f(T) = 0$. O polinômio mônico de menor grau que anula T é chamado de polinômio minimal de T. O polinômio característico de T é dado por $det(Ix - T)$, onde I é a aplicação identidade. Pelo Teorema de Cayley-Hamilton [2], este polinômio é sempre mônico e de grau igual à dimensão de F, neste caso, n. Se existe um vetor $v \in F$ tal que $\{v, T(v), T^2(v), \ldots, T^{n-1}(v)\}$ gera o espaço vetorial F, então v é um vetor cíclico.

Lema 1.4.13. *Seja T um operador linear no espaço vetorial V de dimensão finita. Então T tem um vetor cíclico se, e somente se, os polinômios característicos e minimais de T forem idênticos.*

Demonstração. Sejam m_T e g_T os polinômios minimal e característico, respectivamente do operador linear T.

Suponha que α é um vetor cíclico de T. Então $\{\alpha, T(\alpha), T^2(\alpha), \ldots, T^{n-1}(\alpha)\}$ é uma base de V e $dim(V) = n$. Sabemos que $\deg(m_T) \leq \deg(g_T) = n$. Se $\deg(m_T) < n$, então

$$0 = m_T(\alpha) = c_0\alpha + c_1T(\alpha) + c_2T^2(\alpha) + \cdots + c_{n-1}T^{n-1}(\alpha)$$

com $c_0, c_1, \ldots, c_{n-1}$, não todos nulos, o que implica que $\{\alpha, T(\alpha), T^2(\alpha), \ldots, T^{n-1}(\alpha)\}$ é linearmente dependente. Contradição. Logo, $\deg(m_T) = n = \deg(g_T)$ e portanto, $m_T = g_T$.

Agora considere $m_T = g_T$ e suponha que não existe vetor cíclico em V. Então, o conjunto $\{\alpha, T(\alpha), T^2(\alpha), \ldots, T^{n-1}(\alpha)\}$ é linearmente dependente para todo $\alpha \in V$, e portanto, existem elementos $c_0, c_1, \ldots, c_{n-1} \in K$, não todos nulos, tais que

$$c_0\alpha + c_1T(\alpha) + c_2T^2(\alpha) + \cdots + c_{n-1}T^{n-1}(\alpha) = 0, \ \forall\alpha \in V.$$

Seja $q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in V[X]$. Temos que $q(T)(\alpha) = c_0\alpha + c_1T(\alpha) + c_2T^2(\alpha) + \cdots + c_{n-1}T^{n-1}(\alpha) = 0, \ \forall\alpha \in V$, e então, $q(T) = 0$, e portanto, $m_T|q$. Mas $n-1 \geq \deg(q) \geq \deg(m_T) = n$. Contradição. Portanto, existe vetor cíclico em V.

□

Lema 1.4.14. *(Teorema da Base Normal) Para todo corpo finito K e toda extensão finita F, existe uma base normal de F sobre K.*

Demonstração. Considere $n \geq 2$. Pelo Teorema 1.3.11 e o parágrafo que segue após sua demonstração, sabemos que os automorfismos de F sobre K são da forma $\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ onde $\sigma(\alpha) = \alpha^q \ \ \forall\alpha \in F$, σ^j indica a composição de σ consigo mesma j vezes, e ε é a aplicação identidade em F. Podemos afirmar que σ é um operador linear de F sobre K, pois estes automorfismos preservam as propriedades $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$, e $\sigma(c\alpha) = c \cdot \sigma(\alpha), \ \forall\alpha, \beta \in F, \ c \in K$. Como $\sigma^n = \varepsilon$, o polinômio $x^n - 1 \in K[X]$ anula σ, e portanto, o polinômio minimal de σ divide $x^n - 1$. Pelo Lema 1.4.12, aplicado em $\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{n-1}$, vemos que nenhum polinômio não nulo em $K[X]$ de grau menor que n anula σ. Logo, $x^n - 1$ é o minimal de σ. Como o polinômio característico de σ é mônico, de grau n, e divisível pelo minimal, segue que o polinômio característico também é $x^n - 1$. Logo, pelo Lema 1.4.13, existe um elemento $\alpha \in F$ tal que $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)$ geram o espaço vetorial F, e portanto é uma base de F sobre K. Como este conjunto é formado por um elemento α e seus conjugados com relação a K, esta é uma base normal de F sobre K.

□

Definição 1.4.15. *(Discriminante) Seja $F|K$ uma extensão de corpos finitos de grau n. O* ***discriminante*** *$\Delta_{F/K}(\alpha_1, \ldots, \alpha_n)$ dos elementos $\alpha_1, \ldots, \alpha_n \in F$ é definido como o determinante de ordem n dado por*

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} Tr_{F/K}(\alpha_1\alpha_1) & Tr_{F/K}(\alpha_1\alpha_2) & \cdots & Tr_{F/K}(\alpha_1\alpha_n) \\ Tr_{F/K}(\alpha_2\alpha_1) & Tr_{F/K}(\alpha_2\alpha_2) & \cdots & Tr_{F/K}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{F/K}(\alpha_n\alpha_1) & Tr_{F/K}(\alpha_n\alpha_2) & \cdots & Tr_{F/K}(\alpha_n\alpha_n) \end{vmatrix}$$

Por definição, $\Delta_{F/K}(\alpha_1, \ldots, \alpha_n) \in K$.

Teorema 1.4.16. *Sejam $F|K$ uma extensão de corpos finitos de grau n e $\alpha_1, \ldots, \alpha_n$ elementos de F. Então, $\{\alpha_1, \ldots, \alpha_n\}$ é base de F sobre K se, e somente se, $\Delta_{F/K}(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Demonstração. ($\Rightarrow$) Basta mostrar que cada vetor-linha da matriz é linearmente independente. Sejam $c_1, \ldots, c_n \in K$ tais que $c_1 Tr_{F/K}(\alpha_j\alpha_1) + \cdots + c_n Tr_{F/K}(\alpha_j\alpha_n) = 0$ para $1 \leq j \leq n$. Defina $\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$. Então, $Tr_{F/K}(\alpha_j\beta) = 0$ para $1 \leq j \leq n$. Como $\{\alpha_1, \ldots, \alpha_n\}$ é base de F sobre K, $Tr_{F/K}(\alpha\beta) = 0 \ \ \forall \alpha \in F$, ou seja, $\beta = 0$. Consequentemente, $c_1 = \cdots = c_n = 0$, e portanto, o conjunto $\{Tr_{F/K}(\alpha_j\alpha_1), \ldots, Tr_{F/K}(\alpha_j\alpha_n)\}$ é linearmente independente para $1 \leq j \leq n$.

($\Leftarrow$) Basta mostrar que $\{\alpha_1, \ldots, \alpha_n\}$ é linearmente independente. Sejam $c_1, \ldots, c_n$ elementos de K tais que $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$. Multiplicando a equação por um α_j fixo e aplicando o traço temos $c_1 Tr_{F/K}(\alpha_j\alpha_1) + \cdots + c_n Tr_{F/K}(\alpha_j\alpha_n) = 0$. Mas por hipótese os vetores-linha da matriz são linearmente independentes, então $c_1 = \cdots = c_n = 0$, logo, $\{\alpha_1, \ldots, \alpha_n\}$ é base de F sobre K.

□

Podemos utilizar outro determinante de ordem n, onde as entradas são elementos de F, com o mesmo propósito de $\Delta_{F/K}(\alpha_1, \ldots, \alpha_n)$. Sejam $\beta_1, \ldots, \beta_n \in F$, e A a matriz $n \times n$ cuja entrada na i-ésima linha e j-ésima coluna é igual a $\beta_j^{q^{i-1}}$, onde q é o número de elementos de K. Se A^T representa a matriz transposta de A, então $A^T \cdot A = B$ onde B é a matriz $n \times n$ cuja entrada na i-ésima linha e j-ésima coluna é igual a $Tr_{F/K}(\beta_i\beta_j)$.

Corolário 1.4.17. *Sejam $\beta_1, \ldots, \beta_n \in F$. O conjunto $\{\beta_1, \ldots, \beta_n\}$ é base de F sobre K se, e somente se,*

$$\begin{vmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ (\beta_1)^q & (\beta_2)^q & \cdots & (\beta_n)^q \\ \vdots & \vdots & \ddots & \vdots \\ (\beta_1)^{q^{n-1}} & (\beta_2)^{q^{n-1}} & \cdots & (\beta_n)^{q^{n-1}} \end{vmatrix} \neq 0.$$

Demonstração. Seja A a matriz definida acima.

Então, $A^T.A = \begin{bmatrix} Tr_{F/K}(\beta_1\beta_1) & Tr_{F/K}(\beta_1\beta_2) & \cdots & Tr_{F/K}(\beta_1\beta_n) \\ Tr_{F/K}(\beta_2\beta_1) & Tr_{F/K}(\beta_2\beta_2) & \cdots & Tr_{F/K}(\beta_2\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{F/K}(\beta_n\beta_1) & Tr_{F/K}(\beta_n\beta_2) & \cdots & Tr_{F/K}(\beta_n\beta_n) \end{bmatrix}$.

Logo, $\Delta_{F/K}(\beta_1, \ldots, \beta_n) = det(A^T.A) = det(A^T).det(A) = det(A)^2$. Sabemos que $det(A)^2 = 0 \Leftrightarrow det(A) = 0$, e então $\Delta_{F/K}(\beta_1, \ldots, \beta_n) = 0 \Leftrightarrow det(A) = 0$, e pelo Teorema 1.4.16, $det(A) = 0 \Leftrightarrow \{\beta_1, \ldots, \beta_n\}$ é base de F sobre K.

□

Vejamos agora uma definição importante que será utilizada no teorema seguinte e também nos próximos capítulos.

Definição 1.4.18. *(Matriz de Sylvester) Sejam dois polinômios em $K[X]$ da forma $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, $m, n \in \mathbb{N}$. A **matriz de Sylvester** S(f,g) destes dois polinômios é definida por*

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{bmatrix}$$

*e tem ordem $(m+n) \times (m+n)$. O determinante $R(f,g)$ de ordem $m+n$ desta matriz é chamado de **resultante** de f e g.*

Considerando γ_i uma raiz de f, e ζ_j um raiz de g, com $1 \leq i \leq n$ e $1 \leq j \leq m$, estes dois polinômios podem ser escritos como $f(x) = a_n(x - \gamma_1) \cdots (x - \gamma_n)$ e $g(x) = b_m(x-\zeta_1) \cdots (x-\zeta_m)$. Daí, é possível mostrar por indução que o determinante $R(f,g)$ pode ser escrito como

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\gamma_i - \zeta_j).$$

Assim podemos concluir que $R(f,g) = 0$ se, e somente se, f e g possuem uma raiz em comum, ou seja, se possuem um divisor comum de grau maior que zero.

Teorema 1.4.19. *Para todo $\alpha \in F$, os seus conjugados $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ formam uma base de F sobre K se, e somente se, os polinômios $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ e $x^n - 1$ em $F[X]$ são primos ente si.*

Demonstração. Definindo $\beta_1 = \alpha,\ \beta_2 = \alpha^q, \ldots, \beta_n = \alpha^{q^{n-1}}$, o determinante do Corolário 1.4.17, após algumas permutações de linhas, torna-se

$$\pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} \\ \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \alpha & \cdots & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{vmatrix}$$

Sejam $f(x) = x^n - 1$ e $g(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ em $F[X]$. Considere $R(f, g)$ o determinante de ordem $2n - 1$, e adicione

- a $(n + 1)$-ésima coluna à $1^{\underline{a}}$ coluna,
- a $(n + 2)$-ésima coluna à $2^{\underline{a}}$ coluna,

e assim por diante, até adicionar a $(2n + 1)$-ésima coluna à $(n + 1)$-ésima coluna. O determinante resultante se fatora como o produto do determinante da matriz de ordem $(n - 1) \times (n - 1)$ preenchida por -1 na diagonal principal e 0 nas demais entradas; e o determinante descrito acima. Isto é, é igual ao determinante acima a menos de sinal. Como $R(f, g) \neq 0$ se, e somente se, f e g são primos entre si, segue do Corolário 1.4.17 que $\{\beta_1, \ldots, \beta_n\} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ é base de F sobre K se, e somente se, f e g são primos ente si.

□

Este resultado nos levará à definição de um tipo particular de elemento, chamados de elementos k-normais, que será definido na Seção 3.3. Estes elementos são chave no objetivo principal deste trabalho.

Capítulo 2

Ferramentas úteis em Corpos Finitos

Neste capítulo apresentamos algumas ferramentas que serão úteis nos capítulos seguintes. Na primeira seção apresentamos definições e importantes resultados relacionados a polinômios linearizados (ou q-polinômios, onde q é uma potência de um número primo). Posteriormente, definimos e apresentamos propriedades de um tipo especial de homomorfismos de grupos, chamados de Caracteres, que podem estar relacionados ao grupo aditivo ou multiplicativo de um corpo finito. Por fim, definimos um caso particular de soma exponencial, denominados Soma de Gauss.

2.1 Polinômios linearizados

Polinômios desempenham um importante papel no estudo da estrutura algébrica de um corpo finito de forma geral. Polinômios irredutíveis são fundamentais na construção de corpos finitos e realização de cálculos com seus elementos.

Um tipo especial de polinômios é definido a seguir. Uma das principais utilidades destes polinômios é a facilidade na determinação do conjunto de suas raízes devido à sua estrutura, além de desempenhar um papel fundamental em caracterizações de elementos k-normais amplamente utilizadas.

Definição 2.1.1. *(q-polinômio) Sejam $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e $\alpha_0, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Um polinômio da forma*

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$$

*é chamado de q-**polinômio** (ou polinômio linearizado) sobre $\mathbb{F}_{q^n}$.*

Se $\mathbb{F}_{q^s}$ é uma extensão de $\mathbb{F}_{q^n}$, então

$$\begin{aligned} L(\beta+\gamma) &= \sum_{i=0}^{m} \alpha_i (\beta+\gamma)^{q^i} = \sum_{i=0}^{m} \alpha_i (\beta^{q^i} + \gamma^{q^i}) \\ &= \sum_{i=0}^{m} \alpha_i \beta^{q^i} + \sum_{i=0}^{m} \alpha_i \gamma^{q^i} = L(\beta) + L(\gamma) \end{aligned}$$

e também

$$L(c\beta) = \sum_{i=0}^{m} \alpha_i (c\beta)^{q^i} = \sum_{i=0}^{m} \alpha_i (c^{q^i} \beta^{q^i}) = \sum_{i=0}^{m} \alpha_i (c\beta^{q^i})$$
$$= c \sum_{i=0}^{m} \alpha_i (\beta^{q^i}) = cL(\beta)$$

para todo $\beta, \gamma \in \mathbb{F}_{q^s},\ c \in \mathbb{F}_q$. Isso mostra que $L(x)$ é um operador linear de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$.

