CYNTHIA MARTINS DIÓRIO

CARACTERIZAÇÃO DOS POLINÔMIOS DE PERMUTAÇÃO

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

Orientador: Bhavinkumar Kishor Sinh Moriya

VIÇOSA - MINAS GERAIS
2019

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T
D593c
2019

Diório, Cynthia Martins, 1989-
Caracterização dos polinômios de permutação / Cynthia Martins Diório. – Viçosa, MG, 2019.
60 f. : il. ; 29 cm.

Orientador: Bhavinkumar Kishor Sinh Moriya.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 59-60.

1. Grupos finitos. 2. Polinômios. 3. Grupos de permutação. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 512.21

CYNTHIA MARTINS DIÓRIO

CARACTERIZAÇÃO DOS POLINÔMIOS DE PERMUTAÇÃO

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

APROVADA: 27 de agosto de 2019.

Assentimento:

Cynthia Martins Diório
Autora

Bhavnikumar Kishor Sinh Moriya
Orientador

Dedico este trabalho aos meus pais Margarida e Aureliano, com amor e carinho

"Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível"

Charles Chaplin

Agradecimentos

Primeiramente, agradeço a Deus, pois sem sua graça não conseguiria as vitórias que me foram concedidas. Por seu amor infinito e suas bênçãos diárias, que me deram força para vencer cada passo dessa caminhada.

A minha mãe Margarida pelo amor e apoio em todos os obstáculos. Meu pai Aureliano, que mesmo não estando mais entre nós sempre se fez luz na minha memória e sempre teve a certeza que eu chegaria aonde eu quisesse, bastando apenas determinação e foco. Ao Pedro, meu melhor amigo e meu amor, por ter me dado forças no final dessa jornada me fazendo confiar que eu era capaz e que iria vencer mais esse sonho.

Agradeço, em especial, ao meu orientador Bhavinkumar, por acreditar na minha capacidade, pela paciência em todos os momentos, por ser minha inspiração e por me proporcionar tantos ensinamentos. Ao DMA-UFV, professores e funcionários que colaboraram de forma significativa para a minha formação.

Por fim, aos meus amigos e amigas de Viçosa que se fizeram minha família, meu porto seguro, me trazendo tantas risadas, tanta felicidade e paz, que tornaram essa caminhada mais feliz e possível.

Resumo

DIÓRIO, Cynthia Martins., M.Sc., Universidade Federal de Viçosa, agosto de 2019. **Caracterização dos Polinômios de Permutação**. Orientador: Bhavinkumar Kishor Sinh Moriya.

Neste trabalho o principal conceito usado é Polinômio de Permutação. Estes polinômios surgiram primeiro no trabalho de Betti [4], Mathieu [9] e Hermite [6] como forma de representar permutações. Uma teoria geral foi desenvolvida por Hermite [6] e Dickson [5], com muitos desenvolvimentos subsequentes. Produzir polinômios de permutação é um problema díficil. Recentemente, Akbary, Wang e Wang [1, 3] estudaram binômios da forma $x^u + x^r$ sobre $\mathbb{F}_q$ no caso $d = mdc(q-1, u-r)$ satisfazendo $(q-1)/d \in \{3, 5, 7\}$. Seus resultados forneceram critérios necessários e suficientes para que tais binômios permutem $\mathbb{F}_q$, em termos do período de uma generalização da sequência de Lucas em $\mathbb{F}_q$. Porém as provas encontradas para tais critérios eram bastante complicadas, além de possuir uma demonstração para cada caso $(q-1)/d \in \{3, 5, 7\}$. Naturalmente, se pergunta se pode haver uma abordagem uniforme que funcione para qualquer d arbitrário, e produza assim, os outros resultados ditos acima como casos especiais. Dessa forma, o artigo de Michael Zieve [11] apresenta métodos com uma abordagem mais curta e simples que se aplica à classe mais geral de polinômios sem utilizar dos métodos usados por Akbary, Wang e Wang. Diante do exposto, o objetivo neste trabalho será estudar tais demonstrações se preocupando com a classe de polinômios da forma $f(x) = x^r h_k(x^v)^t$ onde $h_k(x) = x^{k-1} + x^{k-2} + ... + x + 1$ com r, v, k, t inteiros positivos.

Palavras-chave: Corpos Finitos. Polinômios. Polinômios de Permutação.

Abstract

DIÓRIO, Cynthia Martins., M.Sc., Universidade Federal de Viçosa, August, 2019. **Characterization the Permutation Polynomials**. Adviser: Bhavinkumar Kishor Sinh Moriya.

In this work the main concept used is Permutation Polynomial. These polynomials first appeared in the work of Betti [4], Mathieu [9] and Hermite [6] as a way of representing permutations. A general theory was developed by Hermite [6] and Dickson [5], with many subsequent developments. Producing permutation polynomials is a difficult problem. Recently, Akbary, Wang and Wang [1, 3] studied binomials of the form $x^u + x^r$ over $\mathbb{F}_q$ in the case $d = mdc(q-1, u-r)$ satisfying $(q-1)/d \in \{3, 5, 7\}$. Their results provided necessary and sufficient criteria for such binomials to exchange $\mathbb{F}_q$, in terms of the period of a generalization of the Lucas sequence in $\mathbb{F}_q$. However, the evidence found for such criteria was quite complicated, besides having a demonstration for each case $(q-1)/d \in \{3, 5, 7\}$. Naturally, one wonders if there can be a uniform approach that works for any arbitrary d, and thus produces the other results said above as special cases. Thus, Michael Zieve's paper [11] presents methods with a shorter and simpler approach that applies to the more general class of polynomials without using the methods used by Akbary, Wang and Wang. Given the above, the aim of this paper will be to study such demonstrations worrying about the class of polynomials of the form $f(x) = x^r h_k(x^v)^t$ where $h_k(x) = x^{k-1} + x^{k-2} + ... + x + 1$ with r, v, k, t positive integers.

Keywords: Finite Fields. Polynomials. Permutation Polynomials.

Sumário

Introdução

O estudo de corpos finitos teve seu início no século 19 com os trabalhos de Gauss e Hermite, e o interesse era essencialmente teórico. Um corpo é uma estrutura algébrica no qual as operações de soma, subtração, multiplicação e divisão estão bem definidas e satisfazem certas propriedades. Os números reais são provavelmente o exemplo mais conhecido, juntamente com o corpo dos racionais e números complexos, todos exemplos de corpos infinitos, uma vez que possuem uma quantidade infinita de elementos. Certos conjuntos finitos também satisfazem as propriedades do corpo quando são atribuídas operações apropriadas. Esses conjuntos são chamados corpos finitos, e os corpos finitos serão o ingrediente mais importante para o principal tópico de estudo deste trabalho: Polinômios de Permutação.

O conceito de permutação expressa a ideia de que vários objetos possam ser arranjados de inúmeras formas distintas. Em álgebra e combinatória, esse conceito é bastante estudado. Neste texto, nosso objetivo é estudar os aspectos e as propriedades de polinômios de permutação sobre corpos finitos. Para entendermos melhor esse conceito, segue a definição de polinômio de permutação: Seja q uma potência de um primo p e $\mathbb{F}_q$ um corpo com q elementos. Um polinômio $f(x) \in \mathbb{F}_q[x]$ é chamado de polinômio de permutação de $\mathbb{F}_q$ se a aplicação $a \mapsto f(a)$ permuta os elementos de $\mathbb{F}_q$.

A propriedade de permutação em corpos finitos é um fato que atrai muita atenção, principalmente com o avanço da era digital. Seu estudo teve aplicações práticas em criptografia, desenhos combinatórios, códigos corretores de erros etc, além de interesses puramente teóricos. A nossa motivação em estudar polinômios de permutações sobre corpos finitos se deve, principalmente, ao fato de existirem muitos problemas interessantes, tanto teóricos como aplicações práticas, e que foram pouco explorados na área.

Historicamente, o início do estudo de polinômios de permutação se deu com Hermite [6], que investigou permutações sobre corpos primos. Dickson [5] foi o primeiro a analisá-los sobre corpos finitos arbitrários. Atualmente, vários resultados envolvendo polinômios de permutação têm sido publicados, grande parte desses apresentando novas famílias de polinômios de permutação, bem como resultados envolvendo aspectos relacionados aos mesmos. No artigo *Permutation polynomials over finite fields: A survey of recent advances*[16], encontramos um levantamento dos avanços atuais nesta área, bem como as contribuições feitas nos últimos anos.

Em 1897, Dickson deu o que ele alegou ser uma lista completa de Polinômios de Permutação de grau, no máximo, 6. No entanto, há sugestões recentes de que essa classificação pode estar incompleta, Xiang Fan encontrou grau de no máximo

8. Infelizmente, a alegação de Dickson de uma caracterização completa não é facilmente verificada, visto que sua prova publicada é de difícil compreenção, devido principalmente à terminologia antiquada.

O primeiro capítulo deste trabalho consiste em uma introdução aos corpos finitos, onde são apresentados resultados importantes, que serão utilizados no decorrer do texto. No Capítulo 2, iremos estudar um pouco sobre polinômios irredutíveis sobre corpos finitos, definições e alguns resultados envolvendo ordem de um polinômio e polinômio primitivo. No Capítulo 3, apresentamos o conceito de polinômio de permutação e resultados que serão de suma importância para o nosso propósito neste trabalho: estudar resultados que nos ajudem a encontrar polinômios de permutação. O principal teorema deste capítulo é o *Hermite's Criterion*, que nos fornece duas condições para um polinômio sobre um corpo finito $\mathbb{F}_q$ ser polinômio de permutação sobre este corpo. Este Critério será fortemente usado também no Capítulo 4 na demostração de alguns resultados.

Por fim, no Capítulo 4, que é o foco deste trabalho, faremos um estudo do artigo de Michael Zieve intitulado *Some families of permutation polynomials over finite fields* [11], que irá trazer resultados importantes sobre Caracterização de Polinômios de Permutação. Encontrar polinômios de permutação com estruturas de fácil computabilidade é um problema importante na área de polinômios de permutação. Por esse motivo, este capítulo contém alguns resultados já conhecidos envolvendo polinômios de permutação, bem como teoremas que nos permitem encontrar famílias de polinômios de permutação. Uma das questões mais importantes no estudo de polinômios de permutação sobre corpos finitos é a contagem desses polinômios com determinada propriedade. Nos últimos resultados deste capítulo, Hermite [6] e Betti [4] fornecem técnicas para a contagem desses polinômios de permutação com certa característica.

Capítulo 1

Introdução a Corpos Finitos

De forma simples, podemos definir um corpo como um conjunto no qual podemos somar, subtrair, multiplicar e dividir por um número não nulo, no qual valem todas as propriedades usuais de tais operações, incluindo a comutatividade na adição e na multiplicação. Exemplos de corpos são os racionais $\mathbb{Q}$, os reais $\mathbb{R}$, os complexos $\mathbb{C}$ e para p primo, $\mathbb{Z}/p\mathbb{Z}$ (conjunto dos inteiros módulo p). Alguns exemplos de conjuntos que não são corpos são os inteiros $\mathbb{Z}$, os polinômios com coeficientes em $\mathbb{R}$ e as matrizes reais quadradas de ordem $n \geq 2$. Corpos finitos nada mais são, que corpos que possuem uma quantidade finita de elementos.

Este capítulo é de importância central, pois contém vários resultados fundamentais e propriedades de corpos finitos. O corpo dos inteiros é o exemplo mais familiar de corpo finito, mas muitas propriedades se estendem para corpos finitos arbitrários. A caracterização de corpos finitos que será vista na Seção 1.1 mostra que todo corpo finito tem como ordem a potência de um número primo. De modo inverso, para toda potência de um primo, existe um corpo finito cujo número de elementos é exatamente um número primo elevado a essa potência. Além disso, corpos finitos com o mesmo número de elementos são isomorfos, de forma que podem ser identificados por corpos particulares, denominados corpos de Galois de ordem p^n.

As próximas duas seções fornecem informações sobre as raízes dos polinômios irredutíveis, levando a uma interpretação de olharmos corpos finitos como corpos de decomposição de polinômios irredutíveis. Iremos também definir a função Traço e Norma, bem como bases relativas para corpos de extensão.

Na Seção 1.4 iremos tratar as raízes da unidade do ponto de vista da teoria geral de corpo, enquanto na Seção 1.5 iremos apresentar diferentes maneiras de representar os elementos de um corpo finito.

Ao longo deste Capítulo usaremos as seguintes notações: p é número primo e $\mathbb{F}_q$ é um corpo finito com $q = p^n$ elementos, para $n \in \mathbb{N}$.

1.1 Caracterização de Corpos Finitos

Nesta seção vamos estudar alguns resultados e propriedades fundamentais dos corpos finitos, enquanto no Capítulo 3 iremos descrever uma das suas muitas aplicações: Os polinômios de permutação.

Lema 1.1. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então F tem q^m elementos, onde $m = [F : K]$ é o grau de F sobre K.*

Demonstração. Claramente F é um espaço vetorial sobre K, e sendo F finito, F é um espaço vetorial de dimensão finita sobre K. Se $m = [F : K]$, então F tem uma base sobre K consistindo de m elementos, a saber, $b_1, b_2, ..., b_m$. Assim, cada elemento de F pode ser representado de maneira única na forma $a_1b_1 + a_2b_2 + ... + a_mb_m$, onde cada $a_i \in K$, com $i \in \{1, 2, ..., m\}$. Como cada a_i pode ter q valores, F tem exatamente q^m elementos. □

Teorema 1.2. *Seja F um corpo finito. Então F tem p^n elementos, onde o primo p é a característica de F, e n é o grau de F sobre seu subcorpo primo.*

Demonstração. Sabemos que todo corpo finito tem característica prima. Logo, F tem característica prima p. Assim sendo, temos que o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ (vide Teorema 1.78 pag. 30 em [8]). Portanto, K contém p elementos. Pelo Lema 1.1, sendo $n = [F : K]$, segue que F contém p^n elementos. □

Teorema 1.3. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ de elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Considere o grupo $\mathbb{F}_q^*$. Se $q = 2$, temos que $|\mathbb{F}_q^*| = 1$, logo cíclico. Suponha então $q \geq 3$, $q = p^n$ com p primo, e considere $h = q-1 = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}$, onde $p_1, p_2, ..., p_m$ são primos distintos. Para cada i, $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ possui no máximo h/p_i raízes em $\mathbb{F}_q^*$. Assim, como $h/p_i < h$, segue que existem elementos em $\mathbb{F}_q^*$ que não são raízes do polinômio $x^{h/p_i} - 1 (*)$. Seja a_i um elemento de $\mathbb{F}_q^*$ que não seja raiz do polinômio $(*)$ e considere $b_i = {a_i}^{h/{p_i}^{r_i}}$. Temos que ${b_i}^{{p_i}^{r_i}} = {a_i}^h = 1$. Disso, a ordem de b_i(suponha ser ${p_i}^{s_i}$ com $0 \leq s_i \leq r_i$), é um divisor de ${p_i}^{r_i}$. Por outro lado, por $(*)$ temos:

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

e dessa forma, segue que a ordem de b_i é ${p_i}^{r_i}$. Seja $b = b_1 \cdot b_2 \cdot ... \cdot b_m \in \mathbb{F}_p^*$ e s a ordem de b. Temos que $s|h$, onde h é a ordem de $|\mathbb{F}_p^*|$. Suponha que $s < h$. Como $h = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}$ e $s|h$, temos que $p_j \mid \frac{h}{s}$, para algum $j \in \{1, 2, ..., m\}$. Logo, $\frac{h}{p_j} = s \cdot k$ com $k \in N$. Daí, $b^{\frac{h}{p_j}} = (b^s)^k = 1$. Suponha, sem perda de generalizada que $j = 1$. Assim,

$$ 1 = b^{\frac{h}{p_1}} = {b_1}^{\frac{h}{p_1}} \cdot {b_2}^{\frac{h}{p_1}} \cdot ... \cdot {b_m}^{\frac{h}{p_1}} $$

Disso, segue ${b_1}^{\frac{h}{p_1}} = 1$. Logo, a ordem de b_1 divide h/p_1. Porém, ${p_1}^{r_1}$ não divide h/p_1, pois $\frac{h}{p_1} = p_1^{r_1-1} \cdot p_2^{r_2} \cdot ... \cdot p_m^{r_m}$. Sendo assim, segue que $s = h$. Portanto, $\mathbb{F}_p^*$ é cíclico, com $\mathbb{F}_q^* = \langle b \rangle$. □

Lema 1.4. *Se F é um corpo finito com q elementos, então para todo $a \in F$, temos $a^q = a$.*

Demonstração. Se $a = 0$, segue que $a^q = a$. Por outro lado, os elementos não-nulos de F formam um grupo de ordem $q - 1$ com a multiplicação. Assim, $a^{q-1} = 1$, para todo $a \in F$ com $a \neq 0$. Então, $a \cdot a^{q-1} = a \cdot 1$ implica em $a^q = a$, para todo $a \in F$, donde segue o queríamos demonstrar. □

Definição 1.5. *Dado $f(x) \in F[x]$, uma extensão finita E de F é chamada corpo de decomposição sobre F para $f(x)$ se f pode ser fatorado como um produto de fatores lineares sobre $E[x]$ e f não se fatora em nenhum outro subcorpo próprio de E.*

Lema 1.6. *Se F é um corpo finito com q elementos e K um subcorpo de F, então o polinômio $x^q - x \in K[x]$ fatora em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a) \tag{1.1}$$

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

Demonstração. O polinômio $x^q - x$ tem no máximo q raízes em F. Pelo Lema 1.4, $x^q = x$ para todo $x \in F$. Assim, todo elemento de F é uma raiz do polinômio $x^q = x$. Logo, o polinômio dado fatora em F da maneira descrita em (1.1), e não fatora em nenhum outro corpo menor. □

Observando o lema acima, temos que (1.1) nos dá precisamente todas as raízes do polinômio $x^q - x$. Agora, usando como idéia principal o Lema 1.6, iremos provar o principal teorema de caracterização dos corpos finitos.

