Gyan Carlos Robert Morales Solis

Uma introdução aos polinômios sobre corpos finitos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2025

Gyan Carlos Robert Morales Solis

Uma introdução aos polinômios sobre 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. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2025

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

S687 Solis, Gyan Carlos Robert Morales, 1999-
2025 Uma introdução aos polinômios sobre corpos finitos. [recurso eletrônico] / Gyan Carlos Robert Morales Solis. - 2025.

Orientador: Guilherme Chaud Tizziotti .
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2025.446
Inclui bibliografia.

1. Matemática. I. , Guilherme Chaud Tizziotti,1980-, (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, 125, PPGMAT				
Data:	24/07/2025	Hora de início:	9:30	Hora de encerramento:	11:30
Matrícula do Discente:	12322MAT001				
Nome do Discente:	Gyan Carlos Robert Morales Solis				
Título do Trabalho:	Uma introdução aos polinômios sobre corpos finitos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Semigrupos de Weierstrass e suas aplicações				

Reuniu-se em webconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Erik Antonio Rojas Mendoza - Universidade Federal do Rio de Janeiro /UFRJ, João Paulo Guardieiro Sousa - Universidade Estadual de Campinas / UNICAMP e Guilherme Chaud Tizziotti - Instituto de Matemática e Estatística - IME/UFU orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Guilherme Chaud Tizziotti , 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 **Erik Antonio Rojas Mendoza**, **Usuário Externo**, em 24/07/2025, às 11:49, 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 **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 24/07/2025, às 11:54, 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 **João Paulo Guardieiro Sousa**, **Usuário Externo**, em 24/07/2025, às 12:59, 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 **6515921** e o código CRC **8DCECAC0**.

Referência: Processo nº 23117.048830/2025-72 SEI nº 6515921

Dedicatória

À minha mãe, Ana Maria Solis Asencios, ao meu pai, Robert Oscar Morales Solis, e ao meu irmão, Gyan Pool Morales Solis, pelo amor, apoio incondicional e por serem minha motivação nesta jornada.

Agradecimentos

Agradeço, primeiramente, à minha mãe **Ana Maria Solis Asencios** e ao meu pai **Robert Oscar Morales Solis**, por todo o amor, apoio incondicional e ensinamentos que me guiaram ao longo desta caminhada. Ao meu irmão **Gyan Pool Morales Solis**, por sua companhia e incentivo constantes.

Expresso minha sincera gratidão ao meu orientador, **Prof. Dr. Guilherme Chaud Tizziotti**, por sua orientação dedicada, paciência e por acreditar no meu potencial desde o início.

Aos meus amigos **Juan, Samanta, Raul, Josimar, Angela, Eduar, Nati, Ricardo, Fredy, Italo e Luna**, pelo companheirismo, pelas conversas e pela amizade que tornaram este percurso mais leve e significativo.

À **família Morales Solis**, pelo carinho e apoio ao longo da minha formação.

Ao corpo docente do programa de pós-graduação em Matemática da **Universidade Federal de Uberlândia (UFU)**, por todo o conhecimento compartilhado e pela formação sólida oferecida.

Agradeço também à **CAPES**, pelo financiamento e apoio essencial à realização deste mestrado.

MORALES SOLIS G.C.R.. *Uma introdução aos polinômios sobre corpos finitos.* 2025. 79 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, estudamos tópicos da teoria de corpos finitos. Inicialmente, exploramos a estrutura de corpos finitos, abrangendo desde propriedades básicas até representações de seus elementos, como as polinomiais, ciclotômicas e matriciais. Em seguida, concentramo-nos no estudo de polinômios sobre corpos finitos, destacando os polinômios de ordem definida, vinculados à estrutura dos grupos multiplicativos; os polinômios primitivos; e os polinômios irredutíveis, fundamentais para fatoração e construção de extensões de corpos. Por fim, examinamos os q-polinômios, que generalizam estruturas polinomiais clássicas.

Palavras-chave: corpos finitos, extensões algébricas, bases normais, polinômios ciclotômicos, polinômios primitivos, automorfismos de Frobenius, representações algébricas, q-polinômios.

MORALES SOLIS G.C.R.. *Uma introdução aos polinômios sobre corpos finitos.* 2025. 79 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study topics in finite field theory. Initially, we explore the structure of finite fields, covering from basic properties to representations of their elements, such as polynomial, cyclotomic, and matrix representations. Next, we focus on the study of polynomials over finite fields, highlighting: the order-defined polynomials, linked to the structure of multiplicative groups; the primitive polynomials; and the irreducible polynomials, fundamental for factorization and construction of field extensions. Finally, we examine q-polynomials, which generalize classical polynomial structures.

Keywords: finite fields, algebraic extensions, normal bases, cyclotomic polynomials, primitive polynomials, Frobenius automorphisms, algebraic representations, q-polynomials.

Lista de Símbolos

$\mathbb{N}$	conjunto dos números naturais.
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
$\mathbb{K}$	$\mathbb{R}$ ou $\mathbb{C}$
$\mathbb{Z}_n$	o grupo formado pelo conjunto de classes de equivalência modulo n
$\phi(n)$	Função Totiente de Euler de n
$\mathbb{F}_p$	Corpo de Galois de ordem p-primo
$R[x]$	anel formado pelos polinômios sobre R
$[\boldsymbol{L} : \boldsymbol{K}]$	a dimensão do espaço vectorial de $\boldsymbol{L}$ sobre $\boldsymbol{K}$
$R(f, g)$	resultante dos polinômios f e g
$\mathbb{F}_q$	Corpo de Galois de ordem $q = p^n$ com p-primo
$\mathbb{F}_q^*$	grupo multiplicativo do corpo $\mathbb{F}_q$
$\mathrm{Tr}_{F/K}(\alpha)$	aplicação traço de α sobre K
$\mathrm{N}_{F/K}(\alpha)$	aplicação norma de α sobre K
$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$	discriminante dos elementos $\alpha_1, \ldots, \alpha_m \in F$
$K^{(n)}$	n-ésimo corpo ciclotômico sobre K
$E^{(n)}$	conjunto de todas as raízes n-ésimas da unidade sobre K
$Q_n(x)$	Polinômio ciclotômico se ordem n sobre um corpo
$\mathrm{ord}(f)$	ordem do polinômio f
f^*	polinômio reciproco de f
$N_q(d)$	número de polinômios mônicos irredutíveis em $\mathbb{F}_q$ de grau d
$\mu(n)$	função de Möbius
$I(q, n; x)$	produto de todos polinômios mônicos e irredutíveis em $\mathbb{F}_q$ de grau n
$L(x)$	q-polinômio linearizado
$A(x)$	q-polinômio afim

Sumário

Introdução

A teoria de corpos finitos, consolidada como um tópico independente na matemática no final do século XIX, tem suas raízes em desenvolvimentos matemáticos que remontam ao século XVII. A evolução histórica dessa teoria passou por contribuições fundamentais nos séculos XVIII e XIX, culminando, em 1896, no trabalho *A doubly-infinite system of simple groups*, do americano Eliakim Hastings Moore (1862-1932), que introduziu a classificação de corpos finitos, feita principalmente com base na sua ordem, que é o número de elementos que o corpo possui, e estabeleceu as bases axiomáticas modernas para o estudo dos corpos finitos abstratos. Moore também foi responsável por estabelecer expressões como *field of order* s e *Galois-field of order* $s = q^n$.

Vale a pena mencionarmos que a denominação "Galois field" que homenageia as contribuições revolucionárias do matemático francês Évariste Galois (1811-1832), que aos 18 anos estabeleceu resultados fundamentais sobre a existência e estrutura dos corpos finitos, incluindo a classificação de corpos $\mathbb{F}_{p^n}$, a natureza cíclica de seus grupos multiplicativos, e a introdução do automorfismo de Frobenius. Paradoxalmente, muitos desses resultados haviam sido antecipados por Gauss (1777-1855) em manuscritos não publicados, seguindo um padrão histórico recorrente em suas descobertas. Gauss desenvolveu sua abordagem sob o título "Theoria Congruentiarum Superiorum", utilizando formulações baseadas em congruências polinomiais com notação distinta da linguagem moderna de corpos. Essa dicotomia histórica entre as formulações de Gauss e Galois revela como caminhos distintos convergiram para a teoria unificada que conhecemos hoje.

As origens da teoria também podem ser rastreadas através da obra monumental do matemático, também americano, Leonard Eugene Dickson (1874-1954), particularmente em sua obra "History of the Theory of Numbers", de 1919. Seus capítulos sobre divisibilidade, primalidade e congruências superiores documentam meticulosamente as contribuições pré-1918 que anteciparam conceitos posteriormente formalizados como corpos finitos. Dickson havia publicado anteriormente, em 1901, o primeiro tratado exclusivamente dedicado à teoria dos corpos finitos, "Linear Groups with an Exposition of the Galois Field Theory", cuja relevância perdurou até meados do século XX, quando abordagens geométricas mais modernas emergiram, especialmente através da influente obra "Geometric Algebra", do matemático austro-alemão de Emil Artin (1898-1962).

Além da contribuição na matemática pura, em que os corpos finitos contribuem para avanços em teoria dos números, geometria algébrica e combinatória, desde o século passado, observa-se que a teoria dos corpos finitos desempenha um papel fundamental em

diversas áreas da ciência e tecnologia moderna. Na criptografia, esses corpos fornecem a base matemática para sistemas de segurança essenciais, como a criptografia de chave pública, algoritmos de curvas elípticas e protocolos de autenticação digital. Na área de comunicações, são indispensáveis para códigos corretores de erros, como os códigos de Reed-Solomon, amplamente utilizados em sistemas de armazenamento de dados e transmissão digital.

A computação aproveita suas propriedades para desenvolver algoritmos eficientes de álgebra computacional e geração de números pseudoaleatórios. Aplicações emergentes incluem desde a computação quântica, onde auxiliam na correção de erros em qubits, até tecnologias blockchain, que dependem de operações sobre esses corpos para garantir segurança e integridade. Tanto o desenvolvimento teórico quanto suas aplicações passam muito por polinômios sobre corpos finitos $\mathbb{F}_q$, um objeto com uma estrutura algébrica rica, cuja importância surge da interação entre suas propriedades algébricas fundamentais e eficiência computacional. Como exemplos disso, podemos citar a fatoração única de polinômios, uma propriedade essencial para a resolução de equações, ou a construção de extensões de corpos $\mathbb{F}_{q^m}$ via polinômios irredutíveis. Uma aplicação prática é a geração de elementos de ordem máxima: um polinômio primitivo $f \in \mathbb{F}_2[x]$ de grau m satisfazendo

$$x^r \equiv (-1)^m f(0) \bmod f(x) \quad \text{com} \quad r = \frac{2^m - 1}{2 - 1}$$

pode gerar elementos de ordem $2^m - 1$ em $\mathbb{F}_{2^m}$, algo crucial para sequências pseudoaleatórias em criptografia.

Esta dissertação, baseada na obra clássica "Introduction to finite fields and their applications"de Rudolf Lidl e Harald Niederreiter [11], apresenta uma introdução à teoria de corpos finitos e ao estudo de polinômios sobre esses corpos. A dissertação está organizada em três capítulos, que desenvolvem progressivamente os conceitos fundamentais do tema. No Capítulo 1, denominado Preliminares, estabelecemos os fundamentos teóricos necessários, revisitando conceitos essenciais de álgebra abstrata. Além disso fixamos a notação que será adotada consistentemente ao longo do trabalho, garantindo clareza na apresentação dos resultados posteriores. No Capítulo 2, aprofundamos o estudo dessas estruturas algébricas. Inicialmente, examinamos as propriedades fundamentais que caracterizam os corpos finitos, incluindo sua existência e unicidade. Em seguida, investigamos diferentes representações desses corpos através do estudo de bases, com ênfase especial nas bases normais. A terceira parte do capítulo dedica-se às raízes da unidade e sua conexão com os polinômios ciclotômicos. Finalmente, exploramos diversas maneiras de representar os elementos de corpos finitos, incluindo abordagens polinomiais e matriciais. O último capítulo desta dissertação, o Capítulo 3, concentra-se no estudo sistemático de polinômios com coeficientes em corpos finitos. Analisamos critérios de irredutibilidade, técnicas de fatoração e propriedades dos polinômios mínimos.

Através desta estrutura, a dissertação oferece uma introdução à teoria de corpos finitos, servindo tanto como base para estudos mais avançados quanto como referência para aplicações em estudos futuros.

Gyan Carlos Robert Morales Solis
Uberlândia-MG, 24 de julho de 2025.

Capítulo 1

Preliminares

Este trabalho tem como objetivo principal o estudo de polinômios sobre corpos finitos. Para tal, utilizaremos diversos conceitos e resultados fundamentais da teoria de grupos e da teoria de anéis, cuja apresentação será omitida aqui. Neste capítulo, apresentaremos de forma concisa alguns conceitos e resultados essenciais, além de notações, que servirão de base para o desenvolvimento dos tópicos abordados nos capítulos subsequentes.

Começamos com o conceito de característica de um anel. Seja A um anel arbitrário. Se existe um inteiro positivo n tal que $na = 0$, para todo $a \in A$, então, o menor inteiro positivo com essa propriedade é chamado de *característica de* A e diz-se que A tem *característica (positiva)* n. Se nenhum inteiro positivo com essa propriedade existir, então diz-se que o anel A tem *característica 0*.

Um corpo finito com q elementos será denotado por $\mathbb{F}_q$. Sabemos que q é uma potência de um número primo p e que a característica de $\mathbb{F}_q$ é p (veja [11, Corolário 1.45]).

O resultado a seguir é bastante útil no estudo de polinômios sobre corpos finitos.

Teorema 1.0.1. *Seja A um anel comutativo de característica prima p. Então,*

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

para $a, b \in A$ e $n \in \mathbb{N}$.

Demonstração. Como p-primo é característica de A, então $p.a = 0$ para todo $a \in A$, então temos por indução:

- Para $n = 1$ obtemos

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}b^k + b^p,$$

mas sabemos que se $0 < k < p$ então p divide $\binom{p}{k}$ pois

$$\binom{p}{k} = \frac{p.(p-1).\cdots.(p-k+1)}{k!}$$

e portanto nenhum fator de $k!$ divide p. Assim o primeiro fator do numerador não será simplificado e o resto ainda resultará em um inteiro, logo:

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \frac{(p-1).\cdots.(p-k+1)}{k!} \underbrace{pa^{p-k}b^k}_{0} + b^p = a^p + b^p.$$

- Assumimos para o caso $n-1$, o que significa que satisfaz:

$$(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}.$$

Então verificamos o caso n:

$$(a+b)^{p^n} = \left((a+b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = a^{p^n} + b^{p^n}.$$

O caso de $a-b$ é consequência direta do primeiro caso.

□

Um *polinômio* sobre um anel A é uma expressão da forma

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

em que n é um número inteiro não negativo, os coeficientes $a_i \in A$ e x é uma indeterminada (símbolo que não pertence a A). Quando estiver claro o significado de x, também podemos nos referir ao polinômio apenas por f.

Convencionamos que termos da forma $a_i x^i$, com $a_i = 0$, podem ser omitidos. Assim, um polinômio pode ser representado como

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + \cdots + 0x^{n+h},$$

para qualquer inteiro positivo h. Dessa forma, podemos comparar dois polinômios assumindo que ambos envolvem as mesmas potências de x.

Dois polinômios

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{e} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

são *iguais* se, e somente se, $a_i = b_i$ para todo $0 \leq i \leq n$.

A *soma* de $f(x)$ e $g(x)$ é definida por:

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Para definir o *produto* de dois polinômios, sejam:

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{e} \quad g(x) = \sum_{j=0}^{m} b_j x^j,$$

então:

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{onde} \quad c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq n, 0 \leq j \leq m}} a_i b_j.$$

Com essas operações, o conjunto dos polinômios sobre A forma um anel.

Definição 1.0.2. O anel formado pelos polinômios sobre A, com as operações definidas anteriormente, é chamado de *anel de polinômios sobre* A e é denotado por $A[x]$.

Seja $f(x) = \sum_{i=0}^{n} a_i x^i$ um polinômio sobre A que não seja o polinômio nulo, de modo que possamos supor $a_n \neq 0$. Então, a_n é chamado de *coeficiente líder* de $f(x)$, e a_0, o *termo constante*, enquanto n é chamado de *grau de* $f(x)$, ou seja, $n = \deg(f(x)) = \deg(f)$. Por convenção, definimos $\deg(0) = -\infty$. Polinômios de grau ≤ 0 são chamados de *polinômios constantes*. Se A possui identidade 1 e o coeficiente líder de $f(x)$ for igual a 1, então $f(x)$ é chamado de *polinômio mônico*.

Dizemos que o polinômio $f(x)$ é *irredutível* sobre A (ou irredutível em $A[x]$), se f tem grau positivo e se $f = gh$, com $g, h \in A[x]$ implica que ou g ou h é um polinômio constante. Um elemento $b \in A$ é chamado de *raiz* (ou *zero*) do polinômio $f(x)$ se $f(b) = 0$.

Definição 1.0.3. Seja F um corpo e $b \in F$ uma raiz do polinômio $f \in F[x]$. Se existir um inteiro positivo k tal que $f(x)$ seja divisível por $(x-b)^k$, mas não por $(x-b)^{k+1}$, então chamamos k de *multiplicidade* de b.

- Se $k = 1$, dizemos que b é uma *raiz simples* (ou *zero simples*) de f.
- Se $k \geq 2$, então b é uma *raiz múltipla* (ou *zero múltiplo*) de f.

Seja $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$. A *derivada* de f, denotada por f' ou $f'(x)$, é definida por

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in F[x].$$

Teorema 1.0.4. *Seja K um corpo, f un polinômio sobre K de grau ≥ 1 e seja α uma raiz de f, em K. Então a multiplicidade de α em f é maior que 1 se, e somente se, $f'(\alpha) = 0$*

Demonstração. Veja [12, Teorema 4.3.6]. □

Finalizamos este capítulo com alguns conceitos e resultados relacionados à extensões de corpos.

Seja F um corpo. Um subconjunto $K \subseteq F$ que também seja um corpo com as operações de F é chamado de *subcorpo* de F. Nesse caso, F é dito ser uma *extensão* (ou extensão do corpos) de K. Quando $K \neq F$, dizemos que K é um *subcorpo próprio* de F.

Se K é um subcorpo do corpo finito $\mathbb{F}_p$, com p primo, então K deve conter os elementos 0 e 1 e, consequentemente, conterá todos os elementos de $\mathbb{F}_p$. Assim, concluímos que $\mathbb{F}_p$ não possui subcorpos próprios. Isso motiva a seguinte definição.

Definição 1.0.5. Um *corpo primo* é um corpo que não possui subcorpos próprios, ou seja, ele não contém nenhum subcorpo além de si mesmo.

Teorema 1.0.6. *O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou $\mathbb{Q}$, dependendo de a característica de F ser um primo p ou 0.*

Demonstração. Veja [1, Corolario 2.9.7]. □

Definição 1.0.7. Seja K um subcorpo de F e seja $\theta \in F$. Dizemos que θ é *algébrico sobre K* se existe um polinômio não trivial com coeficientes em K tal que θ seja uma raiz, isto é,

$$a_n \theta^n + \cdots + a_1 \theta + a_0 = 0,$$

com $a_i \neq 0$ para algum $i \in \{0, 1, \ldots, n\}$.

Uma extensão L de K é chamada de *extensão algébrica sobre K* se todo elemento de L for algébrico sobre K.

Se $\theta \in F$ é algébrico sobre K, então o polinômio mônico $g \in K[x]$, ele existem pois $K[x]$ é um DIP, unicamente determinado, que gera o ideal $J = \langle f \in K[x] : f(\theta) = 0 \rangle$ de $K[x]$, é chamado de *polinômio mínimo* (ou polinômio definidor, ou polinômio irredutível) de θ sobre K. Pelo grau de θ sobre K, entendemos o grau de g.

Teorema 1.0.8. *Se $\theta \in F$ é algébrico sobre K, então seu polinômio mínimo g sobre K tem as seguintes propriedades:*

(i) g é irredutível em $K[x]$.

(ii) Para $f \in K[x]$, temos $f(\theta) = 0$ se, e somente se, g divide f.

(iii) g é o polinômio mônico em $K[x]$ de menor grau que tem θ como raiz.

.

Demonstração. Veja [11, Teorema 1.82]. □

Seja L uma extensão de corpos de K. Se L, considerado como um espaço vetorial sobre K, tem dimensão finita, então L é chamada de uma *extensão finita* de K. A dimensão do espaço vetorial L sobre K é chamada de grau de L sobre K, denotado por $[\ L : K\ ]$.

Teorema 1.0.9. *Se L é uma extensão finita de K e M é uma extensão finita de L, então M é uma extensão finita de K com*

$$[M : K] = [M : L][L : K].$$

Demonstração. Veja [11, Teoream 1.84]. □

Seja K um corpo e θ um elemento algébrico sobre K. O corpo $K(\theta)$ denota a menor extensão de corpos que contém K e θ, ou seja, a interseção de todos os corpos contendo K e θ. Equivalentemente, é o corpo gerado por θ sobre K.

Teorema 1.0.10. *Seja $\theta \in F$ algébrica de grau n sobre K e seja g o polinômio mínimo de θ sobre K. Então:*

(i) $K(\theta)$ é isomorfo a $K[x]/\langle g \rangle$.

(ii) $[K(\theta) : K] = n$ e $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K.

(iii) Todo $\alpha \in K(\theta)$ é algébrico sobre K e seu grau sobre K é um divisor de n.

Demonstração. Veja [11, Teorema 1.86]. □

Seja F um corpo e $f(x)$ um polinômio não constante em $F[x]$. Diz-se que E é um *corpo de decomposição* de $f(x)$ sobre F, se E é uma extensão finita de F e $f(x)$ decompõe-se como um produto de fatores lineares em $E[x]$, mas não em outra extensão de K tal que $[K : F] < [E : F]$. O resultado a seguir, garante a existência e a unicidade do corpo de decomposição de um polinômio.

Teorema 1.0.11. *Se K é um corpo e f é um polinômio de grau positivo em $K[x]$, então existe um corpo de decomposição de f sobre K. Quaisquer dois corpos de decomposição de f sobre K são isomorfos sob um isomorfismo que mantém os elementos de K fixos e mapeia as raízes de f entre si.*

Demonstração. Veja [7, Teorema 4.1.12 e Corolario 4.1.18]. □

Definição 1.0.12. Seja $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$ e $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in K[x]$ dois polinômios de grau formal n e m, respectivamente, com $n, m \in \mathbb{N}$ (isto é, escritos com termo dominante de grau n e m, independentemente de os coeficientes principais serem nulos ou não).

A *resultante* $R(f, g)$ dos dois polinômios é definida pelo determinante

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & & \cdots & b_m \end{vmatrix}$$

de ordem $m + n$ (onde os coeficientes de f vão sendo distribuídos da esquerda para a direita em m linhas, e os de g, em n linhas).

Se $\deg(f) = n$ (ou seja, se $a_0 \neq 0$) e $f(x) = a_0(x - \alpha_1)\cdots(x - \alpha_n)$ no corpo de decomposição de f sobre K, então $R(f, g)$ também é dado pela fórmula:

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i).$$

Note que $R(f, g) = 0$ se, e somente se, f e g têm uma raiz comum, o que é o mesmo que dizer que f e g têm um divisor comum em $K[x]$ de grau positivo , conforme descrito em [11, p. 36].

Capítulo 2

Uma introdução à teoria de corpos finitos

Neste capítulo, faremos um estudo sobre a estrutura algébrica dos corpos finitos, apresentando os principais resultados teóricos e suas aplicações. A teoria de corpos finitos desempenha um papel fundamental em diversas áreas da matemática, incluindo teoria dos números, álgebra abstrata e criptografia, além de terem importantes aplicações em teoria de códigos e combinatória. Nosso estudo será organizado em seis seções, cada uma abordando aspectos fundamentais desta teoria:

1. **Propriedades fundamentais dos corpos finitos**: Estabeleceremos os resultados básicos sobre existência e unicidade de corpos finitos, incluindo a classificação completa via suas cardinalidades.

2. **Bases de corpos finitos**: Desenvolveremos os operadores de traço e norma, e estudaremos diferentes tipos de bases para extensões de corpos finitos.

3. **Raízes da unidade e polinômios ciclotômicos**: Analisaremos a estrutura das raízes da unidade em corpos finitos e suas conexões com os polinômios ciclotômicos.

4. **Representação dos elementos**: Discutiremos diferentes métodos para representar computacionalmente os elementos de corpos finitos e suas vantagens.

Através desta abordagem estruturada, pretendemos não apenas apresentar os resultados teóricos fundamentais sobre corpos finitos, mas também destacar as conexões entre esses tópicos e suas aplicações. O capítulo servirá como base teórica para os desenvolvimentos posteriores desta dissertação.

2.1 Propriedades fundamentais dos corpos finitos

Para cada número primo p, o anel de classes residuais $\mathbb{Z}/(p)$ constitui um corpo finito com p elementos, sendo comumente identificado com o corpo de Galois $\mathbb{F}_p$. Esses corpos desempenham um papel essencial na teoria dos corpos, pois qualquer corpo de característica p contém uma cópia isomórfica de $\mathbb{F}_p$ e pode ser descrito como uma extensão deste. Essa constatação, aliada ao fato de que todo corpo finito possui característica prima, é

crucial para a classificação dos corpos finitos. Com base nisso, obtém-se uma condição necessária sobre a quantidade de elementos que um corpo finito pode possuir.

Lema 2.1.1. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então, F possui q^m elementos, onde $m = [F : K]$.*

Demonstração. Seja F um corpo finito que contém um subcorpo K com q elementos. Como F é uma extensão finita de K, podemos considerar F como um espaço vetorial sobre K, com dimensão $m = [F : K]$.

Isso significa que existe uma base $\{b_1, b_2, \ldots, b_m\}$ de F sobre K, de modo que qualquer elemento $x \in F$ pode ser escrito de maneira única como

$$x = a_1 b_1 + a_2 b_2 + \cdots + a_m b_m,$$

onde $a_1, a_2, \ldots, a_m$ pertencem a K.

Como K tem exatamente q elementos, cada coeficiente a_i pode assumir q valores distintos. Como há m coeficientes independentes, o número total de combinações possíveis para formar elementos de F é q^m. Portanto, F contém exatamente q^m elementos, como queríamos demonstrar. □

Teorema 2.1.2. *Seja F um corpo finito. Então F tem p^n elementos, onde p é o primo que é a característica de F e n é o grau de F sobre seu subcorpo primo.*

Demonstração. Como F é finito, sua característica é um primo p. Portanto, o subcorpo primo K de F (ele existe pois, se tomamos a interseção de todos os subcorpos de F, obtemos o subcorpo primo de F, e F é subcorpo de F) é isomorfo a $\mathbb{F}_p$ pelo Teorema 1.0.6 e, assim, contém p elementos. Fazemos $n = [F : K]$. A afirmação segue do Lema 2.1.1, ou seja, F tem p^n elementos. □

A partir dos corpos primos $\mathbb{F}_p$, é possível formar corpos finitos maiores por meio da adição de raízes de polinômios. Quando se tem um polinômio irredutível $f \in \mathbb{F}_p[x]$ de grau n, pode-se construir um corpo com p^n elementos ao se incluir uma de suas raízes ao corpo $\mathbb{F}_p$. No entanto, até aqui, ainda não se assegura que exista, para todo inteiro positivo n, um polinômio irredutível de grau n em $\mathbb{F}_p[x]$. Para provar que, dados um número primo p e um natural n, sempre existe um corpo finito com exatamente p^n elementos, utilizamos uma estratégia fundamentada em certos teoremas específicos.

Lema 2.1.3. *Se F é um corpo finito com q elementos, então todo $a \in F$ satisfaz $a^q = a$.*

Demonstração. A identidade $a^q = a$ é trivial para $a = 0$. Por outro lado, os elementos não nulos de F formam um grupo de ordem $q - 1$ sobre a multiplicação. Assim, $a^{q-1} = 1$ para todo $a \in F$ com $a \neq 0$, e a multiplicação por a fornece o resultado desejado. □

Lema 2.1.4. *Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $x^q - x$ em $K[x]$ se fatoriza em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a)$$

e F é um corpo de decomposição de $x^q - x$ sobre K.

Demonstração. O polinômio $x^q - x$, de grau q, tem no máximo q raízes em F. Pelo Lema 2.1.3, sabemos que existem exatamente q raízes, ou seja, todos os elementos de F são raízes desse polinômio. Assim, o polinômio dado se decompõe em F da maneira indicada, e ele não pode se decompor em nenhum corpo menor. □

Agora somos capazes de provar o principal teorema de caracterização para corpos finitos

Teorema 2.1.5 (Existência e Unicidade dos Corpos Finitos)**.** *Para todo número primo p e todo inteiro positivo n, existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. **(Existência)** Seja $q = p^n$, onde p é primo e $n \geq 1$. Considere o polinômio $f(x) = x^q - x \in \mathbb{F}_p[x]$, e seja F o seu corpo de decomposição sobre $\mathbb{F}_p$.

Afirmamos que f possui q raízes distintas em F. De fato, sua derivada formal é

$$f'(x) = qx^{q-1} - 1 = p^n x^{q-1} - 1 = -1 \neq 0,$$

pois $p = 0$ em $\mathbb{F}_p$. Como $\gcd(f, f') = 1$, segue do critério de separabilidade (Teorema 1.0.4) que f não possui raízes múltiplas. Portanto, f decompõe-se completamente em F com q raízes distintas.

Defina $S = \{a \in F \mid a^q - a = 0\}$, o conjunto das raízes de f em F. Vamos mostrar que S é um subcorpo de F:

(i) **Contém 0 e 1:** $0^q - 0 = 0$ e $1^q - 1 = 0$, logo $0, 1 \in S$.