Teorema 2.1.2. *Sejam $L(x)$ um q-polinômio não nulo sobre $\mathbb{F}_{q^n}$ e $\mathbb{F}_{q^s}$ uma extensão de $\mathbb{F}_{q^n}$ contendo todas as raízes de $L(x)$. Então, todas as raízes de $L(x)$ tem a mesma multiplicidade, igual a 1 ou uma potência de q. Além disso, estas raízes formam um subespaço vetorial de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$.*

Demonstração. Das considerações após a Definição 2.1.1, temos que qualquer combinação linear de raízes com coeficientes em $\mathbb{F}_q$ é também uma raiz de $L(x)$. Logo, este conjunto é um subespaço vetorial de $\mathbb{F}_{q^s}$. Além disso, a derivada de $L(x)$ é $L'(x) = \alpha_0$, ou seja, $L(x)$ tem apenas raízes simples caso $\alpha_0 \neq 0$. Caso contrário, seja k o menor índice tal que $\alpha_k \neq 0$, isto é, $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$. Então,

$$L(x) = \sum_{i=k}^{m} \alpha_i x^{q^i} = \sum_{i=k}^{m} \alpha_i^{(q^{nk})} x^{q^i} = \left(\sum_{i=k}^{m} \alpha_i^{\left(q^{(n-1)k}\right)} x^{q^{i-k}} \right)^{q^k} = \left(\sum_{i=0}^{m-k} \alpha_i x^{q^i} \right)^{q^k}$$

que é a q^k-ésima potência de um q-polinômio que possui apenas raízes simples. Logo, as raízes de $L(x)$ neste caso tem multiplicidade q^k.

□

Lema 2.1.3. *Sejam $\beta_1, \ldots, \beta_m \in \mathbb{F}_{q^n}$. Então*

$$\begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{m-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{m-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_m & \beta_m^q & \beta_m^{q^2} & \cdots & \beta_m^{q^{m-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{m-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k \right)$$

e assim este determinante é diferente de zero se, e somente se, $\beta_1, \ldots, \beta_m$ são linearmente independentes sobre $\mathbb{F}_q$.

Demonstração. Seja D_m o determinante do lado esquerdo da equação acima. Vamos utilizar o método de indução sobre m. A equação é válida para $m = 1$. Suponha que o resultado é válido para algum $m > 1$. Considere o polinômio

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{m-1}} & \beta_1^{q^m} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{m-1}} & \beta_2^{q^m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \beta_m & \beta_m^q & \beta_m^{q^2} & \cdots & \beta_m^{q^{m-1}} & \beta_m^{q^m} \\ x & x^q & x^{q^2} & \cdots & x^{q^{m-1}} & x^{q^m} \end{vmatrix} = D_m x^{q^m} + \sum_{i=o}^{m-1} \alpha_i x^{q^i}$$

onde $\alpha_i \in \mathbb{F}_{q^n}$ é o determinante da matriz $n \times n$ resultante após eliminarmos a última linha e a i-ésima coluna, para $0 \leq i \leq m-1$.

Se $\beta_1, \ldots, \beta_m$ são linearmente independentes sobre $\mathbb{F}_q$, então temos $D(\beta_k) = 0$ para $1 \leq k \leq m$. Como $D(x)$ é um q-polinômio sobre $\mathbb{F}_{q^n}$, todas as combinações lineares $c_1\beta_1 + \cdots + c_m\beta_m$, com $c_1, \ldots, c_m \in \mathbb{F}_{q^n}$ são raízes de $D(x)$, e como estas q^m raízes são distintas,

$$D(x) = D_m \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(x - \sum_{k=1}^{m} c_k\beta_k \right).$$

Agora, se $\beta_1, \ldots, \beta_m$ são linearmente dependentes sobre $\mathbb{F}_q$, então $D_m = 0$ e existem $b_1, \ldots, b_m \in \mathbb{F}_q$, pelo menos um não nulo, tais que $b_1\beta_1 + \cdots + b_m\beta_m = 0$. Assim,

$$\sum_{k=1}^{m} b_k\beta_k^{q^j} = \sum_{k=1}^{m} b_k^{q^j}\beta_k^{q^j} = \sum_{k=1}^{m} (b_k\beta_k)^{q^j} = \left(\sum_{k=1}^{m} b_k\beta_k \right)^{q^j} = 0, \text{ para } 0 \leq j \leq m,$$

e as primeiras m linhas de $D(x)$ são linearmente dependentes sobre $\mathbb{F}_q$. Logo, temos $D(x) = 0$, e consequentemente,

$$D(x) = D_m \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(x - \sum_{k=1}^{m} c_k\beta_k \right).$$

Portanto,

$$D_{m+1} = D(\beta_{m+1}) = D_m \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(\beta_{m+1} - \sum_{k=1}^{m} c_k\beta_k \right)$$

e a tese está provada por indução em m.

□

Teorema 2.1.4. *Seja U um subespaço vetorial de $\mathbb{F}_{q^n}$, que por sua vez é um espaço vetorial sobre $\mathbb{F}_q$. Então para todo k natural, o polinômio*

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

é um q-polinômio sobre $\mathbb{F}_{q^n}$.

Demonstração. Como a q^k-ésima potência de um q-polinômio é também um q-polinômio, basta provar o caso $k = 0$. Sejam $\{\beta_1, \ldots, \beta_m\}$ uma base de U, D_m e $D(x)$ os determinantes do lema anterior. Como $\beta \in U$, existem $c_1, \ldots, c_m \in \mathbb{F}_q$ tais que $\beta = c_1\beta_1 + \cdots + c_m\beta_m$, e então

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k} = \prod_{c_1,\ldots,c_m} \left(x - \sum_{i=1}^{m} c_i\beta_i \right) = D_m^{-1} D(x).$$

Como $D(x)$ é um q-polinômio, $L(x)$ também é um q-polinômio.

□

Considerando q-polinômios sobre $\mathbb{F}_q$, é possível verificar que a composição (também chamada de multiplicação simbólica) de polinômios é comutativa, associativa e distributiva. O conjunto de q-polinômios sobre $\mathbb{F}_q$ é um domínio de integridade com as operações de adição usual e multiplicação simbólica, operação que se relaciona com polinômios através do seguinte conceito.

Definição 2.1.5. *(polinômios q-associados) Os polinômios*

$$l(x) = \sum_{i=o}^{m} \alpha_i x^i \quad e \quad L(x) = \sum_{i=o}^{m} \alpha_i x^{q^i}$$

*sobre $\mathbb{F}_{q^n}$ são chamados de **q-associados** um do outro. Mais especificamente, $l(x)$ é q-associado convencional de $L(x)$, e $L(x)$ é q-associado linearizado de $l(x)$.*

Teorema 2.1.6. *Sejam $f, g \in \mathbb{F}_q[X]$ tais que $f(x) = \sum_{i=0}^{r} a_i x^i$, $g(x) = \sum_{j=0}^{t} b_j x^j$, e $L_f(x), L_g(x)$ seus respectivos polinômios q-associados. Então,*

(i) $L_f(x) + L_g(x) = L_{f+g}(x)$;

(ii) $L_{fg}(x) = L_f\left(L_g(x)\right) = L_g\left(L_f(x)\right)$.

Demonstração. (i) Seja $w = \max(r, t)$. Então,

$$L_{f+g}(x) = \sum_{i=0}^{w} (a_i + b_i) x^{q^i} = \sum_{i=0}^{w} a_i x^{q^i} + \sum_{i=0}^{w} b_i x^{q^i} = L_f(x) + L_g(x).$$

(ii) Dado que $f(x).g(x) = \sum_{i=0}^{r} \sum_{j=o}^{t} a_i b_j x^{i+j}$, temos

$$\begin{aligned} L_f\left(L_g(x)\right) = L_f\left(\sum_{j=0}^{t} b_j x^{q^j}\right) &= \sum_{i=0}^{r} a_i \left(\sum_{j=0}^{t} b_j x^{q^j}\right)^{q^i} \\ &= \sum_{i=0}^{r} \sum_{j=o}^{t} a_i b_j x^{q^{i+j}} = L_{fg}(x). \end{aligned}$$

Analogamente, $L_g\left(L_f(x)\right) = L_{fg}(x)$.

□

Definição 2.1.7. *(q-módulo) Seja $\mathcal{M}$ um espaço vetorial sobre $\mathbb{F}_q$ contido em alguma extensão de $\mathbb{F}_q$. Se a q-ésima potência de todo elemento de $\mathcal{M}$ pertence a $\mathcal{M}$, então $\mathcal{M}$ é um **q-módulo**.*

Teorema 2.1.8. *O polinômio mônico $L(x)$ é um q-polinômio sobre $\mathbb{F}_q$ se, e somente se, todas as raízes de $L(x)$ tem a mesma multiplicidade, igual a 1 ou uma potência de q, e estas raízes formam um q-módulo.*

Demonstração. ($\Rightarrow$) Segue do Teorema 2.1.2 e do fato que a q-ésima potência de uma raiz de $L(x)$ também é uma raiz de $L(x)$. Logo, o conjunto destas raízes formam um q-módulo.
($\Leftarrow$) Pelo Teorema 2.1.4, $L(x)$ é um q-polinômio sobre alguma extensão de $\mathbb{F}_q$. Seja $\mathcal{M}$ o q-módulo formado por todas as raízes de $L(x)$. Então existe k natural tal que $L(x) = \prod_{\beta\in\mathcal{M}}(x-\beta)^{q^k}$. Como $\mathcal{M} = \{\beta^q \mid \beta \in \mathcal{M}\}$, temos

$$L(x)^q = \left(\prod_{\beta\in\mathcal{M}}(x-\beta)^{q^k}\right)^q = \prod_{\beta\in\mathcal{M}}(x^q-\beta^q)^{q^k} = \prod_{\beta\in\mathcal{M}}(x^q-\beta)^{q^k} = L(x^q).$$

Isso quer dizer que se $L(x) = \sum_{i=0}^{m}\alpha_i x^{q^i}$, então

$$\sum_{i=0}^{m}\alpha_i^q x^{q^{i+1}} = L(x)^q = L(x^q) = \sum_{i=0}^{m}\alpha_i x^{q^{i+1}}.$$

Ou seja, para $0 \le i \le m$, $\alpha_i^q = \alpha_i \Rightarrow \alpha_i \in \mathbb{F}_q$. Portanto, $L(x)$ é um q-polinômio sobre $\mathbb{F}_q$.

□

Apresentamos, agora, dois conceitos fundamentais no decorrer deste trabalho.

Definição 2.1.9. *(Raiz q-primitiva) Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$, e L(x) um q-polinômio sobre $\mathbb{F}_{q^n}$. Dizemos que α é uma* ***raiz q-primitiva*** *de L(x) se α não é raiz de nenhum q-polinômio de grau menor que $L(x)$.*

Dado um elemento $\alpha \in \mathbb{F}_{q^n}$, definimos o conjunto de anuladores de α como $\mathcal{L}_\alpha = \{f \in \mathbb{F}_q[X] \,/\, L_f(\alpha) = 0\}$, onde $L_f(\alpha)$ é o q-polinômio associado de f aplicado em α. Pelo Teorema 2.1.6, $\mathcal{L}_\alpha$ é um ideal, e como $\mathbb{F}_q[X]$ é um domínio principal, este ideal possui um gerador.

Definição 2.1.10. *($\mathbb{F}_q$-ordem) O polinômio mônico que gera o ideal $\mathcal{L}_\alpha$ é chamado de* ***$\mathbb{F}_q$-ordem*** *de α, e é denotado por* ***Ord(α)****.*

Note que α é uma raiz q-primitiva do q-polinômio associado de $Ord(\alpha)$. Dado um elemento $\alpha \in \mathbb{F}_q$, se $\alpha = 0$ então $Ord(\alpha) = 1$. Caso contrário, seja $f(x) = x - 1$. Temos que $L_f(x) = x^q - x \;\Rightarrow\; L_f(\alpha) = \alpha^q - \alpha = 0$. Logo, $Ord(\alpha) = x-1$, $\forall \alpha \in \mathbb{F}_q{}^*$. Além disso, para $\alpha \in \mathbb{F}_{q^n}$, $\alpha^{q^n} - \alpha = 0$, o que implica que $Ord(\alpha) \mid (x^n - 1)$, $\forall \alpha \in \mathbb{F}_{q^n}$.

2.2 Caracteres

Somas exponenciais são uma ferramenta importante na resolução de problemas na Teoria dos Números, como o Problema de Waring [9]. Um tipo particular destas somas é útil em Corpos Finitos, e envolve um tipo de homomorfismo que é definido a seguir. Nesta seção, G será sempre um grupo abeliano finito, a menos que seja especificado.

Definição 2.2.1. *(Caracter) Um* ***caracter*** χ *de* G *é um homomorfismo de* G *no grupo multiplicativo* U *dos números complexos de módulo igual a 1, isto é, uma função* $\chi\colon G \to U \subset \mathbb{C}^*$*. O conjunto de todos os caracteres de* G *é denotado por* $\widehat{G}$ *e é um grupo abeliano sob a multiplicação de caracteres.*

O caracter χ_0 de G definido por $\chi_0(g) = 1,\ \forall g \in G$, chamado de **caracter trivial**, é considerado a identidade do grupo $\widehat{G}$.

Teorema 2.2.2. *Seja* χ *um caracter de* G*. Então*

(i) $\chi(g_1g_2) = \chi(g_1)\chi(g_2),\ \forall g_1, g_2 \in G$*;*

(ii) $\chi_1(g)\chi_2(g)\dots\chi_n(g) = (\chi_1\chi_2\dots\chi_n)(g),\ \forall g \in G$*;*

(iii) $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1,\ \forall g \in G$*;*

(iv) $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1,\ \forall g \in G$*;*

(v) $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)},\ \forall g \in G$*, onde* $\overline{\chi(g)}$ *é o conjugado complexo de* $\chi(g)$*.*

Demonstração. (i) Segue diretamente da definição.

(ii) Segue diretamente da definição. Neste caso, se $\chi_1 = \chi_2 = \cdots = \chi_n = \chi$, escrevemos χ^n.

(iii) Dado $g \in G$, $\chi(g)^{|G|} = \underbrace{\chi(g)\chi(g)\dots\chi(g)}_{|G| \text{ vezes}} = \chi(g^{|G|}) = \chi(1_G) = 1$.

(iv) Segue diretamente da definição.