Teorema 1.7. ***Existência e Unicidade de Corpos Finitos:*** *Para todo primo p e todo inteiro n, existem corpos finitos com p^n elementos. Além disso, qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. **Existência**: Para $q = p^n$ considere $x^q - x \in \mathbb{F}_p[x]$ e seja F o corpo de decomposição de f. Este polinômio têm q raízes distintas em F, pois seu polinômio derivada $qx^{q-1} - 1 = -1$ em $\mathbb{F}_p[x]$ não tem raízes em comum com $x^q - x$. Disso, segue que $x^q - x$ possui q raízes distintas. Considere agora o conjunto $S = \{a \in F; a^q - a = 0\}$. Temos que S é subcorpo de F. De fato: (i) $0 \in S$ e $1 \in S$, pois $0^q = 0$ e $1^q = 1$. (ii) Dados $a, b \in S$, e sendo F corpo de característica prima p, têm-se $(a - b)^q = a^q - b^q$. Disso, e por $a, b \in F$, segue $(a-b)^q = a^q - b^q = a - b$. Logo, $a - b \in S$. (iii) Por fim, dados $a, b \in S$ com $b \neq 0$ têm-se $(a \cdot b^{-1})^q = a^q \cdot b^{-q}$. Assim, por $a, b \in F$, temos $(a \cdot b^{-1})^q = a^q \cdot b^{-q} = a \cdot b^{-1}$. Logo, $a \cdot b^{-1} \in S$. Logo, S é um subcorpo de F. Por outro lado, $x^q - x$ fatora em

S, e este é o menor corpo tal que isso ocorre. Portanto, $F = S$, uma vez que o corpo de decomposição de um polinômio é único. Assim, segue que F é um corpo finito com q elementos, onde $q = p^n$.
Unicidade: Seja F um corpo finito com $q = p^n$ elementos. Então, F tem característica prima pelo Teorema 2.2 em [8] e contém o subcorpo $\mathbb{F}_p$. Segue pelo Lema 1.6 que F é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Pela existência e unicidade do corpo de decomposição, segue que F é único e qualquer outro corpo finito com $q = p^n$ elementos que fatore $x^q - x$ é isomorfo a F. □

A unicidade do Teorema 1.7 justifica o fato de podermos falar de corpo finito(ou corpo de Galois) com q elementos, ou de ordem q. Iremos denotar este corpo por $\mathbb{F}_q$, onde q é uma potência de p, sendo este a característica prima do corpo $\mathbb{F}_q$.

Teorema 1.8. ***(Critério de Subcorpo)*** *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, todo subcorpo de $\mathbb{F}_q$ têm ordem p^m, onde m é um divisor positivo de n. Por outro lado, se m é um divisor de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. É claro que um subcorpo K de $\mathbb{F}_q$ tem ordem p^m, para algum inteiro $m \leq n$. Pelo Lema 1.1, sendo a ordem de K(subcorpo de $\mathbb{F}_q$) igual a p^m segue que m será um divisor de n. Por outro lado, se m é um divisor de n, então $p^m - 1$ divide $p^n - 1$ e então $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$ em $\mathbb{F}_p[x]$. Consequentemente, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ em $\mathbb{F}_p[x]$. Portanto, toda raiz de $x^{p^m} - x$ é uma raiz de $x^q - x$, e assim pertence a $\mathbb{F}_q$. Segue assim que $\mathbb{F}_q$ contém um subcorpo que é o corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_q$, e como vimos na prova do Teorema 1.7, tal corpo tem ordem p^m. Agora, suponha que exista outro subcorpo de $\mathbb{F}_q$ com ordem p^m. Dessa forma, os dois subcorpos teriam em conjunto mais de p^m raízes distintas de $x^{p^m} - x$, o que é uma contradição. Logo, o subcorpo de $\mathbb{F}_q$ de ordem p^m é único. □

A prova do Teorema 1.8 mostra a unicidade do subcorpo de $\mathbb{F}_{p^n}$ de ordem p^m, onde m é um divisor positivo de n. Além disso, observemos que os elementos do subcorpo $\mathbb{F}_{p^m}$ são precisamente as raízes do polinômio $x^{p^m} - x$ em $\mathbb{F}_{p^n}$.

Para o corpo finito $\mathbb{F}_q$, denotaremos por $\mathbb{F}_q^*$ o grupo multiplicativo de elementos não nulos de $\mathbb{F}_q$.

Definição 1.9. *Um gerador de um grupo $\mathbb{F}_q^*$ é chamado elemento primitivo de $\mathbb{F}_q$*

O corpo finito $\mathbb{F}_q$ contêm $\phi(q-1)$ elementos primitivos, onde ϕ é a função de Euler (vide Teorema 1.15(v) [8]). A existência de elementos primitivos pode ser usada para mostrar um resultado que implica em particular no fato que todo corpo finito pode ser pensado como uma extensão algébrica simples do seu subcorpo primo.

Teorema 1.10. *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ uma extensão 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 ser usado como um elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja ζ um elemento primitivo de $\mathbb{F}_r$. Temos claramente que $\mathbb{F}_q(\zeta) \subseteq \mathbb{F}_r$. Por outro lado, $\mathbb{F}_q(\zeta)$ contém o elemento 0, todas as potências de ζ e então todos os elementos de $\mathbb{F}_r$. Disso, segue que $\mathbb{F}_r \subseteq \mathbb{F}_q(\zeta)$. Portanto, concluímos que $\mathbb{F}_r = \mathbb{F}_q(\zeta)$. □

Corolário 1.11. *Para todo corpo finito $\mathbb{F}_q$ e todo número inteiro n, existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Demonstração. Seja $\mathbb{F}_r$ uma extensão de corpos de $\mathbb{F}_q$ de ordem q^n de modo que $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 1.10, temos $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ para algum $\zeta \in \mathbb{F}_r$. Então o polinômio mínimal de ζ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n(vide Teorema 1.82(i) e Teorema 1.86(ii) em [8]). □

1.2 Raízes e Polinômios Irredutíveis

Nesta seção apresentaremos alguns resultados que envolvem o conjunto de raízes de um polinômio irredutível sobre um corpo finito.

Lema 1.12. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre o corpo finito $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão de corpo $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$ tem-se $h(\alpha) = 0$ se, e somente se, f divide h.*

Demonstração. Seja a o coeficiente do termo de maior grau de f e considere $g(x) = a^{-1}f(x)$. Temos que g é um polinômio mônico irredutível em $\mathbb{F}_q$ com $g(\alpha) = 0$. Pela definição de polinômio minimal, seque que g é o polinômio minimal de α sobre $\mathbb{F}_q$. Então, concluímos que para $h \in \mathbb{F}_q[x]$ têm-se $h(\alpha) = 0$ se, e somente se, f divide h(vide Teorema 1.82(ii) em [8]). □

Lema 1.13. *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. ($\Rightarrow$) Suponha que $f(x)$ divida $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Como $f(\alpha) = 0$ e f divide $x^{q^n} - x$, temos que $\alpha^{q^n} - \alpha = 0$. Disso, temos $\alpha^{q^n} = \alpha$, donde segue que $\alpha \in \mathbb{F}_{q^n}$. Então, $\mathbb{F}_q(\alpha)$ é um subcorpo de F_{q^n}. Porém, como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, segue que m divide n.
($\Leftarrow$) Agora, suponha que m divida n. Pelo Teorema 1.8, temos que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como subcorpo. Se α é uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Disso, segue que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Consequentemente, $\alpha \in \mathbb{F}_{q^n}$ e disso que $\alpha^{q^n} = \alpha$. Portanto, α é uma raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Pelo Teorema 1.12 concluímos que $f(x)$ divide $x^{q^n} - x$. □

Teorema 1.14. *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m, então f tem uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e dadas pelos m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[F_q(\alpha) : \mathbb{F}_q] = m$ e consequentemente $F_q(\alpha) = \mathbb{F}_{q^m}$ e daí $\alpha \in \mathbb{F}_{q^m}$. Agora, mostremos que, se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f, então β^q é também uma raiz de f. Escreva $f(x) = a_m x^m + ... + a_1 x + a_0$ com $a_i \in \mathbb{F}_q$ para $0 \leq i \leq m$. Pelo Lema 1.4, temos:

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

Logo, os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são raízes de f. Basta mostrar agora que essas raízes são distintas. Suponha então que para algum inteiro j e k, com $0 \leq j < k \leq m-1$ temos $\alpha^{q^j} = \alpha^{q^k}$. Então:

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

Logo, pelo Lema 1.12, $f(x)$ divide $x^{q^{j+m-k}} - x$. Pelo Lema 1.13 isso so é possível se m divide $j + m - k$. Porém $0 < m - k + j < m$ donde segue que m não divide $j + m - k$. Logo, $\alpha^{q^j} \neq \alpha^{q^k}$ para todo $1 \leq i, j \leq m-1$, e assim as raízes $\alpha, \alpha^q, \alpha^{a^2}, ..., \alpha^{q^{m-1}}$ de F_{q^m} são distintas como queríamos demonstrar. □

Corolário 1.15. *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 $\mathbb{F}_{q^m}$.*

Demonstração. Pelo Teorema 1.14, temos que f fatora em $\mathbb{F}_{q^m}$. Além disso, $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, para alguma raiz α de f. Logo $\mathbb{F}_{q^m}$ é o corpo de decomposição de f. □

Corolário 1.16. *Dois quaisquer polinômios irredutíveis em $\mathbb{F}_q[x]$ de mesmo grau tem corpos de decomposição isomorfos.*

Definição 1.17. *Seja F_{q^m} uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são chamados conjugados de f em relação a $\mathbb{F}_q$.*

Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com relação a $\mathbb{F}_q$ são distintos se, e somente se, o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau m. Caso contrário, se o grau do polinômio minimal é d, um divisor próprio de m, os conjugados de α em relação a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$ onde cada elemento se repete m/d vezes.

Teorema 1.18. *Os conjugados de $\alpha \in \mathbb{F}_q^*$ com relação a algum subcorpo de $\mathbb{F}_q$ tem a mesma ordem do grupo $\mathbb{F}_q^*$.*

Demonstração. Pelo Teorema 1.3, temos $\mathbb{F}_q^*$ grupo cíclico de ordem $q-1$. Em um grupo ciclico finito $\langle a \rangle$ de ordem m, o elemento a^k gera um subgrupo de ordem $m/mdc(k, m)$ (vide Teorema 1.15 (ii) em [8]. Usando isto, e o fato de que toda potência da caracteristica de $\mathbb{F}_q$ é relativamente prima a ordem do grupo $\mathbb{F}_q^*$, segue o resultado. □

Exemplo 1.19. *Seja $\alpha \in \mathbb{F}_{16}$ uma raiz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Então, como $\mathbb{F}_{16} = \mathbb{F}_{2^4}$, os conjugados de α em relação a $\mathbb{F}_2$ são $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ e $\alpha^8 = \alpha^2 + 1$, onde cada um é um elemento primitivo de $\mathbb{F}_{16}$. De fato, temos que, $0 = f(\alpha) = \alpha^4 + \alpha + 1$. Assim, $\alpha^8 = (\alpha^4)^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1$. Em relação a $\mathbb{F}_4$ os conjugados de α são α e α^4.*

Teorema 1.20. *Os distintos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente $\sigma_0, \sigma_1, \sigma_2, ..., \sigma_{m-1}$ definidos por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leq j \leq m - 1$.*

Demonstração. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$. Por automorfismo σ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, queremos dizer um automorfismo de $\mathbb{F}_{q^m}$ que fixa os elementos de $\mathbb{F}_q$, é injetivo, e para todo α e $\beta \in \mathbb{F}_{q^m}$ temos $\sigma(a+b) = \sigma(\alpha) + \sigma(b)$ e $\sigma(a.b) = \sigma(a).\sigma(b)$. Seja σ_j um automofismo de $\mathbb{F}_{q^m}$ e α, $\beta \in \mathbb{F}_{q^m}$. Segue:

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

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

Além disso, $\sigma_j(\alpha) = 0$ se, e somente se, $\alpha = 0$. Logo, σ_j é injetiva, e assim tem-se σ_j um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Temos que $\sigma_1, \sigma_2, ..., \sigma_{m-1}$ são distintos, uma vez que assumem valores distintos para um elemento primitivo de $\mathbb{F}_{q^m}$. Agora, por outro lado, mostremos que, se σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, então $\sigma_j(\alpha) = \alpha^{q^j}$, com $\alpha \in \mathbb{F}_{q^m}$. De fato, seja σ um automorfismo qualquer de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, β um elemento primitivo de $\mathbb{F}_{q^m}$ e $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \in \mathbb{F}_q[x]$ um polinômio minimal de β. Então,

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + ... + a_0) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + ... + a_0$$

donde segue que $\sigma(\beta)$ é uma raiz de f. Pelo Teorema 1.14, temos $\sigma(\beta) = \beta^{q^j}$ para algum j, $0 \leq j \leq m - 1$. Logo, para todo $\alpha \in \mathbb{F}_{q^m}$, $\sigma(\alpha) = \alpha^{q^j}$. □

Com base no Teorema 1.20, notamos que os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com relação a $\mathbb{F}_q$ são obtidos aplicando todos os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ ao elemento α. Esses automorfismos formam um grupo cuja operação é a composição. Além disso este grupo de automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é um grupo cíclico de ordem m gerado por σ_1.

1.3 Traços, normas e bases

Seja $F = \mathbb{F}_{q^m}$ uma extensão finita do corpo finito $K = \mathbb{F}_q$. Note que F é espaço vetorial sobre K e assim tem dimensão m sobre K, e se $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ é uma base de F sobre K, cada elemento $\alpha \in F$ pode ser escrito de maneira única da seguinte forma:

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + ... + c_m\alpha_m$$

com $c_j \in K$ e $1 \leq j \leq m$.

Definição 1.21. *Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o traço $Tr_{F/K}(\alpha)$ de α sobre K é definido por:*

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

Se K é um subcorpo primo de F, então $Tr_{F/K}(\alpha)$ é chamado traço absoluto de α e denotado por $Tr_F(\alpha)$.

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

Exemplo 1.22. *Seja $f \in K[x]$ polinômio irredutível, $f(x) = (x-a)(x-a^2) = x^2 - (a+a^2)x + a^3$, onde a e a^2 são as raízes de f. Segue assim:*

$$Tr_{F/K}(a) = (a + a^2)$$

Assim, seja $g \in K[x]$ com $g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$, e $\alpha \in F$ uma raiz de g. Assim, temos:

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2}) \cdot ... \cdot (x-\alpha^{q^{m-1}})$$

Disso, e usando o exemplo anterior, vemos que:

$$Tr_{F/K}(\alpha) = -a_{m-1}$$

Sendo assim, concluímos que $Tr_{F/K}(\alpha)$ é sempre um elemento de K.

Teorema 1.23. *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então o $Tr_{F/K}(\alpha)$ satisfaz as seguintes propriedades:*

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

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

(ii) $Tr_{F/K}(\alpha)$ *é uma transformação sobrejetiva de F em K, onde F e K são espaços vetoriais sobre K;*

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

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

Demonstração.

(i) Dados α e $\beta \in F$ segue:

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

(ii) Dado $c \in K$, temos $c^{q^j} = c$, para todo $j \geq 0$. Logo, segue:

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

(iii) As propriedades (i) e (ii) e o fato de que $Tr_{F/K}(\alpha) \in K$ para todo $\alpha \in F$, garantem que $Tr_{F/K}$ é uma transformação linear de F em K. Para mostrar que $Tr_{F/K}$ é sobrejetiva, basta provar que existe $\alpha \in F$ tal que $Tr_{F/K}(\alpha) \neq 0$, uma vez que K tem dimensão 1. Agora, o fato de $Tr_{F/K}(\alpha) = 0$ segue que α é uma raiz do polinômio $x^{q^{m-1}} + ... + x^q + x \in K[x]$ em F. Como o polinômio tem no máximo q^{m-1} raízes em F e F tem q^m elementos, existe $\alpha \in F$ tal que $Tr_{F/K}(\alpha) \neq 0$. Portanto, $Tr_{F/K}$ é sobrejetiva e assim segue que $Tr_{F/K}(\alpha)$ é uma transformação linear sobrejetiva de F em K, onde F e K são espaços vetoriais sobre K.

(iv) Dado $a \in K$, temos $a^{q^i} = a$ para todo $i \geq 1$. Então,

$$Tr_{F/K}(a) = a + a^q + a^{q^2} + ... + a^{q^{m-1}} = a + a + ... + a = ma$$

(v) Para todo $\alpha \in F$, temos que $\alpha^{q^m} = \alpha$. Assim,

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

□

A função Traço não é somente uma transformação linear de F em K. Na verdade descreve todas as transformações lineares de F em K independente da base escolhida, que será provado, no seguinte teorema.

Teorema 1.24. *Seja F uma extensão finita de um corpo finito K. Então, a transformação linear de F sobre K é exatamente L_β, $\beta \in F$, onde $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ para todo $\alpha \in F$. Além disso, $L_\beta \neq L_\gamma$ com γ e β elementos distintos de F.*

Demonstração. Pelo Teorema 1.23, segue que $L_\beta = Tr_{F/K}(\beta\alpha)$ é uma transformação linear de F sobre K. Para $\beta, \gamma \in F$ com $\beta \neq \gamma$, temos:

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

para algum α adequado. Segue assim que $L_\beta \neq L_\alpha$. Se $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$, então L_β produz q^m transformações lineares distintas de F em K. □

Teorema 1.25. *Seja F uma extensão de $K = \mathbb{F}_q$. Então para $\alpha \in F$ temos $T_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q - \beta$ para algum $\beta \in F$.*

Demonstração. Suponha $\alpha = \beta^q - \beta$, para algum $\beta \in F$. Pelo Teorema 1.23, temos que $T_{F/K}(\beta^q) = T_{F/K}(\beta)$ e assim segue $T_{F/K}(\alpha) = T_{F/K}(\beta^q) - T_{F/k}(\beta) = 0$

e portanto $T_{F/K}(\alpha) = 0$. Por outro lado, suponha agora $T_{F/K}(\alpha) = 0$, com $\alpha \in F = \mathbb{F}_{q^m}$ e β uma raiz de $x^q - x - \alpha$ em alguma extensão de corpos de F. Disso, temos $\beta^q - \beta = \alpha$ e

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

Logo, temos $\beta^{q^m} = \beta$ e portanto $\beta \in F$. □

No caso de uma cadeia de corpos de extensão, a composição da função traço procede de acordo com o teorema que segue.

Teorema 1.26. ***(Transitividade do Traço)*** *Seja K um corpo finito, e seja F uma extensão finita de K e E uma extensão finita de F. Então, $T_{E/K}(\alpha) = T_{F/K}(T_{E/F}(\alpha))$ para todo $\alpha \in F$*

Demonstração. Seja $K = \mathbb{F}_q$, e seja $[F : K] = m$ e $[E : F] = n$. Temos $[E : K] = mn$. Assim, para $\alpha \in E$, tem-se:

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

□

Outra função interessante de um corpo finito para um subcorpo é obtida pelo produto dos conjugados de um elemento do corpo em relação ao seu subcorpo. Essa função será chamada Norma, e é definida como segue.

Definição 1.27. *Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, a norma $N_{F/K}(\alpha)$ de α sobre K é definida por:*

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot ... \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}$$

Se $g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ é o polinômio mínimo de α, temos que $N_{F/K}(\alpha) = (-1)^m \cdot a_0$

Exemplo 1.28. *Seja $g \in K[x]$ polinômio irredutível, $g(x) = (x-a)\cdot(x-b)\cdot(x-c)$ com a, b, c as raízes de g. Temos:*

$$\begin{aligned} g(x) &= (x-a)\cdot(x-b)\cdot(x-c) = (x^2 - (a+b)x + ab)\cdot(x-c) \\ &= x^3 - (a+b)x^2 + abx - cx^2 + (a+b)cx - abc \\ &= x^3 - (a+b+c)x^2 + (ab + (a+b)c)x - abc \end{aligned}$$

Donde vemos que $N_{F/K}(a) = (-1)^3 \cdot a_0$ onde, $a_0 = abc$, $b = a^k$, $c = a^l$ e $k, l \in \mathbb{Z}$

Teorema 1.29. *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função norma $N_{F/K}$ satisfaz:*

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

(ii) $N_{F/K}(F^*) = K^*$ *e* $N_{F/K}(F) = K$;

(iii) $N_{F/K}(a) = a^m$ *para todo* $a \in K$;

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

Demonstração.