(ii) **Fechado sob subtração:** Se $a, b \in S$, então pelo Teorema 1.0.1 (o homomorfismo de Frobenius),

$$(a - b)^q = a^q - b^q = a - b,$$

donde $a - b \in S$.

(iii) **Fechado sob inverso multiplicativo:** Se $a, b \in S$ com $b \neq 0$, então

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1},$$

logo $ab^{-1} \in S$.

Assim, S é um subcorpo de F. Como S contém todas as raízes de f e F é gerado por essas raízes, segue que $F \subseteq S$. Por outro lado, $S \subseteq F$ por definição. Portanto, $F = S$, e como $|S| = q$, concluímos que F é um corpo finito com q elementos.

(Unicidade) Seja F um corpo finito qualquer com $q = p^n$ elementos. Pelo Teorema 2.1.2, F tem característica p e contém $\mathbb{F}_p$ como subcorpo primo. Além disso, pelo Lema 2.1.4, todo elemento de F é raiz de $x^q - x$, e assim F é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.

A unicidade segue do fato de que corpos de decomposição são únicos a menos de isomorfismo (Teorema 1.0.11). □

A unicidade garantida pelo Teorema 2.1.5 justifica a utilização da expressão corpo finito (ou corpo de Galois) com q elementos, ou ainda corpo finito de ordem q. Esse corpo é denotado por $\mathbb{F}_q$, considerando-se que q é uma potência de um número primo p, o qual é a característica de $\mathbb{F}_q$. Muitos autores também empregam a notação $GF(q)$.

Teorema 2.1.6. *Seja $\mathbb{F}_q$ o corpo finito com $q = p^n$ elementos. Então, 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 exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. É evidente que qualquer subcorpo K de $\mathbb{F}_q$ deve possuir p^m elementos para algum inteiro positivo $m \leqslant n$. Usando o Lema 2.1.1, como $q = p^n$, essa quantidade deve ser uma potência de p^m, ou seja, podemos escrever $p^n = (p^m)^r$ para algum inteiro r. Assim, m precisa ser um divisor de n.

Por outro lado, suponha que m seja um divisor positivo de n. Nesse caso, $p^m - 1$ divide $p^n - 1$ (pelo estudo de quocientes notáveis), o que implica que $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$ no anel $\mathbb{F}_p[x]$. Como consequência, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ em $\mathbb{F}_p[x]$. Isso significa que todas as raízes de $x^{p^m} - x$ também são raízes de $x^q - x$ e, portanto, pertencem a $\mathbb{F}_q$. Dessa forma, $\mathbb{F}_q$ contém um corpo de decomposição do polinômio $x^{p^m} - x$ sobre $\mathbb{F}_p$, e conforme demonstrado no Teorema 2.1.5, esse corpo tem exatamente p^m elementos.

Se existissem dois subcorpos distintos de $\mathbb{F}_q$ com p^m elementos, juntos eles conteriam mais de p^m raízes do polinômio $x^{p^m} - x$ dentro de $\mathbb{F}_q$, o que levaria a uma contradição. Assim, tal subcorpo é único, completando a demonstração. □

A demonstração do Teorema 2.1.6 mostra que o único subcorpo de $\mathbb{F}_{p^n}$ com ordem p^m, onde m é um divisor positivo de n, consiste precisamente das raízes do polinômio $x^{p^m} - x \in \mathbb{F}_p[x]$ em $\mathbb{F}_{p^n}$.

Exemplo 2.1.7. Vamos ver 2 exemplos:

(i) Os subcorpos do corpo finito $\mathbb{F}_{2^{30}}$ podem ser determinados listando todos os divisores positivos de 30. As relações de inclusão entre esses diversos subcorpos são mostradas no diagrama a seguir.

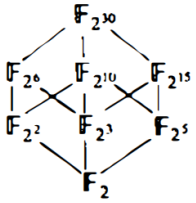

Figura 2.1: Relações de contensão dos subcorpos de $\mathbb{F}_{2^{30}}$. Extraído de [11, Exemplo 2.7].

(ii) Seja p um número primo. Os subcorpos do corpo finito $\mathbb{F}_{p^{105}}$ são:

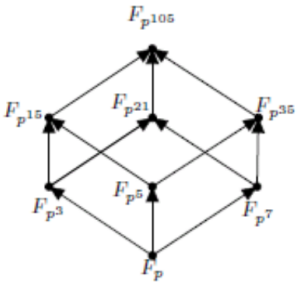

Figura 2.2: Relações de contensão dos subcorpos de $\mathbb{F}_{p^{105}}$. Extraído de [9, Exemplo 1.3.12].

Para um corpo finito $\mathbb{F}_q$, denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo dos elementos não nulos de $\mathbb{F}_q$. O seguinte resultado enuncia uma propriedade útil desse grupo.

Teorema 2.1.8. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ dos elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Podemos assumir que $q > 3$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para cada i, $1 \leqslant i \leqslant m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes em $\mathbb{F}_q$. Como $h/p_i < h$, segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um desses elementos e defina $b_i = a_i^{h/p_i^{r_i}}$. Temos $b_i^{p_i^{r_i}} = 1$ (pois como $a_i \in \mathbb{F}_q$ então $a_i^h = 1$), portanto a ordem de b_i é um divisor de $p_i^{r_i}$ e, portanto, é da forma $p_i^{s_i}$ com $0 \leqslant s_i \leqslant r_i$. Por outro lado,

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$$

(pois a_i não é raiz do polinômio $x^{h/p_i} - 1$) e assim a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. Suponha, ao contrário, que a ordem de b é um divisor próprio de h e, portanto, é divisor de pelo menos um dos m inteiros $h/p_i, 1 \leqslant i \leqslant m$, digamos de h/p_1. Então temos

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Agora, para $2 \leqslant i \leqslant m$, cumpre que $p_i^{r_i}$ divide h/p_1, e portanto $b_i^{h/p_1} = 1$. Assim, $b_1^{h/p_1} = 1$. Isso implica que a ordem de b_1 deve dividir h/p_1, o que é impossível, já que a ordem de b_1 é $p_1^{r_1}$. Assim, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 2.1.9. Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo de $\mathbb{F}_q$.

Usando resultados da teoria de grupos, podemos concluir que $\mathbb{F}_q$ contém $\phi(q-1)$ elementos primitivos, onde ϕ é a função de Euler. A existência de elementos primitivos pode ser usada para demonstrar um resultado que implica, em particular, que todo corpo finito pode ser pensado como uma extensão algébrica simples de seu subcorpo primo.

Teorema 2.1.10. *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ 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 $\mathbb{F}_r$ pode servir como elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Relembre que $K(\alpha)$ é formado por todas as expressões da forma:

$$K(\alpha) = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \;\middle|\; a_i \in K \right\},$$

onde o grau de α sobre K depende do grau do polinômio mínimo de α em K.

Seja ζ um elemento primitivo de $\mathbb{F}_r$. Claramente, temos $\mathbb{F}_q(\zeta) \subseteq \mathbb{F}_r$ (pois $\zeta \in \mathbb{F}_r$ e $\mathbb{F}_q \subset \mathbb{F}_r$). Por outro lado, $\mathbb{F}_q(\zeta)$ contém 0 e todas as potências de ζ, e portanto, todos os elementos de $\mathbb{F}_r$. Logo, $\mathbb{F}_r = \mathbb{F}_q(\zeta)$. □

Corolário 2.1.11. *Para todo corpo finito $\mathbb{F}_q$ e todo número inteiro positivo n, existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Demonstração. Seja $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$ de ordem q^n, de modo que $[\mathbb{F}_r : \mathbb{F}_q] = n$ pelo Lema 2.1.1. Logo pelo Teorema 2.1.10, temos $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ para algum $\zeta \in \mathbb{F}_r$, que é um elemento primitivo de $\mathbb{F}_r$. Então, o polinômio mínimo de ζ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n (pois $[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = [\mathbb{F}_r : \mathbb{F}_q] = n$), de acordo com os Teoremas 1.0.8 (i) e 1.0.10 (ii). □

2.2 Bases de corpos finitos

Considerando $F = \mathbb{F}_{q^m}$ como uma extensão finita do corpo finito $K = \mathbb{F}_q$ sob a perspectiva de espaço vetorial sobre K, temos que F possui dimensão m sobre K. Assim, qualquer conjunto $\{\alpha_1, \ldots, \alpha_m\}$ que forme uma base de F sobre K permite que cada elemento $\alpha \in F$ seja representado de maneira única na forma

$$\alpha = c_1\alpha_1 + \cdots + c_m\alpha_m, \quad \text{com } c_j \in K \text{ para } 1 \leq j \leq m.$$

As bases são fundamentais para a compreensão e manipulação de corpos finitos, permitindo uma representação sistemática dos elementos do corpo, facilitando a realização de diversas operações algébricas e suas aplicações. Nessa seção faremos um estudo sobre esse conceito. Para isso, será necessário estudos prévios envolvendo raízes de polinômios irredutíveis, o traço e a norma de elementos em corpos finitos.

Começamos esta seção reunindo algumas informações sobre o conjunto de raízes de um polinômio irredutível sobre um corpo finito.

Lema 2.2.1. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre um corpo finito $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão de corpos de $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$, temos que $h(\alpha) = 0$ se, e somente se, f divide h.*

Demonstração. Seja a o coeficiente líder de f e defina $g(x) = a^{-1}f(x)$. Então, g é um polinômio mônico irredutível em $\mathbb{F}_q[x]$ com $g(\alpha) = 0$, e assim é o polinômio mínimo de α sobre $\mathbb{F}_q$ (a ideia de irredutibilidade nos dá uma resposta ao polinômio de grau mais baixo que tem α como raiz). O resultado segue diretamente do Teorema 1.0.8(ii). □

Lema 2.2.2. *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. Temos o seguinte:

($\Rightarrow$) Suponha que $f(x)$ divide $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, de modo que $\alpha \in \mathbb{F}_{q^n}$ (lembrando no Lema 2.1.3). Segue-se que $\mathbb{F}_q(\alpha)$ é um subcorpo de $\mathbb{F}_{q^n}$. Mas, como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ (lembrando Teorema 1.0.10(ii) e a hipótese que fala que o grau de f é m) e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, o Teorema 1.0.9 mostra que m divide n pois

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \underbrace{[\mathbb{F}_q(\alpha) : \mathbb{F}_q]}_{m}.$$

($\Leftarrow$) Por outro lado, se m divide n, então o Teorema 2.1.6 implica que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como um subcorpo ($\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$). Se α é uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, e assim $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ (lembre o Lema 2.1.1). Consequentemente, temos $\alpha \in \mathbb{F}_{q^n}$, logo $\alpha^{q^n} = \alpha$. Portanto, α é uma raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Concluímos então, pelo Lema 2.2.1, que $f(x)$ divide $x^{q^n} - x$.

□

O seguinte resultado fundamental descreve completamente o comportamento das raízes de um polinômio irredutível $f \in \mathbb{F}_q[x]$.

Teorema 2.2.3. *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m, então f possui uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e são dadas pelos m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ (Lema 2.1.1), e, em particular, $\alpha \in \mathbb{F}_{q^m}$.

Agora, mostraremos que se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f, então β^q também é uma raiz de f. Escreva $f(x) = a_m x^m + \cdots + a_1 x + a_0$, com $a_i \in \mathbb{F}_q$ para $0 \leqslant i \leqslant m$. Então, usando o Lema 2.1.3 e o Teorema 1.0.1, obtemos:

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \cdots + a_1 \beta^q + a_0 = a_m^q \beta^{qm} + \cdots + a_1^q \beta^q + a_0^q \\ &= (a_m \beta^m + \cdots + a_1 \beta + a_0)^q = f(\beta)^q = 0. \end{aligned}$$

Assim, provamos que α^q é uma raiz, mas se seguirmos a mesma ideia para $\alpha^{q^2}, \alpha^{q^3}, ..., \alpha^{q^{m-1}}$, também conseguiremos o resultado. No entanto, observamos que paramos este processo em α^{q^m}, pois $\alpha^{q^m} = \alpha$.

Portanto, os elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ são raízes de f. Resta provar que esses elementos são distintos.

Suponha, ao contrário, que $\alpha^{q^j} = \alpha^{q^k}$ para alguns inteiros j e k com $0 \leqslant j < k \leqslant m-1$. Elevando essa identidade à potência q^{m-k}, obtemos:

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Então, pelo Lema 2.2.1, segue que $f(x)$ divide $x^{q^{m-k+1}} - x$. Pelo Lema 2.2.2, isso só é possível se m divide $m - k + j$. Mas temos $0 < m - k + j < m$, e assim chegamos a uma contradição. □

Os seguintes corolários são consequências diretas da estrutura das raízes de polinômios irredutíveis sobre corpos finitos e revelam propriedades importantes sobre a relação entre polinômios irredutíveis e extensões de corpos finitos.

Corolário 2.2.4. *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m. Então, o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.*

Demonstração. O Teorema 2.2.3 mostra que f se decompõe em $\mathbb{F}_{q^m}$. Além disso, temos que $\mathbb{F}_q\left(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ para uma raiz α de f em $\mathbb{F}_{q^m}$, onde a segunda identidade é obtida a partir da prova do Teorema 2.2.3. □

Corolário 2.2.5. *Quaisquer dois polinômios irredutíveis em $\mathbb{F}_q[x]$ de mesmo grau têm corpos de decomposição isomorfos.*

Demonstração. O resultado segue do fato, visto no resultado anterior, que qualquer polinômio irredutível de grau m tem como corpo de decomposição $\mathbb{F}_{q^m}$. □

A seguir, introduzimos uma terminologia conveniente para os elementos que aparecem no Teorema 2.2.3, independentemente de $\alpha \in \mathbb{F}_{q^m}$ ser uma raiz de um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m ou não.

Definição 2.2.6. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então, os elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ são chamados os conjugados de α com respeito a $\mathbb{F}_q$.

Seja E uma extensão do corpo do corpo K, E é chamada *normal* se todo polinômio mínimo sobre K de um elemento de E se fatorar completamente em E. No caso de corpos finitos, toda extensão finita $\mathbb{F}_{q^m}$ do corpo finito $\mathbb{F}_q$ é normal, pois $\mathbb{F}_{q^m}$ é o corpo de decomposição de $x^{q^m} - x$ sobre $\mathbb{F}_q$.

Seja $\alpha \in \mathbb{F}_{q^m}$. A estrutura dos conjugados de α sobre $\mathbb{F}_q$ é determinada pelo seu polinômio mínimo $P_\alpha \in \mathbb{F}_q[x]$:

Proposição 2.2.7. *Os seguintes resultados sobre conjugados são válidos:*

(i) Se $\deg(P_\alpha) = m$, *então α possui exatamente m conjugados distintos sobre $\mathbb{F}_q$, dados por:*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

(ii) Se $\deg(P_\alpha) = d$ *com $d \mid m$ e $d < m$, então:*

- *Os conjugados distintos são $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$;*
- *Cada conjugado aparece com multiplicidade $\frac{m}{d}$ no conjunto completo de m conjugados, ou seja, os conjugados de α sobre $\mathbb{F}_q$ serão os elementos distintos $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, cada um aparecendo m/d vezes;*
- *O corpo $\mathbb{F}_q(\alpha)$ é isomorfo a $\mathbb{F}_{q^d}$.*

Justificativa. A estrutura dos conjugados segue diretamente:

- Da ação do grupo de Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \cong \langle\sigma\rangle$, onde σ é o automorfismo de Frobenius de grau q,
- Da relação $\deg(P_\alpha) = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$, e
- Do fato que $\mathbb{F}_{q^m}$ é uma extensão normal de $\mathbb{F}_q$.

□

Teorema 2.2.8. *Os conjugados de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ têm a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Pelo Teorema 2.1.8, temos que $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1$. Seja $q = p^n$ com p primo e tomemos $r = p^m$, onde m divide n. Então, podemos escrever $n = k \cdot m$ para algum inteiro k. Portanto, $\mathbb{F}_r$ é um subcorpo de $\mathbb{F}_q$.

Se quisermos considerar os conjugados de α com respeito a $\mathbb{F}_r$, os elementos são da forma

$$\alpha, \alpha^r, \alpha^{r^2}, \ldots, \alpha^{r^{k-1}}.$$

A lista anterior pode ser reescrita como:

$$\alpha, \alpha^{p^m}, \alpha^{p^{2m}}, \ldots, \alpha^{p^{(k-1)m}}.$$

Agora, seja ζ um elemento primitivo de $\mathbb{F}_q$. Então, podemos escrever $\alpha = \zeta^t$ para algum t inteiro. Portanto, a lista de conjugados se reescreve como:

$$\zeta^t, \zeta^{tp^m}, \zeta^{tp^{2m}}, \ldots, \zeta^{tp^{(k-1)m}}.$$

Observamos que $\mathrm{mdc}(tp^{im}; p^n - 1) = \mathrm{mdc}(t; p^n - 1)$ para todo i inteiro não negativo menor ou igual a $k-1$. Isso implica que a ordem de cada conjugado é a mesma que a de α.

Portanto, demonstramos que todos os conjugados de α têm a mesma ordem no grupo $\mathbb{F}_q^*$. □

Teorema 2.2.9. *Se α é um elemento primitivo de $\mathbb{F}_q$, então o mesmo ocorre para todos os seus conjugados com respeito a qualquer subcorpo de $\mathbb{F}_q$.*

Demonstração. A prova é a mesma que a anterior, considerando $t = 1$, de modo que a ordem de todos os conjugados é $q-1$. □

Exemplo 2.2.10. Seja $\alpha \in \mathbb{F}_8$ uma raiz do polinômio irredutível $f(x) = x^3+x+1 \in \mathbb{F}_2[x]$. Então os conjugados de α sobre $\mathbb{F}_2$ são:

$$\alpha, \quad \alpha^2, \quad \alpha^4 = \alpha^2 + \alpha.$$

O grupo multiplicativo $\mathbb{F}_8^*$ é gerado por α e seus elementos podem ser escritos como combinações lineares de 1, α e α^2 da seguinte forma:

$$\begin{aligned}
\alpha^0 &= 1, \\
\alpha^1 &= \alpha, \\
\alpha^2 &= \alpha^2, \\
\alpha^3 &= \alpha + 1, \\
\alpha^4 &= \alpha^2 + \alpha, \\
\alpha^5 &= \alpha^2 + \alpha + 1, \\
\alpha^6 &= \alpha^2 + 1.
\end{aligned}$$

Assim, as potencias de α são todas distintas $\mathbb{F}_8^*$, e por isso $\langle\alpha\rangle = \mathbb{F}_8^*$, pois sabendo que $\mathbb{F}_8$ é definido como segue pelo Teorema 1.0.10:

$$\mathbb{F}_8 = \{a + b\alpha + c\alpha^2 | a, b, c \in \mathbb{F}_2\}.$$

Logo α é primitivo de $\mathbb{F}_8$, e pelo Teorema,, 2.2.9, α^2 e α^4 também são. Por outro lado os conjugados de α sobre $\mathbb{F}_4$, são: α e α^4.

Um *automorfismo* de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é uma função bijetora $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ que preserva as operações de adição e multiplicação e mantém fixos todos os elementos de $\mathbb{F}_q$, ou seja: $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ para quaisquer $\alpha, \beta \in \mathbb{F}_{q^m}$, além de $\sigma(a) = a$ para todo $a \in \mathbb{F}_q$.

O seguinte teorema descreve completamente a estrutura do grupo de automorfismos de uma extensão de corpos finitos, revelando sua natureza cíclica.

Teorema 2.2.11. *Os automorfismos distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente as aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, definidas por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leqslant j \leqslant m-1$.*

Demonstração. Dividiremos a demonstração em três partes:
Parte 1 - σ_j é automorfismo:

Para cada $0 \leq j \leq m-1$, a aplicação $\sigma_j : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ dada por $\sigma_j(\alpha) = \alpha^{q^j}$ satisfaz:

(i) Homomorfismo: Para quaisquer $\alpha, \beta \in \mathbb{F}_{q^m}$,

- $\sigma_j(\alpha\beta) = (\alpha\beta)^{q^j} = \alpha^{q^j}\beta^{q^j} = \sigma_j(\alpha)\sigma_j(\beta)$
- $\sigma_j(\alpha+\beta) = (\alpha+\beta)^{q^j} = \alpha^{q^j} + \beta^{q^j} = \sigma_j(\alpha) + \sigma_j(\beta)$ (pelo Teorema 1.0.1).

(ii) Injetividade: $\ker(\sigma_j) = \{\alpha \in \mathbb{F}_{q^m} \mid \alpha^{q^j} = 0\} = \{0\}$, pois $\mathbb{F}_{q^m}^*$ é um grupo multiplicativo cíclico.

(iii) Sobrejetividade: Como $\mathbb{F}_{q^m}$ é finito e σ_j é injetiva, segue que σ_j é bijetora.

(iv) Fixação de $\mathbb{F}_q$: Para $a \in \mathbb{F}_q$, pelo Lema 2.1.3 temos $\sigma_j(a) = a^{q^j} = a$.

Parte 2 - Distinção dos automorfismos: Seja β um elemento primitivo de $\mathbb{F}_{q^m}$. As aplicações $\{\sigma_j\}_{j=0}^{m-1}$ são distintas pois, para $i \neq j$, temos $\sigma_i(\beta) = \beta^{q^i} \neq \beta^{q^j} = \sigma_j(\beta)$, já que $q^i \not\equiv q^j \pmod{q^m-1}$ para $0 \leq i, j < m$ com $i \neq j$.

Parte 3 - Integralidade dos automorfismos: Seja σ um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Para β elemento primitivo com polinômio minimal $f(x) = x^m + \sum_{k=0}^{m-1} a_k x^k \in \mathbb{F}_q[x]$, temos:

$$\begin{aligned} 0 &= \sigma(f(\beta)) \\ &= \sigma(\beta^m) + \sum_{k=0}^{m-1} a_k \sigma(\beta)^k \\ &= \sigma(\beta)^m + \sum_{k=0}^{m-1} a_k \sigma(\beta)^k = f(\sigma(\beta)). \end{aligned}$$

Portanto, $\sigma(\beta)$ é raiz de f. Pelo Teorema 2.2.3, $\sigma(\beta) = \beta^{q^j}$ para algum $0 \leq j \leq m-1$. Para qualquer $\alpha = \beta^t \in \mathbb{F}_{q^m}$, temos:

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

Assim, concluímos que $\sigma = \sigma_j$. □

Com base no Teorema 2.2.11, podemos afirmar que os conjugados de um elemento $\alpha \in \mathbb{F}_{q^m}$, com relação ao corpo $\mathbb{F}_q$, são justamente as imagens de α sob todos os automorfismos de $\mathbb{F}_{q^m}$ que fixam $\mathbb{F}_q$. Esses automorfismos constituem um grupo, cuja operação é a composição de funções. O próprio Teorema 2.2.11 garante que esse grupo é cíclico, tem ordem m e é gerado pelo automorfismo σ_1.

Agora, introduziremos o operador traço, um conceito da teoria de corpos finitos que, além de ser importante no estudo de bases, desempenha um papel fundamental como ferramenta tanto teórica quanto computacional.

Definição 2.2.12. Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o traço $\mathrm{Tr}_{F/K}(\alpha)$ de α sobre K é definido por

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

Em outras palavras, o traço de α sobre K é a soma dos conjugados de α em relação a K.

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

Outra descrição do traço pode ser obtida da seguinte forma. Seja $f \in K[x]$ o polinômio mínimo de α sobre K. Como f é irredutível e F/K é uma extensão separável, f possui d raízes distintas, onde $d = \deg(f)$. Além disso, d divide $m = [F : K]$.

O polinômio $g(x) = f(x)^{m/d} \in K[x]$ é denominado **polinômio característico** de α sobre K. Pelo Teorema 2.2.3, as raízes de g em F são exatamente

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}},$$

e, conforme a observação após a Definição 2.2.6, essas raízes coincidem com os conjugados de α em relação a K. Portanto, o polinômio característico pode ser expresso como

$$g(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}) = x^m + a_{m-1}x^{m-1} + \cdots + a_0.$$

Ao expandir o produto, obtemos

$$g(x) = x^m - \left(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}\right)x^{m-1} + \cdots + (-1)^m \alpha\alpha^q \cdots \alpha^{q^{m-1}}.$$

Comparando os coeficientes, concluímos que

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1},$$

o que mostra, em particular, que $\mathrm{Tr}_{F/K}(\alpha)$ pertence a K.

A seguir, vejamos propriedades da função traço.

Teorema 2.2.13. *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função traço $\mathrm{Tr}_{F/K}$ satisfaz as seguintes propriedades:*

(i) ***Aditividade**: Para todos $\alpha, \beta \in F$,*

$$\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta).$$

(ii) ***Homogeneidade**: Para todo $c \in K$ e $\alpha \in F$,*

$$\mathrm{Tr}_{F/K}(c\alpha) = c\,\mathrm{Tr}_{F/K}(\alpha).$$

(iii) ***K-Linearidade sobrejetiva**: $\mathrm{Tr}_{F/K}$ é uma transformação K-linear sobrejetora de F em K, onde F e K são vistos como espaços vetoriais sobre K.*

(iv) ***Traço de elementos de** K: Para todo $a \in K$,*

$$\mathrm{Tr}_{F/K}(a) = ma.$$

(v) ***Invariância por Frobenius**: Para todo $\alpha \in F$,*

$$\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha).$$

Demonstração. (i) Para $\alpha, \beta \in F$, utilizamos o Teorema 1.0.1 para obter:

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

(ii) Para $c \in K$, temos $c^{q^j} = c$ para todo $j \geqslant 0$ pelo Lema 2.1.3. Portanto, obtemos para $\alpha \in F$:

$$\begin{aligned}\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + \cdots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q^{m-1}} \\ &= c\,\mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

(iii) As propriedades (1) e (2), juntamente com o fato de que $\mathrm{Tr}_{F/K}(\alpha) \in K$ para todo $\alpha \in F$, estabelecem que $\mathrm{Tr}_{F/K}$ é uma transformação linear de F em K.

Para demonstrar que esta aplicação é sobrejetora, observamos que:

- Como K é um corpo, os únicos subespaços vetoriais de K (visto como espaço vetorial sobre si mesmo) são $\{0\}$ e o próprio K.
- Portanto, basta exibir um elemento $\alpha \in F$ tal que $\mathrm{Tr}_{F/K}(\alpha) \neq 0$ para concluir que a imagem de $\mathrm{Tr}_{F/K}$ é todo K.

Considere o polinômio:

$$P(x) = x^{q^{m-1}} + \cdots + x^q + x \in K[x].$$

Note que $\mathrm{Tr}_{F/K}(\alpha) = 0$ se e somente se α é raiz de $P(x)$.

Como $P(x)$ tem grau q^{m-1}, pode ter no máximo q^{m-1} raízes em F. Contudo, F possui q^m elementos, onde existem necessariamente elementos $\alpha \in F$ com $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Isto completa a demonstração da sobrejetividade.

(iv) Isto segue imediatamente da definição da função traço e do Lema 2.1.3. Pois se $\alpha \in K$

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

então, $\mathrm{Tr}_{F/K}(\alpha) = m\alpha$.

(v) Para $\alpha \in F$, temos que $\alpha^{q^m} = \alpha$ pelo Lema 2.1.3, e assim $\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} = \alpha^q + \alpha^{q^2} + \cdots \alpha^{q^{m-1}} + \alpha = \mathrm{Tr}_{F/K}(\alpha)$.

□

A aplicação traço $\mathrm{Tr}_{F/K} : F \to K$ possui propriedades importantes que vão além de sua mera linearidade. Tais propriedades são as seguintes.

- **Caracteriza todos os funcionais lineares**: Todo funcional K-linear $\varphi : F \to K$ pode ser expresso como $\varphi(\alpha) = \mathrm{Tr}_{F/K}(\lambda\alpha)$ para algum $\lambda \in F$ fixo. Esta propriedade estabelece um isomorfismo canônico entre o espaço dual F^* e F quando munido da forma bilinear $(\alpha, \beta) \mapsto \mathrm{Tr}_{F/K}(\alpha\beta)$.
- **Independência de base**: Ao contrário de muitas construções em álgebra linear, a definição de $\mathrm{Tr}_{F/K}$ é intrínseca - não depende da escolha de uma base para F como K-espaço vetorial. Esta invariância torna-a particularmente útil em aplicações onde a escolha de coordenadas não é natural.

Estas características fazem do traço uma ferramenta indispensável tanto para desenvolvimentos teóricos quanto para aplicações práticas na teoria de corpos finitos.

Teorema 2.2.14. *Seja F uma extensão finita do corpo finito K, ambos considerados como espaços vetoriais sobre K. Então, as transformações lineares de F em K são exatamente as aplicações L_β, com $\beta \in F$, onde $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ para todo $\alpha \in F$. Além disso, temos $L_\beta \neq L_\gamma$ sempre que β e γ forem elementos distintos de F.*

Demonstração. Pelo Teorema 2.2.13(iii), cada aplicação $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ é uma transformação linear de F em K.

Injetividade: Primeiro, mostramos que $\beta \neq \gamma$ implica $L_\beta \neq L_\gamma$. De fato, para $\beta, \gamma \in F$ distintos:

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}((\beta - \gamma)\alpha),$$

como $\beta - \gamma \neq 0$ e $\mathrm{Tr}_{F/K}$ é sobrejetora (logo não-nula), existe $\alpha \in F$ tal que $\mathrm{Tr}_{F/K}((\beta - \gamma)\alpha) \neq 0$. Portanto, $L_\beta \neq L_\gamma$.

Contagem das transformações lineares: Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$.

- Pela parte anterior, as aplicações $\{L_\beta\}_{\beta\in F}$ produzem q^m transformações lineares distintas.

- Alternativamente, o espaço $\mathcal{L}(F,K)$ de todas as transformações lineares de F em K tem dimensão m sobre K, pois F tem dimensão m sobre K. Logo,

$$|\mathcal{L}(F,K)| = q^m.$$

Como o conjunto $\{L_\beta\}_{\beta\in F}$ já contém todas as q^m transformações lineares possíveis, segue que:

$$\mathcal{L}(F,K) = \{L_\beta \mid \beta \in F\}$$

completando a demonstração. □

O seguinte teorema caracteriza precisamente os elementos de traço nulo, revelando uma conexão entre o traço e equações polinomiais do tipo Artin-Schreier.