(v) Pelo item anterior, $\chi(g)\chi(g^{-1}) = 1$, e como $\chi(g)\chi(g)^{-1} = 1$, temos que $\chi(g^{-1}) = \chi(g)^{-1}$. Como as imagens são complexos de módulo 1, $\chi(g)^{-1} = \overline{\chi(g)}$. □

Exemplo 2.2.3. *Se* G *é um grupo cíclico de ordem* n *e gerador* g*,* $\chi_j(g^k) = e^{\frac{2\pi ijk}{n}}$ *para* $0 \leq j \leq n-1$*, é um caracter de* G*. Por outro lado, se* χ *é um caracter qualquer de* G*, então* $\chi(g)$ *é uma raiz* n*-ésima da unidade. Logo,*

$$1 = \chi(g)^n = e^{i\theta n} = cos(\theta n) + i \cdot sen(\theta n) \ \Rightarrow\ \theta = \frac{2\pi j}{n}$$

para algum j *com* $0 \leq j \leq n-1$*, o que implica que*

$$\chi(g) = e^{i\theta} = e^{\frac{2\pi ij}{n}}.$$

Teorema 2.2.4. *Sejam* H *um subgrupo de* G*, e* ψ *um caracter de* H*. Então* ψ *pode ser extendido a um caracter de* G*, isto é, existe um caracter* χ *de* G *tal que* $\chi(h) = \psi(h)$ *para todo* $h \in H$*.*

Demonstração. Seja $a \in G$ tal que $a \notin H$. Considere H_1 o subgrupo de G gerado por a e H, e m o menor inteiro positivo tal que $a^m \in H$. Daí, todo elemento $g \in H_1$ pode ser escrito (unicamente) como $g = a^j h$ com $0 \leq j \leq m-1$ e $h \in H$. Defina ψ_1 sobre H_1 dada por $\psi_1(g) = w^j \psi(h)$, onde w é um número complexo fixado tal que $w^m = \psi(a^m)$. Vejamos que ψ_1 é caracter de H_1. Sejam $g_1 = a^k h_1,\ 0 \leq k \leq m-1$, e $h_1 \in H$.

- Se $j + k \leq m - 1$, então

$$\psi_1(gg_1) = w^{j+k}\psi(hh_1) = w^j\psi(h)w^k\psi(h_1) = \psi_1(g)\psi_1(g_1).$$

- Se $j + k > m - 1$, então $gg_1 = a^{j+k-m}(a^m hh_1)$, daí

$$\begin{aligned}\psi_1(gg_1) &= w^{j+k-m}\psi(a^m hh_1) = w^{j+k-m}\psi(a^m)\psi(hh_1)\\ &= w^{j+k}\psi(hh_1) = \psi(g)\psi(g_1).\end{aligned}$$

Além disso, $\psi_1(h) = \psi(h),\ \forall h \in H$. Se $H_1 = G$, o teorema está provado. Se H_1 está contido propriamente em G, o processo pode ser repetido um número finito de vezes até chegarmos a uma extensão de ψ a G.

□

Corolário 2.2.5. *Para todo $g_1, g_2 \in G,\ g_1 \neq g_2$, existe um caracter χ de G tal que $\chi(g_1) \neq \chi(g_2)$.*

Demonstração. Sejam $h = g_1 g_2^{-1} \neq 1_G$ e H o subgrupo de G gerado por h. Defina ψ um caracter de H tal que $\psi(h^k) = e^{\frac{2\pi i k}{n}},\ n = |G| > 1$. Logo, $\psi(h) = e^{\frac{2\pi i}{n}}$, e então $\psi(g_1 g_2^{-1}) = \psi(h) = e^{\frac{2\pi i}{n}} \neq 1$. Pelo teorema anterior, ψ pode ser extendido a um caracter χ de G. Como $g_1 = hg_2$, temos que $\chi(g_1) = \chi(hg_2) = \chi(h)\chi(g_2) \neq \chi(g_2)$.

□

Teorema 2.2.6. *Se χ é um caracter não-trivial de G, então*

$$\sum_{g \in G} \chi(g) = 0.$$

Para $g \in G,\ g \neq 1_G$,

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

Demonstração. Com χ é não-trivial, existe $h \in G$ tal que $\chi(h) \neq 1$. Daí,

$$\chi(h)\sum_{g \in G}\chi(g) = \sum_{g \in G}\chi(hg) = \sum_{g \in G}\chi(g),$$

pois se g percorre todos os elementos de G, hg também percorre. Mas $\chi(h) \neq 1$, então $\sum\limits_{g \in G}\chi(g) = 0$. Analogamente, se $g \neq 1_G$ então existe $\psi \in \widehat{G}$ tal que $\psi(g) \neq 1$. Daí,

$$\psi(g)\sum_{\chi \in \widehat{G}}\chi(g) = \sum_{\chi \in \widehat{G}}(\psi\chi)(g) = \sum_{\chi \in \widehat{G}}\chi(g),$$

pois se χ percorre todos os caracteres de G, $\psi\chi$ também percorre. Mas $\psi(g) \neq 1$, então $\sum_{\chi \in \widehat{G}} \chi(g) = 0$.

□

Teorema 2.2.7. *O número de caracteres de um grupo abeliano finito G é igual a $|G|$.*

Demonstração. Pela ortogonalidade dos caracteres temos que

$$|\widehat{G}| = \sum_{g \in G} \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) = |G|.$$

□

Os teoremas 2.2.6 e 2.2.7 nos levam às relações de ortogonalidade para caracteres. Sejam χ e ψ caracteres de G. Então

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0, \text{ se } \chi \neq \psi; \\ 1, \text{ se } \chi = \psi. \end{cases}$$

O primeiro caso é obtido ao aplicar o Teorema 2.2.6 ao caracter $\chi\overline{\psi}$; e para o segundo caso temos que $\chi(g)\overline{\psi(g)} = \chi(g)\overline{\chi(g)} = 1$, portanto o somatório é igual a ordem de G.

Analogamente, se g e h são elementos de G, então

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0, \text{ se } g \neq h; \\ 1, \text{ se } g = h. \end{cases}$$

Em um corpo finito $\mathbb{F}_{q^n}$, temos dois grupos abelianos finitos: o próprio corpo $\mathbb{F}_{q^n}$ é um grupo sob a adição, e $\mathbb{F}_{q^n}^*$ forma um grupo sob a multiplicação. No Capítulo 3 faremos uma distinção entre os caracteres pertencentes a estes dois grupos.

2.3 Soma de Gauss

Como mencionado no início da seção anterior, somas exponenciais envolvendo caracteres são chamadas de Soma de Caracteres. Definimos agora um dos tipos mais importantes deste caso no contexto de corpos finitos, pela propriedade que possuem de juntar as estruturas aditiva e multiplicativa.

Definição 2.3.1. *(Soma de Gauss) Sejam χ um caracter do grupo aditivo $\mathbb{F}_{q^n}$, e ψ um caracter do grupo multiplicativo $\mathbb{F}_{q^n}^*$. A **Soma de Gauss** $G(\chi, \psi)$ é dada por*

$$G(\chi, \psi) = \sum_{c \in \mathbb{F}_{q^n}^*} \chi(c)\psi(c).$$

O valor máximo para $G(\chi, \psi)$ é $q^n - 1$.

Teorema 2.3.2. *Sejam χ e ψ caracteres aditivo e multiplicativo de $\mathbb{F}_{q^n}$, respectivamente. A Soma de Gauss $G(\chi, \psi)$ satisfaz*

$$G(\chi,\psi) = \begin{cases} q^n - 1, & se\ \chi = \chi_0\ e\ \psi = \psi_0; \\ 0 \quad , & se\ \chi = \chi_0\ e\ \psi \neq \psi_0; \\ -1 \quad , & se\ \chi \neq \chi_0\ e\ \psi = \psi_0. \end{cases}$$

Se $\chi \neq \chi_0$ e $\psi \neq \psi_0$, então $|G(\chi, \psi)| = q^{n/2}$.

Demonstração. No primeiro caso $\chi(c)\psi(c) = 1,\ \forall c \in \mathbb{F}_{q^n}$. O segundo caso está provado pelo Teorema 2.2.6. No terceiro caso temos

$$G(\chi,\psi_0) = \sum_{c\in\mathbb{F}_{q^n}^*} \chi(c) = \sum_{c\in\mathbb{F}_{q^n}} \chi(c) - \chi(0) \ = \ 0 - 1 \ = \ -1.$$

Agora, se $\chi \neq \chi_0$ e $\psi \neq \psi_0$, temos

$$\begin{aligned} |G(\chi,\psi)|^2 = G(\chi,\psi)\overline{G(\chi,\psi)} &= \sum_{c\in\mathbb{F}_{q^n}^*} \chi(c)\psi(c) \sum_{d\in\mathbb{F}_{q^n}^*} \overline{\chi(d)\psi(d)} \\ &= \sum_{c\in\mathbb{F}_{q^n}^*} \sum_{d\in\mathbb{F}_{q^n}^*} \chi(c)\psi(c)\overline{\chi(d)\psi(d)} \\ &= \sum_{c\in\mathbb{F}_{q^n}^*} \sum_{d\in\mathbb{F}_{q^n}^*} \chi(c-d)\ \psi(cd^{-1}). \end{aligned}$$

Fazendo $s = cd^{-1}$ obtemos

$$\begin{aligned} |G(\chi,\psi)|^2 &= \sum_{d\in\mathbb{F}_{q^n}^*} \sum_{s\in\mathbb{F}_{q^n}^*} \chi(d(s-1))\ \psi(s) = \sum_{s\in\mathbb{F}_{q^n}^*} \psi(s) \left(\sum_{d\in\mathbb{F}_{q^n}^*} \chi(d(s-1)) \right) \\ &= \sum_{s\in\mathbb{F}_{q^n}^*} \psi(s) \left(\sum_{d\in\mathbb{F}_{q^n}} \chi(d(s-1)) - \chi(0) \right) = \sum_{s\in\mathbb{F}_{q^n}^*} \psi(s) \sum_{d\in\mathbb{F}_{q^n}} \chi(d(s-1)). \end{aligned}$$

O somatório interior será igual a q^n caso $s = 1$, e igual a 0 caso contrário. Portanto, $|G(\chi, \psi)|^2 = \psi(1)q^n = q^n \Longrightarrow |G(\chi, \psi)| = q^{n/2}$.

□

Apresentamos a seguir dois resultados que são úteis para estimar somas de caracteres mais complexas.

Lema 2.3.3. *[13, Teorema 5.41] Seja ψ um caracter multiplicativo de $\mathbb{F}_{q^n}$ de ordem $r > 1$, e $f \in \mathbb{F}_{q^n}[X]$ um polinômio mônico tal que f não é da forma $g(x)^r$ para algum $g \in \mathbb{F}_{q^n}[X]$ com grau maior ou igual a 1. Suponha que s é o número de raízes distintas de f em seu corpo de decomposição sobre $\mathbb{F}_{q^n}$. Para todo $a \in \mathbb{F}_{q^n}$,*

$$\left| \sum_{c \in \mathbb{F}_{q^n}} \psi(af(c)) \right| \leq (s-1)q^{n/2}.$$

Lema 2.3.4. *[18, Teorema 2G] Sejam ψ um caracter multiplicativo de $\mathbb{F}_{q^n}$ de ordem $d \neq 1$, e χ um caracter aditivo não-trivial de $\mathbb{F}_{q^n}$. Se $f \in \mathbb{F}_{q^n}[X]$ tem exatamente m raízes, e $\deg(g) = s$, com $g \in \mathbb{F}_{q^n}[X]$, tais que $mdc(d, \deg(f)) = mdc(s, q) = 1$, então*

$$\left| \sum_{c \in \mathbb{F}_{q^n}} \psi(f(c))\ \chi(g(c)) \right| \leq (m+s-1)q^{n/2}.$$

Estes resultados fornecem condições para existência de elementos primitivos k-normais, conceito abordado no Capítulo 4, e que são o foco deste trabalho.

Capítulo 3

Elementos especiais em Corpos Finitos

Neste capítulo apresentamos um conceito chave para o principal objetivo deste trabalho. A partir de um elemento normal, em [10] os autores introduzem uma generalização destes elementos, chamados de k-normais. Para introduzí-los, nas duas primeiras seções apresentamos o conceito de *liberdade* para números e polinômios. Na literatura, embora esta ideia apareça inicialmente em [4] e [7], o termo é formalizado em [6]. Em [10], os autores introduzem a ideia de liberdade para polinômios.

Na terceira seção, definimos os elementos k-normais e importantes propriedades destes elementos. Um elemento k-normal funciona como um gerador de uma "extensão parcial" com $n-k$ de seus conjugados.

Definição 3.0.1. *(Elemento livre de quadrados) Seja m um número inteiro positivo. Então m é* ***livre de quadrados*** *se não contém quadrados em sua decomposição em fatores primos. Isto é, se m se escreve como $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ com p_i primo, então $k_i = 1$ para $1 \leq i \leq r$.*

Analogamente, seja $M \in \mathbb{F}_q[X]$. Então M é livre de quadrados se não contém quadrados em sua decomposição em polinômios irredutíveis. Isto é, se M se escreve como $M = P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$ com P_i irredutível, então $k_i = 1$ para $1 \leq i \leq r$.

Definição 3.0.2. *Dado um inteiro positivo n, denotamos por $rad(n)$ o maior divisor positivo livre de quadrados de n. Em outras palavras, $rad(n)$ é o produto dos fatores primos de n.*

Na Teoria dos Números, duas conhecidas funções aritméticas para um número inteiro positivo n são a Função de Euler e a Função de Möbius. A seguir, definimos estas funções para polinômios.

Definição 3.0.3. *(Função ϕ de Euler para polinômios) Seja $f \in \mathbb{F}_q[X]$ um polinômio mônico. A Função ϕ de Euler para f é dada por*

$$\phi_q(f) = \left| \left(\frac{\mathbb{F}_q[X]}{\langle f \rangle} \right)^* \right|,$$

onde $\langle f \rangle$ é o ideal gerado por f. Esta função fornece a quantidade de polinômios g tais que $\deg(g) \leq \deg(f)$ e $mdc(f, g) = 1$.