(i) Este item é análogo ao demonstrado para a função Traço.

(ii) Note que $N_{F/K}(\alpha) = 0$ se, e somente se, $\alpha = 0$. Disso, e pelo item (i) segue $N_{F/K} : F^* \to K^*$ é um homomorfismo de grupos com a multiplicação. Temos que:

$$Ker(N_{F/K}) = \{\alpha \in F \mid N_{F/K}(\alpha) = 1\} = \{\alpha \in F \mid \alpha^{(q^m-1)/(q-1)} = 1\}$$

Logo, o núcleo de $N_{F/K}$ é exatamente o conjunto formado pelas raízes do polinômio $x^{(q^m-1)/(q-1)} - 1 \in K[x]$ em F. A ordem d do núcleo é tal que $d \leq (q^m - 1)/(q - 1)$. Assim, como $|F^*| = |Ker(N_{F/K})| \cdot |Im(N_{F/K})|$ onde $|F^*| = q^m - 1$ e $|Ker(N_{F/K})| = d$, segue $|Im(N_{F/K})| = (q^m - 1)/d$, a qual é maior ou igual a $q - 1$ Assim, segue o item (ii).

(iii) Se $a \in K = \mathbb{F}_q$, então $a^q = a$. Logo,

$$N_{F/K}(a) = a \cdot a^q \cdot ... \cdot a^{q^{m-1}} = a \cdot a \cdot a \cdot ... \cdot a = a^m$$

(iv) Se $\alpha \in F$, então $a^{q^m} = \alpha$. Assim:

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

□

Teorema 1.30. ***(Transitividade da Norma)*** *Seja K uma extensão de corpos finito e seja F uma extensão de K e E uma extensão de F. Então: $N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$ para todo $\alpha \in E$.*

Demonstração. Seja $[E : F] = n$ e $[F : K] = m$, com $K = \mathbb{F}_q$. Então,

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

□

Se $\{\alpha_1, ..., \alpha_m\}$ é uma base de um corpo finito F sobre o subcorpo K, assim:

$$\alpha = c_1(\alpha)\alpha_1 + c_2(\alpha)\alpha_2 + ... + c_m(\alpha)\alpha_m$$

para $c_j(\alpha) \in K$, $1 \leq j \leq m$ e $\alpha \in F$ qualquer. Note que $c_j : \alpha \to c_j(\alpha)$ é uma transformação linear de F para K, e portanto, de acordo com o Teorema 1.24, existe $\beta_j \in F$ tal que $c_j(\alpha) = T_{F/K}(\beta_j\alpha)$ para todo $\alpha \in F$. Fazendo $\alpha = \alpha_i$, $1 \leq i \leq m$ temos $\alpha_i = c_1(\alpha_i)\alpha_1 + c_2(\alpha_i)\alpha_2 + ... + c_m(\alpha_i)\alpha_m$. Como α_i se escreve de maneira única como combinação linear da base, segue que $c_j(\alpha_i) = 0$ se $i \neq j$ e $c_j(\alpha_i) = 1$ se $i = j$. Portanto, $T_{F/K}(\beta_i\alpha_j) = 0$ se $i \neq j$ e $T_{F/K}(\beta_i\alpha_j) = 1$ se $i = j$. Além disso, $\{\beta_1, \beta_2, ..., \beta_m\}$ é novamente uma base de F sobre K para o qual

$$d_1\beta_1 + ... + d_m\beta_m = 0$$

com $d_i \in K$ para $1 \leq i \leq m$, então multiplicando por um α_i e aplicando a função Traço $T_{F/K}$, mostramos que $d_i = 0$.

Definição 1.31. *Seja K um corpo finito e F uma extensão finita de K. Então dado as bases $\{\alpha_1, ..., \alpha_m\}$ e $\{\beta_1, ..., \beta_m\}$ de F sobre K, é dito base dual se para $1 \leq i, j \leq m$, temos:*

$$Tr_{F/K}(\alpha_i\beta_i) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

O número de bases distintas de F sobre K é bastante extenso, mas existem dois tipos especiais de bases de importância particular. O primeiro é a base polinomial $\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$. O elemento α é sempre considerado elemento primitivo de F. A outra base, chamada base normal é definida por um elemento adequado de F.

Definição 1.32. *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a base de F sobre K é da forma $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$, definida por um elemento adequado de F e seus conjugados com relação a K, é chamado uma base normal de F sobre K.*

Lema 1.33. ***(Artin Lemma)*** *Sejam $\Psi_i : G \to F^*$, $i \in \{1, 2, ..., m\}$ distintos homomorfismos, onde F é um corpo arbitrário, e sejam $a_i, ..., a_m$ elementos de F tal que existe i com $a_i \neq 0$. Então para algum $g \in G$, temos:*

$$a_1\Psi_1(g) + ... + a_m\Psi_m(g) \neq 0$$

Demonstração. Para demonstrar esse fato usemos indução sobre $m \in \mathbb{N}$. Se $m = 1$, o resultado é imediato. Assumindo $m > 1$, suponha válido a afirmação para $m-1$ homomorfimos distintos. Agora, tome $\Psi_1, ..., \Psi_m$ e $a_1, ..., a_m$. Se $a_1 = 0$ temos $a_1\Psi_1(g) = 0$ e $a_2\Psi_2(g) + ... + a_m\Psi_m(g) \neq 0$ e portanto, pela hipótese de indução, existe $g \in G$ tal que

$$a_1\Psi_1(g) + a_2\Psi_2(g) + ... + a_m\Psi_m(g) \neq 0$$

Suponha então, $a_1 \neq 0$ e

$$a_1\Psi_1(g) + a_2\Psi_2(g) + ... + a_m\Psi_m(g) = 0 \tag{1.2}$$

para todo $g \in G$. Se $\Psi_1 \neq \Psi_m$, então existe $h \in G$ com $\Psi_1(h) \neq \Psi_m(h)$. Assim, substituindo g por hg em (1.2), temos:

$$a_1\Psi_1(g)\Psi_1(h) + a_2\Psi_2(g)\Psi_2(h) + ... + a_m\Psi_m(g)\Psi_m(h) = 0$$

Multiplicando por $\Psi_m(h)^{-1}$, segue:

$$b_1\Psi_1(g) + ... + b_{m-1}\Psi_{m-1}(g) + a_m\Psi_m(g) = 0$$

onde $b_i = a_i\Psi_i(h)\Psi_m(h)^{-1}$ para $1 \leq i \leq m-1$. Subtraindo esta identidade de (1.2) temos:

$$c_1\Psi_1(g) + ... + c_{m-1}\Psi_{m-1}(g) = 0$$

$\forall g \in G$, onde $c_i = a_i - b_i$ e $1 \leq i \leq m-1$. Mas,

$$c_1 = a_1 - b_1 = a_1 - a_1\Psi_1(h)\Psi_m(h)^{-1} \neq 0$$

pois $a_1 \neq 0$. Pela hipótese de indução, temos o lema válido para $m-1$ homomorfismos distintos, o que torna (1.2) um absurdo, uma vez que $c_1 \neq 0$. Logo, segue o lema para todo $m \geq 1$. □

Teorema 1.34. ***(Teorema da Base Normal)*** *Para todo corpo finito K e toda extensão finita F de K, existe uma base normal de F sobre K.*

Demonstração. Vide Teorema 2.35 [8], pág. 60. □

Introduziremos a seguir uma expressão que nos permitirá decidir se determinado conjunto de elementos forma uma base para um corpo de extensão.

Definição 1.35. *Seja K um corpo finito e F uma extensão de K de grau m sobre K. Então o discriminante $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ de elementos $\alpha_1, ..., \alpha_m \in F$ é definido por um determinante de ordem m dado por:*

$$\Delta_{F/K}(\alpha_1, ..., \alpha_m) = \begin{vmatrix} Tr_{F/K}(\alpha_1\alpha_1) & Tr_{F/K}(\alpha_1\alpha_2) & \dots & Tr_{F/K}(\alpha_1\alpha_m) \\ Tr_{F/K}(\alpha_2\alpha_1) & Tr_{F/K}(\alpha_2\alpha_2) & \dots & Tr_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ Tr_{F/K}(\alpha_m\alpha_1) & Tr_{F/K}(\alpha_m\alpha_2) & \dots & Tr_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

Segue portanto pela definição acima que que $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ é sempre um elemento de K.

Teorema 1.36. *Seja K um corpo finito, F uma extensão finita de grau m sobre K e $\alpha_1, ..., \alpha_m \in F$. Então $\{\alpha_1, ..., \alpha_m\}$ é uma base de F sobre K se, e só se, $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$*

Demonstração. Seja $\alpha_1, ..., \alpha_m$ uma base de F sobre K. Para mostrarmos que $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$, basta provar que os vetores linha no determinante da

matriz dada são linearmente independentes. Para isso, suponha que:

$$c_1 Tr_{F/K}(\alpha_1\alpha_j) + ... + c_m Tr_{F/K}(\alpha_m\alpha_j) = 0$$

para $1 \leq j \leq m$ onde $c_1, ..., c_m \in K$. Então, dado $\beta = c_1\alpha_1 + ... + c_m\alpha_m$ segue $Tr_{F/K}(\beta\alpha_j) = 0$ para $1 \leq j \leq m$. Portanto, $Tr_{F/K}(\beta\alpha) = 0$, para todo $\alpha \in F$. Porém, isso só é possível se $\beta = 0$, e então $c_1\alpha_1 + ... + c_m\alpha_m = 0$ implica em $c_1 = ... = c_m = 0$. Disso, temos que os vetores linha no determinante $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ são linearmente independentes.

Por outro lado, suponha agora $\Delta_{F/K}(\alpha_1, ..., \alpha_m) \neq 0$ e $c_1\alpha_1 + ... + c_m\alpha_m = 0$ para $c_1, ..., c_m \in K$. Então

$$c_1\alpha_1\alpha_j + ... + c_m\alpha_m\alpha_j = 0$$

para $1 \leq j \leq m$, e aplicando a função traço, temos

$$c_1 Tr_{F/K}(\alpha_1\alpha_j) + ... + c_m Tr_{F/K}(\alpha_m\alpha_j) = 0$$

para $c_1, ..., c_m \in K$. Como os vetores linha do determinante $\Delta_{F/K}(\alpha_1, ..., \alpha_m)$ são linearmente independente, segue $c_1 = ... = c_m = 0$. Portanto, $\alpha_1, ..., \alpha_m$ são linearmente independentes sobre K. □

Para $\alpha_1, \alpha_2, ..., \alpha_m \in F$, seja A uma matriz $m \times m$ cujas linhas e colunas são da forma ${\alpha_j}^{q^{i-1}}$, onde q é o número de elementos de K. Se A^t denota a matriz transposta de A, então com cálculos simples mostramos que $A^t \cdot A = B$, onde B é a matriz $m \times m$ cujas entradas são da forma $Tr_{F/K}(\alpha_i\alpha_j)$. Assim, usando determinantes, temos

$$\Delta_{F/K}(\alpha_1, \alpha_2, ..., \alpha_m) = det(A)^2$$

Corolário 1.37. *Seja $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{F}_{q^m}$. Então $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se,*

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

Teorema 1.38. *Para $\alpha \in \mathbb{F}_{q^m}$, $\alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ é uma base normal de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se, os polinômios $x^m - 1$ e $\alpha x^{m-1} + \alpha^q x^{m-2} + ... + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ em $\mathbb{F}_{q^m}[x]$ são relativamente primos.*

Demonstração. Vide Teorema 2.39 [8] pág. 62. □

Mencionaremos no teorema abaixo, sem prova, um refinamento do Teorema da base normal.

Teorema 1.39. ***(Teorema da Base Normal Primitiva)*** *Para qualquer extensão finita F de um corpo finito K existe uma base normal de F sobre seu subcorpo primo que consiste de elementos primitivos de F.*

1.4 Raízes da Unidade e Polinômios Ciclotômicos

Nesta seção iremos investigar o corpo de decomposição do polinômio $x^n - 1$ sobre um corpo arbitrário K, onde n é um inteiro positivo. Ao mesmo tempo iremos encontrar uma generalização para um conceito já conhecido no universo dos números complexos: raiz da unidade.

Definição 1.40. *Seja n um número inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre o corpo K é chamado n-ésimo corpo ciclotômico sobre K e denotado por $K^{(n)}$. As raízes de $x^n - 1$ em $K^{(n)}$ são chamados n-ésimas raízes da unidade sobre K e o conjunto de todas essas raízes é denotado por $E^{(n)}$.*

Teorema 1.41. *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 a multiplicação em $K^{(n)}$.

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

Demonstração. (i) O caso $n = 1$ é trivial. Então, supondo $n \geq 2$, $x^n - 1$ e seu polinômio derivado nx^{n-1} não possuem raízes em comum, uma vez que nx^{n-1} só possui o zero como raiz em $K^{(n)}$. Disso, segue que $x^n - 1$ não possui raízes múltiplas. Sendo assim, $E^{(n)}$ possui n elementos. Agora, sejam $\epsilon, \eta \in E^{(n)}$. Note que $(\epsilon\eta^{-1})^n = \epsilon^n(\eta^n)^{-1} = 1$. Logo, $\epsilon\eta^{-1} \in E^{(n)}$ e portanto segue $E^{(n)}$ grupo multiplicativo. Seja $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \ldots \cdot {p_t}^{e_t}$ a decomposição em fatores primos de n. Vamos mostrar que $E^{(n)}$ é cíclico. Usando a mesma idéia da demonstração do Teorema 1.3, para cada $1 \leq i \leq t$, existe um elemento $\alpha_i \in E^{(n)}$ tal que α_i não é uma raiz do polinômio $x^{n/p_i} - 1$. Assim, se $\beta_i = {\alpha_i}^{n/{p_i}^{e_i}}$ então β_i tem ordem ${p_i}^{e_i}$. Assim, $\beta = \beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_t \in E^{(n)}$ tem ordem n, ou seja, β é um gerador de $E^{(n)}$. Logo, $E^{(n)}$ é ciclíco.

(ii) Se p divide n, escreva $n = mp^j$ com inteiros positivos m e j e m não divisível por p. Temos:

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

Disso, e por (i), segue o item (ii). □

Definição 1.42. *Seja K um corpo de característica p e n um inteiro positivo não divisível por p. Então o gerador do grupo ciclíco $E^{(n)}$ é chamado uma n-ésima raiz primitiva da unidade sobre K.*

Usando a definição anterior e o Tereoma 1.15(v) ([8] pág. 7), temos que existem exatamente $\phi(n)$ n-ésimas raízes primitivas da unidade sobre K. Se ξ é uma raiz, então as outras raízes são dadas por ξ^s, com $1 \leq s \leq n$ e $mdc(s,n) = 1$.

Definição 1.43. *Seja K um corpo de característica p, n um inteiro positivo não divisível por p, e ξ uma n-ésima raiz primitiva da unidade sobre K. Então o polinômio,*

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

é chamado n-ésimo polinômio ciclotômico sobre K.

O polinômio $Q_n(x)$ é claramente independente da escolha de ξ. O grau de $Q_n(x)$ é $\phi(n)$ e seus coeficientes pertencem ao n-ésimo polinômio ciclotômico sobre K. Um argumento simples mostrará que esses coeficientes estão contidos no subcorpo primo de K. Usaremos o símbolo $\prod_{d|n}$ para denotar um produto estendido sobre todos os divisores positivos d de um inteiro positivo n.

Teorema 1.44. *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 é o corpo dos números racionais.

Demonstração. (i) Suponha que w é uma raiz de $Q_d(x)$ onde $d \mid n$. Disso, temos que w é uma d-ésima raiz da unidade. Tomando k um inteiro com $n = dk$, temos que $w^n = (w^d)^k = 1^k = 1$. Logo, w é uma raiz de $x^n - 1$. Agora, suponha que w é uma raiz de $x^n - 1$. Então, w é uma n-ésima raiz da unidade. Se d é a ordem de w, $w^d = 1$. Daí temos que w é uma d-ésima raiz da unidade. Assim, w é uma raiz de $Q_d(x)$. Sabemos que as n-ésimas raízes da unidade formam um grupo de n elementos, $d \mid n$ e w é uma raiz de $Q_d(x)$ para algum d, com d divisor de n. Com isto, mostramos que $x^n - 1$ e $\prod_{d|n} Q_d(x)$ possuem as mesmas raízes. Note que, $\prod_{d|n} Q_d(x)$ é mônico, pois é um produto de uma coleção de polinômios mônicos. Disso, $x^n - 1$ e $\prod_{d|n} Q_d(x)$ são ambos mônicos com as mesmas raízes, donde segue que $x^n - 1 = \prod_{d|n} Q_d(x)$.

(ii) Provemos usando indução em m. Note que $Q_n(x)$ é um polinômio mônico. Para $n = 1$, temos $Q_1(x) = x - 1$, e o item (ii) é válido. Agora, seja $n > 1$ e suponha válido para $Q_d(x)$ com $1 \leq d < n$. Então, por (i) temos que $Q_n(x) = (x^n - 1)/f(x)$, onde $f(x) = \prod_{d|n, d<n} Q_d(x)$. A hipótese de indução indica que $f(x)$ é um polinômio com coeficientes em um corpo primo de K ou em $\mathbb{Z}$ no caso

da característica de K ser zero. Fazendo várias divisões com o polinômio $x^n - 1$ e o polinômio mônico $f(x)$, vemos que os coeficientes de $Q_n(x)$ pertencem a um subcorpo primo de K ou $\mathbb{Z}$ respectivamente. □

Exemplo 1.45. *Seja r um número primo e $k \in \mathbb{N}$. Então:*

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

De fato, pelo Teorema 1.44(i), temos:

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

Para $k = 1$, temos simplesmente $Q_r(x) = 1 + x + x^2 + ... + x^{r-1}$.

Para aplicações em corpos finitos, é útil conhecermos algumas propriedades dos corpos ciclotômicos.