Teorema 2.2.15. *Seja F uma extensão finita de $K = \mathbb{F}_q$. Então, para $\alpha \in F$, temos que $\mathrm{Tr}_{F/K}(\alpha) = 0$ se, e somente se, existe um $\beta \in F$ tal que $\alpha = \beta^q - \beta$.*

Demonstração. Temos o seguinte:

($\Rightarrow$) Suponha que $\alpha \in F = \mathbb{F}_{q^m}$ com $\mathrm{Tr}_{F/K}(\alpha) = 0$ e seja β uma raiz de $x^q - x - \alpha$ em alguma extensão de F (temos que provar que $\beta \in F$). Então $\beta^q - \beta = \alpha$ e

$$\begin{aligned} 0 = \mathrm{Tr}_{F/K}(\alpha) &= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^m} - \beta^{q^{m-1}}) \text{ (característica é } p) \\ &= \beta^{q^m} - \beta, \end{aligned}$$

então $\beta^{q^m} = \beta$, de modo que $\beta \in F$.

($\Leftarrow$) Para $\alpha \in F$ temos que existe um $\beta \in F$ tal que $\alpha = \beta^q - \beta$. Usaremos a Teorema 2.2.13(v),

$$\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{F/K}(\beta^q - \beta) = \mathrm{Tr}_{F/K}(\beta^q) - \mathrm{Tr}_{F/K}(\beta) = \mathrm{Tr}_{F/K}(\beta) - \mathrm{Tr}_{F/K}(\beta) = 0.$$

□

No caso de se considerar uma cadeia de corpos de extensão, a composição das funções traço segue uma regra muito simples.

Teorema 2.2.16. *Seja K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) \quad \textit{para todo } \alpha \in E.$$

Demonstração. Seja $K = \mathbb{F}_q$, $[F : K] = m$ e $[E : F] = n$, de modo que $[E : K] = mn$ pelo Teorema 1.84. Então, para $\alpha \in E$, temos

$$\begin{aligned}\mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) &= \sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^i} \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha).\end{aligned}$$

□

Enquanto o operador traço captura propriedades aditivas de extensões de corpos finitos, a função *norma*, que definiremos a seguir, constitui seu análogo multiplicativo. Para uma extensão $F = \mathbb{F}_{q^m}$ de $K = \mathbb{F}_q$, a norma estabelece um homomorfismo multiplicativo entre os grupos de unidades $F^* \to K^*$, revelando relações entre as estruturas multiplicativas dos corpos envolvidos.

Definição 2.2.17. Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, a norma $\mathrm{N}_{F/K}(\alpha)$ de α sobre K é definida por

$$\mathrm{N}_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{m-1}} = \alpha^{\left(\frac{q^m-1}{q-1}\right)}.$$

A norma $\mathrm{N}_{F/K}(\alpha)$ pode ser obtida diretamente do polinômio característico $g(x) \in K[x]$ de α sobre K. Especificamente, se escrevermos

$$g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0,$$

então a norma é dada pelo termo constante do polinômio, a menos de sinal:

$$\mathrm{N}_{F/K}(\alpha) = (-1)^m a_0. \tag{2.1}$$

Esta identidade revela duas propriedades fundamentais:

- A norma $\mathrm{N}_{F/K}(\alpha)$ pertence necessariamente ao corpo base K, pois $a_0 \in K$ por definição do polinômio característico.
- O cálculo da norma pode ser reduzido à determinação do polinômio característico de α, conectando assim a teoria de normas com a estrutura polinomial da extensão.

Teorema 2.2.18. *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função norma $\mathrm{N}_{F/K}$ satisfaz as seguintes propriedades:*

(i) $\mathrm{N}_{F/K}(\alpha\beta) = \mathrm{N}_{F/K}(\alpha)\mathrm{N}_{F/K}(\beta)$ *para todos* $\alpha, \beta \in F$.

(ii) $\mathrm{N}_{F/K}$ *mapeia F sobre K e F^* sobre K^*.*

(iii) $\mathrm{N}_{F/K}(a) = a^m$ *para todo* $a \in K$.

(iv) $\mathrm{N}_{F/K}\left(\alpha^q\right) = \mathrm{N}_{F/K}(\alpha)$ *para todo* $\alpha \in F$.

Demonstração. Veja [11, Teorema 2.28]. □

A aplicação norma possui uma importante propriedade de transitividade que reflete a estrutura das extensões de corpos. Este resultado, análogo ao teorema de transitividade para o operador traço, estabelece que a norma de uma torre de extensões pode ser decomposta em normas sucessivas, preservando assim a estrutura multiplicativa entre os corpos envolvidos. Mais precisamente, temos o seguinte resultado.

Teorema 2.2.19. *Seja K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então,*

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}\left(\mathrm{N}_{E/F}(\alpha)\right) \quad \textit{para todo } \alpha \in E.$$

Demonstração. Com a mesma notação da prova do Teorema 2.2.16, temos para $\alpha \in E$,

$$\begin{aligned} N_{F/K}\left(N_{E/F}(\alpha)\right) &= N_{F/K}\left(\alpha^{(q^{mn}-1)/(q^m-1)}\right) \\ &= \left(\alpha^{(q^{mn}-1)/(q^m-1)}\right)^{(q^m-1)/(q-1)} \\ &= \alpha^{(q^{mn}-1)/(q-1)} = N_{E/K}(\alpha). \end{aligned}$$

□

Dada uma base $\mathcal{B} = \{\alpha_1, \ldots, \alpha_m\}$ do corpo finito F sobre seu subcorpo K, um problema fundamental consiste em determinar os coeficientes $c_j(\alpha) \in K$ na representação única

$$\alpha = \sum_{j=1}^{m} c_j(\alpha)\alpha_j \quad \text{para } \alpha \in F. \tag{2.2}$$

Construção da Base Dual:

- Cada função coeficiente $c_j : F \to K$ é uma transformação linear. Pelo Teorema 2.2.14, existem elementos $\beta_j \in F$ tais que

$$c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha) \quad \text{para todo } \alpha \in F.$$

- Avaliando em $\alpha = \alpha_i$, obtemos as relações de ortogonalidade:

$$\mathrm{Tr}_{F/K}(\beta_j\alpha_i) = \delta_{ij} = \begin{cases} 1 & \text{se } i = j, \\ 0 & \text{se } i \neq j. \end{cases}$$

Verificação da Dualidade: A família $\mathcal{B}^* = \{\beta_1, \ldots, \beta_m\}$ forma a *base dual* de $\mathcal{B}$ em relação ao traço. Para provar sua independência linear, considere uma combinação nula:

$$\sum_{j=1}^{m} d_j\beta_j = 0 \quad \text{com } d_j \in K.$$

Multiplicando por α_i e aplicando o traço, obtemos:

$$\mathrm{Tr}_{F/K}\left(\alpha_i \sum_{j=1}^{m} d_j\beta_j\right) = \sum_{j=1}^{m} d_j \,\mathrm{Tr}_{F/K}(\alpha_i\beta_j) = d_i = 0.$$

Como este argumento vale para cada $1 \leq i \leq m$, concluímos que $\mathcal{B}^*$ é de fato uma base de F sobre K.

Definição 2.2.20. Seja K um corpo finito e F uma extensão finita de K. Então, duas bases $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_m\}$ de F sobre K são ditas bases duais (ou complementares) se, para $1 \leqslant i, j \leqslant m$, temos

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

Na exposição anterior vimos que, dada qualquer base $\{\alpha_1, \ldots, \alpha_m\}$ do corpo F sobre o subcorpo K, é possível encontrar uma base dual correspondente $\{\beta_1, \ldots, \beta_m\}$. Essa base dual é única, pois sua construção garante que os coeficientes $c_j(\alpha)$, para $1 \leq j \leq m$, da expressão (2.2), podem ser obtidos como $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j \alpha)$, para qualquer $\alpha \in F$. Conforme estabelecido no Teorema 2.2.14, cada elemento β_j de F é exclusivamente determinado pela transformação linear $c_j(\cdot)$.

Com o que foi visto antes da definição, já está demonstrada a existência da base dual, vamos provar a unicidade.

Teorema 2.2.21. *Dada uma extensão de corpos F/K de grau m e uma base $\{\alpha_1, \ldots, \alpha_m\}$ de F sobre K, existe uma única base dual $\{\beta_1, \ldots, \beta_m\}$ satisfazendo:*

$$Tr_{F/K}(\alpha_i \beta_j) = \delta_{ij} \quad \textit{para todo } 1 \leq i, j \leq m. \tag{2.3}$$

Demonstração. Suponhamos por absurdo que existam duas bases duais distintas $(\beta_j)_{j=1}^m$ e $(\gamma_j)_{j=1}^m$ para a mesma base $(\alpha_i)_{i=1}^m$. Por definição, ambas satisfazem:

$$Tr_{F/K}(\alpha_i \beta_j) = \delta_{ij}, \tag{2.4}$$
$$Tr_{F/K}(\alpha_i \gamma_j) = \delta_{ij}. \tag{2.5}$$

Como $(\gamma_k)_{k=1}^m$ é base, cada β_j admite uma representação única:

$$\beta_j = \sum_{k=1}^{m} c_{jk} \gamma_k \quad \text{com } c_{jk} \in K. \tag{2.6}$$

Aplicando o operador traço a $\alpha_i \beta_j$ e usando a linearidade:

$$Tr_{F/K}(\alpha_i \beta_j) = \sum_{k=1}^{m} c_{jk} Tr_{F/K}(\alpha_i \gamma_k) = \sum_{k=1}^{m} c_{jk} \delta_{ik} = c_{ji}. \tag{2.7}$$

Por outro lado, de (2.4) temos:

$$Tr_{F/K}(\alpha_i \beta_j) = \delta_{ij}. \tag{2.8}$$

Comparando (2.7) e (2.8), obtemos:

$$c_{ji} = \delta_{ij} \quad \text{para todo } i, j.$$

Substituindo em (2.6):

$$\beta_j = \sum_{k=1}^{m} \delta_{jk} \gamma_k = \gamma_j \quad \text{para cada } j.$$

Portanto, as bases coincidem, contradizendo a hipótese inicial. Segue a unicidade. □

Exemplo 2.2.22. Seja $\alpha \in \mathbb{F}_9$ uma raiz do polinômio irredutível $x^2 + 2x + 2 \in \mathbb{F}_3[x]$, então $\{\alpha, \alpha^3\} = \{\alpha, 2\alpha + 1\}$ é uma base de $\mathbb{F}_9$ sobre $\mathbb{F}_3$.

Para verificar que é uma base, fazemos uma combinação linear da forma

$$c_1\alpha + c_2(2\alpha + 1) = 0,$$

que é equivalente a

$$(c_1 + 2c_2)\alpha + c_2 = 0.$$

Como $\{1, \alpha\}$ é LI (Teorema 1.0.10), temos $c_1 = c_2 = 0$, logo $\{\alpha, 2\alpha + 1\}$ é LI.

O dual desta base é o mesmo conjunto, mas não na mesma ordem. Vamos verificar isso, lembrando que $\alpha^2 + 2\alpha + 2 = 0$:

$$\begin{aligned}
1 &= 1(\alpha) + 1(2\alpha + 1),\\
\alpha^2 &= \alpha + 1 = 2(\alpha) + 1(2\alpha + 1),\\
\alpha^4 &= \alpha(2\alpha + 1) = 2(\alpha + 1) + \alpha = 2 = 2(\alpha) + 2(2\alpha + 1),\\
\alpha^5 &= 2\alpha = 2(\alpha) + 0(2\alpha + 1),\\
\alpha^6 &= 2\alpha^2 = 2\alpha + 2 = 1(\alpha) + 2(2\alpha + 1),\\
\alpha^7 &= \alpha(2\alpha + 2) = 2\alpha^2 + 2\alpha = \alpha + 2 = 0(\alpha) + 2(2\alpha + 1).
\end{aligned}$$

Observamos que α gera $\mathbb{F}_9^*$. Agora, lembrando que $\mathrm{Tr}_{\mathbb{F}_9/\mathbb{F}_3}(x) = x + x^3$, suponha que a base dual é $\{\beta_1, \beta_2\}$:

- Se $\beta_1 = \alpha$, temos $\mathrm{Tr}(\alpha \cdot \alpha) = \alpha^2 + \alpha^6 = (\alpha + 1) + (2\alpha + 2) = 0$ e $\mathrm{Tr}(\alpha \cdot \alpha^3) = \alpha^4 + \alpha^{12} = 2\alpha^4 = 2(2) = 1$. Portanto, $\{\alpha, \alpha^3\}$ não é a base dual de si mesma.
- Se trocarmos $\alpha = \beta_2$, agora procuramos β_1 tal que $\mathrm{Tr}(\beta_1 \cdot \alpha) = 1$ e $\mathrm{Tr}(\beta_1 \cdot \alpha^3) = 0$.
- Tomando $\beta_1 = \alpha^3$, temos $\mathrm{Tr}(\alpha^3 \cdot \alpha) = \alpha^4 + \alpha^{12} = 2 + 2 = 1$ e $\mathrm{Tr}(\alpha^3 \cdot \alpha^3) = \alpha^6 + \alpha^{18} = 2\alpha + 2 + \alpha + 1 = 0$.

  Portanto, a base dual de $\{\alpha, \alpha^3\}$ é $\{\alpha^3, \alpha\}$.

Na teoria de corpos finitos, embora existam infinitas bases possíveis para representar $F = \mathbb{F}_{q^m}$ como espaço vetorial sobre $K = \mathbb{F}_q$, duas classes de bases destacam-se por suas propriedades algébricas e aplicações práticas:

- **Base Polinomial (ou Base de Potências)**: Dado um elemento primitivo $\alpha \in F$ (isto é, um gerador do grupo multiplicativo F^*), a base polinomial tem a forma

  $$\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}.$$

  Esta construção explora diretamente a estrutura de F como extensão simples $K(\alpha)$, onde α é raiz de um polinômio irredutível de grau m sobre K (ver Teorema 2.1.10).

- **Base Normal**: Uma base do tipo especial

  $$\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m-1}}\},$$

  onde $\beta \in F$ é escolhido de modo que seus conjugados formem um conjunto linearmente independente sobre K. Tais bases possuem propriedades de invariância sob a ação do automorfismo de Frobenius, sendo particularmente úteis em implementações eficientes de operações em corpos finitos.

Estas bases não apenas simplificam cálculos teóricos, mas também desempenham papéis fundamentais em aplicações computacionais, como na implementação de criptossistemas e algoritmos de correção de erros.

Definição 2.2.23. Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então, uma base de F sobre K da forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, consistindo em um elemento adequado $\alpha \in F$ e seus conjugados com respeito a K, é chamada de base normal de F sobre K.

A base $\{\alpha, \alpha^3\}$ de $\mathbb{F}_9$ sobre $\mathbb{F}_3$ discutida no Exemplo 2.2.22 é uma base normal de $\mathbb{F}_9$ sobre $\mathbb{F}_3$.

A seguir, mostraremos que uma base normal existe no caso geral.

Lema 2.2.24. *Sejam $\psi_1, \ldots, \psi_m$ homomorfismos distintos de um grupo G no grupo multiplicativo F^* de um corpo arbitrário F, e sejam $a_1, \ldots, a_m$ elementos de F que não são todos iguais a 0. Então, para algum $g \in G$, temos*

$$a_1\psi_1(g) + \cdots + a_m\psi_m(g) \neq 0.$$

Demonstração. Veja [11, Lema 2.33].

□

Seja V um espaço vetorial de dimensão finita sobre um corpo K e $T \in \mathcal{L}(V)$ um operador linear. Para qualquer polinômio $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$, dizemos que f *aniquila* T quando

$$f(T) \equiv \sum_{k=0}^{n} a_k T^k = 0,$$

onde convencionamos $T^0 = I$. Existe um único polinômio mônico não-nulo de grau mínimo satisfazendo esta propriedade, denominado *polinômio mínimo* $T(x)$ de T, que goza das seguintes propriedades:

- $T(x)$ divide todo polinômio que aniquila T,
- $T(x)$ divide o polinômio característico de T que é $\det(xI - T)$ (Teorema de Cayley-Hamilton),
- $\det(xI - T)$ é mônico e $\deg \det(xI - T)$ sendo igual a dimensão de V sobre K.

Um vetor $\alpha \in V$ é dito *cíclico* para T quando

$$V = \operatorname{span}_K\{T^k\alpha \mid k \geq 0\},$$

ou equivalentemente, quando $\{\alpha, T\alpha, \ldots, T^{n-1}\alpha\}$ forma uma base para V, com n igual à dimensão de V sobre K.

Lema 2.2.25. *Seja T um operador linear no espaço vetorial de dimensão finita V. Então, T possui um vetor cíclico se, e somente se, os polinômios característico e mínimo de T são idênticos.*

Demonstração. Veja [11, Lema 2.34]. □

O seguinte resultado garante a existência de uma base normal.

Teorema 2.2.26. *Para qualquer corpo finito K e qualquer extensão finita F de K, existe uma base normal de F sobre K.*

Demonstração. Consideremos $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$ com $m \geqslant 2$. Pelo Teorema 2.2.11 e seus comentários subsequentes, os automorfismos distintos de F sobre K são dados por $\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, onde ε representa a identidade em F, e a aplicação σ é definida por $\sigma(\alpha) = \alpha^q$ para todo $\alpha \in F$. Além disso, a potência σ^j denota a composição de σ consigo mesma j vezes. Como σ preserva a soma e a multiplicação por escalares em K, segue-se que ela atua como um operador linear no espaço vetorial F sobre K.

Sabemos que $\sigma^m = \varepsilon$, o que implica que o polinômio $x^m - 1 \in K[x]$ anula σ. Aplicando o Lema 2.2.24 aos endomorfismos $\varepsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, verifica-se que nenhum polinômio não-nulo de grau inferior a m em $K[x]$ pode anular σ. Logo, $x^m - 1$ é o polinômio mínimo de σ.

Como o polinômio característico de σ é um polinômio mônico de grau m que é divisível pelo polinômio mínimo, segue-se que ele também é dado por $x^m - 1$. Pelo Lema 2.2.25, existe um elemento $\alpha \in F$ tal que o conjunto $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots\}$ gera F.

Removendo elementos repetidos, concluímos que $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{m-1}(\alpha)$ formam uma base de F sobre K. Como essa base é composta por um elemento e seus conjugados em relação a K, trata-se de uma base normal de F sobre K. □

Na sequência, apresentamos uma caracterização eficiente para determinar quando um conjunto de elementos constitui uma base de uma extensão de corpos finitos.

Definição 2.2.27. Seja K um corpo finito e F uma extensão de K de grau m sobre K. Então, o discriminante $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ dos elementos $\alpha_1, \ldots, \alpha_m \in F$ é definido pelo determinante de ordem m dado por

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}.$$

Segue da definição que $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ é sempre um elemento de K. A seguinte caracterização de bases pode agora ser dada.

Teorema 2.2.28. *Seja K um corpo finito, F uma extensão de K de grau m sobre K, e $\alpha_1, \ldots, \alpha_m \in F$. Então, $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de F sobre K se, e somente se, $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.*

Demonstração. Vamos ver o seguinte:

($\Rightarrow$) Seja $\{\alpha_1, \ldots, \alpha_m\}$ uma base de F sobre K. Provamos que $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ mostrando que os vetores linha do determinante que define $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ são linearmente independentes. Tome as linhas como um vetor

$$L_j = \left(\mathrm{Tr}_{F/K}(\alpha_j\alpha_1), \mathrm{Tr}_{F/K}(\alpha_j\alpha_2), \cdots, \mathrm{Tr}_{F/K}(\alpha_j\alpha_m)\right),$$

para $1 \leqslant j \leqslant m$. Suponha que $c_1, \ldots, c_m \in K$, são tais que:

$$c_1L_1 + c_2L_2 + \cdots + c_mL_m = 0$$

$\Leftrightarrow$

$$c_1\left(\mathrm{Tr}_{F/K}(\alpha_1\alpha_1), \cdots, \mathrm{Tr}_{F/K}(\alpha_1\alpha_m)\right) + \cdots + c_m\left(\mathrm{Tr}_{F/K}(\alpha_m\alpha_1), \cdots, \mathrm{Tr}_{F/K}(\alpha_m\alpha_m)\right) = 0$$

$\Leftrightarrow$

$$c_1\,\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + \cdots + c_m\,\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \quad \text{para } 1 \leqslant j \leqslant m,$$

onde $c_1, \ldots, c_m \in K$. Então, com $\beta = c_1\alpha_1 + \cdots + c_m\alpha_m$, obtemos $\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0$ para $1 \leqslant j \leqslant m$. E, como $\alpha_1, \ldots, \alpha_m$ geram F, segue que $\mathrm{Tr}_{F/K}(\beta\alpha) = 0$ para todo $\alpha \in F$. No entanto, isso só é possível se $\beta = 0$ (lembre-se da sobrejetividade), e então $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$, o que implica $c_1 = \cdots = c_m = 0$.

($\Leftarrow$) Reciprocamente, suponha que $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ e que $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$ para alguns $c_1, \ldots, c_m \in K$. Então

$$c_1\alpha_1\alpha_j + \cdots + c_m\alpha_m\alpha_j = 0 \quad \text{para } 1 \leqslant j \leqslant m.$$

Aplicando a função traço, obtemos

$$c_1\,\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + \cdots + c_m\,\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \quad \text{para } 1 \leqslant j \leqslant m.$$

Mas, como os vetores linha do determinante que define $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ são linearmente independentes, segue que $c_1 = \cdots = c_m = 0$. Portanto, $\alpha_1, \ldots, \alpha_m$ são linearmente independentes sobre K.

□

Há outro determinante de ordem m que serve ao mesmo propósito que o discriminante $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$. Os elementos desse determinante são, no entanto, elementos do corpo de extensão F. Para $\alpha_1, \ldots, \alpha_m \in F$, seja A a matriz $m \times m$ cuja entrada na i-ésima linha e j-ésima coluna é $\alpha_j^{q^{i-1}}$, onde q é o número de elementos de K, ou seja,

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \alpha_3^q & \cdots & \alpha_m^q \\ \alpha_1^{q^2} & \alpha_2^{q^2} & \alpha_3^{q^2} & \cdots & \alpha_m^{q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \alpha_3^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{pmatrix}.$$

Se A^{T} denota a transposta de A, então um cálculo simples mostra que $A^{\mathrm{T}}A = B$, onde B é a matriz $m \times m$ cuja entrada na i-ésima linha e j-ésima coluna é $\mathrm{Tr}_{F/K}(\alpha_i\alpha_j)$.

De fato, ao multiplicar A^{T} por A, a entrada na linha i-ésima e coluna j-ésima de $A^{\mathrm{T}}A$ será:

$$\left(A^{\mathrm{T}}A\right)_{ij} = \sum_{k=1}^{m} \alpha_i^{q^{k-1}} \cdot \alpha_j^{q^{k-1}} = \sum_{k=1}^{m} (\alpha_i \cdot \alpha_j)^{q^{k-1}}.$$

Esta soma corresponde à traço de $\alpha_i\alpha_j$ de F para K, ou seja:

$$\left(A^{\mathrm{T}}A\right)_{ij} = \mathrm{Tr}_{F/K}\left(\alpha_i\alpha_j\right).$$

Ao calcular os determinantes, obtemos (lembre a propriedade $\left|A^T\right| = |A|$ e $|A \cdot B| = |A| \cdot |B|$)

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \det(B) = \det(A \cdot A^T) = \det(A)^2.$$

O seguinte resultado agora é implícito pelo Teorema 2.2.28.

Corolário 2.2.29. *Seja $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^m}$. Então, $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se,*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0.$$

Demonstração. :

($\Rightarrow$) Se $\{\alpha_1, \ldots, \alpha_m\} \in \mathbb{F}_{q^m}$ é uma base, tomando a matriz A do que foi afirmado acima do teorema, então

$$0 \neq \Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \det(B) = \det(A \cdot A^T) = \det(A)^2.$$

Assim $\det(A) \neq 0$.

($\Leftarrow$) Se $\det(A) \neq 0$ então

$$0 \neq \det(A)^2 = \det(A \cdot A^T) = \det(B) = \Delta_{F/K}(\alpha_1, \ldots, \alpha_m).$$

□

Teorema 2.2.30. *Para $\alpha \in \mathbb{F}_{q^m}$, o conjunto $\left\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right\}$ é uma base normal de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se, os polinômios $x^m - 1$ e $\alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ em $\mathbb{F}_{q^m}[x]$ forem primos entre si.*

Demonstração. Quando $\alpha_1 = \alpha, \alpha_2 = \alpha^q, \ldots, \alpha_m = \alpha^{q^{m-1}}$, o determinante no Corolário 2.38 torna-se

$$\pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \cdots & \alpha^{q^{m-3}} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{vmatrix} \tag{2.9}$$

após uma permutação adequada das linhas. Agora, considere o resultante $R(f,g)$ dos polinômios $f(x) = x^m - 1$ e $g(x) = \alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ de grau formal m e $m-1$, respectivamente, que é dado por um determinante de ordem $2m-1$, de acordo com a Definição 1.0.12.

$$R(f,g) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & -1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & -1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & 0 & 0 & \cdots & 0 \\ 0 & \alpha & \alpha^q & \cdots & \alpha^{q^{m-3}} & \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha & \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \end{bmatrix}$$

Neste determinante, adicione a coluna $(m+1)$-ésima à primeira coluna, a coluna $(m+2)$-ésima à segunda coluna, e assim por diante, finalmente somando a coluna $(2m-1)$-ésima à $(m-1)$-ésima coluna. O determinante resultante se fatoriza no determinante da matriz diagonal de ordem $m-1$ com entradas -1 ao longo da diagonal principal e no determinante em (2.9).

$$R(f,g) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & -1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & -1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & 0 & 0 & \cdots & 0 \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-3}} & \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \alpha^{q^2} & 0 & 0 & \cdots & \alpha & \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & 0 \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha^{q^{m-1}} & \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \end{bmatrix}$$

Portanto, $R(f,g)$ é, exceto pelo sinal, igual ao determinante em (2.9). A afirmação do teorema segue então do Corolário 2.2.29 e do fato de que $R(f,g) \neq 0$ se e somente se f e g são primos entre si. □

Em relação à discussão anterior, mencionamos, sem demonstração, o seguinte refinamento do teorema da base normal.

Teorema 2.2.31. *Para qualquer extensão finita F de um corpo finito K, existe uma base normal de F sobre K que consiste em elementos primitivos de F.*

Demonstração. Veja o artigo [5]. □

2.3 Raízes da Unidade e Polinômios Ciclotômicos

Nesta parte do estudo, analisamos o corpo de decomposição associado ao polinômio $x^n - 1$, considerando um corpo K qualquer e um número inteiro positivo n. Aproveitamos também para generalizar a noção de raiz da unidade, indo além do caso clássico dos números complexos.

Definição 2.3.1. Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre um corpo K é chamado de n-ésimo corpo ciclotômico sobre K e é denotado por $K^{(n)}$(se $K = \mathbb{F}_q$, então não necessariamente $K^{(n)} = \mathbb{F}_{q^n}$). As raízes de $x^n - 1$ em $K^{(n)}$ são chamadas de n-ésimas raízes da unidade sobre K, e o conjunto de todas essas raízes é denotado por $E^{(n)}$.

Um exemplo particular dessa definição ocorre quando K é o corpo dos números racionais. Nesse cenário, o corpo $K^{(n)}$ está contido no corpo dos números complexos, e as raízes n-ésimas da unidade assumem sua clássica interpretação geométrica: são os vértices de um polígono regular com n lados, inscrito no círculo unitário do plano complexo.

Apesar de nos interessarmos principalmente pelo caso em que K é um corpo finito, muitas propriedades fundamentais das raízes da unidade podem ser desenvolvidas sem essa restrição. A estrutura do grupo $E^{(n)}$ depende essencialmente da relação entre o número n e a característica de K. O próximo teorema trata justamente dessa dependência. Nesta análise, consideramos também o caso em que a característica p de K é zero.

Teorema 2.3.2. *Seja n um inteiro positivo e K um corpo de característica p. Então:*

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

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

Demonstração. Vamos ver o seguinte:

(i) O caso $n = 1$ é trivial. Para $n \geqslant 2$, $x^n - 1$ e sua derivada nx^{n-1} não possuem raízes comuns, pois nx^{n-1} possui apenas a raiz 0 em $K^{(n)}$(pois p não divide n). Portanto, pelo Teorema 1.0.4, $x^n - 1$ não pode ter raízes múltiplas e, assim, $E^{(n)}$ possui n elementos. Agora, se $\zeta, \eta \in E^{(n)}$, então

$$\left(\zeta\eta^{-1}\right)^n = \zeta^n \left(\eta^n\right)^{-1} = 1,$$

logo $\zeta\eta^{-1} \in E^{(n)}$ e portanto $E^{(n)}$ é um grupo multiplicativo. Seja $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ a fatoração em primos de n. Pode-se mostrar, pelo mesmo argumento da demonstração do Teorema 2.1.8, que para cada $i, 1 \leqslant i \leqslant t$, existe um elemento $\alpha_i \in E^{(n)}$ que não é uma raiz do polinômio $x^{n/p_i} - 1$, que

$$\beta_i = \alpha_i^{n/p_i^{e_i}}$$

tem ordem $p_i^{e_i}$, e que $E^{(n)}$ é um grupo cíclico com gerador

$$\beta = \beta_1 \beta_2 \cdots \beta_t.$$

(ii) Isso decorre imediatamente de

$$x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$$

e do item (i).

□

Definição 2.3.3. Seja K um corpo de característica p e n um número inteiro positivo não divisível por p. Um gerador do grupo cíclico $E^{(n)}$ é chamado de uma raiz n-ésima primitiva da unidade sobre K.