Definição 3.0.4. *(Função de Möbius para polinômios) Seja $f \in \mathbb{F}_q[X]$. A Função μ de Möbius para um polinômio é dada por*

$$\mu_q(f) = \begin{cases} 0 \ , \text{ se } f \text{ não for livre de quadrados;} \\ (-1)^r, \text{ se } f \text{ for um produto de } r \text{ fatores irredutíveis distintos.} \end{cases}$$

3.1 Elementos m-livres

Definição 3.1.1. *(Elemento m-livre) Seja $\alpha \in \mathbb{F}_{q^n}$. Dado m divisor de $q^n - 1$, α é m-**livre** se $\alpha = \beta^d$ implica $d = 1$ e $\alpha = \beta$ para todo d divisor de m.*

Sabemos que $\mathbb{F}_{q^n}$ tem $\phi(q^n - 1)$ elementos primitivos (Teorema 1.1.7). Pela definição anterior, podemos ver que α é primitivo se, e somente se, α é $(q^n - 1)$-livre.

Proposição 3.1.2. *Sejam m divisor de $q^n - 1$. Para $\alpha \in \mathbb{F}_{q^n}$,*

(i) Para todo r divisor de m, se α é m-livre então α é r-livre;

(ii) Para todo r divisor de m, se $rad(m)|r$, então α é m-livre se, e somente se, α é r-livre;

(iii) α é m-livre se, e somente se, $mdc\left(\frac{q^n-1}{ord(\alpha)}, m\right) = 1$.

Demonstração. (i) Seja d divisor de r, $\alpha = \beta^d$. Como $d|r$ e $r|m$, temos que $d|m$, e como α é m-livre, temos que $d = 1$. Logo, α é r-livre.

(ii) Pelo item anterior, se α é m-livre então α é r-livre. Agora suponha que α não é m-livre. Então, existe d divisor de m tal que $d \neq 1$ e $\alpha = \beta^d$. Como $z := mdc(d, rad(m)) \neq 1$, temos que $\alpha = \beta^d = (\beta^{\frac{d}{z}})^z$, ou seja, α é uma z-ésima potência de um elemento de $\mathbb{F}_{q^n}$ onde $z|r$ e $z \neq 1$. Logo, α não é r-livre.

(iii) Seja $\alpha \in \mathbb{F}_{q^n}$, e $ord(\alpha) = \frac{q^n-1}{s}$. Sem perda de generalidade, suponha que $\alpha = \eta^s$ onde η é um elemento primitivo de $\mathbb{F}_{q^n}$.

($\Rightarrow$) Seja $s_0 = mdc(s, m)$, $s = s_0 s_1$ para algum $s_1 \in \mathbb{Z}$. Suponha que $s_0 > 1$. Como $\alpha = \eta^s = \eta^{s_0 s_1} = (\eta^{s_1})^{s_0}$, temos que α não é m-livre.

($\Leftarrow$) Considere agora $mdc(s,m) = 1$ e suponha que $\alpha = \beta^d$, onde $\beta \in \mathbb{F}_{q^n}$ e $d|m$. Temos que $\beta = \eta^i$ para algum i com $1 \leq i \leq q^n - 1$. Então $\eta^s = \alpha = \beta^d = (\eta^i)^d = \eta^{id}$, o que implica $s \equiv id \pmod{q^n - 1}$, ou seja, $s = id + c(q^n - 1)$ para algum $c \in \mathbb{Z}$. Como $d|m$ e $m|(q^n - 1)$, temos que $d|(q^n - 1)$, e assim $d|(id + c(q^n - 1))$, ou seja $d|s$, e como $mdc(s,m) = 1$, temos que $d = 1$.

□

Considere o grupo multiplicativo $\mathbb{F}_{q^n}^*$. Os caracteres deste grupo são definidos diretamente através do Exemplo 2.2.3, já que $\mathbb{F}_{q^n}^*$ é um grupo cíclico de ordem $q^n - 1$ (Teorema 1.2.10). Este conceito é formalizado no teorema a seguir.

Teorema 3.1.3. *Seja g um elemento primitivo fixo de $\mathbb{F}_{q^n}^*$. Para $j = 0, 1, \ldots, q^n - 2$, a função ψ_j dada por*

$$\psi_j(g^k) = e^{\frac{2\pi ijk}{q^n - 1}} \text{ para } k = 0, 1, \ldots, q^n - 2$$

define um caracter multiplicativo de $\mathbb{F}_{q^n}^*$, e todo caracter multiplicativo de $\mathbb{F}_{q^n}^*$ é obtido desta forma.

Demonstração. Segue diretamente do Exemplo 2.2.3.

□

Como $\psi_0(g^k) = 1$ para todo $k = 0, 1, \ldots, q - 2$, ψ_0 será sempre o caracter multiplicativo trivial.

Corolário 3.1.4. *O grupo de caracteres multiplicativos de $\mathbb{F}_{q^n}^*$, denotado por $\widehat{\mathbb{F}_{q^n}^*}$, é cíclico, de ordem $q^n - 1$, e tem como identidade o caracter trivial ψ_0.*

Demonstração. Vamos denotar por $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ o grupo dos inteiros módulo $q^n - 1$. Vejamos que $\widehat{\mathbb{F}_{q^n}^*}$ é isomorfo a $\mathbb{Z}/(q^n - 1)\mathbb{Z}$. Seja

$$\begin{aligned} \varphi \colon \widehat{\mathbb{F}_{q^n}^*} &\to \mathbb{Z}/(q^n - 1)\mathbb{Z} \\ \psi_j &\mapsto j. \end{aligned}$$

Temos que

$$(\psi_j \cdot \psi_l)(g^k) = \psi_j(g^k)\psi_l(g^k) = e^{\frac{2\pi ijk}{q^n - 1}} e^{\frac{2\pi ilk}{q^n - 1}} = e^{\frac{2\pi i(j+l)k}{q^n - 1}} = \psi_{((j+l) \pmod{q^n - 1})}(g^k).$$

Portanto, φ é um homomorfismo. Agora seja $j = s(q^n - 1)$. Temos $\psi_j(g^k) = \psi_{s(q^n-1)}(g^k) = \psi_{(q^n-1)}(g^k)^s = 1^s = 1$, ou seja, $\psi_j = \psi_0$. Portanto ψ é um isomorfismo, e assim $\widehat{\mathbb{F}_{q^n}^*}$ é cíclico pois $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ é cíclico e possui $\phi(q^n - 1)$ geradores. A identidade de $\widehat{\mathbb{F}_{q^n}^*}$ é dada por ψ_0.

□

Podemos definir a ordem de um caracter multiplicativo ψ, denotada por $ord(\psi)$, como o menor inteiro positivo d tal que $\psi(\alpha)^d = \psi_0(\alpha) = 1,\ \forall \alpha \in \mathbb{F}_{q^n}^*$. Veremos a seguir o teorema que define a função característica dos elementos m-livres. Considere a notação:

$$\int_{d|t} \psi_d := \sum_{d|t} \frac{\mu(d)}{\phi(d)} \sum_{ord(\psi)=d} \psi,$$

onde ψ_d é um caracter multiplicativo de ordem d, e $\sum_{ord(\psi)=d} \psi$ percorre todos estes caracteres multiplicativos.

Para cada t divisor de $q^n - 1$, defina $\theta(t) = \dfrac{\phi(t)}{t}$.

Teorema 3.1.5. *Para $\alpha \in \mathbb{F}_{q^n}^*$, t um divisor inteiro positivo de $q^n - 1$,*

$$\omega_t(\alpha) = \theta(t) \int_{d|t} \psi_d(\alpha) = \begin{cases} 1, & \text{se } \alpha \text{ é } t\text{-livre;} \\ 0, & \text{caso contrário.} \end{cases}$$

Demonstração. Quando d não é livre de quadrados, $\mu(d) = 0$. Logo, podemos restringir $\sum_{d|t} \frac{\mu(d)}{\phi(d)}$ aos divisores livres de quadrados, isto é, quando $d = r_1 r_2 \dots r_k$ com r_i primo para $1 \leq i \leq k$. Como μ e ϕ são funções multiplicativas, para os fatores primos r de d, temos

$$\int_{d|t} \psi_d(\alpha) = \sum_{d|t} \frac{\mu(d)}{\phi(d)} \sum_{ord(\psi)=d} \psi(\alpha) = \prod_{r|t} \left(1 + \frac{\mu(r)}{\phi(r)} \sum_{ord(\psi)=r} \psi(\alpha) \right)$$

Como r é primo, temos $\mu(r) = -1$ e $\phi(r) = r - 1$. Então

$$\int_{d|t} \psi_d(\alpha) = \prod_{r|t} \left(1 - \frac{1}{r-1} \sum_{ord(\psi)=r} \psi(\alpha) \right).$$

Se α não é t-livre, pelo lema 3.1.2 existe r divisor primo de t tal que α não é r-livre. Então existe $\beta \in \mathbb{F}_{q^n}^*$ tal que $\alpha = \beta^r$. Quando $ord(\psi) = r$, temos $\psi(\alpha) = \psi(\beta^r) = \psi(\beta)^r = 1$, e como existem $r - 1$ caracteres de ordem r, temos

$$\omega_t(\alpha) = \theta(t) \int_{d|t} \psi_d(\alpha) = \theta(t) \prod_{r|t} \left(1 - \frac{1}{r-1} \cdot (r-1) \right) = 0.$$

Agora, se α é t-livre, então para um elemento $\beta \in \mathbb{F}_{q^n}^*$ primitivo, $\alpha = \beta^k$ para algum k inteiro positivo. Suponha que existe s tal que $s|k$ e $s|t$. Daí, existe k' tal que $k = sk'$ e $\alpha = \beta^k = \beta^{sk'} = (\beta^{k'})^s$, mas como $s|t,\ s = 1$, pois α é t-livre. Isso implica que $mdc(k, t) = 1$. Como existe j tal que $\psi = \psi_j$ e $\psi(\beta^r) = e^{\frac{2\pi i j r}{q^n - 1}}$, quando $ord(\psi) = r$, temos $j \neq 0$ (pois $ord(\psi_0) = 1$) e $\psi(\beta^r) = \psi(\beta)^r = e^{\frac{2\pi i j r}{q^n - 1}} = 1$, o que implica que $(q^n - 1) \mid jr$. Então, $j \in \{ \frac{p(q^n-1)}{r} \ / \ 1 \leq p \leq r - 1 \}$. Sejam $j_p = \frac{p(q^n-1)}{r}$

e $\xi = e^{\frac{2\pi i j_p k}{q^n-1}}$. Quando $p = 1$, $\xi = e^{\frac{2\pi i k}{r}}$, logo $\xi^r = 1$. Como $r|t$ e $mdc(t,k) = 1$, $r \nmid k$, logo $\xi \neq 1$. Então,

$$\sum_{ord(\psi)=r} \psi(\alpha) \;=\; \sum_{p=1}^{r-1} \xi^p \;=\; \sum_{p=0}^{r-1} \xi^p - 1 \;=\; \frac{1-\xi^r}{1-\xi} - 1 \;=\; 0 - 1 \;=\; -1.$$

Assim,

$$\prod_{r|t} \left(1 - \frac{1}{r-1} \sum_{ord(\psi)=r} \psi(\alpha)\right) \;=\; \prod_{r|t} \left(1 - \frac{1}{r-1}(-1)\right) \;=\; \prod_{r|t} \left(\frac{r}{r-1}\right) \;= \frac{t}{\phi(t)}.$$

Portanto,

$$\omega_t(\alpha) \;=\; \theta(t) \int_{d|t} \psi_d(\alpha) \;=\; \frac{\phi(t)}{t} \cdot \frac{t}{\phi(t)} = 1.$$

□

Quando $t = q^n - 1$ no Teorema 3.1.5 obtemos a função característica dos elementos primitivos.

3.2 Elementos M-livres

Definição 3.2.1. *(Elemento M-livre) Seja $\alpha \in \mathbb{F}_{q^n}$. Dado M divisor de $x^n - 1$, α é M-**livre** se $\alpha = L_D(\beta)$ implica $D = 1$ e $\alpha = \beta$ para todo D divisor de M, onde L_D é o q-polinômio associado de D.*

Pela definição anterior, podemos ver que α é normal se, e somente se, α é (x^n-1)-livre.

Proposição 3.2.2. *Sejam G divisor de $x^n - 1$. Para $\alpha \in \mathbb{F}_{q^n}$,*

(i) Para todo F divisor de G, se α é G-livre então α é F-livre;

(ii) Para todo F divisor de G, se $rad(G)|F$, então α é G-livre se, e somente se, α é F-livre.

Demonstração. (i) Seja H divisor de F, $\alpha = L_H(\beta)$, onde L_H é o q-polinômio associado de H. Como $H|F$ e $F|G$, temos que $H|G$, e como α é G-livre, temos que $H = 1$. Logo, α é F-livre.

(ii) Pelo item anterior, se α é G-livre então α é F-livre. Agora suponha que α não é G-livre. Então, existe H divisor de G tal que $H \neq 1$ e $\alpha = L_H(\beta)$. Como $Z := mdc(H, rad(G)) \neq 1$, existe $S \in \mathbb{F}_q[X]$ tal que $H = ZS$. Logo, $\alpha = L_H(\beta) = L_{ZS}(\beta) = L_Z(L_S(\beta))$, onde L_Z e L_S são os q-polinômios associados de Z e S, respectivamente. Ou seja, α é igual ao q-polinômio L_Z aplicado em um elemento de $\mathbb{F}_{q^n}$ onde $Z|F$ e $Z \neq 1$. Logo, α não é F-livre.

□

Consideremos agora o grupo aditivo de $\mathbb{F}_{q^n}$. Vejamos como são definidos os caracteres sobre este grupo.

Seja $Tr\colon \mathbb{F}_{q^n} \to \mathbb{F}_p$ a função Traço absoluto de $\mathbb{F}_{q^n}$ em $\mathbb{F}_p$ (Definição 1.4.1), onde p é a característica de $\mathbb{F}_{q^n}$, e $\mathbb{F}_p$ o seu subcorpo primo. Então a função

$$\chi_1(c) = e^{\frac{2\pi i Tr(c)}{p}},\ \forall c \in \mathbb{F}_{q^n}$$

é um caracter do grupo aditivo de $\mathbb{F}_{q^n}$, já que para $c_1, c_2 \in \mathbb{F}_{q^n}$, temos $Tr(c_1+c_2) = Tr(c_1)+Tr(c_2)$, o que implica que

$$\begin{aligned}\chi_1(c_1+c_2) &= e^{\frac{2\pi i Tr(c_1+c_2)}{p}} = e^{\frac{2\pi i (Tr(c_1)+Tr(c_2))}{p}} = e^{\frac{2\pi i Tr(c_1)+2\pi i Tr(c_2)}{p}} = e^{\frac{2\pi i Tr(c_1)+2\pi i Tr(c_2)}{p}} \\ &= e^{\frac{2\pi i Tr(c_1)}{p}}.\ e^{\frac{2\pi i Tr(c_2)}{p}} = \chi_1(c_1)\chi_1(c_2).\end{aligned}$$

Este caracter será chamado de *caracter aditivo canônico de* $\mathbb{F}_{q^n}$. Vejamos agora que todos os caracteres de $\mathbb{F}_{q^n}$ podem ser expressos a partir de χ_1.