Teorema 1.46. *O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K. Além disso:*

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

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

Demonstração. (i) Se existe uma n-ésima raiz primitiva da unidade ξ sobre K, é claro que $K^{(n)} = K(\xi)$, caso contrário, temos a situação descrita no Teorema 1.41. Além disso, sabemos que $\phi(n) = |S|$, onde $S = \{s \mid mdc(n, s) = 1\}$ com $1 \leq s \leq n$. Assim, segue que $[K^{(n)} : K] = \phi(n)$, lembrando que $\xi^s \in K^{(n)}$ se $mdc(n, s) = 1$.
(ii) Seja η uma raiz n-ésima primitiva da unidade sobre $\mathbb{F}_q$. Então, $\eta \in \mathbb{F}_{q^k}$ se, e só se, $\eta^{q^k} = \eta$, e a última igualdade é equivalente a $q^k \equiv 1 \pmod{n}$. O menor número inteiro positivo para o qual isso é válido é $k = d$, e assim $\eta \in \mathbb{F}_{q^d}$, mas em nenhum subcorpo próprio. Assim, o polinômio mínimo de η sobre $\mathbb{F}_q$ tem grau d, e como η é uma raiz arbitrária de Q_n, segue o resultado desejado. □

Exemplo 1.47. *Seja $K = \mathbb{F}_{11}$ a $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_q[x]$. Na notação do Teorema 1.46 temos $d = 2$. $Q_{12}(x)$ se fatora na forma*

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

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

Teorema 1.48. *O corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um dos seus subcorpos.*

Demonstração. O polinômio $x^{q-1}-1$ se fatora em $\mathbb{F}_q$ pois suas raízes são exatamente os elementos não nulos de $\mathbb{F}_q$. Obviamente, esse polinômio não se fatora em nenhum outro subcorpo próprio de $\mathbb{F}_q$, e portanto temos que $\mathbb{F}_q$ é o corpo de decomposição de $x^{q-1}-1$ sobre qualquer um dos seus subcorpos. □

Como $\mathbb{F}_q$ é um grupo cíclico de ordem $q-1$, existe para qualquer divisor positivo n de $q-1$, um subgrupo cíclico $\{1, \alpha, ..., \alpha^{n-1}\}$ de $\mathbb{F}_q^*$ de ordem n. Todos os elementos deste subgrupo são n-ésimas raízes da unidade sobre qualquer subcorpo de $\mathbb{F}_q$, e o elemento gerador α é uma raiz primitiva da unidade sobre qualquer subcorpo de $\mathbb{F}_q$.

Lema 1.49. *Se d é um divisor de um inteiro positivo n com $1 \leq d < n$, então $Q_n(x)$ divide $(x^n-1)/(x^d-1)$ quando $Q_n(x)$ é definido.*

Demonstração. Sabemos que $Q_n(x)$ divide x^n-1. Além disso,

$$x^n - 1 = (x^d - 1) \cdot \frac{x^n - 1}{x^d - 1}$$

Como d é um divisor próprio de n, o polinômio $Q_n(x)$ e x^d-1 não possuem raízes em comum. Consequentemente, $mdc(Q_n(x), x^d-1) = 1$, e dessa forma segue o lema. □

1.5 Representação de elementos de Corpos Finitos

Nesta seção vamos descrever duas diferentes maneiras de representar os elementos de um corpo finito $\mathbb{F}_q$ com $q = p^n$ elementos, onde p é a característica de $\mathbb{F}_q$.

Método 1: Lembremos que $\mathbb{F}_q$ é uma extensão algébrica simples de $\mathbb{F}_p$. De fato, se f é um polinômio irredutível em $\mathbb{F}_p[x]$ de grau n, então f tem uma raiz α em $\mathbb{F}_q$ e então $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Assim, todo elemento de $\mathbb{F}_q$ pode ser expresso de maneira única como um polinômio em α sobre $\mathbb{F}_p$ de grau menor que n.

Exemplo 1.50. *Para representar os elementos de $\mathbb{F}_9$ usando o método 1, recordemos que $\mathbb{F}_9$ é uma extensão simples de $\mathbb{F}_3$ de grau 2, obtida pela junção de uma raiz α de um polinômio quadrático irredutível sobre $\mathbb{F}_3$, a saber, $f(x) = x^2+1 \in \mathbb{F}_3[x]$. Disso, temos que $f(\alpha) = \alpha^2 + 1 = 0$ em $\mathbb{F}_9$ e os nove elementos de $\mathbb{F}_9$ são da forma $\alpha_0 + \alpha_1 \cdot \alpha \in \mathbb{F}_3$ com $a_0, a_1 \in \mathbb{F}_3$. Assim,*

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$$

.

Método 2: Note que $\mathbb{F}_9 = \mathbb{F}_3{}^{(8)}$ é o oitavo corpo ciclotômico sobre $\mathbb{F}_3$. Agora, $Q_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$ e,

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2)$$

é a decomposição de Q_8 em fatores irredutíveis em $\mathbb{F}_3[x]$. Seja ξ uma raiz de $x^2 + x + 2$; então ξ é a oitava raiz primitiva da unidade sobre $\mathbb{F}_3$. Assim, todo elemento não nulo de $\mathbb{F}_9$ pode ser expresso como potências de ξ, e então

$$\mathbb{F}_9 = \{0, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8\}$$

Agora, observe que $x^2 + x + 2 \in \mathbb{F}_3[x]$ tem $\xi = 1 + \alpha$ como uma raiz, onde $\alpha^2 + 1 = 0$. Portanto, a tabela para $\mathbb{F}_9$ pode ser escrita como segue:

i	ξ^i	i	ξ^i
1	$1 + \alpha$	5	$2 + 2\alpha$
2	2α	6	α
3	$1 + 2\alpha$	7	$2 + \alpha$
4	2	8	1

Obtemos, é claro, os mesmos elementos do exemplo anterior em uma ordem diferente.

Capítulo 2

Polinômios sobre Corpos Finitos

A teoria de polinômios sobre corpos finitos é importante para investigarmos a estrutura algébrica de corpos finitos, bem como para muitas outras aplicações como veremos ao longo dos capítulos. Além disso, polinômios irredutíveis são indispensáveis para a construção de corpos finitos.

Na Seção 1.1 iremos introduzir a noção de ordem de um polinômio, além dos aspectos construtivos da irredutibilidade. Por fim, iremos demonstrar resultados que facilitam calcular o polinômio minimal de um elemento em um corpo de extensão. Já na Seção 1.2, serão vistos resultados importantes sobre polinômios irredutíveis.

2.1 Ordem de um polinômio e polinômio primitivo

Além do grau de um polinômio, algo já conhecido a fundo, existe um outro inteiro não nulo intimamente ligado a um polinômio. A esse inteiro chamaremos de ***ordem***. A definição de ***ordem*** de um polinômio será baseada no resultado que segue. Sua demonstração pode ser encontrada em [8] pág. 84.

Lema 2.1. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau $m \geq 1$ com $f(0) \neq 0$. Então existe um inteiro positivo $e \leq q^m - 1$ tal que $f(x)$ divide $x^e - 1$.*

Definição 2.2. *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 $ord(f) = ord(f(x))$. 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 determinados unicamente, e $ord(f)$ é então definido como $ord(g)$.*

Teorema 2.3. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível de grau m sobre $\mathbb{F}_q$ com $f(0) \neq 0$. Então, a $ord(f)$ é igual a ordem de qualquer raiz de f no grupo multiplicativo $\mathbb{F}_{q^m}^*$.*

Demonstração. De acordo com o Colorário 1.15, o corpo de decomposição de f sobre $\mathbb{F}_q$ é $\mathbb{F}_{q^m}$. Pelo Teorema 1.18 temos que as raízes de f têm a mesma ordem

no grupo $\mathbb{F}_{q^m}^*$. Seja $\alpha \in \mathbb{F}_{q^m}^*$ um raiz de f. Então, pelo Teorema 1.12, temos que $\alpha^e = 1$ se, e somente se, $f(x)$ divide $x^e - 1$. Dessa forma, segue que $ord(f) = e$, onde e é a ordem de uma raiz α em $\mathbb{F}_{q^m}^*$. □

Corolário 2.4. *Se $f \in \mathbb{F}_q[x]$ é um polinômio irredutível sobre $\mathbb{F}_q$ de grau m, então a $ord(f)$ divide $q^m - 1$.*

Demonstração. Se $f(x) = cx$ com $c \in \mathbb{F}_q^*$, então $ord(f) = 1$ e o resultado é trivial. Por outro lado, pelo Teorema 2.3, temos que a $ord(f)$ será $q^m - 1$. Segue assim o corolário. □

Para polinômios redutíveis, o resultado do Corolário 2.4 não precisa ser válido (ver exemplo 2.11). Há outra interpretação de $ord(f)$ baseada na associação de uma matriz quadrada de f em uma forma canônica e considerando a ordem desta matriz em um determinado grupo de matrizes (ver Lema 8.26 [8] pág. 408).

O Teorema 2.3 leva a uma fórmula para o número de polinômios mônicos irredutíveis de grau e ordem dados. Usaremos ϕ para denotar a Função de Euler(ver Teorema 1.15(iv) [8] pág. 7). A terminologia a seguir será conveniente: se n é um inteiro positivo e o inteiro b e n são primos entre si, então o menor inteiro positivo k para o qual $b^k \equiv 1 \pmod{n}$, é chamado a ordem multiplicativa de b módulo n.

Observação 2.5. *$f(x) = c$, para $c \in \mathbb{F}_q^*$ tem ordem 1 pois $c \mid x - 1$*

Teorema 2.6. *O número de polinômios mônicos e irredutíveis em $\mathbb{F}_q[x]$ de grau m e ordem e é igual a $\phi(e)/m$ se $e \geq 2$ e m é a ordem multiplicativa de q módulo e. Igual a 2, se $m = e = 1$, e igual a 0 nos outros casos. Em particular, o grau de um polinômio irredutível em $\mathbb{F}_q[x]$ de ordem e deve ser igual a ordem multiplicativa de q módulo e.*

Demonstração. Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ com $f(0) \neq 0$. Então, de acordo com o Teorema 2.1, temos que $ord(f) = e$ se, e somente se, todas as raízes são e-ésimas raízes primitivas da unidade sobre $\mathbb{F}_q$. Em outras palavras, temos que a $ord(f) = e$ se, e só se, f divide o polinômio ciclotômico Q_e. Pelo Teorema 1.46, temos que, qualquer fator mônico irredutível de Q_e tem o mesmo grau m, o menor inteiro positivo tal que $q^m \equiv 1 \pmod{e}$ e além disso, o número de fatores é dado por $\phi(e)/m$. Para $m = e = 1$, levemos em conta o polinômio mônico irredutível $f(x) = x$ e $f(x) = x - 1$. □

Qualquer polinômio de grau positivo pode ser escrito como um produto de polinômios irredutíveis. Assim, o cálculo da ordem desses polinômios pode ser feito se soubermos determinar a ordem de uma potência de um polinômio irredutível e a ordem do produto de pares de polinômios relativamente primos. Os próximos resultados irão tratar dessas questões.

Lema 2.7. *Seja c um inteiro positivo. Então, o polinômio $f \in \mathbb{F}_q[x]$, com $f(0) \neq 0$, divide $x^c - 1$ se, e somente se, a $ord(f)$ divide c.*

Demonstração. Se $e = ord(f)$ divide c, então $f(x)$ divide $x^e - 1$ e $x^e - 1$ divide $x^c - 1$, de modo que $f(x)$ divide $x^c - 1$. Por outro lado, se $f(x)$ divide $x^c - 1$, temos que $c \geq e$, e então podemos escrever $c = me + r$, com $m \in \mathbb{N}$ e $0 \leq r < e$. Como, $x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$, segue que $f(x)$ divide $x^r - 1$ que vale somente se $r = 0$. Portanto, e divide c. □

Corolário 2.8. *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 $d = mdc(e_1, e_2)$.*

Demonstração. Seja $f(x)$ mônico e o maior divisor comum de $x^{e_1} - 1$ e $x^{e_2} - 1$. Sendo $x^d - 1$ um divisor comum de $x^{e_i} - 1$, $i = 1, 2$, segue que $x^d - 1$ divide $f(x)$. Por outro lado, $f(x)$ é um divisor comum de $x^{e_i} - 1$, $i = 1, 2$, e pelo Lema 2.7 segue que $ord(f)$ divide e_1 e e_2. Consequentemente, $ord(f)$ divide d, e portanto $f(x)$ divide $x^d - 1$ pelo Lema 2.7. Mostramos assim que, $f(x) = x^d - 1$. □

Como as potências de x são fatoradas antecipadamente ao determinar a ordem de um polinômio, não precisamos considerar as potências dos polinômios irredutíveis $g(x)$, com $g(0) = 0$.

Teorema 2.9. *Seja $g \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ com $g(0) \neq 0$ e $ord(g) = e$, e seja $f = g^b$ com b inteiro positivo. Seja t o menor inteiro com $p^t \geq b$, onde p é a característica de $\mathbb{F}_q$. Então $ord(f) = ep^t$.*

Demonstração. Suponha que $ord(f) = c$, e note que, $f(x)$ dividir $x^c - 1$, implica em $g(x)$ dividir $x^c - 1$. Disso, pelo Lema 2.7, segue que e divide c. Além disso, como $ord(g) = e$, temos que $g(x)$ divide $x^e - 1$, e portanto divide $(x^e - 1)^b$. Consequentemente, $f(x)$ divide $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Então, pelo Lema 2.7, temos que c divide ep^t. Assim, $c = ep^u$, com $0 \leq u \leq t$. Note que $x^e - 1$ possui somente raízes simples, uma vez que pelo colorário 2.4 temos que e não é multiplo de p. Então, todas as raízes de $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ tem multiplicidade p^u. Mas, $g(x)^b$ divide $x^{ep^u} - 1$ quando $p^u \geq b$. Disso, segue que $u = t$ e $ord(f) = ep^t$. □

Teorema 2.10. *Sejam $g_1, g_2, ..., g_k$ polinômios não nulos sobre $\mathbb{F}_q$, dois a dois primos entre si, e seja $f = g_1 \cdot g_2 \cdot ... \cdot g_k$. Então $ord(f)$ é ao igual mínimo múltiplo comum de $ord(g_1), ..., ord(g_k)$.*

Demonstração. É suficiente considerar o caso $g_i(0) \neq 0$ para $1 \leq i \leq k$. Seja $e = ord(f)$, $e_i = ord(g_i)$ para $1 \leq i \leq k$, e seja $c = mmc(e_1, ..., e_k)$. Então, cada $g_i(x)$ divide $x^{e_i} - 1$, e portanto, $g_i(x)$ divide $x^c - 1$. Pelos polinômios $g_i(x)$ com $1 \leq i \leq k$, serem dois a dois primos entre si, temos que $f(x)$ divide $x^c - 1$. Pelo Lema 2.7, segue que e divide c. Por outro lado, $f(x)$ divide $x^e - 1$, e assim $g_i(x)$ divide $x^e - 1$. Disso, cada e_i divide e, e portanto c divide e. Concluímos então que $c = e$, ou seja, $ord(f) = mmc(ord(g_1), ..., ord(g_k))$. □

Exemplo 2.11. *Vamos calcular a ordem do polinômio* $f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. *A fatoração canônica de* $f(x)$ *sobre* $\mathbb{F}_2$ *é dada por:*

$$f(x) = (x^2 + x + 1)^3 \cdot (x^4 + x + 1)$$

Pela definição 2.2, a ordem de $f \in \mathbb{F}_q[x]$ *é o menor inteiro e para o qual* $f(x)$ *divide* $x^e - 1$. *Como* 3 *é o menor inteiro positivo tal que* $x^2 + x + 1$ *divide* $x^3 - 1$, *segue que* $ord(x^2+x+1) = 3$. *Agora, seja* $h(x) = x^2+x+1$ *e* $L(x) = (x^2 + x + 1)^3$, *com* $ord(h) = 3$. *Note que* 2 *é o menor inteiro para o qual* $2^2 \geq 3$. *Assim, pelo Teorema 2.9,* $ord(L) = 3 \cdot 2^2 = 12$. *Usando novamente a definição 2.2, temos que* $ord(x^4+x+1) = 15$. *Pelo Teorema 2.10, tem - se que* $ord(f) = mmc(12, 15) = 60$. *Logo,* $ord(f) = 60$. *Note que* $ord(f)$ *não divide* $2^{10} - 1$, *o que mostra que o Corolário 2.4 não é mantido para polinômios redutíveis.*

Corolário 2.12. *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* $f = a{f_1}^{b_1} \cdot ... \cdot {f_1}^{b_k}$ *onde* $a \in \mathbb{F}_q$, $b_1, ..., b_k \in \mathbb{N}$, *e* $f_1, ..., f_k$ *polinômios mônicos irredutíveis em* $\mathbb{F}_q[x]$ *e a fatoração canônica de* $f \in \mathbb{F}_q[x]$. *Então,* $ord(f) = ep^t$, *onde* $e = mmc(ord(f_1), ..., ord(f_k))$ *e* t *é o menor inteiro positivo com* $p^t \geq max(b_1, ..., b_k)$.

Definição 2.13. *Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{F}_q[x]$, *com* $a_n \neq 0$. *Então, o polinômio recíproco* f^* *é definido por:*

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

Teorema 2.14. *Seja* f *um polinômio não-nulo em* $\mathbb{F}_q[x]$ *e seu polinômio recíproco* f^*. *Então,* $ord(f) = ord(f^*)$.

Demonstração. Primeiramente, considere $f(0) \neq 0$. Note que, $f(x)$ divide $x^e - 1$ se, e somente se, $f^*(x)$ divide $x^e - 1$. Disso, segue o resultado. Por outro lado, se $f(0) = 0$, escreva $f(x) = x^h g(x)$ com $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$ satisfazendo $g(0) \neq 0$. Sabemos que $ord(f) = ord(g)$, e como mostrado para o caso $f(0) \neq 0$, tem-se $ord(g) = ord(g^*) = ord(f^*)$, pois $f^* = g^*$. □

Teorema 2.15. *Para* q *ímpar, sejam* $f \in \mathbb{F}_q[x]$ *um polinômio de grau positivo com* $f(0) \neq 0$. *Seja* l *e* L *as ordens de* $f(x)$ *e* $f(-x)$ *respectivamente. Então* $L = l$ *se* l *é multiplo de* 4 *e* $L = 2l$ *se* l *é ímpar. Se* l *é duas vezes um número ímpar, então* $L = l/2$ *se todos os fatores ímpares de* f *tem mesma ordem e* $L = l$ *para os outros casos.*

Demonstração. Como $ord(f(x)) = l$, $f(x)$ divide $x^{2l} - 1$ e assim $f(-x)$ divide $(-x)^{2l} - 1 = x^{2l} - 1$. Então, pelo Lema 2.7, L divide $2l$. Usando o mesmo argumento, temos que l divide $2L$, o que somente é possível se L for igual a $2l$, l ou $l/2$. Se l é um mutiplo de 4, então l e L são iguais. De fato, $f(x)$ divide $x^l - 1$, $f(-x)$ divide $(-x)^l - 1 = x^l - 1$. Disso, temos que l divide L. Procedendo de forma análoga, teremos que L divide l, o que implica em $L = l$. Se l é ímpar, então $f(-x)$ divide $(-x)^l - 1 = -x^l - 1 = -(x^l + 1)$. Logo, $f(-x)$ não divide $x^l - 1$, e portanto, resta-se que $L = 2l$.