De acordo com as condições estabelecidas pela Definição 2.3.3, existem exatamente $\phi(n)$ raízes n-ésimas primitivas da unidade distintas sobre K. Se ζ for uma dessas raízes, então todas as demais podem ser expressas como potências de ζ, ou seja, da forma ζ^s, com $1 \leqslant s \leqslant n$ e $\text{mdc}(s, n) = 1$. O polinômio cujas raízes são precisamente essas raízes primitivas n-ésimas da unidade sobre K possui importância central e será objeto de nosso estudo.

Definição 2.3.4. Seja K um corpo de característica p, n um inteiro positivo não divisível por p, e ζ uma raiz primitiva da unidade de ordem n sobre K. Então o polinômio

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} (x - \zeta^s)$$

é chamado de polinômio ciclotômico de ordem n sobre K.

Teorema 2.3.5. *Seja K um corpo de característica p e n um inteiro positivo não divisível por p. Então:*

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

(ii) Os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K, e a $\mathbb{Z}$ se o subcorpo primo de K for o corpo dos números racionais.

Demonstração. :

(i) Cada raiz n-ésima da unidade sobre K é uma raiz d-ésima primitiva da unidade sobre K para exatamente um divisor positivo d de n (pelo "Teorema Fundamental dos Grupos Cíclicos", cada elemento gera um grupo cíclico, divisor de n). Especificamente, se ζ é uma raiz n-ésima primitiva da unidade sobre K e ζ^s é uma raiz n-ésima arbitrária da unidade sobre K, então $d = n/\,\text{mdc}(s, n)$, ou seja, d é a ordem de ζ^s em $E^{(n)}$. Como

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

a fórmula em (i) é obtida agrupando aqueles fatores $(x - \zeta^s)$ para os quais ζ^s é uma raiz d-ésima primitiva da unidade sobre K.

(ii) Isso é demonstrado por indução em n. Note que $Q_n(x)$ é um polinômio mônico. Para $n = 1$, temos $Q_1(x) = x - 1$, e a afirmação é obviamente válida. Agora, seja $n > 1$ e suponha que a proposição seja verdadeira para todo $Q_d(x)$ com $d < n$. Então, temos, por (i), que

$$Q_n(x) = \frac{x^n - 1}{f(x)},$$

onde

$$f(x) = \prod_{d|n,\, d<n} Q_d(x).$$

A hipótese de indução implica que $f(x)$ é um polinômio com coeficientes no subcorpo primo de K ou em $\mathbb{Z}$, no caso de a característica de K ser 0. Usando a divisão longa de $x^n - 1$ pelo polinômio mónico $f(x)$, vemos que os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K ou a $\mathbb{Z}$, respectivamente.

□

Exemplo 2.3.6. Vamos ver 2 exemplos.

(i) Vejamos um exemplo que exemplifica o Teorema 2.3.5 (i). Seja $K = \mathbb{F}_5$ e $x^{12} - 1 \in K[x]$ então, suponha que $\zeta \in E^{(12)}$ é uma raiz 12-ésima primitiva da unidade sobre K, então $|\langle\zeta\rangle| = 12$ e

$$x^{12} - 1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{11}),$$

mas pelo Teorema 2.3.5 (i) e a Definição 2.3.4

$$\begin{aligned} x^{12} - 1 =& Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_4(x) \cdot Q_6(x) \cdot Q_{12}(x) \\ =& [(x-1)] \cdot [(x-\zeta^6)] \cdot [(x-\zeta^4)(x-\zeta^8)] \cdot [(x-\zeta^3)(x-\zeta^9)] \cdot [(x-\zeta^2)(x-\zeta^{10})] \cdot \\ & [(x-\zeta)(x-\zeta^5)(x-\zeta^7)(x-\zeta^{11})]. \end{aligned}$$

(ii) Seja r um número primo e $k \in \mathbb{N}$. Então:

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}}$$

pois

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x)\cdots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}$$

pelo Teorema 2.3.5 (i). Para $k = 1$, temos simplesmente $Q_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$.

Uma fórmula explícita para o polinômio ciclotômico de ordem n, que estende a expressão obtida para $Q_{r^k}(x)$ no Exemplo 2.3.6, será apresentada na Seção 2 do Capítulo 3. No contexto de aplicações envolvendo corpos finitos, torna-se vantajoso compreender certas propriedades associadas aos corpos ciclotômicos.

Teorema 2.3.7. *O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K. Além disso:*

(i) *Se $K = \mathbb{Q}$, então o polinômio ciclotômico Q_n é irredutível sobre K e $\left[K^{(n)} : K\right] = \phi(n)$.*

(ii) *Se $K = \mathbb{F}_q$ com $\text{mdc}(q, n) = 1$, então Q_n se fatoriza em $\phi(n)/d$ polinômios mônicos irredutíveis distintos em $K[x]$, todos com o mesmo grau d. $K^{(n)}$ é o corpo de decomposição de qualquer fator irredutível sobre K, e $\left[K^{(n)} : K\right] = d$, onde d é o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n}$.*

Demonstração. No caso p não divide n: Se existe uma raiz primitiva n-ésima da unidade sobre K, digamos ξ, é claro que $K^{(n)} = K(\xi)$. No caso $n = mp^r$ onde p não divide m, tem-se que $K^{(n)} = K^{(m)}$ e $K^{(m)} = K(\eta)$, onde η é uma raiz m-ésima primitiva (em ambos os casos temos o gerador em ambos os corpos).

(i) Para a demonstração desta parte veja [7, Teorema 9.2.2 e Corolário 9.2.4].

(ii) Seja $f(x)$ um fator irredutível arbitrário de $Q_n(x)$ e seja ξ uma raiz n-ésima primitiva da unidade sobre $\mathbb{F}_q$ que seja raiz de $f(x)$. Então:

$$\xi \in \mathbb{F}_{q^t} \iff \xi^{q^t} = \xi \iff \xi^{q^t-1} = 1 \iff q^t \equiv 1 \pmod{n},$$

de onde se obtém que $\xi \in \mathbb{F}_{q^d}$ e não pertence a nenhum subcorpo próprio de $\mathbb{F}_{q^d}$, já que d é o menor inteiro positivo que satisfaz tal condição. Isto é, o grau do polinômio mínimo de ξ sobre $\mathbb{F}_q$ é igual ao grau de $f(x)$ e, portanto, $\deg(f(x)) = d$. Agora, como $\deg(Q_n(x)) = \phi(n)$, tem-se que o número de fatores irredutíveis de $Q_n(x)$ é $\frac{\phi(n)}{d}$. Para concluir, basta observar que o n-ésimo corpo ciclotômico é $\mathbb{F}_q(\xi)$, onde ξ é uma raiz n-ésima primitiva da unidade.

□

Exemplo 2.3.8. :

(i) Seja $K = \mathbb{F}_{11}$. Então $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$ pois

$$Q_{12}(x) = \frac{x^{12}-1}{Q_1.Q_2.Q_3.Q_4.Q_6} = \frac{x^{12}-1}{Q_1.Q_2.Q_3.Q_4.\frac{x^6-1}{Q_1.Q_2.Q_3}} = \frac{x^{12}-1}{(x^2+1).(x^6-1)} = \frac{x^6+1}{x^2+1}$$
$$= x^4 - x^2 + 1.$$

Na notação do Teorema 2.3.7(ii), temos $d = 2$ (pois $11^2 \equiv 1 \pmod{12}$). Em detalhe, $Q_{12}(x)$ se fatoriza na forma

$$Q_{12}(x) = \left(x^2 + 5x + 1\right)\left(x^2 - 5x + 1\right),$$

com ambos os fatores sendo irredutíveis em $\mathbb{F}_{11}[x]$. O corpo ciclotômico $K^{(12)}$ é igual a $\mathbb{F}_{11^2} = \mathbb{F}_{121}$.

(ii) Outro exemplo poderia ser se $K = \mathbb{F}_5$ e $Q_{16}(x) = Q_{2^4}(x) = 1 + x^8$. Na notação do Teorema 2.3.7(ii), temos $d = 4$ (pois $625 = 5^4 \equiv 1 \pmod{16}$). Em detalhe, $Q_{16}(x)$ se fatoriza na forma

$$Q_{16}(x) = x^8 + 1 = x^8 - 4 = (x^4 - 2)(x^4 + 2),$$

onde $x^4 - 2$ e $x^4 + 2$ são irredutíveis, pois não possuem raízes e nenhum polinômio de ordem 2 (da forma $x^2 + ax + b$) sem raízes pode dividi-los.

□

Uma conexão adicional entre corpos ciclotômicos e corpos finitos é dada pelo seguinte teorema.

Teorema 2.3.9. *O corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um de seus subcorpos.*

Demonstração. Como todas as raízes do polinômio $x^{q-1}-1$ pertencem a $\mathbb{F}_q$, ele se decompõe completamente nesse corpo. No entanto, ele não pode ser fatorado integralmente em nenhum subcorpo próprio de $\mathbb{F}_q$. Portanto, $\mathbb{F}_q$ é o menor corpo no qual $x^{q-1}-1$ se decompõe completamente, caracterizando-se assim como o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um de seus subcorpos. □

De acordo com o Teorema 2.1.8, o conjunto $\mathbb{F}_q^*$ forma um grupo cíclico de ordem $q-1$. Sendo assim, para qualquer inteiro positivo n que divide $q-1$, existe um subgrupo cíclico de ordem n da forma $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Todos os elementos desse subgrupo são n-ésimas raízes da unidade em relação a qualquer subcorpo de $\mathbb{F}_q$, e o elemento α, por gerar o subgrupo, é uma n-ésima raiz primitiva da unidade sobre esses subcorpos.

Encerramos esta seção apresentando um lema que será útil posteriormente.

Lema 2.3.10. *Se d é um divisor do inteiro positivo n com $1 \leqslant d < n$, então $Q_n(x)$ divide $\frac{x^n-1}{x^d-1}$ sempre que $Q_n(x)$ estiver definido(isto é, sempre que a característica do corpo base não divide n).*

Demonstração. Pelo Teorema 2.3.5(i), o polinômio $Q_n(x)$ divide a fatoração

$$x^n - 1 = (x^d - 1) \cdot \Phi_n(x),$$

onde $\Phi_n(x) = \frac{x^n-1}{x^d-1}$.

Como d é um divisor próprio de n, as raízes de $Q_n(x)$ (elementos primitivos de ordem n) são distintas das raízes de $x^d - 1$ (elementos de ordem divisora de d). Portanto,

$$\text{mdc}(Q_n(x), x^d - 1) = 1.$$

Pelo Lema de Euclides aplicado para polinômios, segue necessariamente que

$$Q_n(x) \mid \Phi_n(x) = \frac{x^n - 1}{x^d - 1}.$$

□

2.4 Representação dos Elementos de Corpos Finitos

Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos, onde p é um número primo. Nesta seção, apresentamos três representações fundamentais para os elementos de $\mathbb{F}_q$, cada uma revelando diferentes aspectos de sua estrutura algébrica. Estas três representações - polinomial, ciclotômica e matricial - oferecem perspectivas complementares sobre a estrutura de $\mathbb{F}_q$, sendo cada uma particularmente útil em diferentes contextos algébricos e aplicações.

2.4.1 Representação Polinomial via Extensão Simples

Conforme estabelecido no Teorema 2.1.10, $\mathbb{F}_q$ constitui uma extensão algébrica simples de $\mathbb{F}_p$. Mais precisamente, pelo Teorema 2.2.3, dado qualquer polinômio irredutível $f \in \mathbb{F}_p[x]$ de grau n, existe uma raiz $\alpha \in \mathbb{F}_q$ de f tal que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

Neste contexto, o Teorema 1.0.10 garante que cada elemento $\beta \in \mathbb{F}_q$ admite uma representação única na forma:

$$\beta = \sum_{k=0}^{n-1} c_k \alpha^k, \quad c_k \in \mathbb{F}_p$$

onde os coeficientes c_k são determinados de maneira única. Equivalentemente, podemos identificar $\mathbb{F}_q$ com o anel quociente $\mathbb{F}_p[x]/(f)$, onde (f) denota o ideal principal gerado por f em $\mathbb{F}_p[x]$. Esta correspondência é estabelecida pelo isomorfismo:

$$\mathbb{F}_p[x]/(f) \cong \mathbb{F}_p(\alpha) = \mathbb{F}_q,$$

que associa a classe lateral $[g(x)]$ ao elemento $g(\alpha)$.

Exemplo 2.4.1. Para representar os elementos de $\mathbb{F}_8$ desta forma, consideramos $\mathbb{F}_8$ como uma extensão algébrica simples de $\mathbb{F}_2$ de grau 3, obtida pela adjunção de uma raiz α de um polinômio cúbico irredutível sobre $\mathbb{F}_3$, como $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Assim, $f(\alpha) = \alpha^3 + \alpha + 1 = 0$ em $\mathbb{F}_8$, e os oito elementos de $\mathbb{F}_8$ são dados na forma $a_0 + a_1\alpha + a_2\alpha^2$ com $a_0, a_1, a_2 \in \mathbb{F}_2$. Em detalhe,

$$\mathbb{F}_8 = \left\{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + 1, \alpha + \alpha^2, \alpha + \alpha^2 + 1\right\}.$$

2.4.2 Representação via Corpo Ciclotômico

Uma segunda perspectiva emerge dos Teoremas 2.3.7 e 2.3.9, que revelam $\mathbb{F}_q$ como o $(q-1)$-ésimo corpo ciclotômico sobre $\mathbb{F}_p$. Nesta abordagem:

- O polinômio ciclotômico $Q_{q-1}(x)$ decompõe-se em $\mathbb{F}_p[x]$ como produto de fatores irredutíveis, todos com o mesmo grau.
- Cada fator irredutível possui como raiz uma $(q-1)$-ésima raiz primitiva da unidade $\omega \in \mathbb{F}_q$.
- O corpo $\mathbb{F}_q$ consiste no elemento zero e nas potências sucessivas de ω:

$$\mathbb{F}_q = \{0\} \cup \{\omega^k \mid k = 1, \ldots, q-1\}.$$

Esta representação destaca a estrutura multiplicativa cíclica do grupo $\mathbb{F}_q^*$.

Exemplo 2.4.2. Para aplicar isso à construção de $\mathbb{F}_8$, observamos que $\mathbb{F}_8 = \mathbb{F}_2^{(7)}$, o sétimo corpo ciclotômico sobre $\mathbb{F}_2$. Agora, $Q_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ de acordo com o Exemplo 2.3.6 (ii), e $d = 3$ pois $2^3 \equiv 1 (\mod 7)$, então:

$$Q_7(x) = \left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)$$

é a decomposição de Q_7 em fatores irredutíveis em $\mathbb{F}_2[x]$. Seja ζ uma raiz de x^3+x^2+1; então ζ é uma sétima raiz primitiva da unidade sobre $\mathbb{F}_2$, pois $|\mathbb{F}_8^*| = 7$. Assim, todos os elementos não nulos de $\mathbb{F}_8$ podem ser expressos como potências de $\zeta = \alpha + 1$ do Exemplo 2.4.1 onde $\alpha^3 + \alpha + 1 = 0$, e temos $\mathbb{F}_8 = \{0, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7\}$. Portanto, a tabela de índices para $\mathbb{F}_8$ pode ser escrita da seguinte forma:

i	ζ^i
1	$\alpha+1$
2	α^2+1
3	α^2
4	$\alpha^2+\alpha+1$

e

i	ζ^i
5	α
6	$\alpha^2+\alpha$
7	1

2.4.3 Representação Matricial

A terceira representação utiliza a teoria de matrizes companheiras. Dado um polinômio mônico irredutível $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in \mathbb{F}_p[x]$, sua matriz companheira A é definida por:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Esta matriz possui as seguintes propriedades fundamentais:

- Satisfaz $f(A) = 0$, onde 0 denota a matriz nula.
- O subanel gerado por A sobre $\mathbb{F}_p$ é isomorfo a $\mathbb{F}_q$:

$$\mathbb{F}_q \cong \left\{ \sum_{k=0}^{n-1} c_k A^k \mid c_k \in \mathbb{F}_p \right\}.$$

- A matriz A atua como um operador linear cujo polinômio mínimo é precisamente f.

Exemplo 2.4.3. Seja $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. A matriz companheira de f é:

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

O corpo $\mathbb{F}_8$ pode ser representado na forma:

$$\mathbb{F}_8 = \{0, I, A, A^2, I+A, I+A^2, A+A^2, I+A+A^2\}.$$

Explicitamente:

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$
$$A^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad I + A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad I + A^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$A + A^2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad I + A + A^2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Com $\mathbb{F}_8$ representado dessa maneira, cálculos no corpo podem ser feitos pelas regras usuais da álgebra de matrizes. Por exemplo:

$$(I + A)(A + A^2) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

Capítulo 3

Polinômios sobre corpos finitos

Este capítulo da dissertação explora a teoria de polinômios definidos sobre corpos finitos, estruturas fundamentais para aplicações, principalmente, em criptografia, teoria de códigos e álgebra computacional. Inicialmente, estudaremos a ordem de um polinômio, um conceito central que generaliza a noção de ordem de um elemento em um corpo finito, vinculando-a às propriedades de suas raízes. Em seguida, introduzimos o conceito de polinômio primitivo, fornecendo condições que os caracterizam. A terceira seção, a principal deste capítulo, sera dedicada aos polinômios irredutíveis, analisando critérios de irredutibilidade e métodos de fatoração, além de métodos que permitem a construção desta importante classe de polinômios sobre corpos finitos. Por fim, serão estudados os polinômios linearizados com ênfase em suas propriedades algébricas.

3.1 A ordem de um polinômio

Além do grau, outro invariante numérico de fundamental importância para polinômios não-nulos sobre corpos finitos é sua *ordem*. Este conceito, mais refinado que a simples noção de grau, captura propriedades algébricas profundas relacionadas à dinâmica multiplicativa do polinômio. A definição precisa de ordem polinomial repousa sobre o importante resultado a seguir.

Lema 3.1.1. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau $m \geqslant 1$ com $f(0) \neq 0$. Então, existe um inteiro positivo $e \leqslant q^m - 1$ tal que $f(x)$ divide $x^e - 1$.*

Demonstração. O anel de classes residuais $\mathbb{F}_q[x]/(f)$ contém $q^m - 1$ classes residuais não nulas. De fato como o espaço quociente é um espaço vetorial sobre $\mathbb{F}_q$ com polinômios de grau menor que m então a quantidade é q^m elementos e $q^m - 1$ são diferentes de zero. As q^m classes residuais $x^j + (f), j = 0, 1, \ldots, q^m - 1$, são todas não nulas. Pois x_j tem uma única raiz, é só 0, e essa raiz não é raiz de f. Logo f não pode dividir x_j. Portanto, existem inteiros r e s com $0 \leqslant r < s \leqslant q^m - 1$ tais que $x^s \equiv x^r \pmod{f(x)}$. Como x e $f(x)$ são primos entre si, segue que $x^{s-r} \equiv 1 \pmod{f(x)}$; isto é, $f(x)$ divide $x^{s-r} - 1$ e $0 < s - r \leqslant q^m - 1$. □

Como um polinômio constante não nulo divide $x - 1$, pois $f(x) = c \neq 0$ então o quociente da divisão de $x - 1$ por c é $c^{-1}.(x - 1)$, esses polinômios podem ser incluídos na seguinte definição.

Definição 3.1.2. Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo. Se $f(0) \neq 0$, então o menor inteiro positivo e para o qual $f(x)$ divide $x^e - 1$ é chamado de *ordem de* f e denotado por $\text{ord}(f) = \text{ord}(f(x))$.

Se $f(0) = 0$, então $f(x) = x^h g(x)$, onde $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$ com $g(0) \neq 0$ são unicamente determinados; nesse caso, define-se $\text{ord}(f)$ como $\text{ord}(g)$.

A prova da existência da ordem de um polinômio foi feita no Lema anterior.

Observamos que a ordem de um polinômio também possui as designações equivalentes de *período* ou *expoente*. Para polinômios irredutíveis, este importante invariante admite uma caracterização alternativa particularmente útil, cuja validade repousa sobre o lema anterior, onde demonstramos a existência da ordem para polinômios arbitrários. O resultado a seguir estabelece uma relação fundamental entre a ordem de um polinômio irredutível e a ordem de suas raízes na extensão de corpo associada.

Teorema 3.1.3. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m e com $f(0) \neq 0$. Então,* $\text{ord}(f)$ *é igual à ordem de qualquer raiz de f no grupo multiplicativo $\mathbb{F}_{q^m}^*$.*

Demonstração. Pelo Corolário 2.2.4, sabemos que $\mathbb{F}_{q^m}$ é o corpo de decomposição de f sobre $\mathbb{F}_q$. Além disso, de acordo com o Teorema 2.2.8, todas as raízes de f possuem a mesma ordem dentro do grupo $\mathbb{F}_{q^m}^*$. Seja $\alpha \in \mathbb{F}_{q^m}^*$ uma raiz arbitrária de f. Com base no Lema 2.2.1, sabemos que a condição $\alpha^e = 1$ é satisfeita se, e somente se, $f(x)$ divide $x^e - 1$. Assim, o resultado decorre diretamente das definições da ordem de f e da ordem de α no grupo $\mathbb{F}_{q^m}^*$. □

Corolário 3.1.4. *Se $f \in \mathbb{F}_q[x]$ é um polinômio irredutível sobre $\mathbb{F}_q$ de grau m, então* $\text{ord}(f)$ *divide $q^m - 1$.*

Demonstração. No caso particular em que $f(x) = cx$, com $c \in \mathbb{F}_q^*$, temos que $\text{ord}(f) = 1$, tornando a afirmação evidente. Para os demais casos, o resultado decorre diretamente do Teorema 3.1.3 e do fato de que $\mathbb{F}_{q^m}^*$ constitui um grupo de ordem $q^m - 1$. □

No caso de polinômios que não são irredutíveis, o enunciado do Corolário 3.1.4 pode não ser aplicável (ver Exemplo 3.1.12). Contudo, pode-se interpretar $\text{ord}(f)$ de forma alternativa, por meio da associação natural de f com uma matriz quadrada, e analisando-se a ordem dessa matriz em um grupo específico.

Por outro lado, o Teorema 3.1.3 apresenta uma fórmula para contar quantos polinômios mônicos e irredutíveis existem com grau e ordem determinados. Nessa formulação, usamos a função totiente de Euler, ϕ. É útil também introduzir a definição de ordem multiplicativa: dados $n \in \mathbb{Z}^+$ e b coprimo com n, a ordem multiplicativa de b módulo n é o menor inteiro $k > 0$ tal que $b^k \equiv 1 \pmod{n}$.

Teorema 3.1.5. *O número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau m e ordem e é igual a $\frac{\phi(e)}{m}$ se $e \geqslant 2$ e m for a ordem multiplicativa de q módulo e, igual a 2 se $m = e = 1$, e igual a 0 em todos os outros casos. Em particular, o grau de um polinômio irredutível em $\mathbb{F}_q[x]$ de ordem e deve ser igual à ordem multiplicativa de q módulo e.*

Demonstração. Note que, pela definição de ordem, $e \geqslant m$. Vamos analisar os três casos possíveis.

(i) **Caso** $e \geqslant 2$**.** Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ com $f(0) \neq 0$. Pelo Teorema 3.1.3, a condição $\text{ord}(f) = e$ é satisfeita se, e somente se, todas as raízes de f compartilham essa mesma ordem, ou seja, são raízes primitivas e-ésimas da unidade sobre $\mathbb{F}_q$. Em outras palavras, f tem ordem e se, e somente se, ele divide o polinômio ciclotômico Q_e. De acordo com o Teorema 2.3.7(ii), qualquer fator mônico irredutível de Q_e possui grau m, que é o menor inteiro positivo para o qual $q^m \equiv 1 \pmod{e}$, e o número total desses fatores é dado por $\frac{\phi(e)}{m}$.

(ii) **Caso** $m = e = 1$**.** Aqui usamos novamente a formula $\frac{\phi(1)}{1}$ e também devemos considerar o polinômio mônico irredutível $f(x) = x$ (lembrando a definição do ord onde $f(x) \neq 0$).

(iii) **Caso** $m = e = 0$**.** Note que, se $e = 0$, então $m = 0$ seriam apenas os polinômios irredutíveis $f(x)$ que dividam 0 que não existem.

□

A determinação da ordem de um polinômio não constante sobre um corpo finito pode ser feita por meio de métodos estruturados que se baseiam essencialmente na fatoração do polinômio. Quando se trata de polinômios irredutíveis, sua ordem é descrita pelas propriedades de suas raízes em extensões apropriadas, sendo esses valores amplamente documentados na literatura especializada.

Para o caso geral, isto é, polinômios redutíveis, procede-se com a fatoração total em componentes irredutíveis. Cada um desses fatores exerce uma influência específica na ordem do polinômio original(veja o Teorema 3.1.13). A seguir, explicaremos o procedimento detalhadamente.

Lema 3.1.6. *Seja c um número inteiro positivo. Então, um polinômio $f \in \mathbb{F}_q[x]$ com $f(0) \neq 0$ divide $x^c - 1$ se, e somente se,* $\text{ord}(f)$ *divide c.*

Demonstração. :

($\Leftarrow$) Seja $e := \text{ord}(f)$. Como consequência, $f(x)$ divide $x^e - 1$. Além disso, como e divide c, segue que $x^e - 1$ também divide $x^c - 1$, implicando que $f(x)$ divide $x^c - 1$.

($\Rightarrow$) Suponha que $f(x)$ divide $x^c - 1$. Pela definição da ordem de f, temos que $c \geq e$. Assim, podemos escrever c na forma $c = me + r$, com $m \in \mathbb{N}$ e $0 \leq r < e$. Dessa forma, podemos reescrever:

$$x^c - 1 = (x^{me} - 1)\, x^r + (x^r - 1)\,.$$

Como $f(x)$ divide $x^c - 1$, deve também dividir $x^r - 1$. No entanto, pela definição de $\text{ord}(f)$, isso só pode ocorrer se $r = 0$. Assim, e é um divisor de c.

□

No estudo da aritmética polinomial sobre corpos finitos, a análise dos divisores comuns de polinômios da forma $x^e - 1$ revela propriedades fundamentais que conectam a teoria dos números à álgebra polinomial. O seguinte corolário estabelece uma relação elegante entre a estrutura de divisibilidade desses polinômios e a aritmética inteira dos seus expoentes.

Corolário 3.1.7. *Se e_1 e e_2 são inteiros positivos, então o maior divisor comum de $x^{e_1}-1$ e $x^{e_2}-1$ em $\mathbb{F}_q[x]$ é x^d-1, onde d é o maior divisor comum de e_1 e e_2.*

Demonstração. Denotemos por $f(x)$ o maior divisor comum (mônico) dos polinômios $x^{e_1}-1$ e $x^{e_2}-1$. Sabemos que, sendo d o máximo divisor comum entre e_1 e e_2, o polinômio x^d-1 divide ambos $x^{e_1}-1$ e $x^{e_2}-1$. Portanto, x^d-1 também divide $f(x)$.

Por outro lado, como $f(x)$ é divisor comum de $x^{e_1}-1$ e $x^{e_2}-1$, o Lema 3.1.6 nos assegura que a ordem de f, isto é, $\mathrm{ord}(f)$, deve ser um divisor tanto de e_1 quanto de e_2. Assim, $\mathrm{ord}(f)$ divide d, e mais uma vez aplicando o Lema 3.1.6, concluímos que $f(x)$ divide x^d-1.

Como x^d-1 divide $f(x)$ e $f(x)$ divide x^d-1, segue que $f(x)=x^d-1$, o que completa a demonstração. □

Considere um polinômio $f(x)$ tal que $f(0)=0$. De acordo com a definição de ordem, é possível escrever $f(x)$ como $x^h g(x)$, onde h é um inteiro positivo e $g(x)$ é um polinômio tal que $g(0)\neq 0$. Neste caso, a ordem de f coincide com a ordem de g, isto é, $\mathrm{ord}(f)=\mathrm{ord}(g)$. Além disso, essa decomposição é única para $f(x)$. Por essa razão, nos resultados que se seguem, podemos restringir nossa atenção aos polinômios que **não** se anulam na origem.

Teorema 3.1.8. *Seja $g\in\mathbb{F}_q[x]$ irredutível, com $g(0)\neq 0$ e $\mathrm{ord}(g)=e$, e seja $f=g^b$ com b um número inteiro positivo. Seja t o menor número inteiro tal que $p^t\geqslant b$, onde p é a característica de $\mathbb{F}_q$. Então, $\mathrm{ord}(f)=ep^t$.*

Demonstração. Como f divide x^c-1, onde $c=\mathrm{ord}(f)$, também temos que g divide x^c-1. Pelo Lema 3.1.6, segue que $e\mid c$. Sabemos ainda que $g\mid x^e-1$, então $f=g^b\mid (x^e-1)^b$. Como $p^t\geq b$, então $f\mid (x^e-1)^{p^t}=x^{ep^t}-1$, o que implica, novamente pelo Lema 3.1.6, que $c\mid ep^t$.

Dessa forma, podemos escrever $c=ep^u$, com $0\leq u\leq t$, pois se assumirmos que $c=e_1\cdots e_i p^u$ onde $e=e_1\cdots e_k$ decomposição canônica e $1\leqslant i<k$, como sabemos $e\mid c$ então existe $w\in\mathbb{Z}$ tal que $ew=c$, logo $e_1\cdots e_k w=e_1\cdots e_i p^u$ então $e_{i+1}\cdots e_k w=p^u$, mas pelo Corolário 3.1.4 p não divide e, chegamos a uma contradição.

