Gabriel de Freitas Pinheiro

Sobre certos tipos de polinômios de permutação

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE MATEMÁTICA

2022

Gabriel de Freitas Pinheiro

Sobre certos tipos de polinômios de permutação

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

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

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG

2022

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

P654
2022

Pinheiro, Gabriel de Freitas, 1998-
Sobre certos tipos de polinômios de permutação [recurso eletrônico] / Gabriel de Freitas Pinheiro. - 2022.

Orientador: Guilherme Chaud Tizziotti.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2021.666
Inclui bibliografia.

1. Matemática. I. Tizziotti, Guilherme Chaud,1980-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 98, PPMAT				
Data:	16 de fevereiro de 2022	Hora de início:	14:00	Hora de encerramento:	16:00
Matrícula do Discente:	12012MAT004				
Nome do Discente:	Gabriel de Freitas Pinheiro				
Título do Trabalho:	Sobre certos tipos de polinômios de permutação				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Tópicos relacionados à Teoria de Corpos Finitos				

Reuniu-se em web conferência pela plataforma Mconf-RNP, em conformidade com a PORTARIA Nº 36, DE 19 DE MARÇO DE 2020 da COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, pela Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Luciane Quoos Conte - UFRJ; Alonso Sepúlveda Castellanos - FAMAT/UFU e Guilherme Chaud Tizziotti - FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Guilherme Chaud Tizziotti, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

Aprovado.

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

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

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

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Presidente**, em 16/02/2022, às 15:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alonso Sepulveda Castellanos**, **Professor(a) do Magistério Superior**, em 16/02/2022, às 15:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luciane Quoos Conte**, **Usuário Externo**, em 16/02/2022, às 15:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3331575** e o código CRC **15ED2508**.

Dedicatória

À minha mãe Luciene e minha avó Luzia (*In memorian*) que são as pessoas mais importantes na minha vida e que me tornaram a pessoa que sou hoje. Em especial à minha mãe, que sempre acreditou nos meus sonhos e nunca me deixou desistir, você é a luz que ilumina meu caminho.

À Irene Magalhães Craveiro, minha orientadora de graduação que virou uma grande amiga. Seu apoio foi muito importante para mim durante todo meu período acadêmico na graduação e também no mestrado.

Aos meus amigos antigos e novos.

Aos meus professores, desde o ensino básico até o mestrado.

Agradecimentos

Agradeço primeiramente à minha mãe que é a pessoa que sempre me deu forças para lutar e correr atrás dos meus sonhos, que sempre se interessou pelos meu estudos e que sempre contribuiu emocionalmente para que eu não desanimasse, foi sua força e seu apoio que me fizeram chegar onde estou.

Agradeço também à professora Irene Magalhães Craveiro por todo o suporte no início do mestrado, foi fundamental para que eu conseguisse realizar esse sonho.

Não posso deixar de agradecer à minha prima Lorrayne e seu marido Matheus, sempre lembrarei de todo apoio que vocês me deram.

Agradeço à Universidade Federal de Uberlândia e todos os professores que tive contato durante o mestrado. Vocês me ensinaram muito sobre como é ser um ótimo profissional e como ter um olhar mais humanitário com meus futuros alunos.

Em especial, agradeço ao meu orientador Guilherme Chaud Tizziotti por todo aprendizado, por todo apoio e também pelos conselhos, foi de grande importância para minha formação.

Agradeço também ao professor Alonso Sepúlveda Castellanos que foi um excelente coordenador e sempre estava disponível para ajudar seus alunos. Ao professor Rodolfo Collegari pela ajuda com o Latex. À Meyr, que desde o início foi sempre muito atenciosa e que me recebeu muito bem.

Também agradeço ao meu amigo Walteir que sempre me ajudou desde a graduação, seu apoio foi muito importante para mim. Aos meus amigos que fiz no mestrado, Quezia e Ênio.

Por fim, agradeço à CAPES pelo apoio financeiro durante esses dois anos.

PINHEIRO, Gabriel de Freitas. *Sobre certos tipos de polinômios de permutação.* 2022. xi + 80 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudaremos polinômios de permutação sobre corpos finitos. Inicialmente introduziremos alguns conceitos preliminares sobre corpos finitos para posteriormente apresentarmos alguns critérios para determinar quando um polinômio sobre um certo corpo finito é de permutação e, por fim, exibiremos algumas classes especiais desses polinômios.

Palavras-chave: Corpos finitos; Polinômios de permutação.

PINHEIRO, Gabriel de Freitas. *About certain types of permutation polynomials.* 2022. xi + 80 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, some results regarding permutation polynomials over finite fields will be explored. Initially we will introduce some preliminary concepts about finite fields to later present some criteria to determine when a polynomial over a certain finite field is a permutation one and, finally, we will show some special classes of these polynomials.

Keywords: Finite fields; Permutation polynomials.

Sumário

Introdução

A noção de corpos finitos que temos atualmente deve-se ao matemático francês do século XIX Evariste Galois (1811 - 1832). Considerando um polinômio irredutível f sobre $\mathbb{Z}[X]$, Galois tomou r como uma de suas raízes e começou a analisar expressões da forma

$$b_0 + b_1 r + b_2 r^2 + \cdots + b_{n-1} r^{n-1}, \tag{1}$$

com $b_i \in \mathbb{Z}$, $1 \leq i \leq n-1$. Então, ele definiu o conjunto $\mathbb{E}$ de todas as expressões como em (1) tomando os coeficientes b_i's como sendo inteiros módulo um primo p. Naturalmente, o conjunto $\mathbb{E}$ tem p^n elementos. Em seguida, Galois (com a linguagem usada na época) prova que $\mathbb{E}$ é um corpo. Assim, em homenagem a Galois os corpos finitos também recebem o nome de *corpos de Galois*. Atualmente, a notação mais usual para denotar um corpo finito com $q = p^n$ elementos é $\mathbb{F}_q$, porém, tal corpo também é denotado por $GF(q)$, que vem do inglês *Galois field*.

Polinômios sobre corpos finitos que induzem uma permutação sobre esses corpos são chamados de *polinômios de permutação*. O contexto histórico do surgimento dos polinômios de permutação envolve trabalhos de dois grandes matemáticos do século XIX: Hermite e Dickson. O primeiro investigou permutações sobre corpos primos. Já o segundo explorou permutações sobre corpos finitos quaisquer. No ano de 1897, Dickson apresentou uma lista que dizia conter todos os polinômios de permutação de grau no máximo 6.

Com o avanço da era digital o tema foi ganhando cada vez mais destaque, visto que ele possui várias aplicações práticas, como em criptografia, códigos corretores de erros, desenhos combinatórios, entre outras. Com isso, diversos trabalhos sobre os polinômios de permutação vem sendo publicados nos últimos anos.

Neste trabalho apresentaremos um estudo sobre polinômios de permutação. Além de resultados mais gerais, apresentaremos dois estudos sobre tipos específicos de polinômios de permutação, o primeiro é um estudo feito por Zheng, Yuan e Yu, em [18], sobre polinômios das $cX - X^s + X^{qs}$ e $(X^{q^k} - X + \delta)^s + cX$, e o segundo é estudo feito por Gupta e Sharma, em [4], de certas classes de trinômios de permutação da forma $X^r h(X^{\frac{q-1}{3}})$ sobre corpos de característica par. Toda fundamentação teórica para apresentar esses estudos foi feita principalmente usando o livro *Finite Fields*, de R. Lidl e H. Niederreiter, [10].

Esta dissertação está estruturada da seguinte forma. No Capítulo 1 caracterizamos os corpos finitos, apresentando resultados preliminares que serão muito úteis nos demais capítulos. No Capítulo 2 introduzimos o estudo de polinômios sobre corpos finitos, onde abordamos os principais assuntos

referentes a esse tema, como ordem de polinômios, polinômios primitivos e irredutíveis. Um estudo sobre polinômios de permutação, que é nosso principal objeto de estudo, será apresentado no Capítulo 3, onde exploramos alguns critérios para classificá-los bem como alguns tipos especiais. No Capítulo 4 exploramos os polinômios de permutação das formas $cX - X^s + X^{qs}$ e $(X^{q^k} - X + \delta)^s + cX$. Por fim, no Capítulo 5 estudamos os trinômios de permutação sobre corpos de característica par com a forma $X^r h(X^{\frac{q-1}{3}})$.

Gabriel de Freitas Pinheiro

Uberlândia-MG, 16 de fevereiro de 2022.

Capítulo 1

Caracterização de corpos finitos

A caracterização dos corpos finitos mostra que a ordem de todo corpo finito é potência de um número primo e que, reciprocamente, para toda potência de um primo existe um corpo finito tal que a quantidade de elementos deste corpo é exatamente igual a essa potência. Além disso, temos que corpos finitos com o mesmo número de elementos são isomorfos. O resultado a seguir estabelece uma condição simples, porém necessária, sobre o número de elementos de um corpo finito. Observamos que os resultados encontrados neste capítulo podem ser encontrados em [10, Capítulo 2].

Lema 1.0.1: Seja F um corpo finito contendo um subcorpo K com q elementos. Então, F tem q^m elementos, em que m é o grau da extensão F/K.

Demonstração. Olhando F como um espaço vetorial sobre K, como F é finito, então a dimensão de F como espaço vetorial sobre K é finita. Se $[F:K]=m$, então, F tem uma base sobre K contendo m elementos, digamos $b_1,b_2,\ldots,b_m$. Assim, todo elemento de F pode ser unicamente representado como $a_1b_1+a_2b_2+\cdots+a_mb_m$, onde $a_1,a_2,\ldots,a_m\in K$. Como cada a_i pode assumir q valores distintos, para cada $i=1,2,\ldots,m$, então F terá exatamente q^m elementos. □

Exemplo 1.0.2: Sejam F um corpo finito e K subcorpo de F com três elementos. Suponha que $[F:K]=2$. Então, pelo Lema 1.0.1 segue que F tem exatamente $3^2=9$ elementos.

Começando pelos corpos $\mathbb{F}_p$ podemos construir outros corpos pelo processo de adjunção de raízes. Se $f\in\mathbb{F}_p[X]$ é um polinômio irredutível sobre $\mathbb{F}_p$ de grau n, então por adjunção de raízes de f sobre $\mathbb{F}_p$ geramos um corpo finito com p^n elementos. A fim de estabelecer que para todo primo p e todo $n\in\mathbb{N}$ existe um corpo finito com p^n elementos, usamos uma abordagem sugerida pelos seguintes resultados.