Teorema 3.2.3. *Dado $b \in \mathbb{F}_{q^n}$, a função χ_b dada por $\chi_b(c) = \chi_1(bc),\ \forall c \in \mathbb{F}_{q^n}$ é um caracter aditivo de $\mathbb{F}_{q^n}$, e todo caracter aditivo de $\mathbb{F}_{q^n}$ é obtido desta forma.*

Demonstração. Dados $c_1, c_2 \in \mathbb{F}_{q^n}$, $\chi_b(c_1+c_2) = \chi_1(bc_1+bc_2) = \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2)$. Logo, χ_b é caracter de $\mathbb{F}_{q^n}$. Como Tr é sobrejetora (Teorema 1.4.2(iii)), χ_1 é não-trivial. Portanto, para $a, b \in \mathbb{F}_{q^n},\ a \neq b$, temos

$$\chi_a(c)\chi_b(c)^{-1} = \chi_1(ac)\chi_1(bc)^{-1} = \chi_1(c(a-b)) \neq 1 \text{ para algum } c \in \mathbb{F}_{q^n}$$

e então $\chi_a \neq \chi_b$. Como b percorre $\mathbb{F}_{q^n}$, temos q^n caracteres do tipo χ_b, e pelo Teorema 2.2.7 $\mathbb{F}_{q^n}$, tem exatamente q^n caracteres.

□

Quando $b = 0$ no teorema acima, temos o caracter aditivo trivial χ_0, dado por $\chi_0(c) = 1,\ \forall c \in \mathbb{F}_{q^n}$.

Para obter a função característica de um elemento M-livre, é preciso definir a $\mathbb{F}_q$-ordem de um caracter aditivo. Vejamos antes um conceito da Álgebra Comutativa que será necessário para esta definição.

Definição 3.2.4. *(Módulo) Seja A um anel comutativo com unidade. Um grupo abeliano M é um* ***A-módulo*** *se a operação*

$$\begin{aligned}\varphi\colon A \times M &\to M \\ (a, m) &\mapsto am\end{aligned}$$

preserva as seguintes propriedades:

(i) Distributividade em M: $a(m+n) = am + an$.

(ii) Distributividade em A: $(a+b)m = am + bm$.

(iii) Associatividade: $a(bm) = (ab)m$.

(iv) Possui elemento neutro: $1m = m$, *onde* 1 *é a unidade de* A.

Para todo $a, b \in A,\ m, n \in M$.

Um A-módulo é uma generalização de conceito de espaço vetorial com os escalares em um anel arbitrário. Se A fosse um corpo, o conjunto M se tornaria um espaço vetorial.

De acordo com o Teorema 2.1.6 e pelo fato de L_f ser um operador linear, $\mathbb{F}_{q^n}$ pode ser visto como um $\mathbb{F}_q[X]$-módulo, com a seguinte operação:

$$\begin{aligned} \varphi\colon \mathbb{F}_q[X] \times \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ (f, \alpha) &\mapsto L_f(\alpha). \end{aligned}$$

Portanto, $\widehat{\mathbb{F}_{q^n}}$ também tem a estrutura de um $\mathbb{F}_q[X]$-módulo, com a seguinte operação:

$$\begin{aligned} \varphi\colon \mathbb{F}_q[X] \times \widehat{\mathbb{F}_{q^n}} &\to \widehat{\mathbb{F}_{q^n}} \\ (f, \chi_c) &\mapsto L_f(\chi_c). \end{aligned}$$

Assim, podemos escrever $L_f(\chi_c(\alpha)) = \chi_c(L_f(\alpha)),\ \forall \alpha \in \mathbb{F}_{q^n}$. Podemos então definir a $\mathbb{F}_q$-ordem de um caracter aditivo χ_c.

Definição 3.2.5. *($\mathbb{F}_q$-ordem de um caracter) Seja χ_c um caracter aditivo. A $\mathbb{F}_q$-ordem de χ_c, denotada por* ***Ord(χ_c)****, é o polinômio mônico $f \in \mathbb{F}_q[X]$ de menor grau tal que $L_f(\chi_c(\alpha)) = \chi_0(\alpha) = 1,\ \forall \alpha \in \mathbb{F}_{q^n}$.*

Usando a definição acima, veremos mais a frente o teorema que define a função característica dos elementos M-livres. Vejamos agora um lema necessário e notações que serão utilizadas.

Lema 3.2.6. *Seja $g \in \mathbb{F}_q[x]$ um polinômio não constante. Então:*

$$\prod_{p|g} \left(\frac{q^{\deg(p)}}{q^{\deg(p)} - 1} \right) = \frac{q^{\deg(g)}}{\phi_q(g)}.$$

onde p é um divisor mônico e irredutível de g.

Demonstração. Seja $g = a \cdot p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, onde $a \in \mathbb{F}_q^*$, cada p_i é um polinômio mônico irredutível e cada k_i é um inteiro positivo, com $1 \leq i \leq r$. Para cada $i \in \{1, \ldots, r\}$, o anel $\mathbb{F}_q[X] \,/\, \langle p_i^{k_i} \rangle$ possui $q^{k_i \cdot \deg(p_i)}$ elementos e $q^{(k_i-1)\cdot \deg(p_i)}$ múltiplos de p_i. Então, $\phi_q(p_i^{k_i}) = q^{(k_i-1)\cdot \deg(p_i)}(q^{\deg(p_i)} - 1)$, e assim

$$\prod_{i=1}^{r} \left(\frac{q^{\deg(p_i)}}{q^{\deg(p_i)} - 1} \right) = \prod_{i=1}^{r} \left(\frac{q^{\deg(p_i)}}{\frac{\phi_q(p_i^{k_i})}{q^{(k_i-1)\deg(p_i)}}} \right) = \prod_{i=1}^{r} \left(\frac{q^{k_i \cdot \deg(p_i)}}{\phi_q(p_i^{k_i})} \right) = \frac{q^{\deg(g)}}{\phi_q(g)}.$$

□

Considere a notação:

$$\int_{D|T} \chi_{c_D} := \sum_{D|T} \frac{\mu_q(D)}{\phi_q(D)} \sum_{Ord(\chi_c)=D} \chi_c,$$

onde χ_{c_D} é um caracter aditivo com $Ord(\chi_c) = D$, e $\sum_{Ord(\chi_c)=D} \chi_c$ percorre os caracteres aditivos de ordem D.

Para cada T divisor de $x^n - 1$, defina $\Theta(T) = \dfrac{\phi_q(T)}{q^{\deg(T)}}$.

Teorema 3.2.7. *Para $\alpha \in \mathbb{F}_{q^n}$, T um divisor mônico de $x^n - 1$,*

$$\Omega_T(\alpha) = \Theta(T) \int_{D|T} \chi_{c_D}(\alpha) = \begin{cases} 1, & \textit{se } \alpha \textit{ é } T\textit{-livre;} \\ 0, & \textit{caso contrário.} \end{cases}$$

Demonstração. Vejamos primeiramente que

$$\sum_{Ord(\chi_c)=D} \chi_c(\alpha) = \begin{cases} -1, & \text{se } \alpha \text{ é } D\text{-livre;} \\ q^{\deg(D)} - 1, & \text{caso contrário.} \end{cases}$$

Se α não é D-livre, então existe $\beta \in \mathbb{F}_{q^n}$ tal que $\alpha = L_D(\beta)$. Quando $Ord(\chi_c) = D$, temos $\chi_c(\alpha) = \chi_c(L_D(\beta)) = L_D(\chi_c(\beta)) = \chi_0(\beta) = 1$. Como D é irreduítvel, $\phi_q(D) = q^{\deg(D)} - 1$, e então

$$\sum_{Ord(\chi_c)=D} \chi_c(\alpha) = q^{\deg(D)} - 1.$$

Se α é D-livre, então existe $\beta \in \mathbb{F}_{q^n}$ normal e $G \in \mathbb{F}_q[X]$ co-primo com D tal que $\alpha = L_G(\beta)$. Defina $V_D = \{\chi_c \in \widehat{\mathbb{F}_{q^n}} \;/\; Ord(\chi_c) \mid D\}$. Dados $\chi_{c_1},\ \chi_{c_2} \in V_D$, temos $L_D(\chi_{c_1} - \chi_{c_2}(\alpha)) = L_D(\chi_{c_1}(\alpha)) L_D(\chi_{c_2}(\alpha))^{-1} = 1,\ \forall \alpha \in \mathbb{F}_{q^n}$. Logo, V_D é subgrupo de $\widehat{\mathbb{F}_{q^n}}$. Agora considere um caracter χ_{c_1} com $Ord(\chi_{c_1}) = D$, e suponha que $\chi_{c_1}(\alpha) = 1$, isto é, $\chi_{c_1}(L_G(\beta)) = 1$. Pelo Lema de Bezout, como G e D são primos entre si, existem $F_1, F_2 \in \mathbb{F}_q[X]$ tais que $DF_1 + GF_2 = 1$. Daí

$$\begin{aligned} \chi_{c_1}(\beta) &= L_1(\chi_{c_1}(\beta)) = L_{(DF_1+GF_2)}(\chi_{c_1}(\beta)) = L_{F_1}(L_D(\chi_{c_1}(\beta))) + L_{F_2}(L_G(\chi_{c_1}(\beta))) \\ &= L_{F_1}(\chi_0(\beta)) + L_{F_2}(\chi_0(\beta)) = L_{(F_1+F_2)}(\chi_0(\beta)) = \chi_0(L_{(F_1+F_2)}(\beta)) \\ &= 1. \end{aligned}$$

Mas como β é normal, χ_{c_1} é o caracter trivial. Contradição, pois $Ord(\chi_{c_1}) = D > 1$. Logo, $\chi_{c_1}(\alpha) \neq 1$. Daí,

$$\chi_{c_1}(\alpha) \sum_{\chi_c \in V_D} \chi_c(\alpha) = \sum_{\chi_c \in V_D} (\chi_{c_1} + \chi_c)(\alpha) = \sum_{\chi_c \in V_D} \chi_c(\alpha).$$

Então,

$$0 = \sum_{\chi_c \in V_D} \chi_c(\alpha) = \sum_{Ord(\chi_c)=D} \chi_c(\alpha) + 1.$$

Portanto,

$$\sum_{Ord(\chi_c)=D} \chi_c(\alpha) = -1.$$

Quando D não é livre de quadrados, $\mu_q(D) = 0$. Logo, podemos restringir a soma

$$\sum_{D|T} \frac{\mu_q(D)}{\varphi_q(D)} \sum_{Ord(\chi_c)=D} \chi_c$$

aos divisores de D livres de quadrados, isto é, quando $D = P_1 P_2 \dots P_k$ com P_i mônico e irredutível para $1 \leq i \leq k$. Então, de forma análoga à demonstração do Teorema 3.1.5, temos

$$\int_{D|T} \chi_{c_D}(\alpha) = \sum_{D|T} \frac{\mu_q(D)}{\phi_q(D)} \sum_{Ord(\chi_c)=D} \chi_c = \prod_{P|T} \left(1 + \frac{\mu_q(P)}{\phi_q(P)} \sum_{Ord(\chi_c)=P} \chi_c(\alpha) \right).$$

Quando P é mônico e irredutível, temos $\mu_q(P) = -1$ e $\phi_q(P) = q^{\deg(P)} - 1$. Então

$$\int_{D|T} \chi_{c_D}(\alpha) = \prod_{P|T} \left(1 - \frac{1}{q^{\deg(P)} - 1} \sum_{Ord(\chi_c)=P} \chi_c(\alpha) \right).$$

Se α não é T-livre, pelo Lema 3.2.2 existe P divisor mônico e irredutível de T tal que α não é P-livre. Então

$$\Omega_T(\alpha) = \Theta(T) \int_{D|T} \chi_{P_D}(\alpha) = \Theta(T) \prod_{P|T} \left(1 - \frac{1}{q^{\deg(P)} - 1} (q^{\deg(P)} - 1) \right) = 0.$$

Agora, se α é T-livre, então α é P-livre para todo P divisor de T, e portanto

$$\Omega_T(\alpha) = \Theta(T) \int_{D|T} \chi_{c_D}(\alpha) = \Theta(T) \prod_{P|T} \left(1 - \frac{1}{q^{\deg(P)} - 1} (-1) \right) = \frac{\phi_q(T)}{q^{\deg(T)}} \cdot \frac{q^{\deg(T)}}{\phi_q(T)} = 1,$$

onde a penúltima igualdade vem do Lema 3.2.6.

□

Quando $T = x^n - 1$ no Teorema 3.2.7 obtemos a função característica dos elementos normais.

3.3 Elementos k-normais

Na definição 1.4.11 trouxemos a ideia de elemento normal, e a partir deste conceito, introduzir uma generalização destes elementos, chamados de k-normais. Estes elementos aparecem na construção de bases *quase-normais* em [10] e [14], que são um tipo de base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ que fornece um método eficiente para multiplicações em $\mathbb{F}_{q^n}$.

Sabemos que os conjugados de um elemento normal geram uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. O Teorema 1.4.19 fornece um método para checar se um determinado elemento gera uma base normal. Motivados por este teorema, apresentamos a seguinte definição.

Definição 3.3.1. *(Elemento k-normal) Sejam* $\alpha \in \mathbb{F}_{q^n}$, $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$. *Se* $mdc\,(x^n - 1,\ g_\alpha(x))$ *tem grau* k, *onde* $0 \leq k \leq n$, *então* α *é um elemento* k-***normal*** *de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.

Usando esta nomenclatura, um elemento normal também é chamado de elemento 0-normal. Veja que quando $k = n$, temos que $mdc\,(x^n - 1,\ g_\alpha(x))$ tem grau n, ou seja, é o próprio polinômio $x^n - 1$, e portanto $x^n - 1$ divide $g_\alpha(x)$, que tem grau $n - 1$, e isso só é possível se $g_\alpha(x) = 0$. Logo, $\alpha = 0$. Isso nos mostra que 0 é o único elemento n-normal em $\mathbb{F}_{q^n}$. Na sequência, veremos uma série de resultados utilizados na caracterização de elementos k-normais.