Note que x^e-1 possui apenas raízes simples, pois e não é divisível por p, de acordo com o Corolário 3.1.4 e o Teorema 2.3.2. Assim, todas as raízes de $x^{ep^u}-1=(x^e-1)^{p^u}$ possuem multiplicidade p^u. Como $f=g^b\mid x^{ep^u}-1$, as multiplicidades das raízes indicam que $p^u\geq b$, isto é, $u\geq t$. Como já tínhamos $u\leq t$, concluímos que $u=t$. Portanto, $\mathrm{ord}(f)=ep^t$. □

Teorema 3.1.9. *Sejam $g_1,\ldots,g_k$ polinômios distintos e não nulos em $\mathbb{F}_q[x]$, relativamente primos entre si, e seja $f=g_1\cdots g_k$. Então, $\mathrm{ord}(f)$ é igual ao mínimo múltiplo comum das ordens de $g_1,\ldots,g_k$, ou seja,*

$$\mathrm{ord}(f)=\mathrm{mmc}(\mathrm{ord}(g_1),\ldots,\mathrm{ord}(g_k)).$$

Demonstração. Primeiramente, podemos assumir sem perda de generalidade que $g_i(0)\neq 0$ para todo i. Seja $e=\mathrm{ord}(f)$ e $e_i=\mathrm{ord}(g_i)$ para $i=1,\ldots,k$. Definimos $c=\mathrm{mmc}(e_1,\ldots,e_k)$.

Sabemos que cada $g_i(x)$ divide $x^{e_i} - 1$, logo, como c é um múltiplo de e_i, segue que $g_i(x)$ divide $x^c - 1$. Como os polinômios $g_1, \ldots, g_k$ são relativamente primos dois a dois, obtemos que $f(x)$ divide $x^c - 1$. Aplicando o Lema 3.1.6, concluímos que e divide c.

Por outro lado, $f(x)$ divide $x^e - 1$, o que implica que cada $g_i(x)$ também divide $x^e - 1$. Novamente, pelo Lema 3.1.6, obtemos que e_i divide e para todo i. Consequentemente, c divide e.

Assim, como e divide c e c divide e, segue que $e = c$, finalizando a demonstração. □

Exemplo 3.1.10. Seja $f(x) = x^3 + 2x^2 + x + 2 \in \mathbb{F}_3[x]$. Para encontrar a $\operatorname{ord}(f)$ vamos fatorar em $\mathbb{F}_3$ o polinômio f, e obtemos $f(x) = (x^2 + 1)(x + 2)$.

Pelo Exemplo 3.2.4 a $\operatorname{ord}(x^2 + 1) = 4$ e $\operatorname{ord}(x + 2) = \operatorname{ord}(x - 1) = 1$, então pelo Teorema 3.1.9 temos que $\operatorname{ord}(f) = \operatorname{mmc}(4, 1) = 4$.

Usando o mesmo argumento acima, pode-se, de fato, demonstrar que a ordem do mínimo múltiplo comum de um número finito de polinômios não nulos é igual ao mínimo múltiplo comum das ordens dos polinômios. Representado da seguinte maneira:

Teorema 3.1.11. *Seja $f_1, \ldots, f_n$ um conjunto de polinômios não nulos sobre um corpo finito $\mathbb{F}_q$. Então, a ordem do mínimo múltiplo comum de $f_1, \ldots, f_n$ é igual ao mínimo múltiplo comum das ordens de cada f_i. Ou seja:*

$$\operatorname{ord}(\operatorname{mmc}(f_1, \ldots, f_n)) = \operatorname{mmc}(\operatorname{ord}(f_1), \ldots, \operatorname{ord}(f_n)).$$

Demonstração. Consideremos a fatoração canônica de cada polinômio f_i:

$$f_i = g_1^{b_{i_1}} \cdots g_k^{b_{i_k}}$$

com g_j polinômios irredutível para cada $i = 1, \ldots, n$ e $b_{i_j} \geq 0$ para cada $j = 1, \ldots, k$, admitindo o caso em que $b_{i_j} = 0$. Definimos agora o polinômio:

$$f := \operatorname{mmc}(f_1, \ldots, f_n) = g_1^{\max\{b_{i_1}\}} \cdots g_k^{\max\{b_{i_k}\}} \text{ com } i = 1, \ldots, n.$$

Seja $c_j := \operatorname{ord}(g_j)$. Aplicando os resultados Teorema 3.1.8 e Teorema 3.1.9, considerando p a característica de $\mathbb{F}_q$ e levando em conta que p não divide c_j e que os g_i são primos entre si, obtemos:

$$\operatorname{ord}(f) = \operatorname{mmc}\left(p^{t_1} c_1, \ldots, p^{t_k} c_k\right) = p^t \operatorname{mmc}(c_1, \ldots, c_k),$$

onde t_i é o menor inteiro tal que $p^{t_i} \geq \max\left\{b_{i_j}\right\}$ com $j = 1, \ldots, k$ e $t = \max\{t_i\}$ com $i = 1, \ldots, n$. Por outro lado:

$$\operatorname{ord}(f_i) = \operatorname{mmc}\left(\operatorname{ord}\left(g_1^{b_{i_1}}\right), \ldots, \operatorname{ord}\left(g_k^{b_{i_k}}\right)\right) = \operatorname{mmc}(p^{r_{i1}} c_1, \ldots, p^{r_{ik}} c_k) = p^{h_i} \operatorname{mmc}(c_1, \ldots, c_k),$$

onde r_{ij} é o menor inteiro tal que $p^{r_{ij}} \geq b_{i_j}$ e $h_i = \max\{r_{ij}\}$. Assim, temos:

$$\operatorname{mmc}(\operatorname{ord}(f_1), \ldots, \operatorname{ord}(f_n)) = p^{\max\{h_i\}} \operatorname{mmc}(c_1, \ldots, c_k) = p^t \operatorname{mmc}(c_1, \ldots, c_k) = \operatorname{ord}(f).$$

□

Exemplo 3.1.12. Vamos ver 2 exemplos.

- Vamos calcular a ordem de $f(x) = x^4 + 2x^3 + x + 2$ sobre $\mathbb{F}_3[x]$. A fatoração canônica de $f(x)$ sobre $\mathbb{F}_3$ é dada por $f(x) = (x-1)(x+1)^3$, a $\text{ord}(x-1) = 1$ e $\text{ord}(x+1) = 2$. Então $\text{ord}((x+1)^3) = 2.3^1 = 6$ pois $3^1 \geq 3$ pelo Teorema 3.1.8. Então $\text{ord}(x^4 + 2x^3 + x + 2) = \text{mmc}(1, 6) = 6$.
- Vamos calcular a ordem de $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. A fatoração canônica de $f(x)$ sobre $\mathbb{F}_2$ é dada por $f(x) = (x^2 + x + 1)^3 (x^4 + x + 1)$. Como $\text{ord}(x^2 + x + 1) = 3$, obtemos $\text{ord}((x^2 + x + 1)^3) = 12$ pelo Teorema 3.1.8. Além disso, $\text{ord}(x^4 + x + 1) = 15$, e assim o Teorema 3.1.9 implica que $\text{ord}(f)$ é igual ao mínimo múltiplo comum de 12 e 15; ou seja, $\text{ord}(f) = 60$. Note que $\text{ord}(f)$ não divide $2^{10} - 1$, o que mostra que o Corolário 3.1.4 não precisa ser válido para polinômios redutíveis.

□

Com base nas informações fornecidas acima, chega-se então à seguinte fórmula geral para a ordem de um polinômio. Basta considerar polinômios de grau positivo e com termo constante não nulo.

Teorema 3.1.13. *Seja $\mathbb{F}_q$ um corpo finito de característica p, e seja $f \in \mathbb{F}_q[x]$ um polinômio de grau positivo com $f(0) \neq 0$. Seja*

$$f = a f_1^{b_1} \cdots f_k^{b_k}$$

onde $a \in \mathbb{F}_q$, $b_1, \ldots, b_k \in \mathbb{N}$ e $f_1, \ldots, f_k$ são polinômios mônicos irredutíveis distintos em $\mathbb{F}_q[x]$, sendo essa a fatoração canônica de f em $\mathbb{F}_q[x]$. Então, $\text{ord}(f) = ep^t$ onde e é o mínimo múltiplo comum de $\text{ord}(f_1), \ldots, \text{ord}(f_k)$ e t é o menor inteiro tal que $p^t \geqslant \max(b_1, \ldots, b_k)$.

Demonstração. Lembre-se que se os polinômios são irredutíveis e distintos, significa que são primos entre si em $\mathbb{F}_q$. Suponha que $\text{ord}(f_i) = d_i$, então $\text{ord}(f_i^{b_i}) = d_i p^{t_i}$ pelo Teorema 3.1.8 onde $p^{t_i} \geq b_i$ para todo $i = 1, ..., k$. Logo:

$$\text{ord}(f) = \text{mmc}\left(\text{ord}\left(f_1^{b_1}\right), \text{ord}\left(f_2^{b_2}\right), \ldots, \text{ord}\left(f_k^{b_k}\right)\right)$$

pelo Teorema 3.1.9, então

$$\text{ord}(f) = \text{mmc}\left(p^{t_1} d_1, p^{t_2} d_2, \ldots, p^{t_k} d_k\right).$$

Para simplificar isso, notamos que o mínimo múltiplo comum de $d_1, \ldots, d_k$ é simplesmente e, onde:

$$e = \text{mmc}\left(d_1, d_2, \ldots, d_k\right)$$

e a potência de p no mínimo múltiplo comum é determinada pelo maior dos expoentes t_i, ou seja:

$$t = \max\left(t_1, t_2, \ldots, t_k\right).$$

Como cada t_i é o menor inteiro tal que $p^{t_i} \geq b_i$, isso nos leva à expressão final:

$$\text{ord}(f) = ep^t$$

onde t é o menor inteiro tal que $p^t \geq \max\left(b_1, \ldots, b_k\right)$. □

Um procedimento para determinar a ordem de um polinômio irredutível f em $\mathbb{F}_q[x]$, quando $f(0) \neq 0$, baseia-se no fato de que a ordem e de f é o menor número inteiro positivo que satisfaz $x^e \equiv 1 \bmod f(x)$. Além disso, conforme estabelecido no Corolário 3.1.4, o valor de e deve ser um divisor de $q^m - 1$, onde $m = \deg(f)$. Assumindo que $q^m > 2$, começamos fatorando $q^m - 1$ em números primos:

$$q^m - 1 = \prod_{j=1}^{s} p_j^{r_j}.$$

Para cada j no intervalo $1 \leqslant j \leqslant s$, calculamos os resíduos de $x^{(q^m-1)/p_j} \bmod f(x)$. Esse cálculo é realizado multiplicando adequadamente os resíduos de $x, x^q, x^{q^2}, \ldots, x^{q^{m-1}} \bmod f(x)$.

- Se $x^{(q^m-1)/p_j} \not\equiv 1 \bmod f(x)$, então e deve ser múltiplo de $p_j^{r_j}$.
- Caso contrário, se $x^{(q^m-1)/p_j} \equiv 1 \bmod f(x)$, isso indica que e não é múltiplo de $p_j^{r_j}$.

  Nessa situação, testamos se e é divisível por $p_j^{r_j-1}, p_j^{r_j-2}, \ldots, p_j$, verificando os resíduos de

$$x^{(q^m-1)/p_j^2}, x^{(q^m-1)/p_j^3}, \ldots, x^{(q^m-1)/p_j^{r_j}} \bmod f(x).$$

Esse processo é repetido para cada fator primo de $q^m - 1$.

Exemplo 3.1.14. Vamos ver qual é a ordem do seguinte polinômio $f(x) = x^6 + x + 1$ em $\mathbb{F}_2$, lembrando que f não pode ser dividido entre x^2+x+1, x^3+x+1 e x^3+x^2+1 então f é irredutível, com o método mencionado. Seja $\text{ord}(f(x)) = e$, então $e|2^6 - 1 = 63 = 3^2.7$. Logo temos

- $x^{63/3} = x^{21} \equiv x^5 + x^4 + x^3 + x + 1 \bmod f(x)$ então e é múltiplo de 3^2.
- $x^{63/7} = x^9 \equiv x^4 + x^3 \bmod f(x)$ então e é múltiplo de 7.

Logo $\text{ord}(f(x)) = 63$.

Um ponto essencial desse método é a fatoração do número $q^m - 1$. Existem tabelas amplas com fatorações completas para valores dessa forma, especialmente quando $q = 2$.

Agora, podemos comparar as ordens de polinômios relacionados por transformações algébricas simples. O que segue é um exemplo típico.

Definição 3.1.15. Seja

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$$

com $a_n \neq 0$. Então, o polinômio recíproco de f, denotado por f^*, é definido por

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

O resultado a seguir, nos diz que a ordem de um polinômio e a de seu recíproco são iguais.

Teorema 3.1.16. *Seja f um polinômio não nulo em $\mathbb{F}_q[x]$ e f^* seu polinômio recíproco. Então,*

$$\mathrm{ord}(f) = \mathrm{ord}\,(f^*)\,.$$

Demonstração. Vejamos os seguintes casos, levando em consideração que o grau de f é m.

- Primeiramente, considere o caso $f(0) \neq 0$. Nesse caso, o resultado segue do fato de que $f(x)$ divide $x^e - 1$ se, e somente se, $f^*(x)$ divide $x^e - 1$, ois se $f(x)$ divide $x^e - 1$ então existe $g(x)$ tal que $f(x)g(x) = x^e - 1$, logo

$$\begin{aligned}
& f(x)g(x) = x^e - 1, \quad \text{fazemos } x = \tfrac{1}{x} \\
\Rightarrow\ & f\left(\tfrac{1}{x}\right) g\left(\tfrac{1}{x}\right) = \tfrac{1}{x^e} - 1, \quad \text{multiplicamos por } x^m \\
\Rightarrow\ & x^m f\left(\tfrac{1}{x}\right) g\left(\tfrac{1}{x}\right) = x^{m-e} - x^m \\
\Rightarrow\ & f^*(x) g\left(\tfrac{1}{x}\right) = -x^{m-e}\,(x^e - 1) \\
\Rightarrow\ & -f^*(x)g^*(x) = x^e - 1.
\end{aligned}$$

  Este é o mínimo e, porque se fosse menor, então o grau de g seria menor e contradiz o $ord(f)$.

- Se $f(0) = 0$, escreva $f(x) = x^h g(x)$ com $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$, tal que $g(0) \neq 0$. Então, pelo que já foi mostrado, segue que $\mathrm{ord}(f) = \mathrm{ord}(g) = \mathrm{ord}(g^*) = \mathrm{ord}(f^*)$, onde a última identidade é válida pois $g^* = f^*$. De fato:

$$f(x) = x^h g(x) \Rightarrow f\left(\frac{1}{x}\right) = \frac{1}{x^h} g\left(\frac{1}{x}\right) \Rightarrow x^m f\left(\frac{1}{x}\right) = x^{m-h} g\left(\frac{1}{x}\right) \Rightarrow g^*(x) = f^*(x).$$

□

A análise da relação entre $\mathrm{ord}(f(x))$ e $\mathrm{ord}(f(-x))$ em $\mathbb{F}_q[x]$ é distinta baseada na característica do corpo. No caso de característica $p = 2$, a identidade $1 = -1$ implica imediatamente que $f(x) = f(-x)$ para qualquer polinômio $f \in \mathbb{F}_q[x]$, fazendo com que as ordens coincidam trivialmente.

Para corpos de característica ímpar ($p > 2$), a relação torna-se mais sutil. Neste contexto, a ordem $\mathrm{ord}(f(-x))$ pode ser expressa em termos de $\mathrm{ord}(f(x))$ como veremos a seguir.

Teorema 3.1.17. *Para q ímpar, seja $f \in \mathbb{F}_q[x]$ um polinômio de grau positivo com $f(0) \neq 0$. Sejam e e E as ordens de $f(x)$ e $f(-x)$, respectivamente. Então, $E = e$ se e for múltiplo de 4, e $E = 2e$ se e for ímpar. Se e for o dobro de um número ímpar, então $E = e/2$ se todos os fatores irredutíveis de f tiverem ordem par e $E = e$ caso contrário.*

Demonstração. Lembrando que um número natural só pode ter três opções: ser um múltiplo de 4, ser ímpar ou ser o dobro de um número ímpar. É por isso que temos esses três casos para e.

Como $\text{ord}(f(x)) = e$, então $f(x)$ divide $x^{2e} - 1$, e consequentemente $f(-x)$ divide $(-x)^{2e} - 1 = x^{2e} - 1$. Assim, E divide $2e$ pelo Lema 3.6. Pelo mesmo argumento, e divide $2E$, logo E só pode ser $2e$, e ou $e/2$.

- Se e é múltiplo de 4, então tanto e quanto E são pares. Como $f(x)$ divide $x^e - 1$, segue que $f(-x)$ divide $(-x)^e - 1 = x^e - 1$, e assim E divide e. Da mesma forma, e divide E, logo $E = e$.

- Se e é ímpar, então $f(-x)$ divide $(-x)^e - 1 = -x^e - 1$, ou seja, divide $x^e + 1$. Mas então $f(-x)$ não pode dividir $x^e - 1$, então E não divide e pelo Lema 3.1.6, pois em caso contrario $f(-x)$ pode dividir $(x^e - 1) - (x^e + 1) = -2$ e $f(x)$ tem grau positivo, uma contradição, e portanto a única opção que devemos ter é $E = 2e$.

- No caso restante, temos $e = 2h$, onde h é um número ímpar. Seja f uma potência de um polinômio irredutível em $\mathbb{F}_q[x]$. Então $f(x)$ divide $(x^h - 1)(x^h + 1)$ e $f(x)$ não divide $x^h - 1$, pois $\text{ord}(f) = 2h$. Como $x^h - 1$ e $x^h + 1$ são primos entre si, pois se existisse um polinômio irredutível $d(x)$ que fosse divisor de ambos $x^h - 1$ e $x^h + 1$, então ele também deveria dividir 2, como demonstrado anteriormente. Além disso, dado que o corpo tem característica ímpar, o número 2 é uma unidade em $\mathbb{F}_q$, o que implica que $d(x)$ teria que ser uma constante. No entanto, isso contradiz o fato de que $d(x)$ é irredutível, isso implica que $f(x)$ divide $x^h + 1$. Consequentemente, $f(-x)$ divide $(-x)^h + 1 = -x^h + 1$, ou seja, $x^h - 1$. Portanto, $E = e/2$.

  Note que, pelo Teorema 3.1.8, a potência de um polinômio irredutível tem ordem par se e somente se o próprio polinômio irredutível tem ordem par.

  Para um polinômio geral f, podemos escrever $f = g_1 \cdots g_k$, onde cada g_i é uma potência de um polinômio irredutível e $g_1, \ldots, g_k$ são primos entre si. Além disso, temos que $2h = \text{mmc}(\text{ord}(g_1), \ldots, \text{ord}(g_k))$ pelo Teorema 3.1.9.

  Organizamos os g_i de tal forma que $\text{ord}(g_i) = 2h_i$ para $1 \leq i \leq m$ e $\text{ord}(g_i) = h_i$ para $m + 1 \leq i \leq k$, onde os h_i são números ímpares e $\text{mmc}(h_1, \ldots, h_k) = h$. Pelo que já demonstramos, obtemos $\text{ord}(g_i(-x)) = h_i$ para $1 \leq i \leq m$ e $\text{ord}(g_i(-x)) = 2h_i$ para $m + 1 \leq i \leq k$. Pelo Teorema 3.1.9, segue que

  $$E = \text{mmc}(h_1, \ldots, h_m, 2h_{m+1}, \ldots, 2h_k)$$

  e assim $E = h = e/2$ se $m = k$, e $E = 2h = e$ se $m < k$. Essas fórmulas são equivalentes às dadas na última parte do teorema.

□

Segue-se do Lema 3.1.1 e da Definição 3.1.2 que a ordem de um polinômio de grau $m \geqslant 1$ sobre $\mathbb{F}_q$ é, no máximo, $q^m - 1$. Esse limite é atingido para uma classe importante de polinômios, a saber, os chamados polinômios primitivos. A definição de um polinômio primitivo é baseada na noção de elemento primitivo introduzida na Definição 2.1.9.

3.2 Polinômios primitivos

Na teoria de corpos finitos, um polinômio primitivo sobre $\mathbb{F}_q$ é um polinômio mônico irredutível $f \in \mathbb{F}_q[x]$ cujas raízes são geradoras do grupo multiplicativo de alguma extensão $\mathbb{F}_{q^m}$. Equivalentemente, f é primitivo quando possui uma raiz α que é um elemento primitivo de $\mathbb{F}_{q^m}^*$, ou seja, α tem ordem multiplicativa $q^m - 1$. Formalmente, temos o seguinte.

Definição 3.2.1. Um polinômio $f \in \mathbb{F}_q[x]$ de grau $m \geqslant 1$ é chamado de *polinômio primitivo* sobre $\mathbb{F}_q$ se for o polinômio mínimo sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^m}$.

Dessa maneira, um polinômio primitivo de grau m sobre $\mathbb{F}_q$ é um polinômio mônico e irredutível que possui uma raiz $\alpha \in \mathbb{F}_{q^m}$ tal que α é um gerador do grupo multiplicativo $\mathbb{F}_{q^m}^*$. Além disso, é possível caracterizar os polinômios primitivos também da seguinte forma.

Teorema 3.2.2. *Um polinômio $f \in \mathbb{F}_q[x]$ de grau m é um polinômio primitivo sobre $\mathbb{F}_q$ se, e somente se, f é mônico, $f(0) \neq 0$ e $\operatorname{ord}(f) = q^m - 1$.*

Demonstração. :

($\Rightarrow$) Se f é primitivo sobre $\mathbb{F}_q$, então ele é um polinômio mônico e $f(0) \neq 0$, pois é irredutível. Como f é irredutível sobre $\mathbb{F}_q$, segue do Teorema 3.1.3 que $\operatorname{ord}(f) = q^m - 1$, pois f tem como raiz um elemento primitivo de $\mathbb{F}_{q^m}$, garantindo sua primitividade.

($\Leftarrow$) Reciprocamente, se $\operatorname{ord}(f) = q^m - 1$, então $m \geqslant 1$ devido à definição de ordem. Precisamos mostrar que f é irredutível sobre $\mathbb{F}_q$. Suponhamos, por absurdo, que f seja um polinômio redutível sobre $\mathbb{F}_q$. Isso significa que ele pode ser escrito como uma potência de um polinômio irredutível ou como um produto de dois polinômios coprimos de graus positivos.

No primeiro caso, temos $f = g^b$, onde $g \in \mathbb{F}_q[x]$ é irredutível sobre $\mathbb{F}_q$, $g(0) \neq 0$ e $b \geqslant 2$. Pelo Teorema 3.1.8, $\operatorname{ord}(f)$ é divisível pela característica de $\mathbb{F}_q$, mas $q^m - 1$ não é, levando a uma contradição.

No segundo caso, temos $f = g_1 g_2$, onde g_1 e g_2 são polinômios mônicos coprimos de graus positivos m_1 e m_2, respectivamente. Se $e_i = \operatorname{ord}(g_i)$ para $i = 1, 2$, então, pelo Teorema 3.1.9, temos $\operatorname{ord}(f) \leqslant e_1 e_2$. Além disso, pelo Lema 3.1.1, $e_i \leqslant q^{m_i} - 1$ para $i = 1, 2$. Assim, segue que:

$$\operatorname{ord}(f) \leqslant (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1 + m_2} - 1 = q^m - 1,$$

o que contradiz a hipótese de que $\operatorname{ord}(f) = q^m - 1$. Portanto, f é necessariamente irredutível sobre $\mathbb{F}_q$. Aplicando novamente o Teorema 3.1.3, concluímos que f é um polinômio primitivo sobre $\mathbb{F}_q$.

□

Observamos que a condição $f(0) \neq 0$ no teorema acima é necessária apenas para excluir o polinômio não primitivo $f(x) = x$ no caso em que $q = 2$ e $m = 1$. De fato, se permitíssemos $f(0) = 0$, o polinômio x atenderia às demais condições do teorema, pois é mônico e de grau 1, mas claramente não é primitivo, uma vez que não gera o grupo multiplicativo $\mathbb{F}_{q^m}^*$.

Lema 3.2.3. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau positivo com $f(0) \neq 0$. Seja r o menor inteiro positivo para o qual x^r seja congruente módulo $f(x)$ a algum elemento de $\mathbb{F}_q$, ou seja, $x^r \equiv a \bmod f(x)$ com um $a \in \mathbb{F}_q^*$ unicamente determinado. Então,* $\operatorname{ord}(f) = hr$, *onde h é a ordem de a no grupo multiplicativo $\mathbb{F}_q^*$.*

Demonstração. Defina $e = \operatorname{ord}(f)$. Como $x^e \equiv 1 \bmod f(x)$, devemos ter $e \geqslant r$, pela definição de r. Assim, podemos escrever $e = sr + t$ com $s \in \mathbb{N}$ e $0 \leqslant t < r$. Agora,

$$1 \equiv x^e \equiv x^{sr+t} \equiv (x^r)^s x^t \equiv a^s x^t \bmod f(x). \tag{3.1}$$

Portanto, $x^t \equiv a^{-s} \bmod f(x)$, e devido à definição de r, isso só é possível se $t = 0$. Logo da congruência (3.1) implica que, como $a \in \mathbb{F}_q^*$ e $a^s \equiv 1 \bmod f(x)$, então $a^s = 1$ em $\mathbb{F}_q^*$, e assim $s \geqslant h$ então $e = rs \geqslant hr$. Por outro lado, $x^{hr} \equiv (x^r)^h \equiv a^h \equiv 1 \bmod f(x)$, pela definição de ordem temos que $e|hr$, então $hr \geqslant e$, o que implica $e = hr$. □

Exemplo 3.2.4. Seja $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Note que $f(0) = 1 \neq 0$, portanto podemos aplicar o Lema 3.2.3.

No corpo quociente $\mathbb{F}_3[x]/(f(x))$, denotamos por $\alpha \equiv x \bmod f(x)$. Temos:

$$\alpha^2 = x^2 \equiv -1 \equiv 2 \bmod f(x),$$

isto é, $\alpha^2 \in \mathbb{F}_3^*$. Portanto, o menor r tal que $\alpha^r \in \mathbb{F}_3^*$ é $r = 2$, e $a = 2 \in \mathbb{F}_3^*$.

O próximo passo é determinar a ordem de $a = 2$ no grupo $\mathbb{F}_3^*$. Como:

$$2^1 = 2 \quad \text{e} \quad 2^2 = 4 \equiv 1 \bmod 3,$$

concluímos que $\operatorname{ord}_{\mathbb{F}_3^*}(2) = h = 2$.

Pelo Lema 3.2.3, segue que:

$$\operatorname{ord}(f) = hr = 2 \cdot 2 = 4.$$

Portanto, a ordem do polinômio $f(x) = x^2 + 1$ sobre $\mathbb{F}_3$ é 4.

Concluímos esta seção com um resultado fundamental que estabelece critérios para a primitividade de um polinômio mônico $f(x) \in \mathbb{F}_q[x]$. O resultado a seguir, apresenta uma caracterização abrangente através de duas condições essenciais: uma aritmética, relacionando o termo constante à propriedade de elemento primitivo no corpo base, e outra algébrica, envolvendo a ordem de potências polinomiais módulo $f(x)$.

Teorema 3.2.5. *O polinômio mônico $f(x) \in \mathbb{F}_q[x]$ de grau $m \geqslant 1$ é um polinômio primitivo sobre $\mathbb{F}_q$ se, e somente se, $(-1)^m f(0)$ for um elemento primitivo de $\mathbb{F}_q$ e o menor inteiro positivo r para o qual x^r é congruente* $\bmod f(x)$ *a algum elemento de $\mathbb{F}_q$ for*

$$r = \frac{q^m - 1}{q - 1}.$$

No caso em que f é primitivo sobre $\mathbb{F}_q$, temos

$$x^r \equiv (-1)^m f(0) \bmod f(x).$$

Demonstração. :

($\Rightarrow$) Se f é primitivo sobre $\mathbb{F}_q$, então f possui uma raiz $\alpha \in \mathbb{F}_{q^m}$, que é um elemento primitivo de $\mathbb{F}_{q^m}$. Calculando a norma $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ tanto pela Definição 2.2.17 quanto por (2.1), e observando que f é o polinômio característico de α sobre $\mathbb{F}_q$, obtemos a identidade

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)}. \tag{3.2}$$

Segue-se que a ordem de $(-1)^m f(0)$ em $\mathbb{F}_q^*$ é $q-1$; isto é, $(-1)^m f(0)$ é um elemento primitivo de $\mathbb{F}_q$. Como f é o polinômio mínimo de α sobre $\mathbb{F}_q$, a identidade (3.2) e pelo Teorema 1.0.8 temos que $f(x)|x^{(q^m-1)/(q-1)} - (-1)^m f(0)$ implica que

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \bmod f(x)$$

e, portanto, $r \leqslant (q^m-1)/(q-1)$. Mas o Teorema 3.2.2 e o Lema 3.2.3 (sabemos que r é o número inteiro não negativo mínimo que torna x^r equivalente a algum termo de $\mathbb{F}_q^*$ mas não sabemos a ordem desse elemento, mas sabemos que é um divisor de $q-1$). Garantem que $q^m - 1 = \mathrm{ord}(f) \leqslant (q-1)r$, logo $r = (q^m-1)/(q-1)$.

($\Leftarrow$) Suponha que as condições do teorema sejam satisfeitas. Primeiro provamos que f é irredutível, para isso segue de $r = (q^m-1)/(q-1)$, e do Lema 3.2.3 que $\mathrm{ord}(f)$ é relativamente primo a q pois a ordem do elemento que cumpre a condição do Lema 3.2.3 es divisor de $q-1$ (lembrando na forma de obter a ordem de f com o Lema 3.2.3, a ordem é relativamente primo com q então ordem de f não pode ser da forma $r.p^t$, logo os elementos irredutíveis de f não têm potências, tendo em conta o Teorema 3.1.8). Então, o Teorema 3.1.13 mostra que f admite uma fatoração da forma $f = f_1 \cdots f_k$, onde os f_i são polinômios mônicos irredutíveis distintos sobre $\mathbb{F}_q$. Se $m_i = \deg(f_i)$, então, pelo Corolário 3.1.4, $\mathrm{ord}(f_i)$ divide $q^{m_i} - 1$ para $1 \leqslant i \leqslant k$. Agora, como $q^{m_i} - 1$ divide

$$d = \frac{(q^{m_1}-1)\cdots(q^{m_k}-1)}{(q-1)^{k-1}},$$

temos que $\mathrm{ord}(f_i)$ divide d para $1 \leqslant i \leqslant k$. Do Lema 3.1.6 segue-se que $f_i(x)$ divide $x^d - 1$ para $1 \leqslant i \leqslant k$, logo $f(x)$ divide $x^d - 1$ então $x^d \equiv 1 \bmod f(x)$.