Lema 1.0.3: Se F é um corpo com q elementos, então todo $a\in F$ satisfaz $a^q=a$.

Demonstração. Para $a=0$ o resultado é trivial. Assim, suponha $a\neq 0$. Os elementos $0\neq a\in F$ formam um grupo com $q-1$ elementos com a multiplicação, então $a^{q-1}=1$ e a multiplicação por a em ambos os lados da igualdade nos fornece o resultado desejado. □

Exemplo 1.0.4: Seja $F = \mathbb{F}_3$. Então, pelo Lema 1.0.3 temos que todo $a \in \mathbb{F}_3$ satisfaz $a^3 = a$. De fato, $0^3 = 0, 1^3 = 1$ e $2^3 = 8 = 2$.

Lema 1.0.5: Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $X^q - X \in K[X]$ se fatora em $F[X]$ como $X^q - X = \prod_{a \in F}(X - a)$ e F é o corpo de raízes de $X^q - X$ sobre K

Demonstração. O polinômio $X^q - X$ de grau q tem no máximo q raízes em F. Pelo Lema 1.0.3, todos os q elementos de F serão raízes desse polinômio. Assim, $X^q - X$ se fatora em F como o produto $\prod_{a \in F}(X - a)$, e não pode se decompor em nenhum corpo menor. □

Com os resultados anteriores, provaremos o importante teorema a seguir, o qual é fundamental para a caracterização dos corpos finitos.

Teorema 1.0.6 (Existência e Unicidade de Corpos Finitos): Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de raízes do polinômio $X^q - X$ sobre $\mathbb{F}_p$.

Demonstração. (Existência) Para $q = p^n$ considere $X^q - X$ em $\mathbb{F}_p[X]$ e seja F o corpo de raízes sobre $\mathbb{F}_p$. Esse polinômio tem q raízes distintas em F, pois sua derivada é $qX^{q-1} - 1 = -1$ em $\mathbb{F}_p[X]$ e dessa forma não há raízes comuns em $X^q - X$. Seja $S = \{a \in F : a^q - a = 0\}$. Então, S é um subcorpo de F pois: (i) S contém 0 e 1; (ii) $a, b \in S$ implica que $(a-b)^q = a^q - b^q = a - b$ e, então, $a - b \in S$; (iii) para $a, b \in S$ e $b \neq 0$ temos que $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ e, então, $ab^{-1} \in S$. Mas, por outro lado, $X^q - X$ deve se fatorar em S, pois S contém todas suas raízes. Consequentemente, $F = S$ e, como S tem q elementos, F é um corpo finito com q elementos. (Unicidade) Seja F um corpo finito com $q = p^n$ elementos. Então, F tem característica p e então contém $\mathbb{F}_p$ como um subcorpo. Assim, o resultado segue como consequência da unicidade dos corpos de raízes. □

Pelo teorema anterior podemos concluir que o único (a menos de isomorfismo) corpo finito com $q = p^n$ elementos é o corpo de raízes de $X^q - X$ sobre $\mathbb{F}_p$. A seguir, veremos quais são todos os subcorpos $\mathbb{F}_r$ de um dado corpo $\mathbb{F}_q$.

A parte da unicidade do Teorema 1.0.6 fornece a justificativa para falar em corpos finitos com q elementos ou de ordem q, e denotá-los por $\mathbb{F}_q$, em que q é uma potência de um primo p o qual é a característica do corpo $\mathbb{F}_q$.

Teorema 1.0.7 (Critério para um subcorpo): Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, onde m é um inteiro positivo divisor de n. Reciprocamente, se m é um divisor positivo de n, então, existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.

Demonstração. É claro que um subcorpo K de $\mathbb{F}_q$ tem ordem p^m para algum inteiro positivo $m \leq n$. No Lema 1.0.1 mostramos que $q = p^n$ deve ser uma potência de p^m e, então, m é necessariamente um divisor de n.

Suponha agora que $m \mid n$, então, $m = kn$ com $k \in \mathbb{Z}$. Note que,

$$p^n - 1 = (p^m)^k - 1 = (p^m - 1)\sum_{i=0}^{k-1}(p^m)^i \tag{1.1}$$

ou seja, $p^m - 1$ divide $p^n - 1$. Então, $p^n - 1 = r(p^m - 1)$, com $r \in \mathbb{Z}$. De modo análogo ao que fizemos em (1.1) temos que

$$X^{p^n-1} - 1 = (X^{p^m-1})^r - 1 = (X^{p^m-1} - 1)\sum_{j=0}^{r-1}(X^{p^m-1})^j.$$

Logo, $X^{p^m-1} - 1$ 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 $\mathbb{F}_p[X]$. Assim, toda raíz de $X^{p^m} - X$ é uma raíz de $X^q - X$ e, então, pertence a $\mathbb{F}_q$. Segue que $\mathbb{F}_q$ deve conter como subcorpo um corpo de raízes de $X^{p^m} - x$ sobre $\mathbb{F}_p$ de ordem p^m, como visto no teorema 1.0.6. Se existissem dois subcorpos distintos de ordem p^m em $\mathbb{F}_q$, eles deveriam conter juntos mais do que p^m raízes de $X^{p^m} - X$ em $\mathbb{F}_q$, o que é uma contradição. □

Exemplo 1.0.8: Os subcorpos do corpo finito $\mathbb{F}_{3^{15}}$ podem ser determinados por meio da listagem de todos os divisores positivos de 15. Então, os subcorpos de $\mathbb{F}_{3^{15}}$ são: $\mathbb{F}_3, \mathbb{F}_{3^3}, \mathbb{F}_{3^5}$ e $\mathbb{F}_{3^{15}}$.

Pelo Teorema 1.0.7 as relações de contenção são equivalentes às relações de divisibilidade entre os divisores positivos de 15.

Para um corpo finito $\mathbb{F}_q$ vamos denotar por $\mathbb{F}_q^*$ o grupo multiplicativo de elementos não-nulos de $\mathbb{F}_q$. O resultado a seguir nos fornece uma propriedade muito útil sobre esse grupo.

Teorema 1.0.9: Para todo corpo finito $\mathbb{F}_q$ o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.

Demonstração. Se $q = 2$ o resultado é óbvio. Assim, vamos assumir $q \geq 3$. Seja $h = p_1^{r_1} \dots p_m^{r_m}$ a decomposição em primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para todo $1 \leq i \leq m$, o polinômio $X^{\frac{h}{p_i}} - 1$ tem no máximo $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Como $h/p_i < h$, segue que existem elementos não-nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um elemento não nulo de $\mathbb{F}_q$ que não é raíz do polinômio e seja $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Assim, temos que $b_i^{p_i^{r_i}} = 1$, consequentemente, a ordem de b_i é um divisor de $p_i^{r_i}$ e, então, é da forma $p_i^{s_i}$, com $0 \leq s_i \leq r_i$. Por outro lado, $b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$ e, então, a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 \dots b_m$ tem ordem h. Suponha o contrário, que a ordem de b é um divisor próprio de h e é, portanto, um divisor de pelo menos um dos m inteiros h/p_i, com $1 \leq i \leq m$, digamos h/p_1. Daí temos que $1 = b^{h/p_i} = b_1^{h/p_1} \dots b_m^{h/p_1}$. Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h/p_1 e, consequentemente, $b_i^{h/p_1} = 1$. Portanto, $b_1^{h/p_1} = 1$. Isso implica que a ordem de b_1 deve dividir h/p_1, o qual é impossível pois a ordem de b_1 é $p_1^{r_1}$. Dessa forma, concluímos que $\mathbb{F}_q^*$ é um grupo cíclico gerado por b. □

Exemplo 1.0.10: O grupo multiplicativo $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ é cíclico. De fato, 2 é um gerador desse

grupo:

$$2^1 = 2, 2^2 = 4, 2^3 = 8 = 3, 2^4 = 16 = 1.$$

Ou seja, $\mathbb{F}_5^* = < 2 >$.

Definição 1.0.11: Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado **elemento primitivo** de $\mathbb{F}_q$.

Exemplo 1.0.12: Segue do Exemplo 1.0.10 que 2 é um elemento primitivo de $\mathbb{F}_5$.

Segue por um resultado que $\mathbb{F}_q$ contém $\phi(q-1)$ elementos primitivos, onde ϕ é a função de Euler. A existência de elementos primitivos pode ser usada para mostrar um resultado que implica, em particular, que todo corpo finito pode ser pensado como uma extensão algébrica simples de subcorpos primos.

Exemplo 1.0.13: Sabendo que $\mathbb{F}_q$ tem $\phi(q-1)$ elementos primitivos, temos:

(1) $\mathbb{F}_5$ tem $\phi(4) = 2$ elementos primitivos, os quais são 2 e 3.

(2) $\mathbb{F}_4$ tem $\phi(3) = 2$ elementos primitivos. Expressando $\mathbb{F}_4$ como $\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha+1\}$, onde $\alpha^2 + \alpha + 1 = 0$, temos que ambos α e $\alpha+1$ são elementos primitivos.

Antes de enunciarmos o próximo resultado, recordemos que se $L = K[\alpha]$ é uma extensão simples de K, então, α é um elemento de definição de L sobre K.

Teorema 1.0.14: Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$. Então, $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ pode servir com um elemento de definição de $\mathbb{F}_r$ sobre $\mathbb{F}_q$

Demonstração. Seja ζ um elemento primitivo de $\mathbb{F}_r$. Note que, $\mathbb{F}_q[\zeta] \subseteq \mathbb{F}_r$ e, por outro lado, $\mathbb{F}_q[\zeta]$ contém o 0 e todas as potências de ζ, e consequentemente, todos os elementos de $\mathbb{F}_r$. Portanto, temos que $\mathbb{F}_r = \mathbb{F}_q(\zeta)$. □

Embora a prova do Teorema 1.0.14 use um elemento primitivo de F, não é de fato necessário que β seja um gerador multiplicativo de F^*, como mostra o próximo exemplo.

Exemplo 1.0.15: Considere o corpo finito $\mathbb{F}_9$. Podemos expressar $\mathbb{F}_9$ na forma $\mathbb{F}_3[\beta]$, onde β é raíz do polinômio irredutível $X^2 + 1$ sobre $\mathbb{F}_3$. Contudo, como $\beta^4 = 1$, β não gera todo o $\mathbb{F}_9$, isto é, β não é um elemento primitivo de $\mathbb{F}_9$.