No caso restante, seja $l = 2h$, com h um inteiro 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 $ord(f)=2h$. Como x^h-1 e x^h+1 são primos entre si, segue que $f(x)$ divide x^h+1. Consequentemente, $f(-x)$ divide $(-x)^h+1=-x^h+1=-(x^h-1)$. Logo, segue que E divide h e portanto , $L=l/2$. □

Observação 2.16. *Pelo Teorema 2.9 a potência de um dado polinômio irredutível têm a mesma ordem se, e somente se, o polinômio irredutível tem ordem ímpar. Para qualquer f, seja a fatoração de $f=g_1\cdot ...\cdot g_k$, onde g_i é uma potência de um polinômio irredutível e $g_1,...,g_k$ são dois a dois primos entre si. Além disso, $2h=mmc(ord(g_1),...,ord(g_k))$. Coloque g_i de tal forma que $ord(g_i)=2h_i$, com $1\leq i\leq m$ e $ord(g_i)=h_i$ para $m+1\leq i\leq k$, onde h_i é inteiro ímpar com $mmc(h_1,...,h_k)=h$. Como já mostrado, temos que $ord(g_i(-x))=h_i$ para $1\leq i\leq m$ e $ord(g_i(-x))=2h_i$ para $m+1\leq i\leq k$. Então, pelo Teorema 2.10,*

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

e então $L=h=l/2$ se $m=k$ e $L=2h=l$ se $m<k$.

Segue do Lema 2.1 e da Definição 2.2 que a ordem de um polinômio de grau $m\geq 1$ é no máximo q^m-1. Este limite é atingido por uma classe de polinômios importantes chamados de polinômios primitivos. A definição de polinômio primitivo é baseada na noção de elemento primitivo introduzida no Capítulo 1 na Definição 1.9.

Definição 2.17. *Um polinômio $f\in\mathbb{F}_q[x]$ de grau $m\geq 1$ é chamado polinômio primitivo sobre $\mathbb{F}_q$ se este é o polinômio minimal sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^m}$.*

Um polinômio primitivo sobre $\mathbb{F}_q$ de grau m pode ser descrito como um polinômio mônico irredutível sobre $\mathbb{F}_q$ que possui uma raiz $\alpha\in\mathbb{F}_q$, tal que α gera o grupo multiplicativo de $\mathbb{F}_{q^m}$. Polinômios primitivos também podem ser caracterizados como segue.

Teorema 2.18. *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 $ord(f)=q^m-1$.*

Demonstração. Se f é primitivo sobre $\mathbb{F}_q$, então f é mônico e $f(0)\neq 0$. Desde que f seja irredutível sobre $\mathbb{F}_q[x]$, temos que $ord(f)=q^m-1$.

Como $ord(f)=q^m-1$ segue que $m\geq 1$. Provemos que f é irredutível sobre $\mathbb{F}_q$. De fato, suponha que f seja redutível sobre $\mathbb{F}_q$. Assim, temos duas possibilidades para f. No primeiro caso, temos $f=g^b$, com $g\in\mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$, com $g(0)\neq 0$ e $b\geq 2$. Então, pelo Teorema 2.9, $ord(f)$ é divisível pela característica de $\mathbb{F}_q$, mas q^m-1 não é divisível, o que é uma contradição. No segundo caso, temos $f=g_1g_2$ com g_1,g_2 polinômios mônicos em $\mathbb{F}_q[x]$ primos entre si, de grau m_1 e m_2 respectivamente. Se $e_i=ord(g_i)$, para $i=1,2$, então $ord(f)\leq e_1e_2$ pelo Teorema 2.10. Além disso, $e_i\leq q^{m_i}-1$ para $i=1,2$ pelo Lema 1.48. Então:

$$ord(f)\leq (q^{m_1}-1)\cdot(q^{m_2}-1)<q^{m_1+m_2}-1=q^m-1$$

e portanto, temos uma contradição. Logo, f é irredutível sobre $\mathbb{F}_q$ e segue então pelo Teorema 2.3 que f é um polinômio primitivo sobre $\mathbb{F}_q$. □

Observamos que a condição $f(0) \neq 0$ no teorema acima só é necessário para descartar o polinômio não primitivo $f(x) = x$ no caso $q = 2$ e $m = 1$. Um outra caracterização de polinômio primitivo é baseada no resultado que segue.

Lema 2.19. *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau positivo com $f(0) \neq 0$, e r o menor inteiro positivo para o qual x^r é congruente $\pmod{f(x)}$ para algum elemento de $\mathbb{F}_q$, de modo que $x^r \equiv a \mod f(x)$ para a determinado unicamente, $a \in \mathbb{F}_q^*$. Então, $ord(f) = hr$, onde h é a ordem de a em um grupo multiplicativo $\mathbb{F}_q^*$.*

Demonstração. Faça $e = ord(f)$. Sendo $x^e \equiv 1 \pmod{f(x)}$, temos que $e \geq r$. Então, podemos escrever $e = sr + t$ com $s \in \mathbb{N}$ e $0 \leq t < r$. Temos:

$$\begin{aligned} 1 \equiv x^e \equiv x^{rs+t} \equiv a^s x^t \pmod{f(x)} &\Rightarrow 1 \equiv a^s x^t \pmod{f(x)} \\ &\Rightarrow 1 - a^s x^t = l(x)f(x) \\ &\Rightarrow a^s x^t - 1 = (-l(x))f(x) \\ &\Rightarrow a^{-s}(a^s x^t - 1) = (k(x))f(x) \\ &\Rightarrow x^t - a^{-s} = k(x)f(x) \\ &\Rightarrow x^t \equiv a^{-s} \pmod{f(x)} \end{aligned}$$

para $l, k \in \mathbb{F}_q[x]$. Pela definição de r, $x^t \equiv a^{-s} \pmod{f(x)}$ só é posssível se $t = 0$. Da congruência acima, temos que $a^s \equiv 1 \pmod{f(x)}$ e então $a^s = 1$. Assim, $s \geq h$ e $e \geq hr$. Por outro lado, $x^{hr} \equiv a^h \equiv 1 \pmod{f(x)}$, donde e divide hr e portanto $hr \geq e$. Então, $e = hr$. □

Teorema 2.20. *O polinômio mônico $f \in \mathbb{F}_q[x]$ de grau $m \geq 1$ é um polinômio primitivo sobre $\mathbb{F}_q$ se, e somente se, $(-1)^m f(0)$ é um elemento primitivo de $\mathbb{F}_q$, e o menor inteiro positivo r para o qual x^r é congruente $\pmod{f(x)}$ para algum elemento de $\mathbb{F}_q$ é $r = (q^m - 1)/(q - 1)$. No caso em que f é primitivo sobre $\mathbb{F}_q$, temos $x^r \equiv (-1)^m f(0) \pmod{f(x)}$.*

Demonstração. ($\Rightarrow$) Se f é um polinômio primitivo sobre $\mathbb{F}_q$, então f tem uma raiz $\alpha \in \mathbb{F}_{q^m}$, e α é elemento primitivo de $\mathbb{F}_{q^m}$. Calculando a norma $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, e observando que f é o polinômio característico de α sobre $\mathbb{F}_q$, temos:

$$(-1)^m f(0) = \alpha^{(q^m-1)/(q-1)} \tag{2.1}$$

Disso, segue 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 $\mathbb{F}_q$. Desde que f é um polinômio minimal de α sobre $\mathbb{F}_q$, a igualdade (2.1) implica em:

$$x^{(q^m-1)/(q-1)} \equiv (-1)^m f(0) \pmod{f(x)} \tag{2.2}$$

e então, $r \leq (q^m - 1)/(q - 1)$. Mas, pelo Teorema 2.18 e o Lema 2.19, têm-se, $q^m - 1 = ord(f) \leq (q - 1)r$. Então, $r = (q^m - 1)/(q - 1)$.

($\Leftarrow$) Agora, por outo lado, supondo válido as condições do teorema, provemos que o polinômio mônico $f \in \mathbb{F}_q[x]$ é polinômio primitivo sobre $\mathbb{F}_q$. Então, por $r = (q^m - 1)/(q - 1)$, e pelo Lema 2.19 segue que $ord(f)$ é relativamente prima com q. Então, o Teorema 2.12 mostra que f é fatorado da forma $f = f_1 \cdot ... \cdot f_k$, onde os f_i são polinômios mônicos distintos irredutíveis sobre $\mathbb{F}_q$. Se $m_i = grau(f_i)$, então $ord(f_i)$ divide $q^{m_i} - 1$ para $1 \leq i \leq k$ pelo 2.4. Agora, $q^{m_i} - 1$ divide

$$d = (q^{m_1} - 1) \cdot ... \cdot (q^{m_k} - 1)/(q - 1)^{k-1}$$

Então, $ord(f_i)$ divide d para $1 \leq i \leq k$. Segue pelo Lema 2.7 que $f_i(x)$ divide $x^d - 1$ para $1 \leq i \leq k$, e então, $f(x)$ divide $x^d - 1$. Se $k \geq 2$, então:

$$d < (q^{m_1+m_2+...+m_k} - 1)/(q - 1) = (q^m - 1)/(q - 1) = r$$

uma contradição pela definição de r. Então, $k = 1$ e f é irredutível sobre $\mathbb{F}_q$. Se $\beta \in \mathbb{F}_{q^m}$ é um raiz de f, então o argumento que leva a (2.2) mostra que $\beta^r \equiv (-1)^m f(0)$. Como a ordem de $(-1)^m f(0)$ é $\mathbb{F}_q^*$ é $q-1$, segue pelo Lema 2.19 que $ord(f) = q^m - 1$, donde temos f polinômio primitivo sobre $\mathbb{F}_q$ pelo Teorema 2.18. □

Exemplo 2.21. *Considere o polinômio $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Como f é irredutível sobre $\mathbb{F}_3$, podemos usar o método descrito no Teorema 2.12 para mostrar que $ord(f) = 80 = 3^4 - 1$. Consequentemente, f é um polinômio primitivo sobre $\mathbb{F}_3$ pelo Teorema 2.19. Temos que $x^{40} \equiv 2 \pmod{f(x)}$ de acordo com o Teorema 2.20.*

2.2 Polinômios Irredutíveis

Lembremos que, um polinômio $f \in \mathbb{F}_q[x]$ é dito irredutível sobre $\mathbb{F}_q[x]$ se f tem grau positivo e se $f = gh$ com $g, h \in \mathbb{F}_q[x]$, segue que ou g ou h é uma constante polinomial(ver [8], pág. 23). Dessa forma, toda fatoração de f em $\mathbb{F}_q[x]$ deve envolver uma constante polinomial. Propriedades elementares de polinômios irredutíveis foram discutidas no Capítulo 1, Seção 1.2.

Teorema 2.22. *Para todo corpo finito $\mathbb{F}_q$ e todo $n \in \mathbb{N}$, o produto de todo polinômio mônico irredutível sobre $\mathbb{F}_q$ cujo grau divide n é igual a $x^{q^n} - x$.*

Demonstração. Pelo Lema 1.13, os polinômios mônicos irredutíveis que aparecem na fatoração canônica de $g(x) = x^{q^n} - x$ em $\mathbb{F}_q[x]$ são precisamente aqueles cujos graus dividem n. Como $g'(x) = -1$, segue que g não possui raízes múltiplas no corpo de decomposição de $\mathbb{F}_q$, e então, cada polinômio mônico irredutível sobre $\mathbb{F}_q$ cujos graus dividem n ocorre exatamente uma única vez na fatoração canônica de g em $\mathbb{F}_q[x]$. □

Corolário 2.23. *Se $N_q(d)$ é o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau d, então:*

$$q^n = \sum_{d|n} dN_q(d) \tag{2.3}$$

para todo $n \in \mathbb{N}$, onde a soma percorre todos os divisores positivos d de n.

Demonstração. A igualdade (2.3) segue do Teorema 2.22 comparando o grau de $g(x) = x^{q^n} - x$ com o grau total da fatoração canônica de $g(x)$. □

Usando teoria de números elementar podemos através da igualdade (2.3) encontrar uma fórmula explícita para o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau fixo. Vamos usar uma função aritmética chamada de função de *Möbius*.

Definição 2.24. *A função de Möbius μ é uma função de $\mathbb{N}$ definida por:*

$$\mu(n) = \begin{cases} 1, & \text{se } n\text{=1,} \\ (-1)^k, & \text{se } n \text{ é produto de } k \text{ primos distintos,} \\ 0, & \text{se } n \text{ é divisível por um quadrado de um primo} \end{cases} \tag{2.4}$$

Na igualdade (2.3), usamos o símbolo de somatório $\sum_{d|n}$ para denotar uma soma percorre sobre todos os divisores positivos d de $n \in \mathbb{N}$. Uma convenção similar aplica-se para para o símbolo de produto $\prod_{d|n}$.

Lema 2.25. *Para $n \in \mathbb{N}$ a função de Möbius μ satisfaz:*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & se \quad n = 1 \\ 0, & se \quad n > 1 \end{cases} \tag{2.5}$$

Demonstração. O caso $n = 1$ é tivial. Assim, se $n > 1$, temos que levar em conta apenas os divisores positivos d de n para o qual $\mu(d) \neq 0$, isto é, para o qual $d = 1$ ou d é um produto de primos distintos. Então, para $p_1, p_2, ..., p_k$ divisores primos distintos positivos de n, temos:

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

□

Teorema 2.26. *(Möbius Inversion Formula)*

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

$$H(n) = \sum_{d|n} h(d) \tag{2.6}$$

para todo $n \in \mathbb{N}$ se, e somente se,

$$h(n) = \sum_{d|n} \mu(n/d)H(d) = \sum_{d|n} \mu(d)H(n/d) \tag{2.7}$$

para todo $n \in \mathbb{N}$.

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

$$H(n) = \prod_{d|n} h(d) \tag{2.8}$$

para todo $n \in \mathbb{N}$ se, e somente se,

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H(n/d)^{\mu(d)} \tag{2.9}$$

para todo $n \in \mathbb{N}$.

Demonstração. Assumindo a igualdade (2.6) e usando o Lema 2.25, temos:

$$\begin{aligned} \sum_{d|n} \mu(n/d)H(d) &= \sum_{d|n} \mu(d)H(n/d) = \sum_{d|n} \mu(d) \sum_{c|(n/d)} h(c) \\ &= \sum_{c|n} \sum_{d|n/c} \mu(d)h(c) = \sum_{c|n} h(c) \sum_{d|(n/c)} \mu(d) = h(n) \end{aligned}$$

para todo $n \in \mathbb{N}$. O inverso é feito por um cálculo semelhante. A demonstração da parte (ii) segue imediatamente da parte (i) se substituírmos as somas por produtos e as multiplicações por potências. □

Teorema 2.27. *O número $N_q(n)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau n é dado por:*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d)q^d = \frac{1}{n} \sum_{d|n} \mu(d)q^{n/d} \tag{2.10}$$

Demonstração. Para demonstrar a identidade (2.10), considere o caso (i) do Teorema 2.26 para o grupo $G = \mathbb{Z}$, e sejam $h(n) = nN_q(n)$ e $H(n) = q^n$, para todo $n \in \mathbb{N}$. Pelo Colorário 2.3, segue que $H(n) = \sum_{d|n} dN_q(d)$. Disso, e por $h(n) = nN_q(n)$, tem-se $H(n) = \sum_{d|n} h(d)$, para todo $n \in \mathbb{N}$. Assim, pelo item (i) do Teorema 2.26, temos:

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

como queríamos demonstrar. □

Exemplo 2.28. *O número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau 20 é dado por:*

$$\begin{aligned} N_q(20) &= \frac{1}{20}(\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q \\ &= \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2) \end{aligned}$$

Note que a fórmula do Teorema 2.27 mostra novamente que para cada corpo finito $\mathbb{F}_q$ e cada $n \in \mathbb{N}$, existem polinômios irredutíveis em $\mathbb{F}_q[x]$ de grau n. De fato, usando $\mu(1) = 1$ e $\mu(d) \geq -1$, para todo $d \in \mathbb{N}$, temos:

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

Teorema 2.29. *Para um corpo K de característica p e $n \in \mathbb{N}$ não divisível por p, o n-ésimo polinômio ciclotômico Q_n sobre K satisfaz:*

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

Demonstração. Para mostrar a identidade acima, considere o item (ii) da fórmula do Teorema 2.26 para um grupo multiplicativo de funções racionais não nulas sobre K, e seja $h(n) = Q_n(x)$ e $H(n) = x^n - 1$, para todo $n \in \mathbb{N}$. Sabendo que $x^n - 1 = \prod_{d|n} Q_d(x)$, temos:

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

Disso, pelo Teorema 2.26 item (ii), segue:

$$Q_n(x) = h(n) = \prod_{d|n} (x^q - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$$

□

Exemplo 2.30. *Para um corpo K onde Q_{12} está definido, temos:*

$$\begin{aligned} Q_{12}(x) &= \prod_{d|12} (x^{12/d} - 1)^{\mu(d)} \\ &= (x^{12} - 1)^{\mu(1)} \cdot (x^6 - 1)^{\mu(2)} \cdot (x^4 - 1)^{\mu(3)} \cdot (x^3 - 1)^{\mu(4)} \cdot (x^2 - 1)^{\mu(6)} \\ &\cdot \quad (x - 1)^{\mu(12)} \\ &= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = \frac{x^{14} - x^{12} - x^2 + 1}{x^{10} - x^6 - x^4 + 1} \\ &= x^4 - x^2 + 1 \end{aligned}$$

Teorema 2.31. *O produto $I(q, n; x)$ de todos os polinômios mônicos irredutíveis*

em $\mathbb{F}_q[x]$ *de grau* n *é dado por:*

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

Demonstração. Considere o Teorema 2.26 parte (ii), e seja $h(n) = I(q,d;x)$ e $H(n) = x^{q^n} - x$, para todo $n \in \mathbb{N}$. Pelo Teorema 2.22 , temos que $x^{q^n} - 1 = \prod_{d|n} I(q,d;x)$. Entao, segue que:

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

e portanto, pelo Teorema 2.26 parte (ii), temos:

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

□

Exemplo 2.32. *Para* $q = 2$, $n = 4$, *temos:*

$$\begin{aligned} I(2,4;x) &= (x^{16} - x)^{\mu(1)} \cdot (x^4 - x)^{\mu(2)} \cdot (x^2 - x)^{\mu(4)} \\ &= \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} \\ &= x^{12} + x^9 + x^6 + x^3 + 1 \end{aligned}$$

Todos os polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau n podem ser determinados pela fatoração de $I(q,n;x)$. Para este propósito, seria interessante que tivéssemos a forma fatorada de $I(q,n;x)$. Isto pode ser feito usando o resultado que segue.