Vamos ver um resultado antes de continua: Seja $q = p^r$ com p primo e r um número inteiro positivo. Seja $m, n \geqslant 1$, então é uma verdade que:

$$\begin{aligned} q^m + q^n &> 2 \\ q^{m+n} - 1 &> q^{m+n} - q^m - q^n + 1 \\ q^{m+n} - 1 &> (q^m - 1)(q^n - 1). \end{aligned}$$

Para mais fatores, basta fazer o mesmo processo 2 por 2.

Agora Lembrando a definição de r da hipótese, se $k \geqslant 2$ e usando o resultado anterior, obtemos:

$$d < \frac{q^{m_1+\cdots+m_k} - 1}{q-1} = \frac{q^m - 1}{q-1} = r,$$

o que contradiz a definição de r. Assim, $k = 1$ e f é irredutível sobre $\mathbb{F}_q$.

Se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f, então o argumento que levou a (3.2) mostra que

$$\beta^r = (-1)^m f(0),$$

e, portanto pelo Lema 2.2.1,

$$x^r \equiv (-1)^m f(0) \bmod f(x).$$

Como a ordem de $(-1)^m f(0)$ em $\mathbb{F}_q^*$ é $q-1$, segue do Lema 3.2.3 que $\text{ord}(f) = q^m - 1$, e assim f é primitivo sobre $\mathbb{F}_q$ pelo Teorema 3.2.2.

□

Exemplo 3.2.6. Considere o polinômio

$$f(x) = x^4 + x^3 + x^2 + 2x + 2 \in \mathbb{F}_3[x].$$

Como f é irredutível sobre $\mathbb{F}_3$, pode-se usar o método descrito após o Teorema 3.1.13, primeiro $\text{ord}(f)$ divide $3^4 - 1 = 80 = 2^4.5$, então retiramos cada fator primo e obtemos:

- Dividamos $x^{\frac{80}{2}} = x^{40}$ por f, dá como resíduo -1, então $x^{40} \equiv 2 \mod f(x)$. Logo 2^4 divide $\text{ord}(f)$.
- Dividimos $x^{\frac{80}{5}} = x^{16}$ por f, dá como resíduo $1 - x^3$, então $x^{16} \equiv 1 - x^3 \mod f(x)$. Logo 5 divide $\text{ord}(f)$.

Assim $\text{ord}(f) = 80 = 3^4 - 1$.

Consequentemente, f é primitivo sobre $\mathbb{F}_3$ pelo Teorema 3.2.2. Além disso, temos

$$x^{40} \equiv 2 \mod f(x),$$

de acordo com o Teorema 3.2.5.

3.3 Polinômios irredutíveis

Nesta seção, o nosso objetivo central é determinar quantos polinômios mônicos e irredutíveis existem de um grau fixado sobre um corpo finito, além de apresentar uma fórmula que expressa o produto de todos esses polinômios. Para isso, será necessário introduzir algumas definições preliminares e explorar a chamada *função de Möbius*. Os polinômios ciclotômicos também desempenharão um papel importante neste contexto, e os resultados desenvolvidos aqui permitirão calcular esses polinômios de forma mais eficiente do que o método recorrente utilizado anteriormente.

Recordemos que um polinômio $f \in \mathbb{F}_q[x]$ é dito irredutível sobre $\mathbb{F}_q$ quando tem grau maior que zero e não pode ser escrito como produto de dois polinômios não constantes com coeficientes em $\mathbb{F}_q$.

Teorema 3.3.1. *Para todo corpo finito $\mathbb{F}_q$ e todo $n \in \mathbb{N}$, o produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.*

Demonstração. Considere o polinômio $g(x) = x^{q^n} - x \in \mathbb{F}_q[x]$. Pelo Lema 2.2.2, os fatores mônicos irredutíveis de g em $\mathbb{F}_q[x]$ são exatamente os polinômios irredutíveis cujos graus dividem n. Este resultado reflete a estrutura subjacente das extensões de corpos finitos. Agora, a derivada $g'(x) = -1$ (calculada em característica p) é não-nula e constante. Consequentemente, pelo Teorema 1.0.4, g não possui raízes múltiplas em nenhuma extensão de $\mathbb{F}_q$. Esta propriedade implica que na fatoração completa de g em $\mathbb{F}_q[x]$, cada polinômio irredutível aparece com multiplicidade exatamente 1. A combinação destes dois fatos estabelece que a decomposição de g consiste precisamente na multiplicação (sem repetição) de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus são divisores de n. □

Corolário 3.3.2. *Se $N_q(d)$ representa o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau d, então*

$$q^n = \sum_{d|n} dN_q(d) \quad \textit{para todo } n \in \mathbb{N} \tag{3.3}$$

onde a soma é estendida sobre todos os divisores positivos d de n.

Demonstração. Seja um inteiro positivo n fixo, mas arbitrário. Considere o polinômio $g(x) = x^{q^n} - x$. Aplicando o resultado anterior, g é o produto de todos os polinômios mônicos irredutíveis de $\mathbb{F}_q[x]$ cujos graus dividem n. Mas então segue-se imediatamente que $\deg(g) = q^n$ satisfaz

$$q^n = \sum_{d|n} d \cdot N_q(d)$$

pois cada $d \cdot N_q(d)$ representa o produto entre o grau do polinômio e o número de polinômios, esse é para cada divisor d de n. □

Utilizando conceitos básicos de teoria dos números, é possível deduzir a partir de (3.3) uma fórmula explícita para determinar a quantidade de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ com um grau fixo. Para isso, introduzimos uma função aritmética conhecida como função de Möbius, cuja definição é apresentada a seguir.

Definição 3.3.3. A função de Möbius $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ é a função definida por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ (-1)^k & \text{se } n \text{ é o produto de } k \text{ primos distintos}, \\ 0 & \text{se algum primo na fatoração de } n \text{ tem expoente maior que 1.} \end{cases}$$

Como em (3.3), usamos o símbolo de soma $\Sigma_{d|n}$ para denotar uma soma estendida sobre todos os divisores positivos d de $n \in \mathbb{N}$. Uma convenção semelhante se aplica ao símbolo de produto $\Pi_{d|n}$.

Lema 3.3.4. *Para $n \in \mathbb{N}$, a função de Moebius μ satisfaz*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{se } n = 1, \\ 0 & \textit{se } n > 1. \end{cases}$$

Demonstração. O caso $n = 1$ é imediato.

Para $n > 1$, consideramos apenas os divisores positivos d de n para os quais $\mu(d) \neq 0$, ou seja, aqueles em que $d = 1$ ou d é formado pelo produto de primos distintos. Se $p_1, p_2, \ldots, p_k$ representam os primos distintos que dividem n, temos:

$$\begin{aligned}\sum_{d|n} \mu(d) =& \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1} p_{i_2}) + \cdots + \\ & \sum_{1 \leq i_1 < i_2 \cdots < i_{k-1} \leq k} \mu(p_{i_1} p_{i_2} \ldots p_{i_{k-1}}) + \mu(p_1 p_2 \ldots p_k) \\ =& 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k-1}(-1)^{k-1} + \binom{k}{k}(-1)^k \\ =& (1 + (-1))^k = 0.\end{aligned}$$

□

Teorema 3.3.5 (Fórmula de Imersão Moebius). *Temos 2 fórmulas:*

(i) ***Caso aditivo:*** *Seja h e H duas funções de $\mathbb{N}$ em um grupo abeliano G com adição. Então*

$$H(n) = \sum_{d|n} h(d) \quad \textit{para todo } n \in \mathbb{N} \tag{3.4}$$

se e somente se

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \quad \textit{para todo } n \in \mathbb{N}. \tag{3.5}$$

(ii) ***Caso multiplicativo:*** *Seja h e H duas funções de $\mathbb{N}$ em um grupo abeliano G com multiplicação. Então*

$$H(n) = \prod_{d|n} h(d) \quad \textit{para todo } n \in \mathbb{N} \tag{3.6}$$

se e somente se

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} \quad \textit{para todo } n \in \mathbb{N}. \tag{3.7}$$

Demonstração. Veja [11, Teorema 3.24]. □

Teorema 3.3.6. *A quantidade $N_q(n)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau n é dada por*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Demonstração. Consideremos o caso aditivo da fórmula de inversão de Möbius aplicado ao grupo $G = \mathbb{Z}$, isto é, o grupo aditivo dos inteiros.

Definimos as funções $h(n) = nN_q(n)$ e $H(n) = q^n$ para todo $n \in \mathbb{N}$. Com essa escolha, a relação da equação (3.4) se verifica como consequência direta da identidade (3.3).

Portanto, ao aplicar a inversão de Möbius, obtemos imediatamente (3.5), o que conclui a demonstração da fórmula pretendida. □

Exemplo 3.3.7. Para $n = 18 = 2 \times 3^2$, que possui 6 divisores positivos, o número de polinômios mônicos irredutíveis de grau 18 sobre $\mathbb{F}_q$ é dado por:

$$N_q(18) = \frac{1}{18} \sum_{d|18} \mu(d) q^{18/d}. \tag{3.8}$$

Desenvolvendo a expressão com os valores da função de Möbius μ:

$$\begin{aligned} N_q(18) &= \frac{1}{18} \left(\mu(1)q^{18} + \mu(2)q^9 + \mu(3)q^6 + \mu(9)q^2 + \mu(6)q^3 + \mu(18)q \right) \\ &= \frac{1}{18} \left(q^{18} - q^9 - q^6 + 0 + q^3 + 0 \right), \end{aligned}$$

em que,

- $\mu(1) = 1$,
- $\mu(2) = -1$,
- $\mu(3) = -1$,
- $\mu(6) = \mu(2 \times 3) = (-1)^2 = 1$,
- $\mu(9) = 0$ (contém 3^2),
- $\mu(18) = 0$ (contém 3^2).

Portanto, o número de polinômios mônicos irredutíveis de grau 18 sobre $\mathbb{F}_q$ é

$$N_q(18) = \frac{q^{18} - q^9 - q^6 + q^3}{18}.$$

É importante destacar que a fórmula apresentada no Teorema 3.3.6 confirma mais uma vez que, para qualquer corpo finito $\mathbb{F}_q$ e qualquer número natural n, existe pelo menos um polinômio irredutível de grau n em $\mathbb{F}_q[x]$ (vide também o Corolário 2.1.11). Isso pode ser visto ao observar que $\mu(1) = 1$ e que, para todo $d \in \mathbb{N}$, temos $\mu(d) \geqslant -1$. A partir disso, podemos obter uma estimativa simples:

$$N_q(n) \geqslant \frac{1}{n} \left(q^n - q^{n-1} - q^{n-2} - \cdots - q \right) = \frac{1}{n} \left(q^n - \frac{q^n - q}{q - 1} \right) > 0.$$

Essa desigualdade garante que a quantidade de polinômios mônicos irredutíveis de grau n é sempre positiva. Além disso, como outra aplicação da fórmula de inversão de Möbius, será apresentada a seguir uma expressão explícita para o polinômio ciclotômico $Q_n(x)$.

Teorema 3.3.8. *Seja K um corpo de característica p, e seja $n \in \mathbb{N}$ um número natural que* ***não*** *é divisível por p. Então, o n-ésimo polinômio ciclotômico Q_n sobre K satisfaz:*

$$Q_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)} = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}.$$

Demonstração. Veja [11, Teorema 3.27]. □

Exemplo 3.3.9. Para corpos K nos quais o polinômio ciclotômico Q_{18} está definido, temos:

$$\begin{aligned} Q_{18}(x) &= \prod_{d|18} \left(x^{18/d} - 1\right)^{\mu(d)} \\ &= \left(x^{18} - 1\right)^{\mu(1)} \left(x^9 - 1\right)^{\mu(2)} \left(x^6 - 1\right)^{\mu(3)} \left(x^3 - 1\right)^{\mu(6)} \left(x^2 - 1\right)^{\mu(9)} (x-1)^{\mu(18)} \\ &= \frac{(x^{18} - 1)(x^3 - 1)}{(x^9 - 1)(x^6 - 1)} = x^6 - x^3 + 1. \end{aligned}$$

No Teorema 3.3.6, foi determinada uma fórmula para calcular a quantidade de polinômios mônicos e irredutíveis de grau fixado em $\mathbb{F}_q[x]$. A seguir, será apresentada uma expressão que fornece o produto de todos esses polinômios de mesmo grau.

Teorema 3.3.10. *O produto $I(q, n; x)$ de todos os polinômios mônicos e irredutíveis em $\mathbb{F}_q[x]$ de grau n é dado por*

$$I(q, n; x) = \prod_{d|n} \left(x^{q^d} - x\right)^{\mu(n/d)} = \prod_{d|n} \left(x^{q^{n/d}} - x\right)^{\mu(d)}.$$

Demonstração. Lembrando do Teorema 3.3.1 temos:

$$x^{q^n} - x = \prod_{d|n} I(q, d; x).$$

Vamos usar a fórmula de inversão de Möbius, o caso multiplicativo Teorema 3.3.5. O grupo abeliano multiplicativo G é o conjunto de funções racionais não nulas sobre $\mathbb{F}_q$, definindo $h(n) = I(q, n; x)$ e $H(n) = x^{q^n} - x$ para todo $n \in \mathbb{N}$, pela igualdade anterior, a hipótese da fórmula é cumprida, então obtemos a fórmula desejada. □

Exemplo 3.3.11. Para $q = 3$ e $n = 4$, obtemos:

$$\begin{aligned} I(3, 4; x) &= \prod_{d|4} \left(x^{3^d} - x\right)^{\mu(4/d)} \\ &= \left(x^{3^4} - x\right)^{\mu(1)} \left(x^{3^2} - x\right)^{\mu(2)} \left(x^3 - x\right)^{\mu(4)} \\ &= \frac{x^{81} - x}{x^9 - x} = \frac{x^{80} - 1}{x^8 - 1} \\ &= \sum_{k=0}^{9} \left(x^8\right)^{9-k} \cdot 1^k = x^{72} + x^{64} + x^{56} + x^{48} + x^{40} + x^{32} + x^{24} + x^{16} + x^8 + 1. \end{aligned}$$

Todos os polinômios irredutíveis mônicos de grau n em $\mathbb{F}_q[x]$ podem ser obtidos a partir da fatoração de $I(q,n;x)$. Para facilitar esse processo, é útil dispor de uma forma parcialmente fatorada de $I(q,n;x)$, o que é proporcionado pelo próximo resultado, logo usa o Teorema 2.3.7(ii).

Teorema 3.3.12. *Seja $I(q,n;x)$ como definido no Teorema 3.3.10. Então, para $n>1$, temos*

$$I(q,n;x)=\prod_m Q_m(x), \tag{3.9}$$

onde o produto se estende aos divisores m de q^n-1 tais que n é a ordem multiplicativa de q módulo m, isto é, aqueles divisores m para os quais n é o menor inteiro tal que $q^n \equiv 1 \mod m$, e onde $Q_m(x)$ é o m-ésimo polinômio ciclotômico sobre $\mathbb{F}_q$.

Demonstração. Seja $n>1$ e considere S como o conjunto dos elementos de $\mathbb{F}_{q^n}$ que têm grau exatamente n sobre $\mathbb{F}_q$, o que significa que $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=n$. Cada $\alpha \in S$ possui um polinômio mínimo sobre $\mathbb{F}_q$ de grau n, então $\mathbb{F}_{q^n}=\mathbb{F}_q(\alpha)$, logo é uma raiz de $I(q,n;x)$, lembrando a definição de $I(q,n;x)$ dada na Teorema 3.3.10. Reciprocamente, se β é uma raiz de $I(q,n;x)$, então ela anula algum polinômio irredutível mônico de grau n em $\mathbb{F}_q[x]$, o que implica $\beta \in S$. Assim, temos:

$$I(q,n;x)=\prod_{\alpha\in S}(x-\alpha).$$

É claro que $\alpha \neq 0$, pois o polinômio é mínimo, então $\alpha \in S \subseteq \mathbb{F}_{q^n}^*$ e a ordem multiplicativa de α divide q^n-1. Como estamos procurando elementos que tenham ordem m, de modo que façam parte das raízes de Q_m, sabemos que um elemento $\gamma \in \mathbb{F}_{q^n}^*$ pertence a um subcorpo próprio $\mathbb{F}_{q^d} \subsetneq \mathbb{F}_{q^n}$ se, e somente se, $\gamma^{q^d}=\gamma$, ou seja, sua ordem divide q^d-1. Assim, para que $\alpha \in S$ tenha ordem m que divida q^n-1, é necessário que n seja o menor inteiro positivo, pois se não fosse o mínimo, o grau do polinômio mínimo seria menor que n, tal que $q^n \equiv 1 \pmod m$, ou seja, que n seja a ordem multiplicativa de $q \mod m$.

Logo para cada divisor positivo m de q^n-1 com essa propriedade, seja S_m o subconjunto de elementos de S cuja ordem é exatamente m. É claro que os conjuntos S_m são disjuntos e sua união é S. Então podemos escrever:

$$I(q,n;x)=\prod_m \prod_{\alpha\in S_m}(x-\alpha).$$

Cada conjunto S_m corresponde exatamente ao conjunto das raízes da unidade de ordem m que são primitivas em $\mathbb{F}_{q^n}^*$, ou seja, ele reúne todos os elementos que são raízes do polinômio ciclotômico $Q_m(x)$. Com base na definição desses polinômios (Definição 2.3.4), concluímos que:

$$\prod_{\alpha\in S_m}(x-\alpha)=Q_m(x),$$

o que comprova a identidade proposta dada em (3.9), levando em conta a definição de S_m. □

Exemplo 3.3.13. Vamos determinar todos os polinômios irredutíveis (mônicos) de grau 3 em $\mathbb{F}_3[x]$. Pela identidade (3.9), temos:

$$\begin{aligned} I(3,3;x) &= Q_{13}(x).Q_{26}(x) \\ &= \left(x^{12}+x^{11}+\cdots+x+1\right)\left(\frac{x^{26}-1}{Q_1(x)Q_2(x)Q_{13}(x)}\right) \\ &= \left(x^{12}+x^{11}+\cdots+x+1\right)\left(\frac{x^{26}-1}{(x-1)(x+1)\left(x^{12}+\cdots+1\right)}\right) \\ &= \left(x^{12}+x^{11}+\cdots+x+1\right)\left(x^{12}-x^{11}+x^{10}-x^9+\cdots-x+1\right). \end{aligned}$$

Logo sabemos que $Q_{13}(x)$ e $Q_{26}(x)$ se decompõem em 4 polinômios irredutíveis de grau 3 em $\mathbb{F}_3[x]$ pois $3^3 \equiv 1 \bmod 13$ e $3^3 \equiv 1 \bmod 26$ pelo Teorema 2.3.7(ii). Além disso, sabemos que x^3+x+2 é um polinômio mônico irredutível, então ele tem que dividir um dos dois polinômios,

$$\begin{aligned} x^{12}+x^{11}+\cdots+x+1 =& (x^3+x+2)(x^3+2x+1)(x^3+x^2+2)(x^3+2x^2+1), \\ x^{12}-x^{11}+x^{10}-x^9+\cdots-x+1 =& \left(x^3+2x+2\right)\left(x^3+x^2+x+2\right) \\ & \left(x^3+x^2+2x+1\right)\left(x^3+2x^2+2x+2\right). \end{aligned}$$

Assim, os polinômios mônicos irredutíveis de grau 3 em $\mathbb{F}_3[x]$ são:

$$\begin{gathered} x^3+x+2,\ x^3+2x+1,\ x^3+x^2+2,\ x^3+2x^2+1, \\ x^3+2x+2,\ x^3+x^2+x+2,\ x^3+x^2+2x+1,\ x^3+2x^2+2x+2. \end{gathered}$$

Resumimos agora os fatos mais úteis sobre os polinômios mínimos.

Teorema 3.3.14. *Seja α um elemento da extensão do corpos $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$. Suponha que o grau de α sobre $\mathbb{F}_q$ seja d e que $g \in \mathbb{F}_q[x]$ seja o polinômio mínimo de α sobre $\mathbb{F}_q$. Então:*

(i) g é irredutível sobre $\mathbb{F}_q$ e seu grau d divide m.

(ii) Um polinômio $f \in \mathbb{F}_q[x]$ satisfaz $f(\alpha)=0$ se, e somente se, g divide f.

(iii) Se f é um polinômio irredutível e mônico em $\mathbb{F}_q[x]$ com $f(\alpha)=0$, então $f=g$.

(iv) $g(x)$ divide $x^{q^d}-x$ e $x^{q^m}-x$.

(v) As raízes de g são $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, e g é o polinômio mínimo sobre $\mathbb{F}_q$ de todos esses elementos.

(vi) Se $\alpha \neq 0$, então $\operatorname{ord}(g)$ é igual à ordem de α no grupo multiplicativo $\mathbb{F}_{q^m}^*$.

(vii) g é um polinômio primitivo sobre $\mathbb{F}_q$ se, e somente se, α tem ordem q^d-1 em $\mathbb{F}_{q^m}$.

Demonstração. :

(i) Pela definição de polinômio minimo, g é irredutível sobre $\mathbb{F}_q$, e pelo Teorema 1.0.10(iii) verificamos que d divide m pois $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$.

(ii) É demonstrado diretamente pelo Teorema 1.0.8(ii).

(iii) Como $f(\alpha) = 0$ então por (ii) temos que g divide f, mas como f é irredutível então $f = g$.

(iv) De (i) sabemos que d divide m pelo Lema 2.2.2, temos que g divide $x^{q^d} - x$ e $x^{q^m} - x$.

(v) De (i) sabemos que g é irredutível em $\mathbb{F}_q$ e pelo Teorema 2.2.3 cumpre-se que $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ são raízes de g. Além disso pelo item (iii) g é o polinômio minimo de cada uma de suas raízes.

(vi) Dado que α pertence ao grupo multiplicativo $\mathbb{F}_{q^d}^*$, o qual está contido como subgrupo em $\mathbb{F}_{q^m}^*$, podemos concluir que o resultado segue diretamente do Teorema 3.1.3.

(vii) Se g é um polinômio primitivo sobre $\mathbb{F}_q$, então sua ordem é $q^d - 1$. O que implica, segundo o item (vi), que α tem ordem $q^d - 1$ em $\mathbb{F}_{q^m}^*$. Reciprocamente, se α tem ordem $q^d - 1$ em $\mathbb{F}_{q^m}^*$ (e portanto em $\mathbb{F}_{q^d}^*$), então α é um elemento primitivo de $\mathbb{F}_{q^d}$, e assim g é um polinômio primitivo sobre $\mathbb{F}_q$, conforme a Definição 3.2.1.

□

Recordamos que, dado um inteiro positivo n, se um inteiro b é relativamente primo com n, então o menor inteiro positivo k tal que $b^k \equiv 1 \pmod{n}$ é chamado de *ordem multiplicativa* de b módulo n. Observa-se que essa ordem multiplicativa divide qualquer outro inteiro positivo h que satisfaça $b^h \equiv 1 \pmod{n}$.

Lema 3.3.15. *Sejam $s \geq 2$ e $e \geq 2$ inteiros primos entre si, e seja m a ordem multiplicativa de s módulo e. Seja $t \geq 2$ um inteiro cujos fatores primos dividem e, mas não dividem $(s^m - 1)/e$. Suponha também que $s^m \equiv 1 \pmod{4}$ quando $t \equiv 0 \pmod{4}$. Então, a ordem multiplicativa de s módulo et é igual a mt.*

Demonstração. Veja [11, Lema 3.34]. □

O seguinte resultado estabelece uma importante propriedade de recursividade para os polinômios ciclotômicos $Q_n(x)$.

Lema 3.3.16. *Seja o corpo $\mathbb{F}_q$ com caraterística p, para $m \in \mathbb{N}$ tal que $\mathrm{mdc}(p, m) = 1$ e r primo tal que $r|m$, cumpre-se que:*

$$Q_{mp}(x) = Q_m\left(x^p\right).$$

Demonstração. Seja ζ uma raiz primitiva da unidade de ordem mp, isto é, $\zeta \in E^{(mp)}$ satisfazendo $\zeta^{mp} = 1$ e tal que a ordem multiplicativa de ζ é exatamente mp. Definimos $\xi := \zeta^p$. Então:

$$\xi^m = (\zeta^p)^m = \zeta^{pm} = \zeta^{mp} = 1.$$

Como a ordem de ζ é exatamente mp, segue que a ordem de $\xi = \zeta^p$ é exatamente m. De fato, se o ordem do elemento ζ^p é $d < m$, então $(\zeta^p)^d = 1$, implicando $\zeta^{pd} = 1$, com $pd < mp$, contradizendo que ζ tem ordem mp. Logo, ξ é uma raiz primitiva m-ésima da unidade.

Isso mostra que:

$$\zeta \in \left\{ x \in E^{(mp)} : x^p = \xi, \text{ com } \xi \text{ raiz primitiva } m\text{-ésima} \right\}.$$

Em outras palavras, ζ é uma raiz do polinômio $Q_m(x^p)$, pois para cada raiz primitiva ξ de $Q_m(x)$, as p raízes p-ésimas de ξ aparecem em $Q_m(x^p)$.

Logo, toda raiz de $Q_{mp}(x)$ é também raiz de $Q_m(x^p)$.

Reciprocamente, seja ζ uma raiz de $Q_m(x^p)$. Então existe uma raiz primitiva m-ésima ξ tal que $\zeta^p = \xi$. Como $\xi^m = 1$, temos:

$$\zeta^{pm} = (\zeta^p)^m = \xi^m = 1,$$

ou seja, ζ é uma raiz da unidade de ordem divisora de mp. Vamos verificar que sua ordem é exatamente mp: se a ordem do elemento ζ é $d < mp$, então $d \mid mp$, e ao elevar a p, teríamos que ζ^p teria ordem menor que m, contradizendo o fato de que $\zeta^p = \xi$ tem ordem m. Assim, ζ tem ordem exatamente mp, e é uma raiz primitiva mp-ésima da unidade.

Concluímos que toda raiz de $Q_m(x^p)$ também é raiz de $Q_{mp}(x)$.

Ambos os polinômios são mônicos e possuem o mesmo conjunto de raízes. Portanto, devem coincidir:

$$Q_{mp}(x) = Q_m(x^p).$$

□

O teorema a seguir, estabelece um poderoso método de construção de famílias de polinômios irredutíveis a partir de polinômios conhecidos, mediante transformações de potenciais.

Teorema 3.3.17. *Sejam $f_1(x), f_2(x), \ldots, f_N(x)$ todos os polinômios mônicos e irredutíveis distintos em $\mathbb{F}_q[x]$ de grau m e ordem e, e seja $t \geq 2$ um inteiro cujos fatores primos dividem e, mas não dividem $(q^m - 1)/e$. Suponha também que $q^m \equiv 1 \pmod 4$ quando $t \equiv 0 \pmod 4$. Então, $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ são todos os polinômios mônicos e irredutíveis distintos em $\mathbb{F}_q[x]$ de grau mt e ordem et.*

Demonstração. Como $f_1(x), f_2(x), \ldots, f_N(x)$ são todos os polinômios mônicos e irredutíveis em $\mathbb{F}_q[x]$ de grau m e ordem e, $t \geq 2$ e os fatores primos de t dividem e, então $e \geq 2$. Logo, pelo Teorema 3.1.5, os polinômios existem somente se m for a ordem multiplicativa de q módulo e, e, nesse caso, $N = \phi(e)/m$.

Pelo Lema 3.3.15, a ordem multiplicativa de q módulo et é igual a mt. Pelo [12, Teorema 62] sabemos que $\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$ com p fator primo de m, então como e tem todos os fatores primos de t, temos:

$$\frac{\phi(et)}{mt} = \frac{et}{mt} \prod_{p|et} \left(1 - \frac{1}{p}\right) = \frac{e}{m} \prod_{p|e} \left(1 - \frac{1}{p}\right) = \frac{\phi(e)}{m}.$$

Segue-se que o número de polinômios mônicos e irredutíveis em $\mathbb{F}_q[x]$ de grau mt e ordem et também é $\frac{\phi(et)}{mt} = \frac{\phi(e)}{m} = N$.

Sabemos que os polinômios $f_j(x^t)$, com $1 \leq j \leq N$, são todos mônicos e de grau mt, agora só temos que provar que são irredutíveis e de ordem et. Como $\text{ord}(f_j(x)) = e$, pelo Teorema 3.1.3 as raízes de cada $f_j(x)$ são raízes primitivas da unidade de ordem e sobre

$\mathbb{F}_q$, logo $f_j(x)$ divide o polinômio ciclotômico $Q_e(x)$. Então $f_j(x^t)$ divide $Q_e(x^t)$, e pelo uso repetido do Lema 3.3.16 temos que $Q_e(x^t) = Q_{et}(x)$.