Corolário 1.0.16: Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n existe um polinômio irredutível em $\mathbb{F}_q[X]$ de grau n.

Demonstração. Seja $\mathbb{F}_r$ uma extensão do corpo $\mathbb{F}_q$ de ordem q^n, então, $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 1.0.14 temos que $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ para algum $\zeta \in \mathbb{F}_r$. Então, o polinômio minimal de ζ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[X]$ de grau n. □

Exemplo 1.0.17: Seja $f(X) = X^3 + X + 1 \in \mathbb{F}_5[X]$. Note que $f(0) = 1, f(1) = 3, f(2) = 1, f(3) = 1$ e $f(4) = 4$. Ou seja, f não possui raízes em $\mathbb{F}_5$. Logo, pelo Teorema 1.69 em [10] segue que f é irredutível sobre $\mathbb{F}_5$.

1.1 Raízes de polinômios irredutíveis

Nessa seção iremos coletar algumas informações sobre o conjunto de raízes de um polinômio irredutível sobre um corpo finito. Antes, enunciemos um teorema que nos será muito útil neste trabalho.

Teorema 1.1.1: Se $\alpha \in F$ é algébrico sobre K, então, seu polinômio minimal g sobre K satisfaz as seguintes propriedades:

(1) g é irredutível em $K[X]$;

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

(3) g é o polinômio mônico de menor grau em $K[X]$ que contém α como raíz;

Demonstração. Ver [10] p. 31. □

Lema 1.1.2: Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre um corpo finito $\mathbb{F}_q$ e seja α uma raíz de f na extensão do corpo $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[X]$ temos que $h(\alpha) = 0$ se, e somente se, f divide h.

Demonstração. Seja a o coeficiente líder de f e ponha $h(X) = a^{-1} f(X)$. Então, h é um polinômio mônico irredutível de α sobre $\mathbb{F}_q$. Como f é irredutível em $\mathbb{F}_q[X]$ segue que $h(\alpha) = 0$ se, e somente se, f divide h. □

Exemplo 1.1.3: Sejam $f(X) = X - 1 \in \mathbb{F}_3[X]$ um polinômio irredutível sobre $\mathbb{F}_3$ e $h(X) = X^2 + X + 1 \in \mathbb{F}_3[X]$. Seja $\alpha \in \mathbb{F}_{3^m}$ uma raíz de f em alguma extensão de $\mathbb{F}_3$. Note que $f(\alpha) = 0$, ou seja, $\alpha - 1 = 0$, o que nos dá $\alpha = 1$. Isso implica que $\alpha^2 + \alpha + 1 = 0$. Ou seja, $h(\alpha) = 0$. Logo, pelo Lema 1.1.2 segue que f divide h.

Teorema 1.1.4: Sejam K, L e M corpos. Se L é uma extensão finita de K e M é uma extensão finita de L, então, M é uma entensão finita de K com

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

Demonstração. Ver [10] p. 32. □

Lema 1.1.5: 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. Suponha que $f(X)$ divide $X^{q^n} - X$. Seja α uma raíz de f no corpo de raízes de f sobre $\mathbb{F}_q$. Então, $\alpha^{q^n} = \alpha$ e daí temos que $\alpha \in \mathbb{F}_{q^n}$. Assim, segue que $\mathbb{F}_q(\alpha)$ é um subcorpo de $\mathbb{F}_{q^n}$. Mas,

como $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ e $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$, segue pelo Teorema 1.1.4 que m divide n. Reciprocamente, se m divide n, pelo Teorema 1.0.7 temos que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como um subcorpo. Se α é uma raíz de f no corpo de raízes de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ e, então, $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$. Consequentemente, temos que $\alpha\in\mathbb{F}_q$ e, então, $\alpha^{q^n}=\alpha$ e, portanto, α é uma raíz de $X^{q^n}-X\in\mathbb{F}_q[X]$. Assim, do lema 1.1.2 temos que $f(X)$ divide $X^{q^n}-X$. □

Exemplo 1.1.6: Considere o polinômio $f(X)=X^2+X-1\in\mathbb{F}_3[X]$ irredutível sobre $\mathbb{F}_3$ de grau $m=2$. Então, pelo Lema 1.1.5 f divide $g(X)=X^{3^n}-X$ se, e somente se, $2|n$. Ou seja, $f|g$ se, e somente se, n é par.

Teorema 1.1.7: Seja R um anel comutativo de característica prima p. Então,

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

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

Demonstração. Ver [10] p. 16. □

Teorema 1.1.8: Se f é um polinômio irredutível em $\mathbb{F}_q[X]$ de grau m, então, f tem uma raíz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e são dadas por m elementos distintos $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.

Demonstração. Seja α uma raíz de f no corpo de raízes de f sobre $\mathbb{F}_q$. Então, $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$, consequentemente, $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$ e, em particular, $\alpha\in\mathbb{F}_{q^m}$. Agora, vamos mostrar que se $\beta\in\mathbb{F}_{q^m}$ é uma raíz de f, então, β^q também o é. Escrevendo $f(X)=a_mX^m+\cdots+a_1X+a_0$ com $a_i\in\mathbb{F}_q$ para $0\leq i\leq m$. Então, pelo Lema 1.0.3 e pelo Teorema 1.1.7 temos que:

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

Portanto, os elementos $\alpha,\alpha^q,\ldots,\alpha^{q^{m-1}}$ são raízes de f. Agora, resta provar que esses elementos são distintos. Suponha o contrário, que $a^{q^j}=a^{q^k}$ para algum inteiro j e k com $0\leq j<k\leq m-1$. Elevando essa identidade à potência q^{m-k} nós obtemos $\alpha^{q^{m-k+j}}=\alpha^{q^m}=\alpha$. Daí, segue pelo Lema 1.1.2 que $f(X)$ divide $X^{q^{m-k+j}}-x$. Daí, pelo Lema 1.1.5 a única possibilidade é se m divide $m-k+j$. Mas temos que $0<m-k+j<m$ e daí chegamos numa contradição. □

Corolário 1.1.9: Seja f um polinômio irredutível em $\mathbb{F}_q[X]$ de grau m. Então, o corpo de raízes de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.

Demonstração. Pelo Teorema 1.1.8 temos que f se fatora em $\mathbb{F}_{q^m}$. Além disso, $\mathbb{F}_q(\alpha,\alpha^q,\ldots,\alpha^{q^{m-1}})=\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$ para alguma raíz α de f em $\mathbb{F}_{q^m}$, onde a segunda identidade segue da prova do Teorema 1.1.8. □

Exemplo 1.1.10: Seja X^2+1 um polinômio irredutível sobre $\mathbb{F}_3$. Então, pelo Corolário 1.1.9 temos que o corpo de raízes de X^2+1 sobre $\mathbb{F}_3$ é $\mathbb{F}_9$.

Corolário 1.1.11: Quaisquer dois polinômios de mesmo grau e irredutíveis em $\mathbb{F}_q[X]$ possuem corpos de raízes isomórficos.

Agora, vamos introduzir uma terminologia conveniente para os elementos que apareceram no Teorema 1.1.8, independentemente de $\alpha \in \mathbb{F}_{q^m}$ ser uma raíz de um polinômio irredutível em $\mathbb{F}_q[X]$ de grau m ou não.

Definição 1.1.12: Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então, os elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ são chamados de **conjugados** de α com respeito a $\mathbb{F}_q$.

Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito a $\mathbb{F}_q$ são distintos se, e somente se, o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau m. Por outro lado, o grau d desse polinômio minimal é um divisor próprio de m e, então, os conjugados de α com respeito a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, cada qual repetido m/d vezes. A seguir, enunciaremos um resultado sobre grupos cuja demonstração pode ser encontrada no Terema 2.8 em [10].

Teorema 1.1.13: Em um grupo cíclico finito $< a >$ de ordem m, o elemento a^k gera um subgrupo de ordem $m/mdc(k,m)$, onde $mdc(k,m)$ denota o máximo divisor comum de k e m.

Teorema 1.1.14: Os conjugados de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ tem a mesma ordem no grupo $\mathbb{F}_q^*$.

Demonstração. Como $\mathbb{F}_q^*$ é um grupo cíclico, o resultado segue pelo Teorema 1.1.13 e do fato de que toda potência da característica de $\mathbb{F}_q$ é igual a um número relativamente primo com a ordem $q-1$ de $\mathbb{F}_q^*$. □

Corolário 1.1.15: Se α é um elemento primitivo de $\mathbb{F}_q$, então, os seus conjugados também serão elementos primitivos com respeito a qualquer subcorpo de $\mathbb{F}_q$.

Exemplo 1.1.16: Seja $\alpha \in \mathbb{F}_{27}$ uma raíz de $f(X) = X^2 + 1 \in \mathbb{F}_3[X]$. Logo, $\alpha^2 + 1 = 0$, o que implica que $\alpha^2 = -1 = 2$. Então, os conjugados de α com respeito a $\mathbb{F}_3$ são $\alpha = \alpha^9$ e $\alpha^3 = \alpha^2\alpha = 2\alpha$, cada um deles sendo um elemento primitivo de $\mathbb{F}_{27}$.

Existe uma relação íntima entre os elementos conjugados e os automorfismos de um corpo finito. 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 $\mathbb{F}_q$. Assim, em detalhes, exigimos que σ seja uma aplicação injetiva e sobrejetiva do corpo $\mathbb{F}_{q^m}$ nele mesmo, com $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ para todos $\alpha, \beta \in \mathbb{F}_{q^m}$ e $\sigma(a) = a$ para todo $a \in \mathbb{F}_q$.

Teorema 1.1.17: Os automorfismos distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são as aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ definidas por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leq j \leq m-1$.