Teorema 2.33. *Seja* $I(q,d;x)$ *como definido no Teorema 2.31. Então, para* $n > 1$, *temos:*

$$I(q,n;x) = \prod_{m} Q_m(x) \tag{2.11}$$

onde o produto percorre todos os divisores positivos m *de* $q^n - 1$ *para o qual* n *é a ordem multiplicativa de* q *módulo* m, *e* $Q_m(x)$ *é o* m*-ésimo polinômio ciclotômico sobre* $\mathbb{F}_q$

Demonstração. Para $n > 1$, seja S um conjunto o elementos de $\mathbb{F}_{q^n}$, todos de grau n sobre $\mathbb{F}_q$. Então, todo $\alpha \in S$ tem um polinômio minimal sobre $\mathbb{F}_q$ de grau n, e portanto é uma raiz de $I(q,n;x)$. Por outro lado, se β é uma raiz de $I(q,n;x)$, então β é uma raiz de uma algum polinômio irredutível em $\mathbb{F}_q[x]$ de grau n, o que implica em $\beta \in S$. Assim,

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

Se $\alpha \in S$, então $\alpha \in \mathbb{F}_{q^n}^*$, e assim a ordem de α nesse grupo multiplicativo é um divisor de $q^n - 1$. Note que $\gamma \in \mathbb{F}_{q^n}^*$ é um elemento de um subcorpo próprio $\mathbb{F}_{q^d}$ de $\mathbb{F}_{q^n}$ se, e so se, $\gamma^{q^d} = \gamma$, isto é, se e somente se, a ordem de γ divide $q^d - 1$. Portanto, a ordem m de um elemento α de S deve ser tal que n é o menor inteiro positivo com $q^n \equiv 1 \pmod{m}$, ou melhor, tal que a ordem multiplicativa de q módulo m. Para um divisor positivo m de $q^n - 1$ com essa propriedade, seja S_m o conjunto de elementos de S de ordem m. Então S é a união disjunta de subconjuntos S_m, de modo que possamos escrever

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

Agora, S_m contém exatamente todos os elementos de $\mathbb{F}_{q^n}^*$ de ordem m. Em outras palavras, S_m é o conjunto dos m-ésimas raízes da unidade sobre $\mathbb{F}_q$. Pela definição de polinômio ciclotômico, segue que,

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

donde segue a identidade 2.11. □

Definição 2.34. *Seja F uma extensão do corpo K. Um elemento $\alpha \in F$ é **algébrico** sobre K se existe um polinômio $f \in K[x]$ não-nulo que tenha α como raiz. Seja $f \in K$ algébrico sobre F. Dentre os polinômios não-nulos em $K[x]$ que tem α como raiz, há aqueles cujo grau é mínimo. Se f é um destes, então multiplicando-o por uma constante adequada obtemos um polinômio mônico. Estas propriedades determinam unicamente f, que chamaremos de **polinômio minimal**.*

Polinômios irredutíveis surgem muitas vezes como o polinômio minimal de elementos em uma extensão de corpos. Para uma referência especial a corpos finitos, resumiremos no resultado a seguir os fatos mais úteis sobre polinômios minimais.

Teorema 2.35. *Seja α um elemento de uma extensão de corpo $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$. Suponha que a ordem de α sobre $\mathbb{F}_q$ é d e que $g \in \mathbb{F}_q[x]$ é polinômio minimal 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 mônico irredutível 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 $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$, e g é polinômio minimal sobre $\mathbb{F}_q$ de todos esses elementos;

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

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

Considere inicialmente os lemas que seguem. As respectivas demonstrações se encontram em [8], pág. 31 e 33.

Lema 2.36. *Se $\alpha \in F$ é algébrico sobre K, então o polinômio minimal g sobre K tem as seguintes propriedades:*

(i) g é irredutível em $K[x]$;

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

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

Lema 2.37. *Seja $\alpha \in \mathbb{F}$ algébrico de grau n sobre K, e seja g o polinômio minimal de α sobre K. Então:*

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

(ii) $[K(\alpha) : K] = n$ e $\{1, \alpha, ..., \alpha^{n-1}\}$ é a base de $K(\alpha)$ sobre K;

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

Agora, usando o Lema 2.36 e o Lema 2.37, podemos demonstrar o Teorema 2.35.

Demonstração. (i) A primeira parte segue diretamente do Lema 2.36(i), e a segunda parte segue do Lema 2.37(iii);

(ii) Segue do Lema 2.36(ii);

(iii) Segue imediatamente do item anterior;

(iv) Segue do Lema 2.36(i) e do Lema 1.13;

(v) A primeira parte segue do item (i) e do Teorema 1.14, e a segunda parte do item (iii);

(vi) Desde que $\alpha \in \mathbb{F}^*_{q^m}$ e $\mathbb{F}^*_{q^d}$ é um subgrupo de $\mathbb{F}^*_{q^m}$, basta usarmos o Teorema 2.3. Assim, segue o que queríamos demonstrar;

(vii) Se g é primitivo sobre $\mathbb{F}_q$, a $ord(g) = q^d - 1$ e então α é de ordem $q^d - 1$ em $\mathbb{F}^*_{q^m}$ pelo item (vi). De modo inverso, se α é de ordem $q^d - 1$ em $\mathbb{F}^*_{q^m}$ e então em $\mathbb{F}^*_{q^d}$, segue α elemento primitivo de $\mathbb{F}_{q^d}$, e portanto g é primitivo sobre $\mathbb{F}_q$ pela definição 2.17. □

Capítulo 3

Polinômios de Permutação

O objetivo deste capítulo é apresentar alguns resultados obtidos em polinômios para os quais as funções associadas a esses polinômios são permutações de corpos finitos. Polinômios desse tipo são chamados de *polinômios de permutação*. Estes polinômios surgiram primeiro no trabalho de Betti [4], Mathieu [9] e Hermite [6] como forma de representar permutações. A determinação de polinômios de permutação não é um problema trivial. Na Seção 3.1 apresentaremos um critério que irá facilitar esta questão: ***Critério de Hermite***. Condições para um polinômio arbitrário ser um polinômio de permutação são bastante complicadas. Dessa forma, na Seção 3.2, será apresentado resultados que trazem tipos especias de polinômios de permutação, e estes serão nosso maior foco de interesse.

3.1 Critérios de Polinômios de Permutação

Um polinômio $f \in \mathbb{F}_q[x]$ é chamado *polinômio de permutação* de $\mathbb{F}_q$ se a função $f : c \mapsto f(c)$ de $\mathbb{F}_q$ em $\mathbb{F}_q$ é uma permutação. Obviamente, se f é um polinômio de permutação de $\mathbb{F}_q$, então a equação $f(x) = a$ tem somente uma solução em $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$. Pela finitude de $\mathbb{F}_q$, a definição de polinômio permutação pode ser expressa de várias outras maneiras como veremos nos resultados que seguem.

Lema 3.1. *O polinômio $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, uma das seguintes afirmações é válida:*

(i) a função $f : c \mapsto f(c)$ é injetora;

(ii) a função $f : c \mapsto f(c)$ é sobrejetora;

(iii) $f(x) = a$ tem uma solução em $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$;

(iv) $f(x) = a$ tem uma única solução em $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$.

Teorema 3.2. *Se $x_0, x_1, ..., x_n$ são $n + 1$ números distintos e f é uma função cujos valores nestes números são dados, então existe um único polinômio $P(x)$ de grau no máximo n com*

$$f(x_k) = P(x_k)$$

para $k = 0, 1, 2, ..., n$. *Este polinômio é dado por:*

$$P(x) = f(x_0)L_{n,0}(x) + ... + f(x_n)L_{n,n}(x) = \sum_{k=0}^{n} f(x_k)L_{n,k}(x)$$

onde, para cada $k = 0, 1, 2, ..., n$,

$$L_{n,k}(x) = \prod_{i=0, i\neq k}^{n} \frac{(x - x_i)}{(x_k - x_i)}$$

Observação 3.3. *Se* $\phi : \mathbb{F}_q \to \mathbb{F}_q$ *é uma função arbitrária, então existe um único polinômio* $g \in \mathbb{F}_q[x]$ *com* $grau(g) < q$ *que representa* ϕ *no sentindo de que* $g(c) = \phi(c)$, *para todo* $c \in \mathbb{F}_q$. *O polinômio* g *pode ser encontrado através do cálculo do* ***Polinômio de Interpolação de Lagrange*** *para uma função* ϕ *dada, ou pela fórmula:*

$$g(x) = \sum_{c\in\mathbb{F}_q} \phi(c)\big(1 - (x - c)^{q-1}\big) \tag{3.1}$$

Se ϕ já é dado como uma função polinomial, a saber $\phi : c \mapsto f(c)$ com $f \in \mathbb{F}_q[x]$, então g pode se obtida de f pela redução módulo $x^q - x$ como veremos no resultado a seguir.

Lema 3.4. *Para* $f, g \in \mathbb{F}_q[x]$, *temos* $f(c) = g(c)$ *para todo* $c \in \mathbb{F}_q$ *se, e somente se,* $f(x) \equiv g(x) \pmod{(x^q - x)}$.

Demonstração. Suponha $f(c) = g(c)$, para todo $c \in \mathbb{F}_q$ e escreva $f(x) - g(x) = h(x) \cdot (x^q - x) + r(x)$, com $h, r \in F_q[x]$ e $grau(r) < q$. Então, segue que $f(c) - g(c) = h(c) \cdot (c^q - c) + r(c)$. Como $c \in \mathbb{F}_q$, temos que $c^q = c$, e assim têm-se $r(c) = 0$ para todo $c \in \mathbb{F}_q$. Disso e pelo fato do $grau(r) < q$, concluímos que, $r(x) \equiv 0$. Logo, $f(x) \equiv g(x) \pmod{(x^q - x)}$. Por outro lado, suponha agora $f(x) - g(x) = h(x) \cdot (x^q - x)$, com $h \in \mathbb{F}_q[x]$. Para todo $c \in \mathbb{F}_q$, temos $c^q = c$ e assim $f(c) - g(c) = h(c) \cdot (c^q - c) = 0$, donde segue $f(c) = g(c)$. □

Observação 3.5. *Seja* F *um corpo e seja* $a \in F$, $a \neq 1$. *Então, segue que:*

$$\sum_{i=0}^{n-1} a^i = \frac{1 - a^n}{1 - a}$$

Vamos agora, estabelecer um critério muito útil, e talvez um dos mais importantes neste trabalho para polinômios de permutação: *Hermite's Criterion*. Esse critério nos permite, através de duas condições, verificar se um dado polinômio $f \in \mathbb{F}_q[x]$ é um polinômio de permutação. Antes, iremos demonstrar o lema abaixo, que será nossa base para esse importante critério.

Lema 3.6. *A sequência* $a_0, a_1, ..., a_{q-1}$ *de elementos de* $\mathbb{F}_q$ *satisfaz* $\{a_0, a_1, ..., a_{q-1}\} =$

$\mathbb{F}_q$ *se, e somente se,*

$$\sum_{i=0}^{q-1} {a_i}^t = \begin{cases} 0, & t = 0, 1, ..., q-2 \\ -1, & t = q-1 \end{cases} \tag{3.2}$$

Demonstração. Para cada $0 \leq i \leq q-1$ considere o polinômio

$$g_i(x) = 1 - \sum_{t=0}^{q-1} {a_i}^t x^{q-1-t}$$

. É fácil ver que, $g_i(a_i) = 1$ para todo $0 \leq i \leq q-1$. Note que temos $g_i(b) = 0$ para todo $b \in \mathbb{F}_q$ com $b \neq a_i$. De fato, supondo $b \neq 0$, temos:

$$\begin{aligned} g_i(b) &= 1 - \sum_{t=0}^{q-1} {a_i}^t \cdot b^{q-1-t} = 1 - \sum_{t=0}^{q-1} {a_i}^t \cdot b^{q-1} \cdot b^{-t} \\ &= 1 - \sum_{t=0}^{q-1} {a_i}^t \cdot b^{-t} = 1 - \sum_{t=0}^{q-1} \left(a_i \cdot b^{-1}\right)^t \\ &= 1 - \frac{1 - (a_i \cdot b^{-1})^q}{1 - (a_i \cdot b^{-1})} = 1 - 1 = 0 \end{aligned}$$

onde esta última igualdade temos pela Observação 3.5. Além disso, $g_i(0) = 0$ sempre que $a_i \neq 0$. Assim, o polinômio,

$$\begin{aligned} g(x) &= \sum_{i=0}^{q-1} g_i(x) = -\sum_{i=0}^{q-1} \left(\sum_{t=0}^{q-1} {a_i}^t x^{q-1-t} \right) \\ &= -\sum_{t=0}^{q-1} \left(\sum_{i=0}^{q-1} {a_i}^t \right) x^{q-1-t} \end{aligned}$$

Note que

$$g(x) = \begin{cases} 1, & x \in \{a_0, a_1, ..., a_{q-1}\} \\ 0, & x \in \mathbb{F}_q \backslash \{a_0, a_1, ..., a_{q-1}\} \end{cases} \tag{3.3}$$

□

Assim, $g(x)$ leva cada elemento de $\mathbb{F}_q$ em 1 se, e somente se, $\{a_0, a_1, ..., a_{q-1}\} = \mathbb{F}_q$. Como $grau(g) < q$, o Lema 3.4 mostra que o polinômio g leva cada elemento de $\mathbb{F}_q$ em 1 se, e somente se, $g(x) = 1$, o que é equivalente a (3.2).

Teorema 3.7. ***Hermite's Criterion****: Seja $\mathbb{F}_q$ um corpo de característica p, p primo. Então $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q[x]$ se, e somente se, as afirmações a seguir são válidas:*

(i) f tem exatamente uma única raiz em $\mathbb{F}_q$;

(ii) Para cada inteiro t com $1 \leq t \leq q-2$ e t não divisível por p, a redução $f(x)^t \pmod{(x^q - x)}$ tem grau $\leq q-2$

Demonstração. Seja f um polinômio permutação. Logo, a afirmação (i) é trivial. Considere que a redução $f(x)^t \pmod{(x^q - x)}$ seja algum polinômio $h(x) = \sum_{j=0}^{q-1} {b_j}^{(t)} x^j$. Temos assim, $f(x)^t - h(x) = L(x) \cdot (x^q - x)$, com $L(x) \in \mathbb{F}_q[x]$. Disso, se $x_0 \in \mathbb{F}_q$, segue $f(x_0)^t - h(x_0) = L(x_0) \cdot ({x_0}^q - x_0) = 0$ e portanto, ${f(x_0)}^t = h(x_0)$. Assim, pelo fato de f ser polinômio de permutação e pela Observação 3.3, segue que:

$$h(x) = \sum_{c \in \mathbb{F}_q} f(c)^t \cdot (1 - (x - c)^{q-1})$$

Logo, $b_{q-1}^{(t)} = -\sum_{c \in F_q} f(c)^t$. Pelo Lema 3.6, segue $b_{q-1}^{(t)} = 0$ para $t = 1, 2, ..., q-2$, e portanto que $grau(h) \leq q - 2$.

Por outro lado, suponha que as afirmações (i) e (ii) sejam válidas. Por (i) temos que existe um único $c \in \mathbb{F}_q$, tal que $f(c) = 0$. Assim, $f(x) \neq 0$ para todo $x \in \mathbb{F}_q$ sempre que $x \neq c$. Então, segue:

$$\forall x \neq c, f(x) \neq 0 \Rightarrow f(x)^{q-1} = 1 \Rightarrow \sum_{c \in \mathbb{F}_q} f(c)^{q-1} = 0 + 1... + 1 = q - 1 = -1$$

Agora, por (ii) temos que, para todo $x \neq c$, $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para $1 \leq t \leq q - 2$, com t não divisível por p. Se caso t for divisível por p, basta considerar $t = t' \cdot p^j$, onde $1 \leq t' \leq q - 2$ e t' não divisível por p. Temos assim,

$$\sum_{c \in \mathbb{F}_q} f(c)^t = \sum_{c \in \mathbb{F}_q} f(c)^{t' p^j} = \left(\sum_{c \in \mathbb{F}_q} f(c)^{t'} \right)^{p^j} = 0$$

Logo, $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$, para todo $1 \leq t \leq q - 2$. Pelo lema anterior, concluímos que f é um polinômio de permutação de $\mathbb{F}_q$. □

Corolário 3.8. *Se $d > 1$ é um divisor de $q - 1$, então não existe um polinômio de permutação de $\mathbb{F}_q$ de grau d.*

Demonstração. Se $f \in \mathbb{F}_q[x]$ com $grau(f) = d$, d um divisor de $q - 1$, então $grau(f^{(q-1)/d}) = q - 1$. Porém, a condição (ii) do *Hermite's Criterion* não é satisfeita para $t = (q - 1)/d$. Logo, f não é um polinômio de permutação de $\mathbb{F}_q$. □

Teorema 3.9. *Seja $\mathbb{F}_q$ um corpo de característica p, p primo. Então $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q[x]$ se, e somente se, as afirmações a seguir são válidas:*

(i) a redução de $f(x)^{q-1} \pmod{(x^q - x)}$ tem grau $q - 1$;

(ii) Para cada inteiro t com $1 \leq t \leq q - 2$ e t não divisível por p, a redução $f(x)^t \pmod{(x^q - x)}$ tem grau $\leq q - 2$

Demonstração. Supondo f um polinômio de permutação, a afirmação (ii) segue do *Hermite's Criterion*. Agora, usando o fato já demonstrado anteriormente que $b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^t$, temos que $b_{q-1}^{(q-1)} = -\sum_{c \in \mathbb{F}_q} f(c)^{q-1}$. Disso, sendo f

polinômio de permutação de $\mathbb{F}_q$, segue que $b_{q-1}^{(q-1)} = 1$, e portanto, tem-se válida a afirmação (i). Por outro lado, suponha agora os itens (i) e (ii). Pelo item (ii) temos $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$, para $1 \leq t \leq q-2$, e por (i) que $\sum_{c\in\mathbb{F}_q} f(c)^{q-1} \neq 0$. Assim, o polinômio

$$g(x) = -\sum_{j=0}^{q-1} \left(\sum_{c\in\mathbb{F}_q} f(c)^{q-1-j} \right) x^j$$

é uma constante não nula. Se f não for um polinômio de permutação de $\mathbb{F}_q$, então deverá existir um $b \in \mathbb{F}_q$ tal que $g(b) = 0$, o que é uma contradição visto que $g(x) \neq 0$ para todo $x \in \mathbb{F}_q$. Logo, segue que f polinômio de permutação de $\mathbb{F}_q$. □

3.2 Tipos Especiais de Polinômios de Permutação

Nesta seção iremos trabalhar alguns exemplos simples de polinômios de permutação que podem ser obtidos atráves dos resultados que seguem.

Teorema 3.10. *(i)Todo polinômio linear sobre $\mathbb{F}_q$ é um polinômio de permutação.*

(ii)O monômio x^n é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $mdc(n, q-1) = 1$

Demonstração. (i)Trivial. (ii) x^n é um polinômio de permutação se, e somente se, a função $c \mapsto c^n$ com $c \in \mathbb{F}_q$ é sobrejetora, o que ocorre se, e só se, $mdc(n, q-1) = 1$. □

Teorema 3.11. *Seja $\mathbb{F}_q$ um corpo de característica p. Então, o p-polinômio, também chamado de polinômio linearizado,*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$$

é um polinômio de permutação de $\mathbb{F}_q$ se, e só se, $L(x)$ tem somente o zero como raiz em $\mathbb{F}_q$.