Logicamente, $f_j(x^t)$ divide $Q_{et}(x)$. Pelo Teorema 2.3.7(ii), o grau de cada fator irredutível de $Q_{et}(x)$ em $\mathbb{F}_q[x]$ é igual à ordem multiplicativa de q módulo et, que é mt. Como $f_j(x^t)$ tem grau mt, concluímos que $f_j(x^t)$ é irredutível em $\mathbb{F}_q[x]$. Logo, já que ele divide $Q_{et}(x)$ e o corpo de decomposição dos dois é $\mathbb{F}_{q^{mt}}$, que é o mínimo corpo, sua ordem é et. □

Exemplo 3.3.18. Os polinômios mônicos irredutíveis de grau 2 em $\mathbb{F}_3$ são 3

$$x^2 + 1 \qquad , \qquad x^2 + x + 2 \qquad \text{e} \qquad x^2 + 2x + 2$$

pelo Teorema 3.3.6. Logo pelo Teorema 3.1.5 sabemos que existem 2 polinômios de ordem 8, pois 2 é a ordem multiplicativa de 3 modulo 8 ($3^2 \equiv 1 \bmod 8$) e $\phi(8)/2 = 2$, e 1 de ordem 4, pois 1 é a ordem multiplicativo de 3 modulo 4 ($3^2 \equiv 1 \bmod 4$) e $\phi(4)/2 = 1$.

É claro que $x^2 + 1$ é de ordem 4, então os 2 polinômios de grau 2 e de ordem 8 são $x^2 + x + 2$ e $x^2 + 2x + 2$. Para usar o Teorema 3.3.17 temos que usar um t adequado, vamos tomar $t = \{4, 8, 16, \cdots\}$, então os polinômios irredutíveis em $\mathbb{F}_3$:

- De grau 8 e de ordem 32 são $x^8 + x^4 + 2$ e $x^8 + 2x^4 + 2$,
- De grau 16 e de ordem 64 são $x^{16} + x^8 + 2$ e $x^{16} + 2x^8 + 2$,
- De grau 32 e de ordem 128 são $x^{32} + x^{16} + 2$ e $x^{32} + 2x^{16} + 2$.

□

Mostraremos um método sistemático que permite, a partir de um polinômio irredutível com determinada ordem e, construir todos os demais polinômios irredutíveis cujas ordens sejam divisores de e. Vale observar que, como o polinômio $g(x) = x$ sempre satisfaz essa condição (pois sua ordem é 1, que divide qualquer número), restringiremos nossa atenção apenas aos polinômios g para os quais $g(0) \neq 0$. Essa restrição evita que consideremos polinômios triviais e garante que estamos lidando com casos mais significativos.

Suponha que f seja um polinômio irredutível e mônico definido sobre o corpo finito $\mathbb{F}_q$, de grau m, com ordem e, e tal que $f(0) \neq 0$. Escolhemos uma raiz α de f dentro da extensão $\mathbb{F}_{q^m}$, já que todo polinômio irredutível de grau m em $\mathbb{F}_q[x]$ tem suas raízes nesse corpo de extensão.

Para cada número natural t, associamos um polinômio g_t que é o polinômio minimal de α^t sobre $\mathbb{F}_q$. Ou seja, g_t é o polinômio mônico com menor grau e com coeficientes em $\mathbb{F}_q$ que anula α^t.

Para organizar quais desses g_t são realmente distintos (pois diferentes potências de α podem ter o mesmo polinômio minimal), construiremos um conjunto especial $T_f = \{t_1, t_2, \ldots, t_n\}$ de inteiros positivos distintos. A construção desse conjunto assegura que, para todo $t \in \mathbb{N}$, haverá um único índice i, com $1 \leq i \leq n$, e um número inteiro $b \geq 0$, tais que $t \equiv t_i q^b \pmod{e}$. Essa congruência captura a ideia de que α^t e $\alpha^{t_i q^b}$ pertencem à mesma órbita sob a ação do automorfismo de Frobenius, e portanto compartilham o mesmo polinômio minimal.

A construção do conjunto T_f pode ser feita de maneira recursiva. Começamos com $t_1 = 1$. Em seguida, supondo que já tenhamos definido os elementos $t_1, \ldots, t_{j-1}$, escolhemos t_j como o menor inteiro positivo que não seja congruente a nenhum dos anteriores multiplicado por uma potência de q, módulo e. Esse processo garante que os t_i representem classes diferentes sob a ação de q, e como o número de tais classes é finito, o processo termina após um número finito de passos.

Assim, com todas essas definições e construções, obtemos um resultado geral que descreve exatamente como obter todos os polinômios irredutíveis associados a potências de α, cujas ordens sejam divisores de e.

Exemplo 3.3.19. Construção do conjunto T_f a partir de órbitas em $\mathbb{F}_{2^3}$.

Seja o polinômio irredutível

$$f(x) = x^3 + x + 1 \in \mathbb{F}_2[x],$$

que é mônico, satisfaz $f(0) = 1 \neq 0$ e possui grau $m = 3$. O corpo de extensão gerado por uma raiz de f, denotada por α, é $\mathbb{F}_{2^3}$, o qual contém todas as raízes de f. Como $\text{ord}(f) = 7$ então α é uma raiz primitiva pelo Teorema 3.2.2, logo o grupo multiplicativo $\mathbb{F}_8^*$ é cíclico de ordem 7, gerado por α.

Nosso objetivo é construir um subconjunto $T_f \subset \mathbb{N}$, finito e reduzido módulo $e = 7$. Especificamente, buscamos representantes t_i tais que dois elementos α^t e $\alpha^{t'}$ pertençam à mesma órbita se, e somente se,

$$t' \equiv t \cdot 2^b \pmod 7, \quad \text{para algum } b \in \mathbb{N}_0.$$

Para construir T_f, seguimos um processo iterativo:

- Inicialmente, escolhemos $t_1 = 1$. A órbita de 1 sob as potências de 2 mod 7 é

  $$\mathcal{O}_1 = \{1, 2, 4\},$$

  correspondendo aos elementos $\alpha^1, \alpha^2, \alpha^4$, que compartilham o mesmo polinômio minimal.

- O menor inteiro ainda não pertencente a uma órbita anterior é $t_2 = 3$. A órbita de 3 é

  $$\mathcal{O}_2 = \{3, 6, 5\},$$

  associada aos elementos $\alpha^3, \alpha^6, \alpha^5$, que também compartilham um segundo polinômio minimal.

Com isso, temos que

$$T_f = \{1, 3\}$$

é um conjunto completo de representantes de órbitas distintas. Cada elemento de T_f dá origem a um polinômio minimal distinto sobre $\mathbb{F}_2$, de grau 3, e as demais potências de α são raízes desses mesmos polinômios via aplicação de potências de Frobenius.

Este procedimento mostra como o conjunto T_f pode ser construído sistematicamente a partir das órbitas do automorfismo de Frobenius, respeitando a estrutura cíclica do grupo multiplicativo do corpo finito envolvido.

□

Teorema 3.3.20. *Seja $f \in \mathbb{F}_q[x]$ irredutível e mônico de grau m e ordem e. Seja $\alpha \in \mathbb{F}_{q^m}$ tal que $f(\alpha) = 0$. Para cada $i = 1, \ldots, n$, sejam $t_i \in \mathbb{N}$ distintos e $g_{t_i} \in \mathbb{F}_q[x]$ o polinômio mônico irredutível de menor grau tal que $g_{t_i}(\alpha^{t_i}) = 0$. Logo se $t_i \in T_f$, então os polinômios $g_{t_1}, g_{t_2}, \ldots, g_{t_n}$ são exatamente todos os polinômios mônicos e irredutíveis distintos em $\mathbb{F}_q[x]$ cujas ordens dividem e e cujo termo constante é diferente de zero.*

Demonstração. Primeiro, vamos mostrar que a ordem de cada g_{t_i} divide e: Cada polinômio g_t é, por construção, um polinômio mônico e irredutível em $\mathbb{F}_q[x]$, além de satisfazer a condição $g_{t_i}(0) \neq 0$ pois isso significa que ele pode ser fatorado em termos irredutíveis, então não seria mínimo. Observamos também que g_{t_i} possui como raiz o elemento α^{t_i}. Sabemos que a ordem de α^{t_i} no grupo multiplicativo $\mathbb{F}_{q^m}^*$ deve necessariamente dividir a ordem de α, uma vez que α^{t_i} é uma potência de α. Aplicando o Teorema 3.1.3, concluímos que a ordem do polinômio $\mathrm{ord}(g_{t_i})$ divide e. Assim, cada polinômio g_{t_i} está associado a uma ordem que é um divisor de e.

Agora vamos a provar que g um polinômio mônico e irredutível arbitrário em $\mathbb{F}_q[x]$, de ordem d tal que $d \mid e$ e com $g(0) \neq 0$ é algum g_{t_i} do conjunto. Seja um g com essas condições e seja agora β uma raiz do polinômio g. Pelo fato de g ter ordem d, temos que $\beta^d = 1$. Como d divide e, isso implica que $\beta^e = (\beta^d)^{e/d} = 1^{e/d} = 1$, isto é, β também é uma raiz e-ésima da unidade sobre $\mathbb{F}_q$.

Sabendo que α foi escolhida como uma raiz primitiva e-ésima da unidade sobre $\mathbb{F}_q$ (pela definição do ordem e), podemos aplicar o Teorema 2.3.2(i) para concluir que existe algum inteiro $t \in \mathbb{N}$ tal que $\beta = \alpha^t$. Em outras palavras, toda raiz e-ésima da unidade em $\mathbb{F}_{q^m}$ é uma potência de α.

Agora, pela definição do conjunto T_f, sabemos que todo inteiro t satisfaz uma relação da forma $t \equiv t_i q^b \pmod{e}$, para algum índice $1 \leq i \leq n$ e algum inteiro $b \geq 0$. Assim, podemos escrever

$$\beta = \alpha^t = \left(\alpha^{t_i}\right)^{q^b}.$$

Pelo Teorema 2.2.3, essa expressão mostra que β é raiz do polinômio g_{t_i}.

Finalmente, como g é o polinômio minimal de β sobre $\mathbb{F}_q$, e g_{t_i} também é minimal para α^{t_i} (e seus conjugados), e considerando que β é uma potência de α^{t_i}, deduzimos pelo Teorema 3.3.14(iii) que $g = g_{t_i}$. Portanto, qualquer polinômio g com as propriedades consideradas coincide com algum dos polinômios g_{t_i} construídos.

Agora, falta apenas demonstrar que os polinômios g_{t_i}, para $1 \leq i \leq n$, são todos distintos entre si. Suponhamos, com o intuito de obter uma contradição, que existam índices i e j diferentes, isto é, $i \neq j$, tais que $g_{t_i} = g_{t_j}$. Nesse caso, como g_{t_i} é um polinômio irredutível e seus zeros são conjugados sob a ação de Frobenius, teríamos que α^{t_i} e α^{t_j} seriam ambos raízes do mesmo polinômio g_{t_i}.

Aplicando o Teorema 2.2.3, que descreve a relação entre raízes conjugadas de polinômios irredutíveis, concluímos que existe algum inteiro $b \geq 0$ tal que

$$\alpha^{t_j} = \left(\alpha^{t_i}\right)^{q^b}.$$

Elevando ambos os lados da igualdade à potência adequada, obtemos que $t_j \equiv t_i q^b \pmod{e}$.

Entretanto, pela definição do conjunto T_f, os elementos t_i são escolhidos justamente de forma a serem representantes distintos sob a relação de equivalência $t \equiv tq^b \mod e$. Como também temos trivialmente $t_j \equiv t_j q^0 \pmod{e}$, essa nova congruência nos levaria a identificar t_j e t_i como equivalentes, o que é impossível dado o modo como T_f foi construído.

Portanto, a hipótese de que $g_{t_i} = g_{t_j}$ para $i \neq j$ leva a uma contradição, e concluímos que todos os polinômios g_{t_i} são, de fato, distintos entre si. □

O polinômio minimal g_t associado a $\alpha^t \in \mathbb{F}_{q^m}$ sobre o corpo base $\mathbb{F}_q$ é frequentemente determinado a partir do polinômio característico f_t desse elemento sobre $\mathbb{F}_q$. Conforme discutido após a Definição 2.2.12, existe uma relação direta entre eles: $f_t = g_t^r$, em que $r = m/k$, sendo k o grau do polinômio minimal g_t.

Vale destacar que, como g_t é irredutível em $\mathbb{F}_q[x]$, seu grau k coincide com a ordem multiplicativa de q módulo d pelo Teorema 3.1.5, onde $d = \operatorname{ord}(g_t)$. Por sua vez, d é igual à ordem do elemento α^t no grupo multiplicativo $\mathbb{F}_{q^m}^*$. De acordo com a teoria dos grupos, essa ordem é expressa pela fórmula $e/\operatorname{mdc}(t, e)$, onde e é a ordem de α em $\mathbb{F}_{q^m}^*$.

Assim, conhecendo t e e, é possível calcular d de maneira simples. Consequentemente, também se obtém o valor de k e, a partir daí, o valor de r, o que facilita o processo de determinação de g_t e f_t (veja o Exemplo 3.3.23).

Existem diversos métodos para calcular o polinômio característico f_t. Um dos mais práticos aproveita uma relação particular entre f_t e o polinômio f inicialmente fornecido, permitindo um cálculo mais eficiente.

Teorema 3.3.21. *Seja f um polinômio irredutível mônico em $\mathbb{F}_q[x]$ de grau m. Seja $\alpha \in \mathbb{F}_{q^m}$ uma raiz de f, e para $t \in \mathbb{N}$ seja f_t o polinômio característico de $\alpha^t \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Então*

$$f_t\left(x^t\right) = (-1)^{m(t+1)} \prod_{j=1}^{t} f\left(\omega_j x\right)$$

onde $\omega_1, \ldots, \omega_t$ são as raízes t-ésimas da unidade sobre $\mathbb{F}_q$, contadas de acordo com a multiplicidade.

Demonstração. Veja [11, Teorema 3.39]. □

Em resumo, este teorema mostra como o polinômio característico f_t de uma raiz α^t de f pode ser decomposto de uma maneira interessante em termos das t-ésimas raízes da unidade em $\mathbb{F}_q$.

Exemplo 3.3.22. Considere o polinômio irredutível $f(x) = x^3 + x + 1$ em $\mathbb{F}_2[x]$. Para calcular f_3, também temos que encontrar cúbicas da unidade, ou seja $x^3 - 1$ sobre $\mathbb{F}_2$, que são $1, \omega$ e ω^2, onde ω é uma raiz de $x^2 + x + 1 \in \mathbb{F}_2[x]$ em $\mathbb{F}_4$. A partir daí temos que $\omega^2 + \omega + 1 = 0$. Então,

$$f_3\left(x^3\right) = (-1)^{3(4)} f(1x) f(\omega x) f\left(\omega^2 x\right).$$

Agora:

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

- $f(\omega x) = (\omega x)^3 + \omega x + 1 = \omega^3 x^3 + \omega x + 1 = x^3 + \omega x + 1$,
- $f\left(\omega^2 x\right) = \left(\omega^2 x\right)^3 + \omega^2 x + 1 = \omega^6 x^3 + \omega^2 x + 1 = x^3 + \omega^2 x + 1$.

Então:

$$\begin{aligned} f_3\left(x^3\right) &= (-1)^{3(4)} f(1x) f(\omega x) f\left(\omega^2 x\right) \\ &= \left(x^3 + x + 1\right)\left(x^3 + \omega x + 1\right)\left(x^3 + \omega^2 x + 1\right) \\ &= x^9 + x^6 + 1, \end{aligned}$$

de modo que $f_3(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

□

Uma maneira alternativa de calcular f_t é utilizando conceitos da teoria de matrizes. Considere o polinômio $f(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1 x - a_0$ em $\mathbb{F}_q[x]$. A ele, associamos uma matriz especial chamada **matriz companheira** de f, denotada por A. Esta matriz é de ordem $m \times m$ e é construída organizando os coeficientes de $f(x)$ da seguinte forma:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{pmatrix}.$$

Observe que nas primeiras $m-1$ colunas (exceto a última), os elementos imediatamente abaixo da diagonal principal são iguais a 1, enquanto os demais são 0. Já a última coluna contém os coeficientes $a_0, a_1, \ldots, a_{m-1}$.

Em álgebra linear, sabemos que o **polinômio característico** de uma matriz A é dado por $\det(xI - A)$, onde I é a matriz identidade de dimensão $m \times m$. Neste caso, o polinômio característico de A é precisamente $f(x)$.

Agora, para cada inteiro positivo $t \in \mathbb{N}$, o polinômio f_t é definido como o polinômio característico da matriz A^t, ou seja, da matriz A elevada à potência t. Em outras palavras, para encontrar f_t, basta calcular A^t e depois determinar o polinômio característico de A^t.

Portanto, através da multiplicação sucessiva da matriz companheira A, conseguimos obter todos os polinômios f_t desejados.

Do Exemplo 3.3.22 a matriz A e A^3 são:

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{e} \qquad A^3 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

logo o polinômio característico de A^3 é

$$\det\left(xI - A^3\right) = x^3 - 2x^2 - x^2 + 2x - 1 = x^3 + x^2 + 1 \in \mathbb{F}_2[x],$$

obtendo o mesmo resultado.

Exemplo 3.3.23. Um problema interessante na teoria de corpos finitos é identificar em quais casos os polinômios f_t resultam ser irredutíveis no anel $\mathbb{F}_q[x]$. A partir da discussão anterior ao Teorema 3.3.21, sabemos que f_t será irredutível sobre $\mathbb{F}_q$ se, e somente se, a

ordem multiplicativa k de q módulo d for igual ao grau m do polinômio inicial f (lembrando que $r = m/k$). Aqui, d (ordem de g_t, polinômio minimal) é definido como $e/\operatorname{mdc}(t, e)$, onde e representa a ordem de α (uma raiz de f) no corpo de extensão $\mathbb{F}_{q^m}$.

Vamos considerar o caso em que $q = 3$, $m = 4$ e $e = 80$. Nosso objetivo é determinar para quais valores de t o polinômio f_t é irredutível em $\mathbb{F}_3[x]$.

Primeiramente, recordamos que f_t será irredutível se, e somente se, a ordem multiplicativa de q módulo $d = e/\operatorname{mdc}(t, e)$ for igual a m. Como $m = 4$, as possíveis ordens menores que podem ocorrer são divisores de 4, isto é, $k = 1$ ou 2.

Calculando:

$$k = 1: \quad 3^1 - 1 = 2,$$
$$k = 2: \quad 3^2 - 1 = 8.$$

Assim, se d divide 2 ou 8, o polinômio será redutível. Como $e = 80$, os divisores relevantes de 80 associados a ordens pequenas seriam aqueles onde $d = 1, 2, 4$ ou 8. Ou seja, $\operatorname{mdc}(t, 80)$ deveria ser $80, 40, 20$ ou 10 para que $d = 1, 2, 4$ ou 8.

Portanto, f_t será redutível se $\operatorname{mdc}(t, 80) = 10, 20, 40$ ou 80.

Para valores de t entre 1 e 80, concluímos que f_t é irredutível em $\mathbb{F}_3[x]$ sempre que t não satisfaz essas condições específicas.

Na prática, polinômios irredutíveis frequentemente surgem como polinômios minimais de elementos em uma extensão de corpos. Se, na discussão anterior, considerarmos que f é um polinômio primitivo sobre $\mathbb{F}_q$, de forma que $e = q^m - 1$, então as potências de α percorrem todos os elementos não nulos de $\mathbb{F}_{q^m}$. Assim, os métodos apresentados anteriormente podem ser utilizados para calcular o polinômio minimal sobre $\mathbb{F}_q$ de cada elemento de $\mathbb{F}_{q^m}^*$.

Uma outra maneira de encontrar os polinômios mínimos é utilizando o Teorema 3.3.14(v). Para determinar o polinômio mínimo g de um elemento $\beta \in \mathbb{F}_{q^m}$ sobre o corpo $\mathbb{F}_q$, calculamos sucessivamente as potências $\beta, \beta^q, \beta^{q^2}, \ldots$ até encontrar o menor inteiro positivo d tal que $\beta^{q^d} = \beta$. Esse número d corresponde ao grau de g, e o polinômio g é construído da seguinte forma:

$$g(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{d-1}}).$$

Os elementos $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$ representam os conjugados distintos de β em relação a $\mathbb{F}_q$, e o polinômio g é o polinômio mínimo comum a todos esses conjugados.

Exemplo 3.3.24. Calculamos os polinômios mínimos sobre $\mathbb{F}_3$ de todos os elementos de $\mathbb{F}_9$. Seja $\alpha \in \mathbb{F}_9$ uma raiz do polinômio primitivo $x^2 + x + 2$ sobre $\mathbb{F}_3$. Ele é primitivo pois a ordem é 8, pelo Teorema 3.2.2 chegamos a essa conclusão. Agora nós sabemos que os elementos de $\mathbb{F}_9$ podem ser escritos da forma $a + b\alpha$, onde $a, b \in \mathbb{F}_3$, então:

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha\}$$

mas como também sabemos que $\alpha^2 = -\alpha - 2 = 2\alpha + 1$, temos que:

i	α^i
0	1
1	α
2	$2\alpha + 1$
3	$2\alpha + 2$

e

i	α^i
4	2
5	2α
6	$\alpha + 2$
7	$\alpha + 1$

Como a extensão é de grau 2, os polinômios mínimos serão de grau 1 ou 2. Os conjugados de um elemento $\beta \in \mathbb{F}_9$ em relação a $\mathbb{F}_3$ são β e β^3, temos então que:

- Se $\beta = 0$ então $g_1(x) = x$.
- Se $\beta = 1$ então $g_2(x) = x - 1$.
- Se $\beta = \alpha^4 = 2$ e como $\beta^3 = \alpha^{12} = \alpha^4$ então $g_3(x) = x - 2 = x + 1$.
- Se $\beta = \alpha$, os conjugados são α e $\alpha^3 = 2\alpha + 2$, então:

$$\begin{aligned} g_4(x) =& (x - \alpha)\left(x - \alpha^3\right) \\ =& x^2 - \left(\alpha + \alpha^3\right)x + \alpha\alpha^3 \\ =& x^2 + x + 2. \end{aligned}$$

- Se $\beta = \alpha^2$, os conjugados são $\alpha^2 = 2\alpha + 1$ e $\alpha^6 = \alpha + 2$ então:

$$\begin{aligned} g_5(x) =& \left(x - \alpha^2\right)\left(x - \alpha^6\right) \\ =& x^2 - \left(\alpha^2 + \alpha^6\right)x + \alpha^2\alpha^6 \\ =& x^2 + 1. \end{aligned}$$

- Se $\beta = \alpha^5$, os conjugados são $\alpha^5 = 2\alpha$ e $\alpha^{15} = \alpha^7 = \alpha + 1$ então:

$$\begin{aligned} g_6(x) =& \left(x - \alpha^5\right)\left(x - \alpha^7\right) \\ =& x^2 - \left(\alpha^5 + \alpha^7\right)x + \alpha^5\alpha^7 \\ =& x^2 + 2x + 2. \end{aligned}$$

Esses elementos, juntamente com seus conjugados com respeito a $\mathbb{F}_3$.

Teorema 3.3.25. *Seja f um polinômio irredutível sobre $\mathbb{F}_q$ de grau n, e seja $k \in \mathbb{N}$. Então, f se fatora em d polinômios irredutíveis em $\mathbb{F}_{q^k}[x]$, todos de mesmo grau n/d, onde $d = \mathrm{mdc}(k, n)$.*

Demonstração. É claro que para um polinômio linear, $n = 1$ então $d = 1$, não pode ser fatorado, podemos assumir que $f(0) \neq 0$. Seja g um fator irredutível de f em $\mathbb{F}_{q^k}[x]$. Se $\mathrm{ord}(f) = e$, como as raízes de g também são raízes de f obtemos pelo Teorema 3.1.3 que $\mathrm{ord}(g) = e$. Logo pelo Teorema 3.1.5, n é a ordem multiplicativa de q módulo e e o grau de g é igual à ordem multiplicativa de q^k módulo e. Agora vamos mostrar que potências q^j, para $j = 0, 1, \ldots$, consideradas módulo e, formam um grupo cíclico de ordem n. Definamos:

$$G = \left\{q^j \bmod e \mid j \geq 0\right\}.$$

Queremos mostrar que G é um subgrupo cíclico do grupo multiplicativo $(\mathbb{Z}_e)^*$ de unidades módulo e, e que sua ordem é a ordem multiplicativa de q módulo e.

Como e divide $q^n - 1$ então $\mathrm{mdc}(q, e) = 1$ (são coprimos), portanto $q^j \bmod e$ também é invertível para qualquer $j \geq 0$. Então $G \subseteq (\mathbb{Z}_e)^*$.

Agora temos que mostrar que é um subgrupo:

- $1 = q^0 \equiv 1 \bmod e$, e 1 é o elemento neutro em $(\mathbb{Z}_e)^*$.

- Sejam q^a, $q^b \in G$, então:

$$(q^a \bmod e) \times \left(q^b \bmod e\right) \equiv q^{a+b} \bmod e,$$

  e como $a + b \geq 0$, $q^{a+b} \bmod e \in G$.

- Para qualquer $q^a \in G$, seu inverso é $q^{-a} \bmod e$, onde:

$$q^{-a} \equiv \left(q^{n-a}\right) \mod e$$

  pois n é a ordem multiplicativo de q modulo e.

Pelo argumento mencionado no final, G é cíclico de ordem n.

Assim, como grau de g é igual à ordem multiplicativa de q^k módulo e, o grau de g é igual à ordem de q^k em G, segue-se do teoria dos grupos que a ordem multiplicativa de q^k módulo e é n/d, onde $d = \text{mdc}(k, n)$, então o grau de g é n/d. □

Corolário 3.3.26. *Um polinômio irredutível sobre $\mathbb{F}_q$ de grau n permanece irredutível sobre $\mathbb{F}_{q^k}$ se, e somente se, k e n são primos entre si.*

Demonstração. Usando o Teorema 3.3.25, como k e n são primos entre si, então $d = 1$. Logo permanece irredutível. □

Exemplo 3.3.27. Seja $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$, um polinômio irredutível de grau $n = 4$. Vamos aplicar o Teorema 3.3.25 com $k = 2$.

Calculamos:

$$d = \text{mdc}(k, n) = \text{mdc}(2, 4) = 2.$$

Então, segundo o teorema, $f(x)$ se fatora em $d = 2$ polinômios irredutíveis de grau $\frac{n}{d} = 2$ sobre $\mathbb{F}_{2^2} = \mathbb{F}_4$.

O corpo $\mathbb{F}_4$ pode ser construído como $\mathbb{F}_2[\theta]$, onde θ é uma raiz do polinômio irredutível $x^2 + x + 1 \in \mathbb{F}_2[x]$, então satisfaz $\theta^2 + \theta + 1 = 0$. Assim, $\mathbb{F}_4 = \{0, 1, \theta, \theta + 1\}$.

Neste corpo, a fatoração de $f(x)$ é:

$$f(x) = (x^2 + x + \theta^2)(x^2 + x + \theta),$$

onde ambos os fatores são irredutíveis sobre $\mathbb{F}_4$, como previsto pelo teorema.

□

3.4 q-Polinômios

Tanto na parte teórica quanto nas aplicações práticas, uma certa classe de polinômios, que será apresentada a seguir, desempenha um papel relevante. Um aspecto vantajoso desses polinômios é a forma como suas raízes estão organizadas, o que torna mais simples a identificação dessas raízes. Como é habitual, denotamos por q uma potência de número primo.

Definição 3.4.1. Um polinômio da forma

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

com coeficientes em um corpo de extensão $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$, é chamado de q-polinômio sobre $\mathbb{F}_{q^m}$.

Alguns autores, levando-se em conta que o valor de q é fixo, chamam tal polinômio de *polinômio linearizado*. Essa terminologia se justifica pela seguinte propriedade dos polinômios linearizados. Seja F uma extensão arbitrária de $\mathbb{F}_{q^m}$ e seja $L(x)$ um polinômio linearizado (ou seja, um q-polinômio) sobre $\mathbb{F}_{q^m}$. Então, valem as seguintes identidades:

$$\begin{aligned} L(\beta+\gamma) &= L(\beta) + L(\gamma) \quad \text{para todos } \beta, \gamma \in F, \\ L(c\beta) &= cL(\beta) \quad \text{para todo } c \in \mathbb{F}_q \text{ e todo } \beta \in F, \end{aligned} \tag{3.10}$$

onde a primeira igualdade é pelo Teorema 1.0.1, e a segunda é porque sabemos que satisfaz que $c^{q^i} = c$ para $c \in \mathbb{F}_q$ e $i \geq 0$ pelo Lema 2.1.3. Portanto, se F for considerado como um espaço vetorial sobre $\mathbb{F}_q$, então o polinômio linearizado $L(x)$ define um operador linear em F.

Teorema 3.4.2. *Seja $L(x)$ um q-polinômio não nulo sobre $\mathbb{F}_{q^m}$, e seja $\mathbb{F}_{q^s}$ uma extensão de $\mathbb{F}_{q^m}$ que contém todas as raízes de $L(x)$. Então, cada raiz de $L(x)$ possui a mesma multiplicidade, que é igual a 1 ou a uma potência de q, e o conjunto das raízes forma um subespaço linear de $\mathbb{F}_{q^s}$, onde $\mathbb{F}_{q^s}$ é considerado como um espaço vetorial sobre $\mathbb{F}_q$.*

Demonstração. A primeira coisa que vamos demonstrar é que o conjunto de raízes de $L(x)$, que chamaremos de V, é um subespaço vetorial de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$ (uma coisa óbvia é que $V \subset \mathbb{F}_{q^s}$, pois é seu corpo de decomposição). Seja $a, b \in V$ e $\alpha \in \mathbb{F}_q$:

- É claro pela definição de $L(x)$ que $0 \in V$.
- $L(\alpha a + b) = \alpha L(a) + L(b) = 0$ pelo visto nas Equações (3.10), então $\alpha a + b \in V$.

Isto garante que V é um subespaço vetorial de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$.

Logo como

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

e como sabemos que a característica de $\mathbb{F}_{q^s}$ é p, temos que $L'(x) = \alpha_0$, o que significa que $L(x)$ possui apenas raízes simples no caso em que $\alpha_0 \neq 0$, é aqui que descobrimos que a ordem multiplicativa de cada raiz é 1.