Demonstração. Para cada σ_j e todo $\alpha, \beta \in \mathbb{F}_{q^m}$ temos que $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ e também $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ pelo Teorema 1.1.7, então, segue que σ_j é um endomorfismo de $\mathbb{F}_{q^m}$. Além disso,

$\sigma_j(\alpha) = 0$ se, e somente se, $\alpha = 0$ e, então, σ_j é injetiva. Como $\mathbb{F}_{q^m}$ é um conjunto finito, temos que σ_j é um epimorfismo e, portanto, um automorfismo de $\mathbb{F}_{q^m}$. E mais, temos que $\sigma_j(a) = a$ para todo $a \in \mathbb{F}_q$ pelo Lema 1.0.3 e, então, cada σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. As aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ são distintas pois assumem valores distintos para um elemento primitivo de $\mathbb{F}_{q^m}$. Agora, suponha que σ é um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Seja β um elemento primitivo de $\mathbb{F}_{q^m}$ e seja $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in \mathbb{F}_q[X]$ o polinômio minimal sobre $\mathbb{F}_q$. Então,

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

daí temos que $\sigma(\beta)$ é uma raíz de f em $\mathbb{F}_{q^m}$. Segue do Teorema 1.1.8 que $\sigma(\beta) = \beta^{q^j}$ para algum j, com $0 \leq j \leq m-1$. Como σ é um homomorfismo, temos que $\sigma(\alpha) = \alpha^{q^j}$ para todo $\alpha \in \mathbb{F}_{q^m}$. □

Exemplo 1.1.18: Seja $\alpha \in \mathbb{F}_{2^3}$. Os automorfismos distintos de $\mathbb{F}_{2^3}$ sobre $\mathbb{F}_2$ são definidos por $\sigma_j(\alpha) = \alpha^{2^j}$ com $0 \leq j \leq 2$. Ou seja, os automorfismos distintos são $\sigma_0(\alpha) = \alpha, \sigma_1(\alpha) = \alpha^2$ e $\sigma_2(\alpha) = \alpha^4$.

Com base no Teorema 1.1.17 fica evidente que os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito a $\mathbb{F}_q$ são obtidos por aplicação de todos os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ no elemento α. Os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ formam um grupo com a operação usual de composição de aplicações. As informações fornecidas no Teorema 1.1.17 mostram que esse grupo de automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é um grupo cíclico de ordem m gerado por σ_1.

1.2 Traços e bases

Nesta seção, adotaremos novamente o ponto de vista de considerar uma extensão finita $F = \mathbb{F}_{q^m}$ do corpo finito $K = \mathbb{F}_q$ como um espaço vetorial sobre K. Então, F tem dimensão m sobre K e, se $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de F sobre K, cada elemento $\alpha \in F$ pode ser unicamente representado na forma $\alpha = c_1\alpha_1 + \cdots + c_m\alpha_m$, com $c_j \in K$, para $1 \leq j \leq m$. Vamos introduzir uma importante aplicação de F para K que acabará sendo linear.

Definição 1.2.1: Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o traço $T_{r_{F/K}}(\alpha)$ de α sobre K é definido por

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

Se K é o subcorpo primo de F, então, $T_{r_{F/K}}(\alpha)$ é chamado de *traço absoluto* de α e, denotamos simplesmente por $T_{r_F}(\alpha)$.

O teorema a seguir elenca as principais propriedades da função traço.

Teorema 1.2.2: Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então, a função traço $T_{r_{F/K}}$ satisfaz as seguintes propriedades:

i) $T_{r_{F/K}}(\alpha+\beta) = T_{r_{F/K}}(\alpha) + T_{r_{F/K}}(\beta)$ para todo $\alpha, \beta \in F$;

ii) $T_{r_{F/K}}(c\alpha) = cT_{r_{F/K}}(\alpha)$, para todo $c \in K, \alpha \in F$;

iii) $T_{r_{F/K}}$ é uma transformação linear sobrejetiva de F sobre K, onde ambos F e K são vistos como espaços vetoriais sobre K;

iv) $T_{r_{F/K}}(a) = ma$ para todo $a \in K$;

v) $T_{r_{F/K}}(\alpha^q) = T_{r_{F/K}}(\alpha)$ para todo $\alpha \in F$.

Demonstração. A seguir demonstraremos cada item do teorema.

i) Para $\alpha, \beta \in F$ e usando o Teorema 1.1.7 temos

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

ii) Para $c \in K$ temos que $c^{q^j} = c$ para todo $j \geq 0$ pelo Lema 1.0.5. Então, obtemos para $\alpha \in F$,

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

iii) As propriedades i) e ii), juntas com o fato de que $T_{r_{F/K}}(\alpha) \in K$ para todo $\alpha \in F$ mostram que $T_{r_{F/K}}$ é uma transformação linear de F em K. Para provar que essa aplicação é sobrejetiva é suficiente mostrar a existência de $\alpha \in F$ como $T_{r_{F/K}}(\alpha) \neq 0$. Ou seja, queremos mostrar que dado $a \in K$ existe $\beta \in F$ tal que $T_{r_{F/K}}(\beta) = a$. Se $T_{r_{F/K}}(\alpha) = x \neq 0$, então, $x^{-1}T_{r_{F/K}}(\alpha) = 1$, o que implica que $ax^{-1}T_{r_{F/K}}(\alpha) = a$, ou seja, $T_{r_{F/K}}(ax^{-1}\alpha) = a$. Portanto, existe $\beta = ax^{-1}\alpha$ tal que $f(\beta) = a$. Logo, $T_{r_{F/K}}$ é uma aplicação sobrejetiva.

iv) Esse item segue imediatamente da definição da função traço e do Lema 1.0.5.

v) Para $\alpha \in F$ temos que $\alpha^{q^m} = \alpha$ pelo Lema 1.0.5 e, então, $T_{r_{F/K}}(\alpha^q) = \alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{m-1}}+\alpha^{q^m} = T_{r_{F/K}}(\alpha)$.

□

Definição 1.2.3: 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

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

Teorema 1.2.4: Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função norma $N_{F/K}$ satisfaz as seguintes propriedades:

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

ii) $N_{F/K}$ é uma aplicação sobrejetiva de F sobre K e de F^* sobre 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. Ver [10] p. 57. □

Definição 1.2.5: Sejam K um corpo finito e F uma extensão finita de K de grau m. Seja $\{\alpha_1, \ldots, \alpha_m\}$ uma base de F sobre K. Dizemos que $\{\beta_1, \ldots, \beta_m\}$ é uma base dual (ou complementar) de $\{\alpha_1, \ldots, \alpha_m\}$ se, para $1 \leq i, j \leq m$ temos:

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

Seja F uma extensão finita de K de grau m. O número de bases distintas de F sobre K é bastante grande, mas existem dois tipos especiais de bases de importância particular. O primeiro é uma base polinomial $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, composta das potências de um elemento gerador α de F sobre K. O elemento α é frequentemente considerado um elemento primitivo. Outro tipo de base é uma base normal definida por um elemento adequado de F.

Definição 1.2.6: Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então, uma base de F sobre K da forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ que consiste de um elemento adequado $\alpha \in F$ e seus conjugados com respeito a K, é chamada de uma *base normal* de F sobre K.

Assumiremos a veracidade dos dois lemas a seguir sem demonstração, com a finalidade de demonstrar o teorema que garante a existência de uma base normal de F sobre K.

Lema 1.2.7: (Lema de Artin) Sejam $\psi_1, \ldots, \psi_m$ homomorfismos distintos de um grupo G no grupo multiplicativo F^* de um corpo arbitrário F e, sejam $a_1, \ldots, a_m$ elementos de F onde nem todos são 0. Então, para algum $g \in G$ temos que

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

Antes de enunciar o próximo lema, relembremos alguns conceitos importantes da álgebra linear. Se T é um operador linear do espaço de dimensão finita V sobre um corpo (arbitrário) K, então, o polinômio $f(X) = a_nX^n + \cdots + a_0 \in K[X]$ é dito anulador de T se $a_nT^n + \cdots + a_0I = 0$, onde I é o operador identidade e 0 é o operador zero em V. O polinômio mônico unicamente determinado pelo menor grau positivo com essa propriedade é chamado de *polinômio minimal* para T. Ele divide qualquer outro polinômio de $K[X]$ no anulador de T. Em particular, o polinômio minimal de T divide o polinômio característico $g(X)$ por T, o qual é dado por $g(X) = det(XI - T)$ e é um polinômio mônico de grau igual a dimensão de V. Um vetor $\alpha \in V$ é chamado um *vetor cíclico* para T se os vetores

$T^k(\alpha)$, $k = 0, 1, \ldots$, pertencem ao Span(V) (que é o conjunto das combinações lineares dos elementos de V). O lema a seguir é um resultado da álgebra linear.

Lema 1.2.8: Seja T um operador linear num espaço vetorial de dimensão finita V. Então, T tem um vetor cíclico se, e somente se, os polinômios minimal e característico de T são iguais.

Teorema 1.2.9: (Teorema da base normal) Para qualquer corpo finito K e qualquer extensão finita F de K, existe uma base normal de F sobre K.

Demonstração. Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$ com $m \geq 2$. Do teorema 1.1.17 sabemos que os distintos automorfismos de F sobre K são dados por $e, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, onde e é a aplicação identidade de F, $\sigma(\alpha) = \alpha^q$ para todo $\alpha \in F$ e, uma potência σ^j refere-se a $j-$ésima composição de σ com ele mesmo. Como $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(c\alpha) = c\sigma(\alpha)$ para $\alpha, \beta \in F$ e $c \in K$. A aplicação σ pode ser considerada como um operador linear no espaço vetorial F sobre K. Como $\sigma^m = e$, o polinômio $X^m - 1 \in K[X]$ se anula em σ. O Lema de Artin aplicado a $e, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ visto como endomorfismos de F^* mostram que polinômios diferentes de zero em $K[X]$ de grau menor que m se anulam em σ. Consequentemente, $X^m - 1$ é o polinômio minimal para o operador linear σ. Como o polinômio característico para σ é um polinômio mônico de grau m que é divisível pelo polinômio minimal para σ, segue que o polinômio característico para σ é dado também por $X^m - 1$. O Lema 1.2.8 implica a existência de um elemento $\alpha \in F$ tal que $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots$ peretencem ao Span(F). Eliminando elementos repetidos, vemos que $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{m-1}(\alpha)$ pertencem ao Span(F) e, portanto, formam uma base de F sobre K. Como essa base consiste de α e seus conjugados com respeito a K, segue que essa é uma base normal de F sobre K. □

A seguir introduzimos uma expressão que nos permite decidir se um dado conjunto de elementos forma uma base para extensão de um corpo finito dado.

Definição 1.2.10: Seja K um corpo finito e F uma extensão de K de grau m sobre K. Então, o discriminante $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ dos elementos $\alpha_1, \ldots, \alpha_m \in F$ é definido pelo determinante de ordem m dado por

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) := \begin{vmatrix} T_{r_{F/K}}(\alpha_1\alpha_1) & T_{r_{F/K}}(\alpha_1\alpha_2) & \cdots & T_{r_{F/K}}(\alpha_1\alpha_m) \\ T_{r_{F/K}}(\alpha_2\alpha_1) & T_{r_{F/K}}(\alpha_2\alpha_2) & \cdots & T_{r_{F/K}}(\alpha_2\alpha_m) \\ \vdots & \vdots & \vdots & \vdots \\ T_{r_{F/K}}(\alpha_m\alpha_1) & T_{r_{F/K}}(\alpha_m\alpha_2) & \cdots & T_{r_{F/K}}(\alpha_m\alpha_m) \end{vmatrix}$$

Segue da definição que o discriminante $\Delta_{F/K}$ é sempre um elemento de K. A seguir apresentaremos uma simples caracterização para bases por meio da definição anterior.