Demonstração. Temos que $L : c \mapsto L(c)$, com $c \in \mathbb{F}_q$ é um operador linear do espaço vetorial $\mathbb{F}_q$ sobre $\mathbb{F}_q$. Assim, L é injetora se, e somente se, o polinômio $L(x)$ tem apenas o zero como raiz em $\mathbb{F}_q$. □

Outros exemplos podem ser gerados a partir Teorema 3.11, observando que o conjunto de polinômios de permutação é fechado para a composição, isto é, se $f(x)$ e $g(x)$ são ambos polinômios de permutação de $\mathbb{F}_q$, então $f(g(x))$ também será um polinômio de permutação de $\mathbb{F}_q$. No próximo teorema iremos ver uma outra classe de polinômio de permutação.

Teorema 3.12. *Seja $r \in \mathbb{N}$ com $mdc(r, q-1) = 1$ e s um inteiro positivo divisor de $q-1$ e $g \in \mathbb{F}_q[x]$. Se g é tal que $g(x^s)$ não possua raiz diferente de zero em $\mathbb{F}_q$, então*

$$f(x) = x^r(g(x^s))^{(q-1)/s}$$

é um polinômio de permutação de $\mathbb{F}_q$.

Demonstração. Para demonstrar esse teorema, basta mostrarmos que f satisfaz as condições (i) e (ii) do *Hermite's Criterion*. Para provar (i), suponha que f possua duas raízes distintas, a saber, a e b. Disso, temos que $0 = f(a) = a^r(g(a^s))^{(q-1)/s}$ e $0 = f(b) = b^r(g(b^s))^{(q-1)/s}$. Logo, f possui uma única raiz em $\mathbb{F}_q$. Para provar (ii), tome $t \in \mathbb{Z}$ com $1 \leq t \leq q-2$ e suponha primeiramente que s não divida t. Note que $f(x)^t$ é uma soma de termos cujos expoentes são da forma $rt + ms$, com $m \in \mathbb{Z}$ e $m \geq 1$. Temos por hipótese que $mdc(r, q-1) = 1$ e $s \mid q-1$, segue $mdc(r, s) = 1$. Disso, os expoentes da forma $rt + ms$ não são divisíveis por s, e portanto não divisível por $q-1$. Consequentemente, a redução de $f(x)^t \pmod{(x^q - x)}$ tem $grau \leq q-2$. Agora, se $t = ks$, $k \in \mathbb{Z}$, então $f(x)^t = x^{rt}(g(x^s))^{(q-1)k}$. Se $h(x) = x^{rt}$, temos $f(c)^t = h(c)$ para $c \in \mathbb{F}_q^*$ desde que $g(c^s) \neq 0$, e também que $f(0)^t = h(0)$. Entao, pelo Lema 3.4, temos $f(x)^t \equiv x^{rt} \pmod{(x^q - x)}$ e como rt não é divisível por $q-1$ segue que a redução $f(x)^t \pmod{(x^q - x)}$ tem $grau \leq q-2$. Logo, segue o item (ii). □

Do que se observou após o Teorema 3.11, segue em particular que se $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ e $b, c, d \in \mathbb{F}_q$ com $c \neq 0$, então $f_1(x) = cf(x+b) + d$ é novamente um polinômio de permutação de $\mathbb{F}_q$. Escolhendo b, c, d adequadamente, podemos obter f_1 na forma normalizada, isto é, f_1 é mônico, $f_1(0) = 0$ e quando o grau n de f nao for divisível pela característica de $\mathbb{F}_q$, o coeficiente de x^{n-1} é 0. Basta, portanto, estudar apenas os polinômios de permutação normalizados.

Definição 3.13. *Seja $\mathbb{F}_q$ um corpo finito de $p = q^n$ elementos. Para um inteiro $n \geq 1$ e um parâmetro a em $\mathbb{F}_q$, o n-ésimo **polinômio de Dickson** do primeiro tipo $D_n(x, a) \in \mathbb{F}_q$ é definido por:*

$$D_n(x, a) = \sum_{i=0}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

Teorema 3.14. *O polinômio de Dickson $D_n(x, a)$, $a \in \mathbb{F}_q^*$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $mdc(n, q^2 - 1) = 1$.*

Demonstração. Vide pág. 356 em [8] □

Capítulo 4

Caracterização de Polinômios de Permutação

4.1 Introdução

Neste capítulo, faremos um estudo do artigo *Some families of permutation polynomials over finite fields* [11]. Nosso foco principal será a demonstração da Proposição 4.3. Este resultado irá nos fornecer 5 condições necessárias e suficientes para um polinômio da forma $f(x) := x^r h_k(x^v)^t$ permutar $\mathbb{F}_q$, onde $h_k(x) = x^{k-1} + x^{k-2} + ... + x + 1$ com r, v, k, t inteiros positivos. Nos resultados deste capítulo, usaremos as seguintes notações: $s = mdc(v, q-1)$, $d = (q-1)/s$, $e = v/s$ e μ_d é o conjunto das d-ésimas raízes primitivas da unidade em $\mathbb{F}_q$.

4.2 Resultados

Começaremos com um lema que reduz a pergunta de se um dado polinômio f permuta $\mathbb{F}_q$ a questão de se um dado polinômio relacionado permuta um subgrupo particular de $\mathbb{F}_q$, que nesse caso iremos ver que se trata do conjunto μ_d, conjunto das d-ésimas raíses da unidade.

Lema 4.1. *Escolha $d, r > 0$ com $d \mid (q-1)$, e seja $h \in \mathbb{F}_q[x]$. Então $f(x) = x^r h(x^{(q-1)/d})$ permuta $\mathbb{F}_q$ se, e só se:*

(i) $mdc(r, (q-1)/d) = 1$,

(ii) $x^r h(x)^{(q-1)/d}$ *permuta* μ_d.

Demonstração. Escreva $s = q - 1/d$.
($\Rightarrow$) Seja $\zeta \in \mu_s$. Note que $f(\zeta x) = \zeta^r f(x)$ para qualquer $r \in \mathbb{Z}$. Suponha que $mdc(r, s) = k \neq 1$. Disso, segue $r = kl$ e $s = kt$ para $l, t \in \mathbb{Z}$. Observe que $f(\zeta^A x) = \zeta^{Ar} f(x)$, para todo $A \in \mathbb{Z}$. Tome, $A = s/k$ e $\mu_s = \langle \zeta \rangle$. Disso, têm-se:

$$f(\zeta^A x) = \zeta^{\frac{s}{k} r} f(x) = (\zeta^s)^{\frac{r}{k}} f(x) = f(x)$$

Como f permuta $\mathbb{F}_q$, concluímos que $\zeta^A x = x$. Disso, segue $\zeta^A = 1$, o que contradiz o fato de ζ ser de ordem s. Portanto, $mdc(r,s) = 1$, e assim fica provado o item (i).

Agora, provemos o item (ii). Note que

$$f(x)^s = x^{rs} h(x^s)^s = g(x^s) \tag{4.1}$$

para todo $x \in \mathbb{F}_q$. Assim, $\{f(x)^s : x \in \mathbb{F}_q\} = \{g(x) : x \in (\mathbb{F}_q)^s\}$. Sabemos que $\mathbb{F}_q^* = \langle a \rangle$. Assim,

$$(\mathbb{F}_q^*)^s = \langle a^s \rangle = \langle a^{\frac{q-1}{d}} \rangle = \mu_d$$

Por (4.1), $g(\mu_d) \subset \mu_d$. Consequentemente, provar o item (ii) é equivalente a provar que g é injetiva. Então, seja $g(x^s) = g(y^s)$, para $x^s, y^s \in \mu_d$. Assim,

$$f(x)^s = f(y)^s \Rightarrow f(x) = f(y)\zeta, \tag{4.2}$$

onde $\zeta \in \mu_s$. Como $mdc(r,s) = 1$, existem $\lambda, \mu \in \mathbb{Z}$ tal que $\lambda r + \mu s = 1$. Disso, $\zeta = \zeta^{\lambda r + \mu s} = \zeta^{\lambda r}$. Como já visto anteriormente, $f(\zeta^\lambda y) = \zeta^{\lambda r} f(y) = \zeta f(y)$. Por (4.2), $f(\zeta^\lambda y) = f(x)$. Como f permuta $\mathbb{F}_q$, segue $\zeta^\lambda y = x$ e portanto temos $x^s = y^s$. Concluímos a partir disso que g é injetiva, donde segue o item (ii).
($\Leftarrow$) Suponha válido (i) e (ii). Queremos provar que f permuta $\mathbb{F}_q$. Assim, seja $f(x) = f(y)$ para $x, y \in \mathbb{F}_q$, $f(x) \neq 0$. Desde que $x, y \neq 0$, temos:

$$f(x)^s = f(y)^s \Rightarrow g(x^s) = g(y^s) \Rightarrow x^s = y^s \Rightarrow x = \zeta y,$$

para algum $\zeta \in \mu_s$. Como observado, $f(\zeta y) = \zeta^r f(y)$. Consequentemente, $f(x) = \zeta^r f(y)$. Disso, e por (4.2), temos $\zeta^r = 1$. Por (i), existem $\lambda, \mu \in \mathbb{Z}$ tal que $\lambda r + \mu s = 1$. Como consequência, $\zeta = \zeta^{\lambda r + \mu s} = 1$. Portanto, $x = y$. Acabamos de provar que, se $f(x) = f(y)$, com $x, y \in \mathbb{F}_q$ e $f(x) \neq 0$, então $x = y$. Agora, considere $f(x) = f(y) = 0$. Queremos provar que $x = y = 0$. Suponha $x \neq 0$. Consequentemente, $x^s \in \mu_d$. Disso, $0 = f(x)^s = g(x^s) \in \mu_d$, o que é um absurdo. Logo, $x = 0$, e fica provado que, se $f(x) = f(y) = 0$, então $x = y = 0$. Por fim, temos g injetiva, donde segue que f permuta $\mathbb{F}_q$. □

No próximo resultado, iremos provar uns casos mais fáceis para um valor pequeno de d: $d = 1$ e $d = 2$.

Proposição 4.2. *Se $d = 1$, então $f(x)$ permuta $\mathbb{F}_q$ se, e somente se, $mdc(k,p) = mdc(r,s) = 1$. Se $d = 2$ então $f(x)$ permuta $\mathbb{F}_q$ se, e somente se, $mdc(k,2) = mdc(r,s) = 1$ e $k^{st} \equiv (-1)^{r+1} \pmod{p}$.*

Demonstração. (*Caso 1:* $d = 1$)
($\Rightarrow$) Pelo Lema 4.1, temos $mdc(r,s) = 1$ e $g(x) = x^r h(x)^s$, com $h(x) = h_k(x^e)^t$ permuta μ_d. Se $d = 1$, então $\mu_d = \{1\}$. Disso, $1 = g(1) = 1^r h(1)^{st} = k^{st}$. Assim sendo, $mdc(k,p) = 1$, onde p é a característica de $\mathbb{F}_q$.
($\Leftarrow$) Suponha $mdc(r,s) = mdc(k,p) = 1$. Seja $g(x) = x^r h(x)^s$ com $h(x) = h_k(x^e)^t$. Como acima, $g(1) = k^{st} \neq 0$ e $mdc(k,p) = 1$. Consequentemente, $g(k^{st})^d = k^{(q-1)t} = 1$, o que implica em g permutar μ_d. Pelo Lema 4.1, segue que f permuta $\mathbb{F}_q$.
(*Caso 2:* $d = 2$)

($\Rightarrow$) Pelo Lema 4.1, $g(x) = x^r h_k(x^e)^{st}$ permuta μ_d. Note que $\mu_d = \mu_2 = \{1, -1\}$ e $g(-1) = (-1)^r h_k((-1)^e)^{st}$. Como g permuta μ_d, $g(-1) \neq 0$. Sabemos que $mdc(v, q-1) = s$, $d = (q-1)/s$ e $e = v/s$. Como $d = 2$, temos $s = (q-1)/2$. Suponha e número par. Assim, $e = 2l$ para algum $l \in \mathbb{Z}$. Portanto, $\frac{2v}{q-1} = 2l$, e então, $v = (q-1)l$, o que resulta em $mdc(v, q-1) = q-1 = s$, uma contradição com fato de $s = (q-1)/2$. Logo e é ímpar, e então, $h_k((-1)^e) = h_k(-1)$. Se k é par, então $h_k(-1) = 0$. Como consequência $g(-1) = 0$, o que é uma contradição. Segue então k ímpar, com $h_k(-1) = 1$. Disso, temos $g(-1) = (-1)^r$.Observe que, $g(-1) = (1)^r h_k(1^e)^{st} = k^{st}$. Como g permuta μ_2 e $g(-1) = (-1)^r$, temos $g(-1) = k^{st} = (-1)^{r+1} \pmod p$.
($\Leftarrow$) Suponha $mdc(k, 2) = mdc(r, s) = 1$ e $k^{st} \equiv (-1)^{r+1} \pmod p$. Pelo Lema 4.1, é suficiente mostrar que $g(x) = x^r h_k(x^e)^{st}$ permuta μ_2. Como observado, $g(1) = k^{st} \equiv (-1)^{r+1} \pmod p$, o que implica em $g(1) \in \mu_2$. Sendo $mdc(k, 2) = 1$, têm-se $h_k(-1) = 1$. Como feito já anteriormente, $g(-1) = (-1)^r \in \mu_2$. Então, g permuta μ_2, e pelo Lema 4.1, f permuta $\mathbb{F}_q$. □

Poderíamos provar para mais alguns valores de d usando o mesmo método acima, mas isso requer trabalhar com vários casos para $d = 3$. Retornaremos a essa questão mais tarde na Proposição 4.4 depois de provar alguns resultados que simplificam a análise. O próximo resultado que apresentaremos, fornece condições necessárias e suficientes para f permutar $\mathbb{F}_q$; essas condições refinam as que obtemos diretamente do Lema 4.1.

Proposição 4.3. *$f(x) = x^r h_k(x^s)$ permuta $\mathbb{F}_q$ se, e somente se, as seguintes afirmações são válidas:*

(i) $mdc(r, s) = mdc(d, k) = 1$

(ii) $mdc(d, 2r + vt(k-1)) \leq 2$

(iii) $k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod p$

(iv) $g(x) := x^r((1-x^{ke})/(1-x^e))^{st}$ *é injetiva no* $\mu_d \setminus \mu_1$

(v) $(-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1)$.

Demonstração. ($\Rightarrow$) (i) Suponha que f permuta $\mathbb{F}_q$. Iremos provar que as cinco condições da proposição são válidas. Pelo Lema 4.1, $mdc(r, s) = 1$ e $\hat{g}(x) = x^r h_k(x^e)^{st}$ permuta μ_d. Lembremos que $h_k(x) = x^{k-1} + x^{k-2} + ... + x + 1$ e $\hat{g}(x^s) = f(x)^s$ para todo $x \in \mathbb{F}_q$. Sabemos que $mdc(e, d) = 1$, e como consequência temos $\mu_d \cap \mu_e = \{1\}$. Note que

$$g(\xi) = \hat{g}(\xi) = \xi^r \left(\frac{1 - \xi^{ke}}{1 - \xi^e} \right)^{st}$$

para todo $\xi \in \mu_d \setminus \mu_1$. Suponha $mdc(d, k) = a > 1$. Seja $\mu_d = \langle \xi \rangle$. Portanto,

$\xi^{d/a} \neq 1$. Observe que:

$$(\xi^{d/a})^k = (\xi^d)^{\frac{k}{a}} = 1 \quad \Rightarrow \quad \xi^{d/a} \in \mu_k \subset \mu_{ke} \tag{4.3}$$
$$\Rightarrow \quad \hat{g}(\xi^{d/a}) = 0 \tag{4.4}$$
$$\Rightarrow \quad \hat{g}(\xi^{d/a}) \notin \mu_d \tag{4.5}$$

Pelo Lema 4.1, $\hat{g}$ permuta μ_d, donde temos uma contradição com (4.5). Portanto, $mdc(d,k) = 1$. Dessa forma, fica provado o item (i).

(ii) Se $d \leq 2$, o item (ii) claramente é válido. Assuma então, $d \geq 3$. Assim, existe $\zeta \in \mu_d$ tal que $\zeta^2 \neq 1$. Consequentemente, $\zeta, \zeta^2 \in \mu_d$ e $\zeta \neq \frac{1}{\zeta}$. Observe que:

$$\hat{g}(1/\zeta) = \frac{1}{\zeta^r}\left(\frac{\zeta^{ke}-1}{\zeta^e-1}\frac{\zeta^e}{\zeta^{ke}}\right)^{st} \tag{4.6}$$
$$= \zeta^r\left(\frac{\zeta^{ke}-1}{\zeta^e-1}\right)^{st}\zeta^{-((k-1)est+2r)} \tag{4.7}$$
$$= \hat{g}(\zeta)\cdot\zeta^{-((k-1)est+2r)} \tag{4.8}$$
$$= \frac{\hat{g}(\zeta)}{\zeta^\delta} \tag{4.9}$$

onde $\delta = 2r + (k-1)vt$.
Suponha $mdc(\delta, d) = B > 2$. Sabemos que $\mu_d = \langle\chi\rangle$. Então, $\chi^{d/B} \in \mu_d$. Se $(\chi^{d/B})^2 = 1$, então $\frac{2d}{B} \equiv 0 \pmod{d}$. Disso, segue que B divide 2, o que é uma contradição. Então, $\zeta = \chi^{d/B} \in \mu_d \setminus \mu_2$ e temos:

$$\zeta^\delta = \left(\chi^{d/B}\right)^\delta = \left(\chi^d\right)^{\delta/B} = 1$$

Por (4.9), $\hat{g}(1/\zeta) = \hat{g}(\zeta)$, o que contradiz o fato de $\hat{g}$ permutar μ_d. Assim, segue que $mdc(2r + (k-1)vt, d) \leq 2$, e portanto temos válido o item (ii).