Lema 3.3.2. *Dados um corpo* F *e dois polinômios não nulos* $f, g \in F[X]$,

$$posto\,(S(f,g)) = \deg(f) + \deg(g) - \deg\,(mdc(f,g))\,.$$

Demonstração. Sejam $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$. Sabemos que a matriz de Sylvester $S(f,g)$ é dada por

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{bmatrix}.$$

Pelo Teorema do Núcleo e da Imagem,

$$dim(ker(\varphi)) + dim(Im(\varphi)) = dim(F) \Rightarrow dim(ker(\varphi)) + posto(S(f,g)) = m + n,$$

onde φ é a transformação linear associada à matriz $S(f,g)$. Como sabemos que $dim(ker(\varphi)) = \deg(mdc(f,g))$ (ver [3, Lema 2.5]), temos

$$posto(S(f,g)) = m + n - dim(ker(\varphi)) = dim(f) + dim(g) - \deg(mdc(f,g)).$$

□

Teorema 3.3.3. *Um elemento $\alpha \in \mathbb{F}_{q^n}$ é k-normal sobre $\mathbb{F}_q$ se, e somente se, posto$(A_\alpha) = n - k$, onde*

$$A_\alpha = \begin{bmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{bmatrix}.$$

Demonstração. Sejam $f(x) = x^n - 1$, $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$. A matriz de Sylvester dos polinômios f e g_α é dada por

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} & 0 & 0 & 0 & \cdots & 0 \\ 0 & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \alpha & \cdots & \alpha^{q^{n-3}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \end{bmatrix}.$$

Sobre esta matriz, aplique as seguintes operações:

- Troque a coluna n pela coluna $n+1$, a coluna $n+1$ pela coluna $n+2$, e assim por diante até trocar a coluna $2n-2$ pela coluna $2n-1$;
- Adicione a coluna 1 à coluna n, a coluna 2 à coluna $n+1$, e assim por diante, até adicionar a coluna $n-1$ à coluna $2n-2$;
- Escalone as primeiras $n-1$ colunas.

O resultado será a matriz:

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ 0 & 0 & 0 & \cdots & 0 & \alpha^{q^{n-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} \\ 0 & 0 & 0 & \cdots & 0 & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \alpha & \cdots & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \alpha^q & \alpha^{q^2} & \alpha^{q^{n-3}} & \cdots & \alpha \end{bmatrix}$$

que também pode ser vista como

$$S'(f, g_\alpha) = \begin{bmatrix} I_{n-1,n-1} & 0_{n-1,n} \\ 0_{n,n-1} & A_\alpha \end{bmatrix}$$

onde $I_{n-1,n-1}$ é a matriz identidade de ordem $n-1$, $0_{n-1,n}$ e $0_{n,n-1}$ são matrizes nulas, e A_α é a matriz como definida no enunciado do teorema. Logo,

$$posto(S(f, g_\alpha)) = posto(S'(f, g_\alpha)) = posto(I_{n-1,n-1}) + posto(A_\alpha).$$

Pelo Lema 3.3.2,

$$posto(S(f, g_\alpha)) = n + (n-1) - \deg(mdc(f, g_\alpha)).$$

Como $posto(I_{n-1,n-1}) = n-1$, combinando ambas as equações, temos

$$n - 1 + posto(A_\alpha) = n + (n-1) - \deg(mdc(f, g_\alpha)),$$

o que implica que

$$\deg(mdc(f, g_\alpha)) = n - posto(A_\alpha).$$

Portanto, $mdc(f, g_\alpha)$ tem grau k se, e somente se, $posto(A_\alpha) = n - k$. Ou seja α é k-normal sobre $\mathbb{F}_q$ se, e somente se, $posto(A_\alpha) = n - k$.

□

Corolário 3.3.4. *Seja $\alpha \in \mathbb{F}_{q^n}$. Se α é k-normal sobre $\mathbb{F}_q$, então qualquer conjugado de α também é k-normal sobre $\mathbb{F}_q$.*

Demonstração. Seja α^{q^i} um conjugado de α com respeito a $\mathbb{F}_q$, $1 \leq i \leq n-1$. Então, a matriz $A_{\alpha^{q^i}}$ é dada por

$$A_{\alpha^{q^i}} = \begin{bmatrix} \alpha^{q^i} & \alpha^{q^{i+1}} & \alpha^{q^{i+2}} & \cdots & \alpha^{q^{i+n-1}} \\ \alpha^{q^{i+n-1}} & \alpha^{q^i} & \alpha^{q^{i+1}} & \cdots & \alpha^{q^{i+n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{i+1}} & \alpha^{q^{i+2}} & \alpha^{q^{i+3}} & \cdots & \alpha^{q^i} \end{bmatrix}.$$

Após algumas permutações de colunas chega-se a matriz A_α. Portanto, $posto(A_{\alpha^{q^i}}) = posto(A_\alpha) = n - k$, o que implica que $\deg(mdc(f, g_{\alpha^{q^i}})) = \deg(mdc(f, g_\alpha)) = k$, e assim α^{q^i} é k-normal sobre $\mathbb{F}_q$.

□

Lema 3.3.5. *Sejam $\alpha \in \mathbb{F}_{q^n}$, A_α a matriz definida no Teorema 3.3.3, e $\mathcal{M}$ o espaço vetorial sobre $\mathbb{F}_q$ gerado por $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$. Então, $posto(A_\alpha) = dim(\mathcal{M})$.*

Demonstração. O espaço coluna de A_α é o espaço gerado por $\{c_0, c_1, \ldots, c_{n-1}\}$ onde cada c_i é a coluna formada pelo vetor transposto $\left[\alpha^{q^i}, (\alpha^{q^i})^{q^n}(\alpha^{q^i})^{n-2}, \ldots, (\alpha^{q^i})^q\right]$. Seja m a dimensão de $\mathcal{M}$ como espaço vetorial sobre $\mathbb{F}_q$. Então uma base de $\mathcal{M}$ sobre $\mathbb{F}_q$ tem m elementos. Seja $\mathcal{S} = \{\alpha^{q^{j_1}}, \alpha^{q^{j_2}}, \ldots, \alpha^{q^{j_m}}\}$ com $0 \leq j_i \leq n-1$, para $1 \leq i \leq m$, a referida base. Note que $\mathcal{S}$ é o maior subconjunto de $\mathcal{B}$ linearmente independente. Dada uma combinação linear das colunas da matriz A_α, do tipo $d_0c_0 + d_1c_1 + \cdots + d_{n-1}c_{n-1} = 0$, a primeira linha da matriz formada será $d_0\alpha + d_1\alpha^q + \cdots + d_{n-1}\alpha^{q^{n-1}} = 0$, que pode ser reduzida a $d_{j_1}\alpha^{q^{j_1}} + d_{j_2}\alpha^{q^{j_2}} + \cdots + d_{j_m}\alpha^{q^{j_m}} = 0$, tendo assim, m colunas de A_α linearmente independentes. Logo, $m = posto(A_\alpha)$.

□

Teorema 3.3.6. *Seja $\alpha \in \mathbb{F}_{q^n}$. As seguintes propriedades são equivalentes:*

(i) α *é k-normal sobre* $\mathbb{F}_q$*;*

(ii) α *gera a base* $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ *de um q-módulo de dimensão* $n-k$ *sobre* $\mathbb{F}_q$*;*

(iii) $\deg(Ord(\alpha)) = n - k$.

Demonstração. (i) $\Rightarrow$ (ii). Se α é k-normal sobre $\mathbb{F}_q$, pelo Teorema 3.3.3 o posto de A_α é $n-k$, e pelo Lema 3.3.5, o espaço vetorial $\mathcal{M}$ gerado por $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ tem dimensão $n-k$ sobre $\mathbb{F}_q$. O conjunto $\mathcal{S} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ é uma base de $\mathcal{M}$, pois para cada $i = n-k, n-k+1, \ldots, n-1$, temos que $\mathcal{S} \cup \{\alpha^{q^i}\}$ é linearmente dependente, já que possui $n-k+1$ elementos. Se $\beta \in \mathcal{M}$, então $\beta = \sum_{i=o}^{n-k-1} a_i \alpha^{q^i}$ e $\beta^q = \sum_{i=o}^{n-k-1} a_i \alpha^{q^{i+1}}$. Logo, $\beta^q \in \mathcal{M}$, e portanto $\mathcal{M}$ é um q-módulo cuja dimensão sobre $\mathbb{F}_q$ é igual a $n-k$.

(ii) $\Rightarrow$ (iii). Sejam $\mathcal{M}$ o q-módulo da hipótese e $L(x) = \prod_{\beta \in \mathcal{M}}(x-\beta)$. Pelo Teorema 2.1.8, $L(x)$ é um q-polinômio (mônico) de grau q^{n-k} sobre $\mathbb{F}_q$. Como $\alpha \in \mathcal{M}$, α é uma raiz de $L(x)$, mas a base tem $n-k$ elementos e é um conjunto linearmente independente, então α não pode ser raiz de nenhum q-polinômio de grau menor que q^{n-k}, isto é, α é raiz q-primitiva de $L(x)$. Logo, $Ord(\alpha) = l(x)$, que é o polinômio associado de $L(x)$, de grau $n-k$ (veja Definição 2.1.5).

(iii) $\Rightarrow$ (i). Como $\deg(Ord(\alpha)) = n-k$, α é raiz q-primitiva de um q-polinômio de grau q^{n-k} sobre $\mathbb{F}_q$, então o conjunto $\mathcal{S} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ é uma base do espaço vetorial $\mathcal{M}$ do Lema 3.3.5, e assim a matriz A_α tem posto $n-k$. Logo, pelo Teorema 3.3.3, α é k-normal sobre $\mathbb{F}_q$.

□

Exemplo 3.3.7. *Considere uma raiz* α *de* x^4+x+1 *adjuntada ao corpo* $\mathbb{F}_2 = \{0,1\}$*, gerando a seguinte extensão:*

$$\begin{array}{c} \mathbb{F}_2(\alpha) \cong \mathbb{F}_{16} \\ \Big| 4 \\ \mathbb{F}_2 \end{array}$$

onde $\alpha^4 = \alpha + 1$ *e* $\alpha^8 = (\alpha^4)^2 = (\alpha+1)^2 = \alpha^2 + 1$.

Os conjugados de α *são* $\{\alpha, \alpha^2, \alpha^4, \alpha^8\} = \{\alpha, \alpha^2, \alpha+1, \alpha^2+1\}$*. Mas como* α^2+1 *é uma combinação linear dos demais elementos, o conjunto* $\{\alpha, \alpha^2, \alpha+1\}$ *é uma base de* $\mathbb{F}_2(\alpha)$ *sobre* $\mathbb{F}_2$*, e portanto* $dim_{\mathbb{F}_2}\ \langle \alpha, \alpha^2, \alpha^4, \alpha^8 \rangle = 3$*. Pelo Teorema 3.3.6(ii),* α *é* ***1-normal*** *sobre* $\mathbb{F}_2$*.*
Agora considere o elemento α^3*. Seus conjugados são*

- $\alpha^6 = \alpha^2\alpha^4 = \alpha^2(\alpha+1) = \alpha^3 + \alpha^2$*;*
- $\alpha^{12} = (\alpha^4)^3 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1$*;*
- $\alpha^{24} = \alpha^9 = \alpha^8\alpha = (\alpha^2+1)\alpha = \alpha^3 + \alpha$.

Vejamos agora que os conjugados de α^3 formam um conjunto linearmente independente. Sejam $c_1, c_2, c_3, c_4 \in \mathbb{F}_2$ tais que $c_1\alpha^3 + c_2(\alpha^3 + \alpha) + c_3(\alpha^3 + \alpha^2) + c_4(\alpha^3 + \alpha^2 + \alpha + 1) = 0$. Então,

$$(c_1 + c_2 + c_3 + c_4)\alpha^3 + (c_3 + c_4)\alpha^2 + (c_2 + c_4)\alpha + c_4 = 0$$

$$c_4 = 0 \Rightarrow c_2 = c_3 = 0 \Rightarrow c_1 = 0.$$

*Portanto, os conjugados de α^3 são uma base de $\mathbb{F}_2(\alpha^3)$ sobre $\mathbb{F}_2$, e assim temos $dim_{\mathbb{F}_2} \langle \alpha^3, \alpha^6, \alpha^9, \alpha^{12} \rangle = 4$. Pelo Teorema 3.3.6(ii), α é **0-normal** (ou simplesmente, normal) sobre $\mathbb{F}_2$.*

Observação 3.3.8. *A ideia de elemento k-normal depende fortemente do corpo base: vimos no exemplo anterior que α é 1-normal sobre $\mathbb{F}_2$. Porém, com respeito a $\mathbb{F}_4$ os conjugados de α são $\{\alpha, \alpha^4\} = \{\alpha, \alpha + 1\}$. Este conjunto é uma base de $\mathbb{F}_2(\alpha)$ sobre $\mathbb{F}_4$, e assim $dim_{\mathbb{F}_4} \langle \alpha, \alpha^4 \rangle = 2$. Pelo Teorema 3.3.6(ii), α é normal sobre $\mathbb{F}_4$.*

No intuito de encontrar a quantidade de elementos k-normais em um corpo $\mathbb{F}_{q^n}$, precisamos de dois resultados que são apresentados a seguir.

Lema 3.3.9. *Sejam $\alpha \in \mathbb{F}_{q^n}$ um elemento normal sobre $\mathbb{F}_q$, e $f \in \mathbb{F}_q[X]$ de grau menor ou igual a $n-1$. Então $Ord(L_f(\alpha)) = \frac{x^n-1}{mdc(x^n-1,\ f)}$, onde L_f é o q-polinômio associado de f.*

Demonstração. Seja $g = \frac{x^n-1}{mdc(x^n-1,\ f)}$. Então

$$L_g(L_f(\alpha)) = L_f(L_g(\alpha)) = L_f\left(L_{\frac{x^n-1}{mdc(x^n-1,\ f)}}(\alpha)\right) = L_{\frac{f}{mdc(x^n-1,\ f)}}(L_{x^n-1}(\alpha)) = 0.$$

Portanto, $Ord(L_f(\alpha)) \mid g$. Reciprocamente, se $L_h(L_f(\alpha)) = 0$, então $(x^n - 1) \mid fh$, logo $\frac{x^n-1}{mdc(x^n-1,\ f)} \mid \frac{fh}{mdc(x^n-1,\ f)}$, e como g e $\frac{f}{mdc(x^n-1,\ f)}$ são co-primos, $g|h$. Em particular, $L_{Ord(L_f(\alpha))}(L_f(\alpha)) = 0$, logo $g \mid Ord(L_f(\alpha))$. Ou seja, $Ord(L_f(\alpha)) = g$.