Teorema 1.2.11: Sejam K um corpo finito, F uma extensão de K de grau m sobre K e $\alpha_1, \ldots, \alpha_m \in F$. Então, o conjunto $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de F sobre K se, e somente se, $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.

Demonstração. Seja $\{\alpha_1, \ldots, \alpha_m\}$ uma base de F sobre K. Provaremos que $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ mostrando que os vetores linha do determinante que define $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ são linearmente

independentes. Para isso, suponha que

$$c_1 T_{r_{F/K}}(\alpha_1\alpha_j) + \cdots + c_m T_{r_{F/K}}(\alpha_m\alpha_j) = 0,$$

com $1 \leq j \leq m$ e $c_1, \ldots, c_m \in K$. Então, pondo $\beta = c_1\alpha_1 + \cdots + c_m\alpha_m$ temos que $T_{r_{F/K}}(\beta\alpha_j) = 0$ para $1 \leq j \leq m$ e, como $\alpha_1, \ldots, \alpha_m \in Span(F)$, segue que $T_{r_{F/K}}(\beta\alpha) = 0$ para todo $\alpha \in F$. Contudo, isso é possível somente se $\beta = 0$ e, então, $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$ o que implica $c_1 = \cdots = c_m = 0$. Reciprocamente, suponha que $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ e $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$ para algum $c_1, \ldots, c_m \in K$. Então,

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

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

$$c_1 T_{r_{F/K}}(\alpha_1\alpha_j) + \cdots + c_m T_{r_{F/K}}(\alpha_m\alpha_j) = 0$$

para $1 \leq j \leq m$. Mas, como os vetores linhas do determinante definido por $\Delta_{F/k}(\alpha_1, \ldots, \alpha_m)$ são linearmente independentes, segue que $c_1 = \cdots = c_m = 0$. Então, $\alpha_1, \ldots, \alpha_m$ são linearmente independentes sobre K. □

Existe um outro determinante de ordem m que serve o mesmo propósito do discriminante. As entradas desse determinante são, contudo, elementos da extensão do corpo F. Para $\alpha_1, \ldots, \alpha_m \in F$, seja A a matriz $m \times m$ cuja entrada $i-$ésima linha e $j-$ésima coluna é $\alpha_j^{q^{i-1}}$ onde q é o número de elementos de K. Se A^T denota a transposta de A, então um simples cálculo mostra que $A^T A = B$, onde B é a matriz $m \times m$ cuja entrada na $i-$ésima linha e $j-$ésima coluna é $T_{r_{F/K}}(\alpha_i\alpha_j)$. Tomando determinantes, obtemos $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = det(A)^2$.

O próximo resultado é consequência do teorema anterior.

Corolário 1.2.12: Sejam $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^m}$. Então, $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se,

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

A partir do critério acima, somos levados a uma maneira relativamente simples de verificar se um determinado elemento dá origem a uma base normal.

Teorema 1.2.13: Para $\alpha \in \mathbb{F}_{q^m}$, o conjunto $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ é uma base normal de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se, os polinômios $X^m - 1$ e $\alpha X^{m-1} + \alpha^q X^{m-2} + \cdots + \alpha^{q^{m-2}} X + \alpha^{q^{m-1}}$ em $\mathbb{F}_{q^m}[X]$ são relativamente primos.

Demonstração. Quando $\alpha_1 = \alpha, \alpha_2 = \alpha^q, \ldots, \alpha_m = \alpha^{q^{m-1}}$ o determinante do corolário anterior se torna

$$\pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \vdots & \vdots & \vdots & \vdots & \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{vmatrix} \tag{1.2}$$

após uma permutação adequada das linhas. Agora, considere o resultante $R(f,g)$ dos polinômios $f(X) = X^m - 1$ e $g(X) = \alpha X^{m-1} + \alpha^q X^{m-2} + \cdots + \alpha^{q^{m-2}} X + \alpha^{q^{m-1}}$ de graus, respectivamente, m e $m-1$, o qual é dado pelo determinante de ordem $2m-1$. Nesse determinante, adicione a $(m+1)-$ésima coluna à primeira coluna, a $(m+2)-$ésima coluna à segunda coluna e, então, finalmente adicione a $(2m-1)-$ésima à $(m-1)-$ésima coluna. O determinante resultante é fatorado no determinante da matriz diagonal de ordem $m-1$ com entradas -1 ao longo do determinante da diagonal principal e o determinante em (1.2). Então, $R(f,g)$ é, a menos do sinal, igual ao determinante em (1.2). Assim, o resultado segue do corolário 1.2.12 e do fato que $R(f,g) \neq 0$ se, e somente se, f e g são relativamente primos. □

Em conexão com a discussão anterior, mencionamos sem prova o seguinte refinamento do teorema da base normal.

Teorema 1.2.14: Para qualquer corpo finito F existe uma base normal de F sobre um subcorpo primo que consiste dos elementos primitivos de F.

1.3 Raízes da unidade e polinômios ciclotômicos

Nessa seção investigaremos o corpo de separação do polinômio $X^n - 1$ sobre um corpo arbitrário K, onde n é um inteiro positivo. Além disso, obteremos uma generalização do conceito de raízes da unidade, também conhecido por números complexos.

Definição 1.3.1: Seja n um inteiro positivo. O corpo de decomposição de $X^n - 1$ sobre um corpo K é chamado de $n-$ésimo corpo ciclotômico de K e denotamos por $K^{(n)}$. As raízes de $X^n - 1$ em $K^{(n)}$ são chamadas de $n-$ésimas raízes da unidade sobre K e o conjunto de todas essas raízes é denotado por $E^{(n)}$.

Exemplo 1.3.2: O corpo $\mathbb{F}_9$ é o corpo de separação do polinômio $X^8 - 1$ sobre $\mathbb{F}_3$. Então, $\mathbb{F}_9$ é o $8-$ésimo corpo ciclotômico de $\mathbb{F}_3$ e o denotamos por $\mathbb{F}_3^{(8)}$.

Um caso especial dessa definição geral é obtido se K é o corpo dos número racionais. Então, $K^{(n)}$ é um subcorpo do corpo dos números complexos e as $n-$ésimas ráizes da unidade assume interpretação

geométrica como sendo os vértices de um polígono regular com n vértices inscrito no círculo unitário no plano complexo.

Para nosso propósito, o caso mais importante é para um corpo finito K. Mas, as propriedades básicas das raízes da unidade podem, contudo, ser estabelecidas sem o uso dessa restrição. A estrutura de $E^{(n)}$ é determinada pela relação de n com a característica de K, como o teorema a seguir mostrará. Assim, quando nos referirmos à característica p de K nessa discussão, também permitiremos que p assuma o valor 0.

Teorema 1.3.3: Seja n um inteiro positivo e K um corpo de característica p. Então:

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

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

Demonstração. Segue a demonstração de cada item:

(i) O caso $n = 1$ é trivial. Para $n \geq 2$, o polinômio $X^n - 1$ e sua derivada nX^{n-1} não têm raízes em comum, pois nX^{n-1} tem somente 0 como raíz em $K^{(n)}$. Então, $X^n - 1$ não tem raízes múltiplas e, consequentemente, $E^{(n)}$ tem n elementos. Agora, se $\zeta, \eta \in E^{(n)}$, então, $(\zeta\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1$, portanto, $\zeta\eta^{-1} \in E^{(n)}$. Assim, segue que $E^{(n)}$ é um grupo multiplicativo. Seja $n = p_1^{e_1} \dots p_t^{e_t}$ a decomposição em fatores primos de n. Por um argumento semelhante à prova do teorema 1.0.9 temos que para cada i, com $1 \leq i \leq t$, existe um elemento $\alpha_i \in E^{(n)}$ que não é uma raíz do polinômio $X^{n/p_i} - 1$, que $\beta_i = \alpha_i^{n/p_i^{e_i}}$ tem ordem $p_i^{e_i}$ e $E^{(n)}$ é um grupo cíclico com gerador $\beta = \beta_1 \dots \beta_t$.

(ii) Segue imediatamente do fato que $X^n - 1 = X^{mp^e} - 1 = (X^m - 1)^{p^e}$ e do item (i).

□

Exemplo 1.3.4: Sejam $n = 3$, $\mathbb{F}_4$ o corpo de separação de $X^3 - 1$ sobre $\mathbb{F}_2$ e $p = 2$ a característica de $\mathbb{F}_4$. Observe que $2 \nmid 3$ e $X^3 - 1 = (X-1)(X^2 + X + 1)$. Seja $\zeta \in \mathbb{F}_4$ uma raíz de $X^2 + X + 1 \in \mathbb{F}_2[X]$. Então, $\zeta^2 + \zeta + 1 = 0$ e daí $\zeta^2 = 1 + \zeta$. Note que $1 + \zeta$ também é raíz de $X^2 + X + 1$, pois

$$(1+\zeta)^2 + (1+\zeta) + 1 = 1 + 2\zeta + \zeta^2 + 1\zeta + 1 = 3 + 3\zeta + (1+\zeta) = 4 + 4\zeta = 0.$$

Logo, $E^{(3)} = \{1, \zeta, \zeta^2 = 1 + \zeta\}$. Mas note que $\zeta^1 = \zeta, \zeta^2 = 1 + \zeta$ e $\zeta^3 = \zeta^2\zeta = (1+\zeta)\zeta = \zeta + \zeta^2 = \zeta + (1+\zeta) = 1 + 2\zeta = 1$. Ou seja, $E^{(3)} =< \zeta >$. Portanto, $E^{(3)}$ é um grupo cíclico de ordem 3 com respeito à multiplicação de $\mathbb{F}_4 = \mathbb{F}_2^{(3)}$.

Definição 1.3.5: Sejam K um corpo de característica p e n um inteiro positivo não divisível por p. Então, um gerador do grupo cíclico $E^{(n)}$ é chamado de $n-$ésima raíz primitiva da unidade sobre K.