Vemos o caso em que $\alpha_0 = 0$, mas para generalizar vamos supor que temos $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$, mas $\alpha_k \neq 0$ para algum $k \geqslant 1$, então podemos reescrever $L(x)$ na seguinte forma:

$$L(x) = \sum_{i=k}^{n} \alpha_i x^{q^i}.$$

Logo como sabemos que $\alpha_i^{q^{mk}} = \alpha_i$, pois $\alpha_i \in \mathbb{F}_{q^m}$, portanto pelo Teorema 2.1.6 temos que $\alpha_i \in \mathbb{F}_{q^{mk}}$, então:

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

Também usando o Teorema 1.0.1 para a última igualdade. Logo a última igualdade mostra que $L(x)$ é a potência q^k-ésima de um q-polinômio que possui apenas raízes simples. Nesse caso, cada raiz de $L(x)$ tem multiplicidade q^k. □

Existem uma versão da recíproca do teorema anterior, mas precisamos do seguinte resultado preliminar antes de prová-lo.

Lema 3.4.3. *Sejam $\beta_1, \beta_2, \ldots, \beta_n$ elementos de $\mathbb{F}_{q^m}$. Então:*

$$D_n := \begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \cdots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k \right), \tag{3.11}$$

e, portanto, o determinante é diferente de zero se, e somente se, $\beta_1, \beta_2, \ldots, \beta_n$ forem linearmente independentes sobre $\mathbb{F}_q$.

Demonstração. Veja [11, Lema 3.51]. □

Teorema 3.4.4. *Seja U um subespaço linear de $\mathbb{F}_{q^m}$, considerado como um espaço vetorial sobre $\mathbb{F}_q$. Então, para qualquer inteiro não negativo k, o polinômio*

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

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

Demonstração. Primeiro podemos fatorar o expoente q^k de cada fator do produto, e obtemos:

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

Só temos que provar que $\widetilde{L}(x) = \prod_{\beta \in U}(x - \beta)$ é um q-polinômio sobre $\mathbb{F}_{q^m}$, pois se aplicarmos a potência q^k ela permanece como um q-polinômio. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de U sobre $\mathbb{F}_q$, então o determinante D_n da Equação (3.11), é diferente de zero pelo Lema 3.4.3. Como temos que $\beta \in U$, então existem $c_1, ..., c_k \in \mathbb{F}_q$ tais que $\beta = c_1\beta_1 + \cdots + c_n\beta_n$, logo temos:

$$\widetilde{L}(x) = \prod_{\beta \in U} (x - \beta) = \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right). \tag{3.12}$$

Agora vamos definir o seguinte polinômio na forma de um determinante de uma matriz,

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \vdots & \vdots & & \vdots & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ x & x^q & \cdots & x^{q^{n-1}} & x^{q^n} \end{vmatrix}.$$

Desenvolvendo o determinante usando a última linha obtemos:

$$D(x) = D_n x^{q^n} + \sum_{i=0}^{n-1} \alpha_i x^{q^i}$$

com $\alpha_i \in U$. Pela definição de $D(x)$ como determinante, sabemos que $D(\beta_i) = 0$ para $1 \leq i \leq n$, da segunda forma de $D(x)$ sabemos que é um q-polinômio sobre $\mathbb{F}_{q^m}$, logo toda combinação linear $c_1\beta_1 + \cdots + c_n\beta_n$ é uma raiz de $D(x)$. Assim $D(x)$ tem q^n raízes, que é o grau $D(x)$, então podemos fatorá-lo da seguinte maneira:

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

Da Equação (3.12) e a última igualdade obtemos que

$$\widetilde{L}(x) = D_n^{-1} D(x).$$

Logo $\widetilde{L}(x)$ é um q-polinômio sobre $\mathbb{F}_{q^m}$, então $L(x)$ é um q-polinômio sobre $\mathbb{F}_{q^m}$. □

As propriedades dos q-polinômios nos permitem utilizar um método bastante eficiente para determinar suas raízes. Seja

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

um q-polinômio sobre o corpo finito $\mathbb{F}_{q^m}$, e suponha que desejamos encontrar todas as raízes de $L(x)$ em uma extensão finita F de $\mathbb{F}_{q^m}$. Como foi observado anteriormente, a aplicação

$$L : \beta \in F \mapsto L(\beta) \in F$$

é um operador linear no espaço vetorial F, considerado como espaço vetorial sobre $\mathbb{F}_q$. Isso decorre do fato de que os q-polinômios preservam a adição e a multiplicação escalar por elementos de $\mathbb{F}_q$.

Dado que L é uma transformação linear, ela pode ser representada por uma matriz com entradas em $\mathbb{F}_q$. Para isso, fixamos uma base $\{\beta_1, \ldots, \beta_s\}$ de F como espaço vetorial sobre $\mathbb{F}_q$. Assim, qualquer elemento $\beta \in F$ pode ser escrito unicamente como

$$\beta = \sum_{j=1}^{s} c_j \beta_j \quad \text{com } c_j \in \mathbb{F}_q \text{ para } 1 \leqslant j \leqslant s.$$

Aplicando L a esse vetor, temos

$$L(\beta) = \sum_{j=1}^{s} c_j L(\beta_j),$$

isto é, a imagem de β por L é determinada pelas imagens dos vetores da base. Escrevemos cada imagem $L(\beta_j)$ como uma combinação linear dos vetores da base:

$$L(\beta_j) = \sum_{k=1}^{s} b_{jk}\beta_k \quad \text{para } 1 \leqslant j \leqslant s,$$

onde os coeficientes $b_{jk} \in \mathbb{F}_q$. Com isso, podemos formar a matriz B de ordem $s \times s$ cujas entradas são justamente os coeficientes b_{jk}, isto é, a entrada na posição (j,k) de B é b_{jk}. Então, se

$$(c_1, \ldots, c_s)B = (d_1, \ldots, d_s),$$

obtemos

$$L(\beta) = \sum_{k=1}^{s} d_k\beta_k.$$

Logo, a equação $L(\beta) = 0$ equivale a resolver

$$(c_1, \ldots, c_s)B = (0, \ldots, 0), \tag{3.13}$$

ou seja, trata-se de um sistema linear homogêneo com coeficientes em $\mathbb{F}_q$. Esse sistema possui um número de soluções igual a q^{s-r}, onde r é o posto (ou posto de linha) da matriz B. Cada vetor solução $(c_1, \ldots, c_s)$ determina uma raiz do polinômio $L(x)$, dada por

$$\beta = \sum_{j=1}^{s} c_j\beta_j.$$

Portanto, o problema de encontrar as raízes do polinômio linearizado $L(x)$ em F se reduz a resolver um sistema linear homogêneo sobre $\mathbb{F}_q$, o que é computacionalmente muito mais simples e eficiente.

Exemplo 3.4.5. Seja o polinômio linearizado sobre o corpo $\mathbb{F}_2$:

$$L(x) = x + x^2 + x^4.$$

Nosso objetivo é encontrar as raízes de $L(x)$ no corpo $\mathbb{F}_{64}$, que é uma extensão de grau 6 de $\mathbb{F}_2$. Construímos $\mathbb{F}_{64} = \mathbb{F}_2[\theta]/(\theta^6 + \theta + 1)$, onde θ é uma raiz primitiva do polinômio irredutível $x^6 + x + 1 \in \mathbb{F}_2[x]$ (é primitiva pelo Exemplo 3.1.14).

A base de $\mathbb{F}_{64}$ sobre $\mathbb{F}_2$ é:

$$\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}.$$

Aplicamos o polinômio $L(x)$ a cada elemento da base:

- $L(1) = 1 + 1 + 1 = 1$ do qual obtemos o seguinte vetor $(1,0,0,0,0,0)$.
- $L(\theta) = \theta + \theta^2 + \theta^4$ do qual obtemos o seguinte vetor $(0,1,1,0,1,0)$.

- $L(\theta^2) = \theta^2 + \theta^4 + \theta^8 = \theta^3 + \theta^4$ do qual obtemos o seguinte vetor $(0,0,0,1,1,0)$.
- $L(\theta^3) = \theta^3 + \theta^6 + \theta^{12} = \theta + \theta^2 + \theta^3$ do qual obtemos o seguinte vetor $(0,1,1,1,0,0)$.
- $L(\theta^4) = \theta^4 + \theta^8 + \theta^{16} = 1 + \theta + \theta^2 + \theta^3$ do qual obtemos o seguinte vetor $(1,1,1,1,0,0)$.
- $L(\theta^5) = \theta^5 + \theta^{10} + \theta^{20} = \theta^2 + \theta^3 + \theta^5$ do qual obtemos o seguinte vetor $(0,0,1,1,0,1)$.

Logo, a matriz associada B da aplicação linear L, na base $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$, é:

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Para encontrar as raízes de L, basta resolver o sistema:

$$(c_1, c_2, c_3, c_4, c_5, c_6)B = (0,0,0,0,0,0).$$

Como o posto de B é 4, então o sistema tem $2^{6-4} = 4$ soluções, que são $t(1,1,1,0,1,0) + s(0,1,1,1,0,0)$ com $s, t \in \mathbb{F}_2$, logo as raízes de $L(x)$ em $\mathbb{F}_{64}$ são $\eta_1 = 0$, $\eta_2 = 1 + \theta + \theta^2 + \theta^4$, $\eta_3 = \theta + \theta^2 + \theta^3$ e $\eta_4 = 1 + \theta^3 + \theta^4$.

Se tomarmos este polinômio $L(x)$ como um em $\mathbb{F}_2[x]$, ele será fatorado da seguinte forma $L(x) = x(x^3 + x + 1)$, onde o fator do lado direito é irredutível em $\mathbb{F}_2$, e tem suas raízes em $\mathbb{F}_8$, então η_2, η_3 e η_4 são elementos de $\mathbb{F}_8$, que é um subcorpo de $\mathbb{F}_{64}$ pelo Teorema 2.1.6.

Esse procedimento para encontrar raízes também pode ser estendido para uma classe um pouco mais ampla de polinômios, conhecidos como *polinômios afins*.

Definição 3.4.6. Um polinômio da forma $A(x) = L(x) - \alpha$, onde $L(x)$ é um q-polinômio sobre $\mathbb{F}_{q^m}$ e $\alpha \in \mathbb{F}_{q^m}$, é denominado um *$q$-polinômio afim* sobre $\mathbb{F}_{q^m}$.

Um elemento $\beta \in F$ será uma raiz do polinômio $A(x)$ se, e somente se, ao aplicarmos o polinômio linearizado $L(x)$ sobre β, obtivermos o valor α, ou seja, $L(\beta) = \alpha$. De acordo com a notação apresentada na Equação (3.13), essa condição equivale a resolver o seguinte sistema de equações lineares:

$$(c_1, \ldots, c_s)B = (d_1, \ldots, d_s), \tag{3.14}$$

em que a constante α é expressa como combinação linear da base $\{\beta_1, \ldots, \beta_s\}$, isto é, $\alpha = \sum_{k=1}^{s} d_k \beta_k$. Assim, ao encontrar uma solução para os coeficientes $c_1, \ldots, c_s$, podemos construir a raiz correspondente $\beta = \sum_{j=1}^{s} c_j \beta_j$ do polinômio $A(x)$ no corpo F.

Dado um polinômio $f(x) \in \mathbb{F}_{q^m}[x]$ de grau $n \geq 1$, é possível determinar suas raízes em uma extensão F de $\mathbb{F}_{q^m}$ por meio de um polinômio q-afim $A(x)$ que seja múltiplo de $f(x)$. Para isso, buscamos um polinômio da forma

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha,$$

em que os coeficientes $\alpha_i \in \mathbb{F}_{q^m}$ não são todos nulos, e $\alpha \in \mathbb{F}_{q^m}$.

Para construí-lo, consideramos os resíduos $r_i(x)$ de x^{q^i} módulo $f(x)$, ou seja, polinômios de grau menor que n tais que

$$x^{q^i} \equiv r_i(x) \mod f(x), \quad \text{para } i = 0, 1, \ldots, n-1.$$

Em seguida, buscamos coeficientes $\alpha_i \in \mathbb{F}_{q^m}$, não todos nulos, tais que a combinação linear

$$\sum_{i=0}^{n-1} \alpha_i r_i(x)$$

seja um polinômio constante $\alpha \in \mathbb{F}_{q^m}$. Isso equivale a anular os coeficientes de x^j para $j = 1, 2, \ldots, n-1$, o que nos leva a um sistema homogêneo de $n-1$ equações lineares em n variáveis $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, o qual sempre admite uma solução não trivial.

Uma vez determinada essa combinação, temos:

$$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \alpha \mod f(x),$$

e, subtraindo α dos dois lados, obtemos:

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha \equiv 0 \mod f(x).$$

Ou seja, por construção, $A(x)$ é um múltiplo de $f(x)$, o que garante que todas as raízes de $f(x)$ também serão raízes de $A(x)$. Assim, podemos encontrar as raízes de $f(x)$ identificando todas as raízes de $A(x)$ no corpo F, e verificando quais delas anulam $f(x)$. Esse método é particularmente eficiente porque a estrutura dos polinômios q-afins permite determinar todas as suas raízes com base em um sistema linear, como foi demonstrado anteriormente da Equação 3.14.

Exemplo 3.4.7. Seja $f(x) = x^3 + \alpha x^2 + \alpha x + \alpha^2 \in \mathbb{F}_4[x]$ com $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Lembrando que $\alpha^2 = \alpha + 1$, encontramos as raízes de $f(x)$ em $\mathbb{F}_{16}$. Primeiro, encontraremos o q-polinômio afim, um múltiplo de $f(x)$, usando o método descrito com $q = 2$ e $n = 3$. Para $i = 0, 1, 2$ temos:

- $i = 0$, $r_0(x) \equiv x^{2^0} \mod f(x)$ então $r_0(x) = x$.
- $i = 1$, $r_1(x) \equiv x^{2^1} \mod f(x)$ então $r_1(x) = x^2$.
- $i = 2$, $r_2(x) \equiv x^{2^2} \mod f(x)$ então $r_2(x) = x^2 + 1$.

Depois temos que fazer uma combinação linear deles com a condição de que a combinação linear: nem todas as constantes sejam 0 em $\mathbb{F}_4$ e $R(x) = \alpha_0 r_0(x) + \alpha_1 r_1(x) + \alpha_2 r_2(x)$ tenha que nos dar uma constante em $\mathbb{F}_4[x]$, então fazemos:

$$R(x) = \alpha_0 x + \alpha_1 x^2 + \alpha_2 \left(x^2 + 1\right)$$

logo

$$R(x) = x\left(\alpha_0\right) + x^2\left(\alpha_1 + \alpha_2\right) + \alpha_2,$$

queremos eliminar os termos com variáveis, por isso fazemos:

$$\begin{cases} \alpha_1 + \alpha_2 = 0 \\ \alpha_0 = 0 \end{cases}.$$

Agora se $\alpha_2 = 1$ obtemos que $\alpha_1 = 1$, e o polinômio constante $R(x) = 1$, que é o resultado da combinação linear.

Então,

$$A(x) = \alpha_0 x^{2^0} + \alpha_1 x^{2^1} + \alpha_2 x^{2^2} - R(x) = x^2 + x^4 - 1,$$

é um q-polinômio afim múltiplo de $f(x)$ sobre $\mathbb{F}_4$. Agora temos que encontrar as raízes de $A(x)$ em $\mathbb{F}_{16}$, que é o mesmo que resolver $L(x) = \alpha$, com $L(x) = x^2 + x^4$. Seja θ uma raiz primitiva de $x^4 + x + 1$ sobre $\mathbb{F}_2$ que gera $\mathbb{F}_{16}^*$ e $\{1, \theta, \theta^2, \theta^3\}$ é uma base para $\mathbb{F}_{16}$ sobre $\mathbb{F}_2$. Como α é uma raiz primitiva terceira da unidade sobre $\mathbb{F}_2$, obtemos $\alpha = \theta^5 = \theta^2 + \theta$ e também usando $\alpha^2 = \alpha + 1 = \theta^2 + \theta + 1$, fazemos:

- $L(1) = 1^2 + 1^4 = 0$ do qual obtemos o seguinte vetor $(0, 0, 0, 0)$.
- $L(\theta) = \theta^2 + \theta^4 + = 1 + \theta + \theta^2$ do qual obtemos o seguinte vetor $(1, 1, 1, 0)$.
- $L\left(\theta^2\right) = \theta^4 + \theta^8 = \theta + \theta^2$ do qual obtemos o seguinte vetor $(0, 1, 1, 0)$.
- $L\left(\theta^3\right) = \theta^6 + \theta^{12} = 1 + \theta$ do qual obtemos o seguinte vetor $(1, 1, 0, 0)$.

Assim a matriz B da Equação (3.14) é feito da seguinte maneira:

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

A representação de 1 em termos da base $\{1, \theta, \theta^2, \theta^3\}$ é $(1, 0, 0, 0)$. Queremos resolver o seguinte sistema:

$$(c_1, c_2, c_3, c_4) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = (1, 0, 0, 0).$$

A solução é $c_1(1, 0, 0, 0) + (0, 1, 0, 0) + (0, 0, 1, 0)$ com $c_1 \in \mathbb{F}_2$, logo as raízes de $A(x)$ são $x_1 = 1 + \theta + \theta^2 = \alpha^2$ e $x_2 = \theta + \theta^2 = \alpha$, que ambas são raízes de f em $\mathbb{F}_{16}$, pela foma das raízes.

Vamos ver outro exemplo.

Exemplo 3.4.8. Seja $f(x) = x^4 + \alpha^2 x^3 + \alpha x^2 + \alpha^2 \in \mathbb{F}_4[x]$ com $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Lembrando que $\alpha^2 = \alpha + 1$ encontramos as raízes de $f(x)$ em $\mathbb{F}_{64}$. Primeiro, encontraremos o q-polinômio afim, um múltiplo de $f(x)$, usando o método descrito com $q = 2$ e $n = 4$, então temos:

- $i = 0$, $r_0(x) \equiv x^{2^0} \bmod f(x)$ então $r_0 = x$.
- $i = 1$, $r_1(x) \equiv x^{2^1} \bmod f(x)$ então $r_1(x) = x^2$.

- $i = 2$, $r_2(x) \equiv x^{2^2} \bmod f(x)$ então $r_2(x) = \alpha^2 x^3 + \alpha x^2 + \alpha^2$.
- $i = 3$, $r_3(x) \equiv x^{2^3} \bmod f(x)$ então $r_3(x) = \alpha^2 x$.

Depois temos que fazer uma combinação linear deles com a condição de que a combinação linear: nem todas as constantes sejam 0 em $\mathbb{F}_4$ e $R(x) = \alpha_0 r_0(x) + \alpha_1 r_1(x) + \alpha_2 r_2(x) + \alpha_3 r_3(x)$ tenha que nos dar uma função constante em $\mathbb{F}_4[x]$, temos:

$$R(x) = \alpha_0 x + \alpha_1 x^2 + \alpha_2 \left(\alpha^2 x^3 + \alpha x^2 + \alpha^2\right) + \alpha_3 \left(\alpha^2 x\right),$$

logo

$$R(x) = \left(\alpha_2 \alpha^2\right) x^3 + \left(\alpha_1 + \alpha_2 \alpha\right) x^2 + \left(\alpha_0 + \alpha_3 \alpha^2\right) x + \alpha_2 \alpha^2.$$

Da condição obtemos:

$$\begin{cases} \alpha_2 \alpha^2 = 0 \\ \alpha_1 + \alpha_2 \alpha = 0 \\ \alpha_0 + \alpha_3 \alpha^2 = 0 \end{cases}.$$

Agora se $\alpha_3 = 1$, então $\alpha_0 = \alpha^2$, $\alpha_1 = 0$, $c_2 = 0$ e a constante é $R(x) = \alpha_2 \alpha^2 = 0$.

Consequentemente, obtém-se o 2-polinômio afim sobre $\mathbb{F}_4$:

$$A(x) = \alpha_0 x^{2^0} + \alpha_1 x^{2^1} + \alpha_2 x^{2^2} + \alpha_3 x^{2^3} - 0 = \alpha^2 x + x^8$$

Onde $A(x)$ é um q-polinômio afim múltiplo de $f(x)$ sobre $\mathbb{F}_4$. Agora temos que encontrar as raízes de $A(x)$ em $\mathbb{F}_{64}$, que é o mesmo que resolver $L(x) = 0$, com $L(x) = \alpha^2 x + x^8$. Construímos $\mathbb{F}_{64} = \mathbb{F}_2[\theta]/(\theta^6 + \theta + 1)$, onde θ é uma raiz primitiva desse polinômio irredutível $x^6 + x + 1 \in \mathbb{F}_2[x]$ (é primitiva pelo Exemplo 3.1.14).

A base de $\mathbb{F}_{64}$ sobre $\mathbb{F}_2$ é:

$$\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}.$$

Como α é uma raiz primitiva terceira da unidade sobre $\mathbb{F}_2$, obtemos $\alpha = \theta^{21} = 1 + \theta + \theta^3 + \theta^4 + \theta^5$, (também usando $\alpha^2 = \alpha + 1 = \theta + \theta^3 + \theta^4 + \theta^5$) obtemos:

$$\begin{aligned}
L(1) &= 1 + \theta + 0 + \theta^3 + \theta^4 + \theta^5, \\
L(\theta) &= 1 + \theta + 0 + \theta^3 + \theta^4 + \theta^5, \\
L(\theta^2) &= 0 + \theta + \theta^2 + \theta^3 + \theta^4 + \theta^5, \\
L(\theta^3) &= 0 + 0 + 0 + \theta^3 + 0 + 0, \\
L(\theta^4) &= 1 + \theta + 0 + \theta^3 + \theta^4 + \theta^5, \\
L(\theta^5) &= 0 + 0 + 0 + \theta^3 + 0 + 0.
\end{aligned}$$

Assim a matriz B da Equação (3.14) é feito da seguinte maneira:

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

A representação de $R(x) = 0$ em termos da base $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ é $(0,0,0,0,0,0)$. Queremos resolver o seguinte sistema:

$$(a_0, a_1, a_2, a_3, a_4, a_5) \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = (0,0,0,0,0,0)\,.$$

A solução é $c_1\,(1,0,0,0,1,0) + c_2\,(0,1,0,0,1,0) + c_3\,(0,0,0,1,0,1)$ com $c_1, c_2, c_3 \in \mathbb{F}_2$, logo as raízes do $A(x)$ são :

- $\eta_1 = 0$,
- $\eta_2 = 1 + \theta^4$,
- $\eta_3 = \theta + \theta^4$,
- $\eta_4 = \theta^3 + \theta^5$,
- $\eta_5 = 1 + \theta$,
- $\eta_6 = 1 + \theta^3 + \theta^4 + \theta^5$,
- $\eta_7 = \theta + \theta^3 + \theta^4 + \theta^5 = \alpha^2$,
- $\eta_8 = 1 + \theta + \theta^3 + \theta^5$.

Agora temos que verificar quais dessas raízes também são raízes de $f(x)$, que são η_7, η_2, η_3, η_5 em $\mathbb{F}_{64}$.

O método para encontrar as raízes de um polinômio q-afim em um corpo finito, como mostrado no exemplo anterior, revela que o conjunto de soluções forma um *subespaço afim* de $\mathbb{F}_{q^n}$. Isso significa que as raízes não apenas satisfazem uma estrutura algébrica, mas também possuem uma organização geométrica: elas constituem uma translação de um subespaço vetorial, ou seja, são obtidas ao somar um vetor fixo a todos os elementos de um subespaço linear.

Essa propriedade pode ser compreendida tanto por meio do algoritmo explícito de cálculo (como a construção do polinômio afim e a análise da matriz associada), quanto por princípios mais abstratos da álgebra linear sobre corpos finitos. Em particular, quando as raízes de um polinômio afim são vistas como soluções de uma equação linear em um espaço vetorial, elas naturalmente formam uma estrutura fechada sob adição com um vetor fixo, o que caracteriza um subespaço afim.

Além disso, o comportamento das multiplicidades das raízes e a estrutura do polinômio envolvido reforçam essa interpretação geométrica das soluções.

Teorema 3.4.9. *Seja $A(x)$ um polinômio q-afim de grau positivo sobre $\mathbb{F}_{q^m}$, e seja $\mathbb{F}_{q^s}$ uma extensão de $\mathbb{F}_{q^m}$ que contém todas as raízes de $A(x)$. Então, cada raiz de $A(x)$ tem a mesma multiplicidade, que é igual a 1 ou uma potência de q, e o conjunto das raízes forma um subespaço afim de $\mathbb{F}_{q^s}$, onde $\mathbb{F}_{q^s}$ é considerado como um espaço vetorial sobre $\mathbb{F}_q$.*

Demonstração. Considere um polinômio $A(x)$ da forma $A(x) = L(x) - \alpha$, onde $L(x)$ é um q-polinômio sobre o corpo finito $\mathbb{F}_{q^m}$, e $\alpha \in \mathbb{F}_{q^m}$. Assumimos que todas as raízes de $A(x)$ pertencem a uma extensão $\mathbb{F}_{q^s}$ de $\mathbb{F}_{q^m}$.

Seja $\beta \in \mathbb{F}_{q^s}$ uma raiz fixa de $A(x)$, ou seja, $A(\beta) = 0$, o que implica que $L(\beta) = \alpha$. Agora, seja $\gamma \in \mathbb{F}_{q^s}$ qualquer elemento. Temos que γ é também raiz de $A(x)$ se, e somente se, $L(\gamma) = \alpha$. Isso equivale a dizer que $L(\gamma) = L(\beta)$, ou seja, $L(\gamma - \beta) = 0$, pela linearidade $\mathbb{F}_q$-linear de $L(x)$.

Assim, o conjunto de raízes de $A(x)$ é precisamente o conjunto dos elementos da forma $\beta + u$, com $u \in \ker L$, ou seja:

$$\{\gamma \in \mathbb{F}_{q^s} : A(\gamma) = 0\} = \beta + \ker L.$$

O conjunto $\ker L$, sendo o núcleo de um q-polinômio (isto é, uma função $\mathbb{F}_q$-linear), é um subespaço vetorial de $\mathbb{F}_{q^s}$ sobre $\mathbb{F}_q$. Portanto, as raízes de $A(x)$ formam uma translação desse subespaço linear, isto é, um subespaço afim.

Quanto às multiplicidades, todas as raízes de $A(x)$ têm a mesma multiplicidade. Este resultado decorre de argumentos similares aos utilizados na prova do Teorema 3.4.2 e está relacionado à estrutura especial dos q-polinômios, cujas derivadas preservam propriedades de multiplicidade uniforme nas raízes. □

Capítulo 4

Conclusão

Esta dissertação dedicou-se ao estudo de aspectos fundamentais da teoria de corpos finitos e sua relação com polinômios sobre esses corpos. Fizemos uma breve introdução à teoria de corpos finitos, estudando as propriedades estruturais desses corpos, abordando desde resultados elementares até representações avançadas de seus elementos, incluindo as representações polinomiais, ciclotômicas e matriciais.

No que diz respeito aos polinômios sobre corpos finitos, investigamos suas propriedades algébricas, com destaque para três classes particulares: os polinômios de ordem definida, cujo estudo está profundamente ligado à estrutura dos grupos multiplicativos em extensões de corpos finitos; os polinômios primitivos, que desempenham papel crucial na construção de geradores pseudoaleatórios e códigos corretores de erros devido à sua conexão com elementos primitivos; e os polinômios irredutíveis, essenciais tanto para a fatoração de polinômios quanto para a construção explícita de extensões de corpos. Além disso, examinamos os q-polinômios, que generalizam estruturas polinomiais tradicionais.

Os resultados aqui apresentados não apenas consolidam conhecimentos clássicos da teoria de corpos finitos e dos polinômios a eles associados, mas também sugerem caminhos para investigações futuras. Em particular, seria interessante explorar generalizações desses conceitos para corpos de funções e curvas algébricas, ampliando assim as conexões entre teoria dos números, geometria algébrica e teoria de códigos.

Referências Bibliográficas

[1] Á. del Río , J. J. Simón e A. del Valle, *Álgebra básica*. DM, Murcia, 2006.

[2] É. Rousseau, *Efficient Arithmetic of Finite Field Extensions*. Dissertação de doutorado, Institut Polytechnique de Paris, 2021. https://theses.hal.science/tel-03299466

[3] G. Bard, *Algebraic Cryptanalysis*, Springer, 2009. https://doi.org/10.1007/978-0-387-88757-9

[4] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, 6ª ed., Oxford University Press (Clarendon Press), Oxford, 2008. https://doi.org/10.1093/oso/9780199219858.001.0001

[5] H. W. Lenstra Jr. e R. J. Schoof, *Primitive normal bases for finite fields*, Mathematics of Computation, **48** (1987), 217–231. https://doi.org/10.2307/2007886

[6] I. Stewart, *Galois Theory*, 5ª ed., Chapman and Hall/CRC, 2022. https://doi.org/10.1201/9781003213949

[7] J. Asensio Mayor, J. R. Caruncho Castro e J. Martínez Hernández, *Ecuaciones algebraicas*, Serie Texto-Guía, DM, Murcia, 2002.

[8] J. von zur Gathen e J. Gerhard, *Modern Computer Algebra*, 3rd ed., Cambridge University Press, Cambridge, 2013. https://doi.org/10.1017/CBO9781139856065

[9] L. Gómez Saura, *Introducción a la teoría de cuerpos finitos*, Trabalho de Conclusão de Curso (TCC), Universidade de Múrcia, 2015. https://www.um.es/web/matematicas/tfg-cuerpos-finitos-gomez-saura-2015

[10] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, 1ª ed., Springer (Kluwer Academic Publishers), Boston, 1987. https://doi.org/10.1007/978-1-4613-1983-2

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

[12] S. Lang, *Álgebra para graduação*, Ed. Ciência Moderna, Rio de Janeiro, 2008.

[13] Z. X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, Singapore; River Edge, NJ, 2003. https://doi.org/10.1142/5350