□

Lema 3.3.10. *Seja $f \in \mathbb{F}_q[X]$ um polinômio mônico e primo com x. O número de elementos α no fecho algébrico de $\mathbb{F}_q$ tais que $Ord(\alpha) = f$ é dado por $\phi_q(f)$.*

Demonstração. Seja $f \in \mathbb{F}_q[X]$ um polinômio mônico de grau m, e $mdc(f, x) = 1$. Como a derivada de L_f é igual a a_0, L_f tem q^m raízes distintas, que estão contidas em alguma extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$, com n natural. Assim, $\alpha \in \mathbb{F}_{q^n}$, logo, $\alpha^{q^n} - \alpha = 0$, e portanto, $L_f \mid (x^{q^n} - x)$ e $f \mid (x^n - 1)$.

Como toda extensão do tipo $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ possui uma base normal, existe um elemento normal β tal que

$$\mathbb{F}_{q^n} = \{L_g(\beta) \ / \ g \in \mathbb{F}_q[X] \text{ e } \deg(g) \leq n - 1\}.$$

Considere V o conjunto dos elementos γ no fecho algébrico de $\mathbb{F}_q$ onde $Ord(\gamma) = f$. Como cada γ está em $\mathbb{F}_{q^n}$, temos

$$V = \{\gamma \in \overline{\mathbb{F}_q} \ / \ Ord(\gamma) = f\} \subset \mathbb{F}_{q^n} \ \Rightarrow \ V = \{\gamma \in \mathbb{F}_{q^n} \ / \ Ord(\gamma) = f\}.$$

Assim podemos escrever

$$V = \{L_g(\beta) \ / \ g \in \mathbb{F}_q[X], \ \deg(g) \leq n-1 \text{ e } Ord(L_g(\beta)) = f\}.$$

Como β é normal, pelo lema anterior, $f = Ord(L_g(\beta)) = \frac{x^n-1}{mdc(x^n-1,g)}$, ou seja, $\frac{x^n-1}{f} \ \big| \ g$. Então existe $h \in \mathbb{F}_q[X]$ tal que $g = h \cdot \frac{x^n-1}{f}$, e assim,

$$\deg(h) + n - \deg(f) = \deg(g) \leq n-1 \ \Rightarrow \ \deg(h) \leq \deg(f) - 1.$$

E como $mdc(x^n-1, g) = mdc(x^n-1, h \cdot \frac{x^n-1}{f}) = \frac{x^n-1}{f}$, temos que $mdc(h, f) = 1$. Isto implica que

$$V = \{L_g(\beta) \ / \ f, g, h \in \mathbb{F}_q[X], \ g = h \cdot \frac{x^n-1}{f}, \ \deg(h) \leq \deg(f) - 1 \text{ e } mdc(f,h) = 1\}.$$

A quantidade de polinômios h tais que $\deg(h) \leq \deg(f) - 1$ e $mdc(f, h) = 1$ é dada por $\phi_q(f)$. Logo, $|V| = \phi_q(f)$.

□

Teorema 3.3.11. *O número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é dado por*

$$\sum_{\substack{h | x^n-1 \\ \deg(h) = n-k}} \phi_q(h)$$

onde h é mônico e a divisão polinomial é feita sobre $\mathbb{F}_q$.

Demonstração. Seja $h \in \mathbb{F}_q[X]$ de grau $n-k$. Pelo Lema 3.3.10, o número de elementos α tais que $Ord(\alpha) = h$ é igual a $\phi_q(h)$, e como $\deg(h) = \deg(Ord(\alpha)) = n-k$, pelo Teorema 3.3.6(iii), α é k-normal. Logo, a quantidade de elementos k-normais é igual a soma acima.

□

Observação 3.3.12. *Existem elementos k-normais em $\mathbb{F}_{q^n}$ se, e somente se, $x^n - 1$ é divisível por um polinômio $h \in \mathbb{F}_q[X]$ de grau $n-k$ (ou k).*

Um polinômio cujas raízes são todas as raízes primitivas n-ésimas da unidade é chamado de *n-ésimo polinômio ciclotômico*, denotado por $\Phi_n(x)$, e são os fatores que compõem o polinômio $x^n - 1$, ou seja

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

Isto mostra que a fórmula mencionada no Teorema 3.3.11 depende da fatorização de polinômios ciclotômicos em $\mathbb{F}_q$, o que se torna inviável para valores de n muito grandes.

Em [10] os autores propõem o seguinte problema: para quais valores de q, n e k é possível obter fórmulas "acessíveis" para o número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$? Em [17], os autores calculam o número de elementos k-normais para valores específicos de q e n, como mostram as tabelas a seguir.

k	0	1	2
$\#k$-normais	5832	972	54

Tabela 3.1: Quantidade de elementos k-normais de $\mathbb{F}_{19^3}$ sobre $\mathbb{F}_{19}$.

k	0	1	2	3
$\#k$-normais	147456	147456	67584	21504
k	4	5	6	7
$\#k$-normais	5440	1024	144	16

Tabela 3.2: Quantidade de elementos k-normais de $\mathbb{F}_{5^8}$ sobre $\mathbb{F}_5$.

k	0	1	2	3
$\#k$-normais	16777216	16777216	7340032	1835008
k	4	5	6	7
$\#k$-normais	286720	28672	1792	64

Tabela 3.3: Quantidade de elementos k-normais de $\mathbb{F}_{9^8}$ sobre $\mathbb{F}_9$.

k	0	1	2	3
$\#k$-normais	3981312	1327104	359424	82944
k	4	5	6	7
$\#k$-normais	12096	1728	180	12

Tabela 3.4: Quantidade de elementos k-normais de $\mathbb{F}_{7^8}$ sobre $\mathbb{F}_7$.

k	0	1	2	3
$\#k$-normais	13107200	13107200	8192000	4915200
k	4	5	6	7
$\#k$-normais	2170880	942080	384000	148480
k	8	9	10	11
$\#k$-normais	54528	17408	5760	1408
k	12	13	14	15
$\#k$-normais	448	96	28	4

Tabela 3.5: Quantidade de elementos k-normais de $\mathbb{F}_{3^{16}}$ sobre $\mathbb{F}_3$.

Capítulo 4

Elementos primitivos k-normais

Sabemos que elementos normais, e elementos que são simultaneamente primitivos e normais sempre existem em extensões de corpos finitos pelo Teorema da Base Normal Primitiva [11]. A partir da noção de elemento k-normal introduzida no capítulo anterior buscamos, agora, encontrar elementos que sejam simultaneamente primitivos e k-normais.

A busca por tais elementos visa encontrar estruturas que, embora não sejam estritamente bases normais, oferecem uma combinação poderosa de propriedades multiplicativas (primitividade) e aditivas em um espaço vetorial (k-normalidade), com aplicações na construção de bases que otimizam a multiplicação em corpos finitos.

Neste capítulo, encontramos as condições necessárias para a existência destes elementos e posteriormente mostramos exemplos encontrados em trabalhos recentes na área.

4.1 Condições para existência de elementos primitivos k-normais

Lema 4.1.1. *Sejam $f, g, h \in \mathbb{F}_q[X]$ polinômios não nulos tais que $mdc(g, h) = 1$. Então existe $g' \in \mathbb{F}_q[X]$ tal que $mdc(f, h + gg') = 1$.*

Demonstração. Se f é constante, o resultado é óbvio. Caso contrário, defina

$$g' = \prod_{\substack{i=1 \\ r_i \nmid h}}^{k} r_i,$$

onde $rad(f) = r_1 r_2 \dots r_k$. Se $r_i | h$ então $r_i \nmid gg'$, e consequentemente $r_i \nmid h + gg'$; e se $r_i \nmid h$ então $r_i \nmid h + gg'$. Ou seja, em qualquer dos casos, $r_i \nmid h + gg'$ para $1 \leq i \leq k$. Portanto, $mdc(f, h + gg') = 1$.

□

Proposição 4.1.2. *Sejam $\beta \in \mathbb{F}_{q^n}$ um elemento normal sobre $\mathbb{F}_q$ e $f \in \mathbb{F}_q[X]$ um divisor de $x^n - 1$ de grau k. Então $\alpha = L_f(\beta)$ é k-normal, onde L_f é o q-polinômio associado de f. Além disso, todo elemento k-normal é obtido desta forma.*

Demonstração. Vamos demonstrar que $Ord(\alpha) = \frac{x^n-1}{f}$. Seja $s = \frac{x^n-1}{f}$. Temos

$$L_s(\alpha) = L_s(L_f(\beta)) = L_{sf}(\beta) = L_{\frac{x^n-1}{f}f}(\beta) = L_{x^n-1}(\beta) = \beta^{q^n} - \beta = 0.$$

Logo, $Ord(\alpha)$ divide s. Suponha que $Ord(\alpha) \neq s$. Então existe $g \in \mathbb{F}_q[X]$ mônico, de grau pelo menos 1, tal que $s = Ord(\alpha).g$, implicando que $Ord(\alpha) = \frac{x^n-1}{fg}$. Daí,

$$0 = L_{\frac{x^n-1}{fg}}(\alpha) = L_{\frac{x^n-1}{fg}}(L_f(\beta)) = L_{\frac{x^n-1}{g}}(\beta),$$

o que implica $\deg(Ord(\beta)) < n$. Mas $\beta \in \mathbb{F}_{q^n}$ é normal, logo, pelo Teorema 3.3.6, $\deg(Ord(\beta)) = n$. Contradição. Portanto, $Ord(\alpha) = s = \frac{x^n-1}{f}$, e α é k-normal.

Vejamos agora que todo elemento k-normal é obtido desta forma. Suponha que α é um elemento k-normal. Defina $g = Ord(\alpha)$ e $f = \frac{x^n-1}{g}$. Então, $\deg(g) = n-k$. Seja $\gamma \in \mathbb{F}_{q^n}$ um elemento normal sobre $\mathbb{F}_q$. Então existe $h \in \mathbb{F}_q[X]$ tal que $\alpha = L_h(\gamma)$. Daí, $0 = L_g(\alpha) = L_g(L_h(\gamma)) = L_{gh}(\gamma)$. Como $(x^n - 1) \mid gh$, obtemos $f|h$, e então existe $f' \in \mathbb{F}_q[X]$ tal que $h = f.f'$. Isso implica que

$$\begin{aligned} L_{\frac{g}{mdc(g,f')}}(\alpha) &= L_{\frac{g}{mdc(g,f')}}(L_h(\gamma)) = L_{\frac{gh}{mdc(g,f')}}(\gamma) = L_{\frac{gff'}{mdc(g,f')}}(\gamma) \\ &= L_{gf}\left(L_{\frac{f'}{mdc(g,f')}}(\gamma)\right) = L_{x^n-1}\left(L_{\frac{f'}{mdc(g,f')}}(\gamma)\right) \\ &= 0, \end{aligned}$$

ou seja, $mdc(g, f') = 1$. Então, pelo Lema 4.1.1, existe um polinômio $g' \in \mathbb{F}_q[X]$ tal que $mdc(x^n - 1, f' + g.g') = 1$, e pelo Teorema 3.3.9, $\beta = L_{(f'+gg')}(\gamma)$ é normal. Logo,

$$\begin{aligned} L_f(\beta) &= L_f(L_{(f'+gg')}(\gamma)) = L_{(ff'+fgg')}(\gamma) = L_{(h+(x^n-1)g')}(\gamma) \\ &= L_h(\gamma) + L_{x^n-1}(L_{g'}(\gamma)) = L_h(\gamma) \\ &= \alpha. \end{aligned}$$

□

Pelo Teorema 3.3.11, elementos k-normais existem em $\mathbb{F}_{q^n}$ se, e somente se, x^n-1 tem divisor de grau k (ou $n-k$). Pelo teorema anterior, é possível construir um elemento k-normal encontrando um divisor $f \in \mathbb{F}_q[X]$ de $x^n - 1$ de grau k, e um elemento normal $\beta \in \mathbb{F}_{q^n}$, daí $\alpha = L_f(\beta)$ é um elemento k-normal de $\mathbb{F}_{q^n}$.

De acordo com o Teorema 3.1.5, Sabemos que um elemento $\alpha \in \mathbb{F}_{q^n}$ é primitivo se, e somente se, $\omega_{q^n-1}(\alpha) = 1$. E pelo Teorema 3.2.7, sabemos que um elemento $\alpha \in \mathbb{F}_{q^n}$ é normal se, e somente se, $\Omega_{x^n-1}(\alpha) = 1$. Logo, se $\omega_{q^n-1}(\alpha)\Omega_{x^n-1}(\alpha) = 1$, α é simultaneamente primitivo e normal.

No restante deste capítulo, veremos condições para a existência de elementos em $\mathbb{F}_{q^n}$ que sejam simultaneamente primitivos e k-normais. Para isso, considere o seguinte somatório:

$$\eta_f = \sum_{\alpha \in \mathbb{F}_{q^n}} \omega_{q^n-1}(L_f(\alpha))\Omega_{x^n-1}(\alpha).$$

Note que η_f contabiliza a quantidade de elementos primitivos e k-normais, pois se α é normal, dado um polinômio $f \in \mathbb{F}_q[X]$ divisor de $x^n - 1$ de grau k, o elemento $L_f(\alpha)$ é k-normal.

Em particular, elementos primitivos k-normais existem em $\mathbb{F}_{q^n}$ se $\eta_f > 0$.

Proposição 4.1.3. *Sejam $\alpha \in \mathbb{F}_{q^n}, f \in \mathbb{F}_q[X]$ divisor de $x^n - 1$ de grau k. Então*

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} = \sum_{\alpha \in \mathbb{F}_{q^n}} \int_{d|q^n-1} \int_{D|x^n-1} \chi_{c_D}(\alpha)\psi_d(L_f(\alpha)).$$

Demonstração. Vamos denotar as funções características $\Omega_{q^n-1}(\alpha)$ e $\omega_{x^n-1}(\alpha)$ apenas por $\Omega(\alpha)$ e $\omega(\alpha)$, respectivamente. Pelos Teoremas 3.1.5 e 3.2.7, temos

$$\begin{aligned}
\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} &= \frac{\sum\limits_{\alpha \in \mathbb{F}_{q^n}} \omega(L_f(\alpha))\Omega(\alpha)}{\theta(q^n-1)\Theta(x^n-1)} \\
&= \frac{\sum\limits_{\alpha \in \mathbb{F}_{q^n}} \theta(q^n-1) \int\limits_{d|q^n-1} \psi_d(L_f(\alpha))\Theta(x^n-1) \int\limits_{D|x^n-1} \chi_{c_D}(\alpha)}{\theta(q^n-1)\Theta(x^n-1)} \\
&= \sum_{\alpha \in \mathbb{F}_{q^n}} \int_{d|q^n-1} \psi_d(L_f(\alpha)) \int_{D|x^n-1} \chi_{c_D}(\alpha) \\
&= \sum_{\alpha \in \mathbb{F}_{q^n}} \int_{d|q^n-1} \int_{D|x^n-1} \chi_{c_D}(\alpha)\psi_d(L_f(\alpha)).
\end{aligned}$$

□

Finalmente mostraremos o resultado principal deste trabalho, que consiste em apresentar uma condição suficiente para a existência dos elementos primitivos k-normais. Para isso, usaremos a seguinte definição.