Exemplo 1.3.6: Do Exemplo 1.3.4 temos que $E^{(3)} =< \zeta >$. Então, ζ é uma $3-$ésima raíz primitiva da unidade sobre $\mathbb{F}_2$.

Definição 1.3.7: Sejam K um corpo de característica p, n um inteiro positivo não divisível por p e ζ a $n-$ésima raíz primitiva da unidade sobre K. Então, o polinômio

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

com $mdc(s,n) = 1$, é chamado de $n-$ésimo polinômio ciclotômico sobre K. O polinômio $Q_n(X)$ independe da escolha de ζ. O grau de $Q_n(X)$ é $\phi(n)$ e seus coeficientes pertencem ao $n-$ésimo corpo ciclotômico sobre K. Um simples argumento mostra que estes estão contidos no subcorpo primo de K. Usamos os símbolo do produto $\prod_{d|n}$ para denotar o produto extendido sobre todos os divisores positivos d do inteiro positivo n.

Teorema 1.3.8: Sejam K um corpo finito 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. Seguem as demonstrações:

(i) Cada $n-$ésima raíz da unidade sobre K é uma $d-$ésima raíz primitiva da unidade sobre K para exatamente um divisor positivo d de n. Em detalhes, se ζ é uma $n-$ésima raíz primitiva da unidade sobre K e ζ^s é uma $n-$ésima raíz arbitrária da unidade sobre K, então, $d = n/mdc(s,n)$, além disso, d é a ordem de ζ^s em $E^{(n)}$. Como

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

a fórmula é obtida em (i) por coleções dos fatores $(X - \zeta^s)$ onde ζ^s é uma $d-$ésima raíz primitiva da unidade sobre K.

(ii) Faremos a demonstração deste item por indução sobre n. Inicialmente note que $Q_n(X)$ é um polinômio mônico. Se $n = 1$ temos que $Q_1(X) = X - 1$ e a afirmação é válida. Agora, considere $n > 1$ e suponha que a proposição é verdadeira para todos os polinômios $Q_d(X)$ com $1 \leq d < n$. Então, segue do item (i) que $Q_n(X) = (X^n - 1)/f(X)$, onde $f(X) = \prod_{d|n} Q_d(X)$. A hipótese de indução implica que $f(X)$ é um polinômio com coeficientes no subcorpo primo de K ou em $\mathbb{Z}$ no caso em que a característica de K é 0. Usando divisão longa com $X^n - 1$ e o polinômio mônico $f(X)$, vemos que os coeficientes de $Q_n(X)$ pertencem ao subcorpo primo de K ou de $\mathbb{Z}$, respectivamente.

□

Exemplo 1.3.9: Sejam $n = 3$, K um corpo finito qualquer com característica diferente de 3 e ζ uma raíz cúbica da unidade sobre K. Então,

$$Q_3(X) = (X-\zeta)(X-\zeta^2) = X^2 - (\zeta+\zeta^2)x + \zeta^3 = X^2 + X + 1.$$

Exemplo 1.3.10: Sejam r um primo e $k \in \mathbb{N}$. Então,

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

mas, pelo Teorema 1.3.8 temos

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

Para $k = 1$ nós simplesmente temos $Q_r(X) = 1 + X + X^2 + \cdots + X^{r-1}$.

Teorema 1.3.11: O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K. E mais,

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

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

Demonstração. Se existe uma $n-$ésima raíz primitiva da unidade ζ sobre K, é claro que $K^{(n)} = K(\zeta)$. Por outro lado, pela situação descrita no Teorema 1.3.3 item (ii), temos que $K^{(n)} = K^{(m)}$ e segue o resultado. Provemos o item (ii). Seja η uma $n-$ésima raíz primitiva da unidade sobre $\mathbb{F}_q$. Então, $\eta \in \mathbb{F}_{q^k}$ se, e somente se, $\eta^{q^k} = \eta$ e a última identidade é equivalente a $q^k \equiv 1(mod\ n)$. O menor inteiro para o qual ainda vale a congruência é $k = d$ e, então, $\eta \in \mathbb{F}_{q^d}$, mas em nenhum subcorpo adequado. Portanto, o polinômio minimal de η sobre $\mathbb{F}_q$ tem grau d e, então, η é uma raíz arbitrária de Q_n, daí segue o resultado desejado. □

Exemplo 1.3.12: Sejam $K = \mathbb{F}_{11}$ e $Q_{12}(X) = X^4 - X^2 + 1 \in \mathbb{F}_{11}[X]$. Pela notação do teorema anterior temos que $d = 2$. Em detalhes, $Q_{12}(X)$ se fatora da forma $Q_{12}(X) = (X^2 + 5X + 1)(X^2 - 5X + 1)$, com ambos os fatores sendo irredutíveis em $\mathbb{F}_{11}[X]$. O corpo ciclotômico $K^{(12)}$ é igual a $\mathbb{F}_{121}$.

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

Teorema 1.3.13: O corpo finito $\mathbb{F}_q$ é o $(q-1)-$ésimo corpo ciclotômico sobre qualquer um de seus outros subcorpos.

Demonstração. O polinômio $X^{q-1} - 1$ se separa em $\mathbb{F}_q$ pois suas raízes são exatamente os elementos não nulos de $\mathbb{F}_q$. Obviamente, o polinômio não se separa em qualuqer outro subcorpo próprio de $\mathbb{F}_q$, então, $\mathbb{F}_q$ é o corpo de separação de $X^{q-1} - 1$ sobre qualquer um de seus outros subcorpos. □

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

Concluímos esta seção com um lema que usaremos mais tarde.

Lema 1.3.14: Se d é um divisor do inteiro positivo n com $1 \leq d \leq n$, então $Q_n(X)$ divide $(X^n-1)/(X^d-1)$ sempre que $Q_n(X)$ é definido.

Demonstração. Do teorema 1.3.8 item (i) sabemos que $Q_n(X)$ divide

$$X^n-1 = (X^d-1)\frac{X^n-1}{X^d-1}.$$

Como d é um divisor próprio de n, os polinômios $Q_n(X)$ e X^d-1 não têm raízes em comum, consequentemente $mdc(Q_n(X), X^d-1) = 1$ e segue o resultado desejado. □

1.4 Representação de elementos em corpos finitos

Nessa seção descreveremos três maneiras diferentes de representar os elementos em um corpo finito $\mathbb{F}_q$ com $q = p^n$ elementos, onde p é a característica de $\mathbb{F}_q$. Notemos que $\mathbb{F}_q$ é uma extensão algébrica simples de $\mathbb{F}_p$, como exposto no Teorema 1.0.14. De fato, se f é um polinômio irredutível em $\mathbb{F}_p[X]$ de grau n, então, f tem uma raíz $\alpha \in \mathbb{F}_q$ como mostra o Teorema 1.1.8 e, então, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Além disso, todo elemento de $\mathbb{F}_q$ pode ser unicamente expressado como um polinômio em α sobre $\mathbb{F}_p$ de grau menor que n. Podemos também visualizar $\mathbb{F}_q$ como a classe de resíduos do anel $\mathbb{F}_p[X]/ < f >$.

Exemplo 1.4.1: Considere $\mathbb{F}_8$ como uma extensão algébrica simples de $\mathbb{F}_2$ de grau 3, o qual é obtido por adjunção de uma raíz α de um polinômio cúbico irredutível sobre $\mathbb{F}_2$, digamos $f(X) = X^3+X+1 \in \mathbb{F}_2[X]$. Consequentemente, $f(\alpha) = \alpha^3+\alpha+1 = 0$ em $\mathbb{F}_8$ e, os oito elementos de $\mathbb{F}_8$ são da forma $a_0+a_1\alpha+a_2\alpha^2$, com $a_0,a_1,a_2 \in \mathbb{F}_2$. Em detalhes, $\mathbb{F}_8 = \{0,1,\alpha,\alpha^2,1+\alpha,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\}$.

Exemplo 1.4.2: Analogamente ao exemplo anterior, considere $\mathbb{F}_9$ como uma extensão algébrica simples de $\mathbb{F}_3$ de grau 2, o qual é obtido por adjunção de uma raíz α de um polinômio quadrático irredutível sobre $\mathbb{F}_3$, digamos $f(X) = X^2+1 \in \mathbb{F}_3[X]$. Assim, $f(\alpha) = \alpha^2+1 = 0$ em $\mathbb{F}_9$, além disso, os nove elementos de $\mathbb{F}_9$ são da forma $a_0+a_1\alpha$, com $a_0,a_1 \in \mathbb{F}_3$. Ou seja, $\mathbb{F}_9 = \{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$.

Se usarmos os Teoremas 1.3.11 e 1.3.13 podemos exibir outra possibilidade de expressar os elementos de $\mathbb{F}_q$. Como $\mathbb{F}_q$ é o $(q-1)-$ésimo corpo ciclotômico sobre $\mathbb{F}_p$, podemos construi-lo encontrando a decomposição do $(q-1)-$ésimo polinômio ciclotômico $Q_{q-1} \in \mathbb{F}_p[X]$ em fatores irredutíveis em $\mathbb{F}_p[X]$, o qual são todos de mesmo grau. Uma raíz de um desses fatores é, então, uma $(q-1)-$ésima

raíz primitiva da unidade sobre $\mathbb{F}_p$ e, então, um elemento primitivo de $\mathbb{F}_q$. Consequentemente, $\mathbb{F}_q$ consiste do 0 e de potências apropriadas de um elemento primitivo.

Exemplo 1.4.3: Para aplicar o que vimos anteriormente à construção de $\mathbb{F}_9$, notemos que $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, o oitavo corpo ciclotômico sobre $\mathbb{F}_3$. Agora, $Q_8(X) = X^4 + 1 \in \mathbb{F}_3[X]$ pelo Exemplo 1.3.10, e mais

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

é a decomposição de Q_8 em fatores irredutíveis em $\mathbb{F}_3[X]$. Seja ζ uma raíz de $X^2 + X + 2$, então, ζ é a oitava raíz primitiva da unidade sobre $\mathbb{F}_3$. Consequentemente, todos os elementos não nulos de $\mathbb{F}_9$ podem ser expressos como potências de ζ e, então, $\mathbb{F}_9 = \{0, \zeta, \zeta^2, \ldots, \zeta^8\}$. Podemos organizar os elementos diferentes de zero de $\mathbb{F}_9$ em uma chamada tabela de índices, onde nós listamos os elementos ζ^i, com $i = 1, 2, \ldots, 8$, de acordo com seus expoentes i. A fim de estabelecer a conexão com a representação no Exemplo 1.4.2, nós observamos que $X^2 + X + 2 \in \mathbb{F}_3[X]$ tem $\zeta = 1 + \alpha$ como uma raíz, onde $\alpha^2 + 1 = 0$, como no Exemplo 1.4.2. Então, as tabelas de índices para $\mathbb{F}_9$ podem ser escritas como segue:

Tabela 1: índices de 1 a 4

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

Tabela 2: índices de 5 a 8

i	ζ^i
5	$2+2\alpha$
6	α
7	$2+\alpha$
8	1

Assim, por meio das tabelas vemos que obtemos, claramente, os mesmos elementos do Exemplo 1.4.2, apenas em ordem diferente.