(iii) Sabemos que $\hat{g}$ permuta μ_d. Suponha $\mathbb{F}_q^* = \langle a\rangle$ e $\mu_d = \langle\xi\rangle$, com $\xi = a^{\frac{q-1}{d}}$. Então:

$$\prod_{\xi\in\mu_d}\hat{g}(\xi) = \prod_{i=1}^{d}\xi^i = \xi^{\frac{d(d+1)}{2}} = \left(a^{\frac{q-1}{d}}\right)^{\frac{d(d+1)}{2}} = \left(a^{\frac{q-1}{2}}\right)^{d+1} = (-1)^{d+1} \tag{4.10}$$

Defina $F : \mu_d \to \mu_d$ com $F(a) = a^k$. Como $mdc(d,k) = 1$, F é bijetora. Portanto,

$$\prod_{\xi\in\mu_d\setminus\mu_1}(1-\xi^{ke}) = \prod_{\xi\in\mu_d\setminus\mu_1}(1-\xi^e) \Rightarrow \prod_{\xi\in\mu_d\setminus\mu_1}\frac{1-\xi^{ke}}{1-\xi^e} = 1$$

Como observado,

$$\prod_{\xi\in\mu_d\setminus\mu_1}\xi^r = (-1)^{(d+1)r}$$

Portanto,

$$\prod_{\xi\in\mu_d}\hat{g}(\xi)=\hat{g}(1)\prod_{\xi\in\mu_d\setminus\mu_1}\hat{g}(\xi)=k^{st}(-1)^{(d+1)r} \tag{4.11}$$

Por (4.10) e (4.11), $k^{st}(-1)^{(d+1)r}\equiv(-1)^{(d+1)} \pmod p$. Portanto, $k^{st}\equiv(-1)^{(d+1)(r+1)} \pmod p$

(iv) Como observado anteriormente, $\hat{g}(\xi)=g(\xi)$, para todo $\xi\in\mu_d\setminus\mu_1$. Como $\hat{g}$ é injetiva em μ_d, g é injetiva em $\mu_d\setminus\mu_1$.

(v) Sabemos que $\hat{g}$ permuta μ_d. Portanto, $\hat{g}(1)\notin\hat{g}(\mu_d\setminus\mu_1)$. Consequentemente, $k^{st}\notin\hat{g}(\mu_d\setminus\mu_1)=g(\mu_d\setminus\mu_1)$. Pelo item (iii), $(-1)^{(d+1)(r+1)}\equiv k^{st} \pmod p$. Portanto, $(-1)^{(d+1)(r+1)}\notin g(\mu_d\setminus\mu_1)$.

($\Leftarrow$) Suponha as cinco condições da proposição válidas. Queremos mostrar que f permuta $\mathbb{F}_q$. Lembremos que $\hat{g}(a)=g(a)$ para todo $a\in\mu_d\setminus\mu_1$. Além disso, é claro ver que $\hat{g}(\mu_d)\subset\mu_d$. Pelo item (iv), $\hat{g}$ é injetiva em $\mu_d\setminus\mu_1$. Temos também que $\hat{g}(1)=k^{st}$. Pelo item (iii) e (v), $\hat{g}(1)\notin\hat{g}(\mu_d\setminus\mu_1)=g(\mu_d\setminus\mu_1)$. Portanto, $\hat{g}$ é injetiva em μ_d o que implica em g permutar μ_d. Pelo Lema 4.1, temos que f permuta $\mathbb{F}_q$. □

O fato de $k^{st}\equiv(-1)^{(d+1)(r+1)} \pmod p$ foi provado por Park e Lee [10](caso $t=1$). O caso $t=1$ na Proposição 4.3 melhora o resultado de [3]; os autores deram algumas condições necessárias para f permutar $\mathbb{F}_q$, e algumas condições suficientes para o caso especial de d ser um primo ímpar menor que $2p+1$.

Quando d for um primo ímpar, o critério usado na Proposição 4.3 pode ser feito em termos da permutação de $\mathbb{F}_d$:

Corolário 4.4. *Suponha que as três primeiras condições da Proposição 4.3 sejam válidas, e tome d um primo ímpar. Escolha $w\in\mathbb{F}_q$ de ordem d. Então f permuta $\mathbb{F}_q$ se, e somente se, existe $\theta\in\mathbb{F}_d[x]$ com $\theta(0)=0$ e $grau(\theta)<(d-1)/2$ tal que $(2r+(k-1)vt)x+\theta(x^2)$ permuta $\mathbb{F}_d$ e, para todo i, com $0<i<d/2$, temos:*

$$w^{\theta(i^2)}=\left(\frac{w^{ike}-w^{-ike}}{w^{ie}-w^{-ie}}\right)^{st}$$

Demonstração. Suponha que as três primeiras condições da Proposição 4.3 sejam válidas, e tome d um primo ímpar. Como já foi observado, $\mu_d=\{x^2\mid x\in\mu_d\}$. Assim, a injetividade de $g(x^2)$ em $\mu_d\setminus\mu_1$ é equivalente a condição (iv) da

proposição anterior. Para $\zeta \in \mu_d \setminus \mu_1$, temos:

$$\begin{aligned} g(\zeta^2) &= \zeta^{2r}\left(\frac{1-\zeta^{2ke}}{1-\zeta^{2e}}\right)^{st} \\ &= \zeta^{2r}\zeta^{(k-1)est}\left(\frac{1-\zeta^{2ke}}{1-\zeta^{2e}}\right)^{st}\frac{1}{\zeta^{(k-1)est}} \\ &= \zeta^{2r+(k-1)est}\left(\frac{1-\zeta^{2ke}}{1-\zeta^{2e}}\cdot\frac{\zeta^{-ke}}{\zeta^{-e}}\right)^{st} \\ &= \zeta^{2r+(k-1)est}\left(\frac{\zeta^{ke}-\zeta^{-ke}}{\zeta^{e}-\zeta^{-e}}\right)^{st} \end{aligned}$$

Agora, suponha $\mu_d = \langle w \rangle$. Então, $w^{2i} \in \mu_d$ e

$$g(w^{2i}) = w^{i(2r+(k-1)est)}\left(\frac{w^{ike}-w^{-ike}}{w^{ie}-w^{-ie}}\right)^{st}$$

Note que $g(w^{2i}) \in \mu_d$. Logo,

$$g(w^{2i})\cdot w^{-i(2r+(k-1)est)} = \left(\frac{w^{ike}-w^{-ike}}{w^{ie}-w^{-ie}}\right)^{st} \in \mu_d$$

Como $\hat{g} = g$ em $\mu_d \setminus \mu_1$, para cada $i \in \mathbb{Z} \setminus d\mathbb{Z}$, existe e é único $\psi(i) \in \mathbb{Z}_d$ tal que

$$w^{\psi(i)} = \left(\frac{w^{ike}-w^{-ike}}{w^{ie}-w^{-ie}}\right)^{st}$$

Definindo $\psi(i) = 0$ se $i \in d\mathbb{Z}$, segue que ψ induz uma função de $\mathbb{Z}_d$ para $\mathbb{Z}_d$ com as seguinte propriedades: $\psi(i) = \psi(-i)$ e $g(w^{2i}) = w^{i(2r+(k-1)est)+\psi(i)}$.

Afirmação: (iv) e (v) da Proposição 4.3 são válidas se, e somente se, $\chi : i \mapsto in + \psi(i)$ em $\mathbb{Z}_d$, onde $n := 2r + (k-1)vt$ é bijetiva.
($\Rightarrow$) Seja $i, j \in \mathbb{Z}_d \setminus 0$ com $i \neq j$. Como d é ímpar, $2i \neq 2j$. Além disso, sendo g injetiva em $\mu_d \setminus \mu_1$, temos que $g(w^{2i}) \neq g(w^{2j})$. Lembrando que $\mu_d = \langle w \rangle$, segue:

$$\begin{aligned} w^{in+\psi(i)} \neq w^{jn+\psi(j)} &\Rightarrow in + \psi(i) \neq jn + \psi(j) \pmod d \\ &\Rightarrow \chi(i) \neq \chi(j) \pmod d \end{aligned}$$

Suponha $\chi(i) = 0$. Queremos mostrar que $i = 0 \in \mathbb{Z}_d$. Caso contrário, supondo $i \neq 0$, temos:

$$\chi(i) = in + \psi(i) = 0 \Rightarrow g(w^{2i}) = w^{in+\psi(i)} = w^0 = 1 \in \mu_1$$

Desde que $i \neq 0$, tem-se $w^{2i} \neq 1$. Além disso, $1 = (-1)^{(d+1)(r+1)} = g(w^{2i}) \in g(\mu_d \setminus \mu_1)$, o que é contradiz (v) na Proposição 4.3. Assim, $i = 0$, e segue χ bijetora.
($\Leftarrow$). Suponha que χ seja bijetiva. Desde que $\chi(0) = 0$, temos que $\chi(i) \neq 0$ para todo $i \in \mathbb{Z}_d \setminus 0$. Portanto, $in + \psi(i) \neq 0$ para todo $i \in \mathbb{Z}_d \setminus 0$. Disso, resulta que $g(w^{2i}) = w^{in+\psi(i)} \neq 1 = (-1)^{(d+1)(r+1)}$. Segue, $(-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1)$, donde

temos o item (v) válido. Agora, temos $\chi(i) \neq \chi(j)$ para todo $i, j \in \mathbb{Z}_d \setminus 0$ com $i \neq j$. Assim,

$$in + \psi(i) \neq jn + \psi(j) \Rightarrow g(w^{2i}) \neq g(w^{2j})$$

o que implica que g injetiva em $\mu_d \setminus \mu_1$. Disso, segue válido o item (iv). Concluímos por fim, que a afirmação é verdadeira.

Agora, desde que $\psi(i) = \psi(-i)$, escrevamos $\psi(i) = \theta(i^2)$. Pelo *Teorema da Interpolação de Lagrange*, existe um polinômio $\theta \in \mathbb{F}_q[x]$, passando pelos pontos $\{(i^2, \psi(i)) : i \in \mathbb{Z}_d\}$. Como este conjunto possui $(d-1)/2$ elementos, temos que o grau de θ é no máximo $(d-1)/2$. Temos assim, $xn+\theta(x^2)$ polinômio permutação de $\mathbb{F}_d[x]$. Note que, $grau(xn+\theta(x^2)) = 2 \cdot grau(\theta)$. Se $grau(\theta) = (d-1)/2$, então $grau(xn + \theta(x^2)) = d - 1$, o que contradiz o *Hermite's Criterion* (Teorema 3.7). Logo, o grau de θ é menor que $(d-1)/2$. Além disso, $\theta(0) = 0$.
Como já visto anteriormente,

$$w^{\psi(i)} = \left(\frac{w^{ike} - w^{-ike}}{w^{ie} - w^{-ie}}\right)^{st} \Rightarrow w^{\theta(i^2)} = \left(\frac{w^{ike} - w^{-ike}}{w^{ie} - w^{-ie}}\right)^{st}$$

para todo i, com $0 < i < \frac{d}{2}$
Por outro lado, suponha que exista $\theta \in \mathbb{F}_d[x]$ com $\theta(0) = 0$ e $grau(\theta) < (d-1)/2$ tal que, $nx + \theta(x^2)$ permuta $\mathbb{F}_d$ e

$$w^{\psi(i)} = \left(\frac{w^{ike} - w^{-ike}}{w^{ie} - w^{-ie}}\right)^{st}$$

para todo i, com $0 < i < \frac{d}{2}$. Defina, $\psi(i) = \theta(i^2)$. Temos que $\mathbb{F}_d$ e $\mathbb{Z}_d$ são isomoformos. Disso, e pelo fato de $nx + \theta(i^2)$ permutar $\mathbb{F}_d$, χ definida por $\chi(i) = in + \psi(i)$, para todo $i \in \mathbb{Z}_d$, é bijetiva. Então, a existência de θ como mencionado na proposição, garante a validade de (iv) e (v) na Proposição 4.3. Portanto, f permutar $\mathbb{F}_q$ é equivalente a existência de θ como mencionado na proposição. □

Para um pequeno d, todas essa funções $\hat{\theta} : \mathbb{F}_d \to \mathbb{F}_d$ ocorrem para o qual $x + \hat{\theta}(x^2)$ permuta $\mathbb{F}_d$; isso, por sua vez, gera descrições gerenciáveis dos possíveis polinômios de permutação nesses casos. Assumindo $\hat{\theta}(0) = 0$ $grau(\hat{\theta}) < (d-1)/2$, a única função para $d = 3$ e $d = 5$ é $\hat{\theta} = 0$. Para $d = 7$ existem três possibilidades para $\hat{\theta}$, a saber, $\hat{\theta} = \mu x^2$ com $\mu \in \{0, 2, -2\}$. Para $d = 11$, existem 25 possibilidades para $\hat{\theta}$, mas estes compreendem apenas cinco classes de equivalência $\hat{\theta}(x) \sim \hat{\theta}(\alpha^2 x)/a$ com $\alpha \in \mathbb{F}_d^*$. Para $d = 13$ existem 133 possibilidades para θ, incluindo 14 classes acima. Nós verificamos via computador que, para esses valores de d, todos essas funções $\hat{\theta}$ ocorre como $\theta/(2r + (k-1)vt)$ para algum polinômio de permutação de f como no Colorário 3.7, mesmo se restringirmos a $k = 2$ e $t = e = 1$.

Corolário 4.5. *Suponha as três primeiras condições da Proposição 4.3 válidas, e seja d um primo ímpar. Escolha $w \in \mathbb{F}_q$ de ordem d.*

(a) Se

$$\frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \in \mu_{st} \tag{4.12}$$

para todo $\zeta \in \mu_d \setminus \mu_1$, então f permuta $\mathbb{F}_q$.

(b) Se $d = 3$ então f sempre permuta $\mathbb{F}_q$.

(c) Se $d = 5$ então f permuta $\mathbb{F}_q$ se, e somente se, (4.12) é satisfeita.

(d) Se $d = 7$ então f permuta $\mathbb{F}_q$ se, e somente se, ou (4.12) é satisfeita ou existem $\epsilon \in \{1, -1\}$ tal que

$$\left(\frac{w^{ike} - w^{-ike}}{w^{ie} - w^{-ie}}\right)^{st} = w^{2\epsilon(2r+(k-1)vt)i}$$

para todo $i \in \{1, 2, 4\}$

(e) Se $d = 11$ então f permuta $\mathbb{F}_q$ se, e somente se, ou (4.12) é satisfeita ou existe algum $\psi \in \tau$, tal que:

$$\left(\frac{w^{ike} - w^{-ike}}{w^{ie} - w^{-ie}}\right)^{st} = w^{(2r+(k-1)vt)\psi(i)}$$

para todo $i \in (\mathbb{F}_{11}^*)^2$, onde τ é a união dos conjuntos $\{mi : m \in \{\pm 3, \pm 5\}\}$, $\{5m^3i^4 + m^7i^3 - 2mi^2 - 4m^5i : m \in \mathbb{F}_{11}^*$ e $\{4m^3i^4 + m^7i^3 - 2mi^2 - 5m^5i : m \in \mathbb{F}_{11}^*$.

Demonstração. (a) Vamos manter a notação do Colorário 4.4. A condição (4.12) é um caso tivial de $\theta = 0$. Sendo d primo ímpar, têm-se $mdc(d, n) = 1$. Portanto, nx permuta $\mathbb{F}_d$. Como resultado, a condição (4.12) é o mesmo que escolher $\theta = 0$ no Colorário 3.6, e assim, f permuta $\mathbb{F}_q$.
(b) Se $d = 3$ ou $d = 5$, como já comentado anteriormente, podemos verificar através de uma pequena lista de polinômios de permutação de interesse. De fato, Betti [4] em 1851 verificou que $\theta = 0$ é a escolha certa. O caso $d = 3$, pode-se abordar de diferentes maneiras. Na Proposição 3.6, a condição (iii), implica em $k^{st} \equiv \pm 1 \pmod 3$. Portanto,

$$\zeta^k - \zeta^k = \pm\left(\zeta - \zeta^{-1}\right) \tag{4.13}$$

Como $d = 3$, $s = (q-1)/3$. Disso, resulta que ou q é par, ou s é par. Portanto,

$$\zeta^k - \zeta^k = \left(\zeta - \zeta^{-1}\right) \tag{4.14}$$

Assim, (4.12) é válida, e pelo item (a), segue que f permuta $\mathbb{F}_q$.

Se $d = 7$, então $mdc(7, n) = 1$ pela condição (ii) da Proposição 4.3. Como dito antes, podemos determinar uma lista de polinômios de grau adequado e fica

fácil calculá-los através do computador se dado polinômio satisfaz as condições do Colorário 4.4. De fato, Hermite [6] em 1863, computou que $\theta = \mu x^2$ onde $\mu \in \{0, 2n, -2n\}$ era válido para o propósito. O caso $d = 11$ é tratado de forma similar fazendo cálculos sobre possíveis polinômios. □

Considerações Finais

O presente trabalho, baseado na conceito de Polinômios de Permutação, forneceu condições necessárias e suficientes para um polinômio da forma $x^r(1+x^v+x^{2v}+...+x^{kv})^t$ permutar os elementos de um corpo finito $\mathbb{F}_q$.

Além disso, o Lema 4.1 nos forneceu como resultado algo gradioso: a pergunta de se um dado polinômio f permuta $\mathbb{F}_q$, pode ser reduzida a questão de se um dado polinômio relacionado permuta um subgrupo particular de $\mathbb{F}_q$, que nesse caso vimos ser o conjunto das d-ésimas raízes da unidade (μ_d).

Referências Bibliográficas

[1] Akbary, A.; Wang, Q. *A generalized Lucas sequence and permutation binomials,* Proc. Amer. Math. Soc. 134 (2006), no. 1, 15 - 22.

[2] Akbary, A.; Wang, Q. *On some permutation polynomials over finite fields,* Int. J. Math. Sci. 2005, no. 16, 2631–2640.

[3] Akbary, A.; Wang, Q.; Alaric S. *On some classes of permutation polynomials,* Int. J. Number Theory, to appear, Vol 04, no. 01, pp. 121–133 (2008)

[4] Betti, E. *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo,* Ann. Sci. Mat. Fis, 2 (1851) 5-19, (Opere Matematiche, v.1,17-27).

[5] Dickson, E.L. *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group,* Ann. of Math, 11 (1–6) (1896/97) 161–183.

[6] Hermite, C. *Sur les fonctions de sept lettres,* C. R. Acad. Sci, Paris 57 (1863) 750–757.

[7] Herstein, I.N. *Topics in Algebra,* 3 ed. University of Chicago: Wiley, (1975).

[8] Lidl, R.; Niederreiter, H. *Finite Fields,* Encyclopedia of Mathematics and its applications. Cambridge University Press, (2008).

[9] Mathieu, E. *Mèmoire sur l'ètude des fonctions de plusieurs quantitès sur la manière de les former et sur les substitutions qui les laissent invariables*, J. Math. Pures Appl, 6 (1861), 241-323.

[10] Park, Y. H.; Lee, J.B. *Permutation polynomials with exponents in an arithmetic progression,* Bull. Austral. Math. Soc, 57 (1998), 243-252.

[11] Zieve, M. E. *Some families of permutation polynomials over finite fields,* Int. J. Number Theory 4 (2008), no. 5, 851–857.

[12] Wang, Q.; Yucas, J. *Dickson polynomials over finite fields,* Finite Fields and Their Applications (2012), 814–831.

[13] Wang, L. *Dickson polynomials over finite fields,* Finite Fields and Their Applications (2012), 814–831.

[14] Wang, D.; Lidl, R. *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure,* Monatsh. Math, 112 (1991) 149-163.

[15] Wang, L. *On permutation polynomials,* Finite Fields Appl, 8 (2002) 311-322.

[16] Xiang dong, H. *Permutation polynomials over finite fields, a survey of recent advances,* Finite Fields Appl, 32 (2015), 82-119.