Definição 4.1.4. *Seja h um número inteiro postivo (ou um polinômio mônico). A função $W(h)$ contabiliza o número de divisores (mônicos) livres de quadrados de h.*

Teorema 4.1.5. *Sejam $f \in \mathbb{F}_q[X]$ divisor de $x^n - 1$ de grau k e η_f o número de elementos normais $\alpha \in \mathbb{F}_{q^n}$ tais que $L_f(\alpha)$ é primitivo. Então*

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} > q^n - q^{k+\frac{n}{2}} \cdot W(q^n-1) \cdot W(x^n-1).$$

Em particular, se $q^{\frac{n}{2}-k} \geq W(q^n-1)W(x^n-1)$, então existem elementos primitivos k-normais em $\mathbb{F}_{q^n}$.

Demonstração. Para cada divisor d de q^n-1, e cada divisor D de x^n-1, defina a seguinte Soma de Gauss:

$$G_f(\psi_d,\ \chi_{c_D}) = \sum_{\alpha \in \mathbb{F}_{q^n}} \psi_d(L_f(\alpha))\chi_{c_D}(\alpha),$$

e também

$$\int_{\substack{d|q^n-1 \\ D|x^n-1}} G_f(\psi_d,\ \chi_{c_D}) = \sum_{\substack{d|q^n-1 \\ D|x^n-1}} \frac{\mu(d)\mu_q(D)}{\phi(d)\phi_q(D)}\ G_f(\psi_d,\ \chi_{c_D}).$$

Pela proposição anterior, temos

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} = S_0 + S_1 + S_2 + S_3,$$

onde

- $S_0 = G_f(\psi_1,\ \chi_0)$;
- $S_1 = \int\limits_{\substack{D|x^n-1 \\ D\ \neq 1}} G_f(\psi_1,\ \chi_{c_D})$;
- $S_2 = \int\limits_{\substack{d|q^n-1 \\ d\ \neq 1}} G_f(\psi_d,\ \chi_0)$;
- $S_3 = \int\limits_{\substack{d|q^n-1 \\ d\ \neq 1}} \int\limits_{\substack{D|x^n-1 \\ D\ \neq 1}} G_f(\psi_d,\ \chi_{c_D})$.

A seguir, vamos encontrar cotas para cada S_i.

- Para S_0, temos $\sum\limits_{\alpha \in \mathbb{F}_{q^n}} \psi_1(L_f(\alpha))\chi_0(\alpha) = q^n$.

- Para estimar o valor de S_1, usamos a ortogonalidade dos caracteres, dada no Teorema 2.2.6, para ver que

$$\sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ D \neq 1}} \psi_1(L_f(\alpha))\chi_{c_D}(\alpha) = \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ D \neq 1}} \chi_{c_D}(\alpha) = 0.$$

  Logo, $S_1 = 0$.

Em S_2 e S_3, cada $G_f(\psi_d,\ \chi_{c_D})$ contém o fator $\mu(d)\mu_q(D)$ em sua expressão, que resulta em 0 caso d ou D não seja livre de quadrados. Ou seja, podemos considerar apenas os casos onde d e D são livres de quadrados.

- Em S_2, a soma terá $W(q^n-1)-1$ termos. Defina $M_2 = \max|G_f(\psi_d,\ \chi_0)|$, e assim $|S_2| \leq M_2 \cdot (W(q^n-1)-1)$. Agora, com o intuito de utilizar o Lema 2.3.3, vejamos que suas condições são satisfeitas:

  Escreva $f = \sum_{i=0}^{k} a_i x^i$. Como $f|(x^n-1)$, temos que $f \nmid x$, logo $a_0 \neq 0$. E como $L_f' = a_0$, todas as raízes de L_f são distintas, e L_f não pode ser da forma $y \cdot g(x)^r$ para nenhum $y \in \mathbb{F}_{q^n},\ g \in \mathbb{F}_q[X],\ r > 1$. Além disso, $\deg(f) = k$, implicando que $\deg(L_f) = q^k$. Assim $mdc(\deg(L_f), q^n-1) = 1$, ou seja, L_f tem q^k raízes distintas em $\mathbb{F}_{q^n}$, e estas raízes formam um subespaço vetorial de $\mathbb{F}_{q^n}$ de dimensão k (Teorema 2.1.2).

  Portanto, do Lema 2.3.3, temos que

  $$|G_f(\psi_d,\ \chi_0)| = \left|\sum_{\alpha\in\mathbb{F}_{q^n}} \psi_d(L_f(\alpha))\chi_0(\alpha)\right| = \left|\sum_{\alpha\in\mathbb{F}_{q^n}} \psi_d(L_f(\alpha))\right| \leq (q^k-1)q^{\frac{n}{2}} < q^{k+\frac{n}{2}},$$

  e assim $|S_2| \leq q^{k+\frac{n}{2}} \cdot (W(q^n-1)-1)$.

- Em S_3, a soma terá $(W(q^n-1)-1)(W(x^n-1)-1)$ termos. Defina $M_3 = \max|G_f(\psi_d,\ \chi_{c_D})|$, e assim $|S_3| \leq M_3 \cdot (W(q^n-1)-1) \cdot (W(x^n-1)-1)$.

  Analogamente ao caso de S_2, podemos ver que as condições do Lema 2.3.4 são satisfeitas. Portanto

  $$|G_f(\psi_d,\ \chi_{c_D})| = \left|\sum_{\alpha\in\mathbb{F}_{q^n}} \psi_d(L_f(\alpha))\chi_{c_D}(\alpha)\right| \leq (q^k+1-1)q^{\frac{n}{2}} = q^{k+\frac{n}{2}},$$

  e assim $|S_3| \leq q^{k+\frac{n}{2}} \cdot (W(q^n-1)-1) \cdot (W(x^n-1)-1)$.

Logo,

$$\begin{aligned} |S_2| + |S_3| &\leq q^{k+\frac{n}{2}} \cdot (W(q^n-1)-1) \cdot (1 + (W(x^n-1)-1) \\ &< q^{k+\frac{n}{2}} \cdot W(q^n-1) \cdot W(x^n-1). \end{aligned}$$

Agora, lembrando que

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} = S_0 + S_1 + S_2 + S_3,$$

podemos usar a desigualdade triangular e as estimativas encontradas anteriormente para obter

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} \geq q^n - |S_2| - |S_3|,$$

e portanto,

$$\frac{\eta_f}{\theta(q^n-1)\Theta(x^n-1)} > q^n - q^{k+\frac{n}{2}} \cdot W(q^n-1) \cdot W(x^n-1).$$

□

A desigualdade obtida como condição necessária para existência dos elementos primitivos k-normais pode ser transformada em uma desigualdade do tipo $q > c(n)$ pois existem cotas superiores para a função W. Em [1] os autores estabeleceram que, para uma potência de primo q, existem $a, b \in \mathbb{N}$ tais que $W(x^n-1) \leq 2^{\frac{n+a}{b}}$ (ver [1, Lema 3.7]). Isto nos permite dizer que para valores de q suficientemente grandes a existência de tais elementos está garantida. Mas para valores pequenos de q a desigualdade deve ser analisada caso a caso para valores de n e k específicos.

4.2 Exemplos

Em [10] os autores fornecem a quantidade de elementos primitivos k-normais, com $0 \leq k \leq n-1$ para certos valores de (q, n). As tabelas abaixo mostram, para $(q, n) \in \{(2, 6), (5, 6), (5, 7)\}$, a quantidade de elementos k-normais, primitivos k-normais, e a densidade destes elementos, isto é, a porcentagem em relação à ordem de $\mathbb{F}_{q^n}$ com aproximação de 2 casas decimais - exceto no caso $(q, n, k) = (5, 7, 6)$.

k	#k-normais	(%)	#primitivos k-normais	(%)
0	24	37,50	18	28,12
1	12	18,75	12	18,75
2	18	28,12	6	9,37
3	3	4,69	0	0
4	5	7,81	0	0
5	1	1,56	0	0

Tabela 4.1: Elementos k-normais e primitivos k-normais de $\mathbb{F}_{2^6}$ sobre $\mathbb{F}_2$.

k	#k-normais	(%)	#primitivos k-normais	(%)
0	9216	58,98	2568	16,44
1	4608	29,49	1320	8,45
2	1344	8,60	360	2,30
3	384	2,46	72	4,61
4	64	0,41	0	0
5	8	0,05	0	0

Tabela 4.2: Elementos k-normais e primitivos k-normais de $\mathbb{F}_{5^6}$ sobre $\mathbb{F}_5$.

k	#k-normais	(%)	#primitivos k-normais	(%)
0	62496	79,99	31248	39,99
1	15264	19,99	7812	9,99
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	4	$5{,}12.10^{-3}$	0	0

Tabela 4.3: Elementos k-normais e primitivos k-normais de $\mathbb{F}_{5^7}$ sobre $\mathbb{F}_5$.

Nos últimos anos diversos autores se dedicaram a encontrar valores específicos de q, n e k para os quais elementos primitivos k-normais sempre existem, e também a quantidade destes elementos para certos valores. Para $k = 0$, ou seja, elementos primitivos normais, os autores provaram em [11] que tais elementos sempre existem. Em [16] e [1], os autores estabelecem as condições para existência destes elementos quando $k = 1$ e $k = 2$, respectivamente, como mostram os teoremas a seguir.

Teorema 4.2.1. *[16, Teorema 1.3] (Teorema dos Primitivos 1-Normais) Sejam q uma potência de um número primo, $n \geq 3$ um inteiro positivo. Então existe um elemento primitivo 1-normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Além disso, quando $n = 2$ não existem elementos primitivos 1-normais de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$.*

Teorema 4.2.2. *[1, Teorema 1.2] (Teorema dos Primitivos 2-Normais). Sejam q uma potência de um número primo, n um inteiro positivo. Então existe um elemento primitivo 2-normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, $n \geq 5$ e $mdc(q^3 - 1, n) \neq 1$ ou $n = 4$ e $q \equiv 1 \pmod 4$.*

Trabalhos continuam sendo realizados na área, já que a vantagem dos elementos k-normais primitivos sobre os elementos k-normais gerais reside na combinação da eficiência computacional das bases normais com a propriedade de serem primitivos, ou seja, geram todo o grupo multiplicativo do corpo, permitindo logaritmos discretos eficientes e maior segurança criptográfica, resultando em esquemas de troca de chaves mais robustos e sequências pseudoaleatórias. Essencialmente, estes elementos oferecem maior controle e melhores propriedades por serem geradores simultâneos de estruturas aditivas e multiplicativas, o que é valioso em aplicações avançadas.

Referências Bibliográficas

[1] Aguirre, J. e Neumann, V.. "Existence of primitive 2-normal elements in finite fields". Finite Fields Appl. 73: 101864 (2021). https://doi.org/10.1016/j.ffa.2021.101864

[2] Bernhardt, C.. "A Proof of the Cayley-Hamilton Theorem". Amer. Math. Monthly, 116(5): 456–457 (2009). https://doi.org/10.4169/193009709X470353

[3] Bernal, G. L. R.. "Existência e propriedades de elementos k-normais em corpos finitos". Dissertação (Mestrado em Matemática) - Universidade Federal de Uberlândia (2023). http://doi.org/10.14393/ufu.di.2023.369

[4] Carlitz, L.. "Primitive roots in a finite field". Trans. Amer. Math. Soc. 73: 373-382 (1952). https://doi.org/10.1090/S0002-9947-1952-0051869-9

[5] Groth, P. e Bressi, T. W.. "Disquisitiones Arithmeticae". New Haven: Yale University Press, 2006. (Original publicado em 1801). https://doi.org/10.12987/9780300194258

[6] Cohen, S. D. e Huczynska, S.. "The Primitive Normal Basis Theorem – Without a Computer". J. Lond. Math. Soc. 67: 41-56 (2003). https://doi.org/10.1112/S0024610702003782

[7] Davenport, H.. "Bases for Finite Fields". J. Lond. Math. Soc. (2): 378-378 (1968). https://doi.org/10.1112/jlms/s1-44.1.378-s

[8] Diffie, W. e Hellman, M.E.. "New directions in cryptography". IEEE Trans. Inform. Theory 22: 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638

[9] Harper, A. J.. "Minor arcs, mean values, and restriction theory for exponential sums over smooth numbers". Compos. Math. 152: 1121 - 1158 (2014). https://doi.org/10.1112/S0010437X15007782

[10] Huczynska, S.; Mullen, G. L.; Panario, D. e Thomson, D.. "Existence and properties of k-normal elements over finite fields". Finite Fields Appl. 24: 170-183 (2013). https://doi.org/10.1016/j.ffa.2013.07.004

[11] Lenstra, H. W. e Schoof, R.. "Primitive normal bases for finite fields". Math. Comp. 48: 217-231 (1987). https://doi.org/10.1090/S0025-5718-1987-0866111-3

[12] Lidl, R. e Niederreiter, H.. “Finite Fields: Encyclopedia of Mathematics and Its Applications”. 2nd ed. Cambridge: Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511525926

[13] Lidl, R. e Niederreiter, H.. “Introduction to Finite Fields and their Applications”. 2nd ed. Cambridge: Cambridge University Press, 1994. https://doi.org/10.1017/CBO9781139172769

[14] Nègre, C.. “Finite field arithmetic using quasi-normal bases”. Finite Fields Appl. 13: 635-647 (2007). https://doi.org/10.1016/j.ffa.2006.09.008

[15] Reis, L.. “Existence results on k-normal elements over finite fields”. Rev. Mat. Iberoam. 35: 805-822 (2019). https://doi.org/10.4171/rmi/1070

[16] Reis, L. e Thomson, D.. “Existence of primitive 1-normal elements in finite fields”. Finite Fields Appl. 51: 238-269 (2017). https://doi.org/10.1016/j.ffa.2018.02.002

[17] Saygı, Z.; Tilenbaev, E. e Ürtiş, C.. “On the number of k-normal elements over finite fields”. Turkish J. Math. 43 (2): 795-812 (2019). https://doi.org/10.3906/mat-1805-113

[18] Schmidt, W. M.. “Equations over Finite Fields: An Elementary Approach”. Heidelberg: Springer Berlin, 1976. https://doi.org/10.1007/BFb0080437