Exemplo 1.4.4: Analogamente ao que vimos no exemplo anterior, façamos o mesmo procedimento para o corpo $\mathbb{F}_8$. Para isso, note que $\mathbb{F}_8 = \mathbb{F}_2^{(7)}$ é o sétimo corpo ciclotômico sobre $\mathbb{F}_2$. Assim $Q_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, logo, $Q_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1)$ é a decomposição de Q_7 em fatores irredutíveis em $\mathbb{F}_2[X]$. Seja η uma raíz de $X^3 + X + 1$, então, η é a sétima raíz primitiva da unidade sobre $\mathbb{F}_2$. Logo, todos os elementos não nulos de $\mathbb{F}_8$ podem ser expressos como potências de η, ou seja, $\mathbb{F}_8 = \{0, \eta, \eta^2, \ldots, \eta^7\}$. Com isso, podemos organizar os elementos diferentes de zero de $\mathbb{F}_8$ por meio da tabela de índices. A fim de estabelecer a conexão com a representação no Exemplo 1.4.1, nós observamos que $X^3 + X + 1 \in \mathbb{F}_2[X]$ tem $\eta = \alpha + \alpha^2$ como uma raíz, onde $\alpha^3 + \alpha + 1 = 0$. Então, as tabelas de índices para $\mathbb{F}_8$ podem ser escritas como segue:

Tabela 1: índices de 1 a 4

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

Tabela 2: índices de 5 a 7

i	η^i
5	$1 + \alpha^2$
6	$1 + \alpha$
7	1

Note que obtemos, a menos da ordem, os mesmos elementos do Exemplo 1.4.1.

Uma terceira possibilidade de representar os elementos de $\mathbb{F}_q$ é dada por meio de matrizes. Em geral, a matriz companheira de um polinômio mônico $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ de grau positivo n sobre um corpo é definida pela matriz $n \times n$

$$A = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}$$

É bem conhecido na Álgebra Linear que A satisfaz a equação $f(A) = 0$, que é, $a_0I + a_1A + \cdots + a_{n-1}A^{n-1} + A^n = 0$, onde I é a matriz identidade $n \times n$.

Consequentemente, se A é a matriz companheira de um polinômio mônico irredutível f sobre $\mathbb{F}_p$ de grau n, então, $f(A) = 0$ e A pode desempenhar o papel de uma raíz de f. Os polinômios em A sobre $\mathbb{F}_p$ de grau menor que n produz uma representação de elementos de $\mathbb{F}_q$.

Exemplo 1.4.5: Considere o polinômio $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$ do Exemplo 1.4.1. A matriz companheira de f é

$$B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

O corpo $\mathbb{F}_8$ pode ser representado na forma $\mathbb{F}_8 = \{0, I, B, B^2, I+B, I+B^2, B+B^2, I+B+B^2\}$. Onde,

$$0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, B^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Exemplo 1.4.6: Como no Exemplo 1.4.2, seja $f(X) = X^2 + 1 \in \mathbb{F}_3[X]$. A matriz companheira de f é

$$A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$$

O corpo $\mathbb{F}_9$ pode ser representado na forma $\mathbb{F}_9 = \{0, I, 2I, A, I+A, 2I+A, 2A, I+2A, 2I+2A\}$. Explicitamente:

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, 2I = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix},$$

$$I+A=\begin{bmatrix}1&2\\1&1\end{bmatrix}, 2I+A=\begin{bmatrix}2&2\\1&2\end{bmatrix}, 2A=\begin{bmatrix}0&1\\2&0\end{bmatrix},$$

$$I+2A=\begin{bmatrix}1&1\\1&2\end{bmatrix}, 2I+2A=\begin{bmatrix}2&1\\2&2\end{bmatrix}.$$

Com $\mathbb{F}_9$ dado dessa forma, cálculos neste corpo finito são então realizados pelas regras usuais da álgebra de matrizes. Por exemplo,

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

Do mesmo modo, o método baseado na fatorização do polinômio ciclotômico Q_{q-1} em $\mathbb{F}_p[X]$ pode ser adaptado para produzir uma representação dos elementos de $\mathbb{F}_q$ em termos de matrizes.

Exemplo 1.4.7: Como no Exemplo 1.4.3, seja $h(X)=X^2+X+2\in\mathbb{F}_3[X]$ um fator irredutível do polinômio ciclotômico $Q_8\in\mathbb{F}_3[X]$. A matriz companheira de h é

$$C=\begin{bmatrix}0&1\\1&2\end{bmatrix}.$$

O corpo $\mathbb{F}_9$ pode, então, ser representado na forma $\mathbb{F}_9=\{0,C,C^2,\ldots,C^8\}$. Explicitamente,

$$0=\begin{bmatrix}0&0\\0&0\end{bmatrix}, C=\begin{bmatrix}0&1\\1&2\end{bmatrix}, C^2=\begin{bmatrix}1&2\\2&2\end{bmatrix}$$

$$C^3=\begin{bmatrix}2&2\\2&0\end{bmatrix}, C^4=\begin{bmatrix}2&0\\0&2\end{bmatrix}, C^5=\begin{bmatrix}0&2\\2&1\end{bmatrix}$$

$$C^6=\begin{bmatrix}2&1\\1&1\end{bmatrix}, C^7=\begin{bmatrix}1&1\\1&0\end{bmatrix}, C^8=\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

Os cálculos procedem das regras da álgebra de matrizes. Por exemplo,

$$C^6+C=\begin{bmatrix}2&1\\1&1\end{bmatrix}+\begin{bmatrix}0&1\\1&2\end{bmatrix}=\begin{bmatrix}2&2\\2&0\end{bmatrix}=C^3.$$

Capítulo 2

Polinômios sobre corpos finitos

Nessa seção investigaremos as estruturas algébricas de corpos finitos bem como suas aplicações. Assim, os polinômios irredutíveis, que são os elementos irredutíveis de um anel de polinômios sobre um corpo finito, serão indispensáveis para construirmos corpos finitos e computarmos com os elementos desses corpos.

Na primeira seção vamos introduzir a noção de ordem de um polinômio. Além disso, veremos que existe uma relação entre o polinômio minimal de um elemento primitivo (também chamado de polinômio primitivo) e polinômios de maior ordem possível para um grau dado. Resultados sobre polinômios irredutíveis além daqueles discutidos nos capítulos anteriores são apresentados na segunda seção. A próxima seção é dedicada aos aspectos construtivos da irredutibilidade e trata também do problema de calcular o polinômio minimal de um elemento em uma extensão de um corpo. Certos tipos especiais de polinômios são discutidos nas duas últimas seções.

2.1 Ordem de polinômios e polinômios primitivos

Além do grau, há outro número inteiro importante anexado a um polinômio diferente de zero sobre um corpo finito, a saber, sua ordem. A definição da ordem de um polinômio é baseada no seguinte resultado.

Lema 2.1.1: 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 $X^e - 1$.

Demonstração. A classe residual do anel $\mathbb{F}_q[X]/ < f >$ contém $q^m - 1$ classes residuais não nulas. As q^m classes residuais $X^j + < f >, j = 0, 1, \ldots, q^m - 1$, são todas não-nulas e, então, existem inteiros r e s com $0 \leq r < s \leq q^m - 1$ tais que $X^s \equiv X^r (\text{mod } f(X))$. Como X e $f(X)$ são relativamente primos, segue que $X^{s-r} \equiv 1 (\text{mod } f(X))$, isto é, $f(X)$ divide $X^{s-r} - 1$ e $0 < s - r \leq q^m - 1$. □

Exemplo 2.1.2: Seja $f(X) = X^2 + X + 1 \in \mathbb{F}_3[X]$. Note que $f \nmid X - 1, f \nmid X^2 - 1$ mas $f \mid X^3 - 1 = (X - 1)(X^2 + X + 1)$. Logo, $e = 3$.

Definição 2.1.3: 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 é 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 unicamente determinados, assim, $ord(f)$ é então definida pela $ord(g)$.

Exemplo 2.1.4: Segue do Exemplo 2.1.2 que $e = 3$ é a ordem de f.

Exemplo 2.1.5: Considere agora o polinômio $f(X) = X^3 - X \in \mathbb{F}_2[X]$ com $f(0) = 0$. Mas observe que $f(X) = X(X^2 - 1)$ com $h = 1$ e $g(X) := X^2 - 1$. Além disso, $g \mid g$, logo, $ord(g) = 2$. Segue da Definição 2.1.3 que $ord(f) = 2$.

A ordem de um polinômio f é, às vezes, chamada de período de f ou expoente de f. A ordem de um polinômio irredutível f pode também ser caracterizada como no seguinte teorema.

Teorema 2.1.6: Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m e com $f(0) \neq 0$. Então, $ord(f)$ é igual a ordem de alguma raíz de f no grupo multiplicativo $\mathbb{F}_{q^m}^*$

Demonstração. Sabemos que $\mathbb{F}_{q^m}$ é o corpo de separação de f sobre $\mathbb{F}_q$. Além disso, as raízes de f têm a mesma ordem no grupo $\mathbb{F}_{q^m}^*$. Seja $\alpha \in \mathbb{F}_{q^m}^*$ uma raíz de f. Então, temos que $\alpha^e \equiv 1$ se, e somente se, $f(X)$ divide $X^e - 1$. O resultado segue das definições de $ord(f)$ e da ordem de α no grupo multiplicativo $\mathbb{F}_{q^m}^*$. □

Exemplo 2.1.7: Seja $f(X) = X^2 + X + 2 \in \mathbb{F}_3[X]$ um polinômio irredutível sobre $\mathbb{F}_3$ de grau 2 e com $f(0) = 2 \neq 0$. Seja α uma raíz de $f(X)$ em alguma extensão de $\mathbb{F}_3$, então, $\alpha^2 = -(2+\alpha) = 2(2+\alpha) = 1 + 2\alpha$. Daí, $\alpha^8 = 1$ Logo, a ordem de α é 8. Então, pelo Teorema 2.1.6 segue que $ord(f) = 8$.

Corolário 2.1.8: Se $f \in \mathbb{F}_q[X]$ é um polinômio irredutível sobre $\mathbb{F}_q$ de grau m, então, $ord(f)$ divide $q^m - 1$.

Demonstração. Se $f(X) = cX$ com $c \in \mathbb{F}_q^*$, então, $ord(f) = 1$ e o resultado é trivial. Caso contrário, o resultado segue do Teorema 2.1.6 e do fato que $\mathbb{F}_{q^m}^*$ é um grupo de ordem $q^m - 1$. □

Exemplo 2.1.9: Agora, tome $f(X) = X^2 + 1$ irredutível sobre $\mathbb{F}_3$ de grau 2. Então, $ord(f)$ divide $3^2 - 1 = 8$. Assim, $ord(f) \in \{1, 2, 4, 8\}$. Como f não divide $X - 1$ e $X^2 - 1$, temos que $ord(f) \in \{4, 8\}$. Note que $X^4 - 1 = (X^2 + 1)(X^2 - 1)$ e $X^8 - 1 = (X^4 + 1)(X^4 - 1) = (X^4 + 1)(X^2 + 1)(X^2 - 1)$. Como queremos o menor inteiro positivo e tal que f divide $X^e - 1$ segue que $ord(f) = 4$.

Existe outra interpretação da $ord(f)$ baseada em associar uma matriz quadrada a f e considerar a ordem dessa matriz em um certo grupo de matrizes.

A terminologia seguinte nos será muito conveniente: se n é um inteiro positivo e o inteiro positivo b é relativamente primo a n, então, o menor inteiro positivo k para o qual $b^k \equiv 1 \pmod{n}$ é chamado de *ordem multiplicativa* de b módulo n.

Teorema 2.1.10: O número de polinômios mônicos 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 em todos os outros casos. Em particular, o grau de um polinômio irredutível em $\mathbb{F}_q[X]$ de ordem e deve ser igual à ordem multiplicativa de q módulo e.

Demonstração. Seja f um polinômio irredutível em $\mathbb{F}_q[X]$ com $f(0) \neq 0$. Então, pelo Teorema 2.1.6 temos que $ord(f) = e$ se, e somente se, todas as raízes de f são as $e-$ésimas raízes primitivas da unidade sobre $\mathbb{F}_q$. Em outras palavras temos que $ord(f) = e$ se, e somente se, f divide o polinômio ciclotômico Q_e. Como qualquer fator mônico irredutível de Q_e tem o mesmo grau m, o menor inteiro positivo tal que $q^m \equiv 1 (\text{ mod } e)$ e o número de tais fatores é dado por $\phi(e)/m$. Para $m = e = 1$ também temos que levar em consideração o polinômio mônico irredutível $f(X) = x$. □

Exemplo 2.1.11: Sejam $m = 2, e = 3$. Observe que $5^2 \equiv 1 \pmod 3$, ou seja, 2 é a ordem multiplicativa de 5 módulo 3. Logo, pelo Teorema 2.1.10 segue que existe $1 = \phi(3)/2$ polinômio mônico irredutível em $\mathbb{F}_5[X]$ de grau 2 e ordem 3.

Como qualquer polinômio de grau positivo pode ser escrito como um produto de polinômios irredutíveis, computar a ordem de polinômios pode ser alcançado se souber como determinar a ordem de uma potência de um polinômio irredutível e a ordem do produto de polinômios relativamente primos dois a dois. A discussão subsequente é dedicada a essas questões.

Lema 2.1.12: 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, $ord(f)$ divide c.

Demonstração. Se $e = ord(f)$ divide c, então, $f(X)$ divide $X^e - 1$ e $X^e - 1$ divide $X^c - 1$, logo, $f(X)$ divide $X^c - 1$. Reciprocamente, se $f(X)$ divide $X^c - 1$ temos que $c \geq e$, 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 $X^r - 1$, o qual só é possível para $r = 0$. Então, e divide c. □

Exemplo 2.1.13: Vimos no Exemplo 2.1.9 que a ordem do polinômio $f(X) = X^2 + 1$ sobre $\mathbb{F}_3$ é 4. Então, pelo Lema 2.1.12 segue que $f(X)$ divide o polinômio $X^{64} - 1$, pois, $4 \mid 64$.

Corolário 2.1.14: Se e_1 e e_2 são inteiros positivos, então, o maior divisor comum de $X^{e_1} - 1$ e $X^{e_2} - 1$ em $\mathbb{F}_q[X]$ é $X^d - 1$, onde d é o máximo divisor comum de e_1 e e_2.

Demonstração. Seja $f(X)$ o maior divisor comum (mônico) de $X^{e_1} - 1$ e $X^{e_2} - 1$. Como $X^d - 1$ é 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, então, o Lema 2.1.12 implica que $ord(f)$ divide e_1 e e_2. Consequentemente, $ord(f)$ divide d e, consequentemente, $f(X)$ divide $X^d - 1$ pelo 2.1.12. Assim, mostramos que $f(X) = X^d - 1$. □

Uma vez que 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 $g(0) = 0$.

Exemplo 2.1.15: Sejam $f(X) = X^{14} - 1$ e $g(X) = X^{21} - 1$ polinômios em $\mathbb{F}_{2^5}[X]$. Então, pelo Corolário 2.1.14 temos que o maior divisor comum de f e g em $\mathbb{F}_{2^5}[X]$ é $X^7 - 1$, onde $7 = mdc(14,21)$.

Teorema 2.1.16: Seja $g \in \mathbb{F}_q[X]$ irredutível sobre $\mathbb{F}_q$ com $g(0) \neq 0$, $ord(g) = e$ e seja $f = g^b$ com b um 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. Pondo $c = ord(f)$ e notando que a divisibilidade de $X^c - 1$ por $f(X)$ implica a divisibilidade de $X^c - 1$ por $g(X)$, obtemos que e divide c pelo Lema 2.1.12. Além disso, $g(X)$ divide $X^e - 1$, então, $f(X)$ divide $(X^e - 1)^b$ e, a priori, divide $(X^e - 1)^{p^t} = X^{ep^t} - 1$. Assim, de acordo com o Lema 2.1.12, c divide ep^t. Segue daí que temos que mostrar então que c é da forma $c = ep^u$ com $0 \leq u \leq t$. Notamos assim que $X^e - 1$ tem somente raízes simples, como e não é um múltiplo de p pelo Corolário 2.1.8. Então, todas as raízes de $X^{ep^u} - 1 = (X^e - 1)^{p^u}$ tem multiplicidade p^u. Mas, $g(X)^b$ divide $X^{ep^u} - 1$, daí $p^u \geq b$ por comparação da multiplicidade das raízes e, então, $u \geq t$. Consequentemente temos que $u = t$ e $c = ep^t$. □

Exemplo 2.1.17: Seja $g(X) = X + 1$ um polinômio irredutível sobre $\mathbb{F}_3$ de grau 1. Note que $g(0) = 1 \neq 0$. Como g é irredutível segue que $ord(g) \mid 3 - 1 = 2$, ou seja, $ord(f) \in \{1,2\}$. Claramente $X + 1 \nmid X - 1$. Portanto, $ord(g) = 2$. Seja $f(X) = g(X)^2 = (X+1)^2 = X^2 + 2X + 1$. Logo, pelo Teorema 2.1.16 segue que $ord(f) = 2 \cdot 3 = 6$.

Teorema 2.1.18: Sejam $g_1, \ldots, g_k$ polinômios não nulos sobre $\mathbb{F}_q$ relativamente primos dois a dois e, seja $f = g_1 \ldots g_k$. Então, $ord(f)$ é igual ao mínimo múltiplo comum de $ord(g_1), \ldots, ord(g_k)$.

Demonstração. É fácil ver que é suficiente considerar o caso onde $g_i(0) \neq 0$ para $i = 1, \ldots, k$. Seja $e = ord(f)$ e $e_i = ord(g_i)$ para $i = 1, \ldots, k$ e, seja $c = mmc(e_1, \ldots, e_k)$. Então, cada $g_i(X)$ divide $X^{e_1} - 1$ e então $g_i(X)$ divide $X^c - 1$. Como os polinômios $g_1, \ldots, g_k$ são relativamente primos dois a dois segue que $f(X)$ divide $X^c - 1$. Por uma aplicação do Lema 2.1.12 obtemos que e divide c. Por outro lado, $f(X)$ divide $X^e - 1$ e, então, cada $g_i(X)$ divide $X^e - 1$. Aplicando novamente o Lema 2.1.12 segue que cada e_i divide e e, então, c divide e. Consequentemente, concluimos que $e = c$. □

Definição 2.1.19: Seja $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{F}_q[X]$ com $a_n \neq 0$. Então, o polinômio recíproco de f^* de f é definido por

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

Exemplo 2.1.20: Seja $f(X) = X^3 + X + 1 \in \mathbb{F}_5[X]$. Então, o polinômio recíproco de f é dado por $f^*[X] = X^3 f(1/x) = X^3(1/X^3 + 1/X + 1) = 1 + X^2 + X^3$.

Teorema 2.1.21: Seja f um polinômio não nulo em $\mathbb{F}_q[X]$ e f^* seu polinômio recíproco. Então, $ord(f) = ord(f^*)$.

Demonstração. Primeiro, considere o caso $f(0) \neq 0$. Então, o resultado segue do fato que $f(X)$ divide $X^e - 1$ se, e somente se, $f^*(X)$ também o divide. Se $f(0) = 0$, ponha $f(X) = X^h g(X)$ com $h \in \mathbb{N}$

e $g \in \mathbb{F}_q[X]$ satisfazendo $g(0) \neq 0$. Então, segue que $ord(f) = ord(g) = ord(g^*) = ord(f^*)$ onde a última identidade é válida desde que $g^* = f^*$. □

Existe também uma relação restrita entre as ordens de $f(X)$ e $f(-X)$. Se $f(X) = f(-X)$ é suficiente considerar corpos finitos de característica ímpar.

Teorema 2.1.22: Para q ímpar, seja $f \in \mathbb{F}_q[X]$ um polinômio de grau positivo com $f(0) \neq 0$. Seja e e E as ordens de $f(X)$ e $f(-X)$, respectivamente. Então, $E = e$ se, e somente se, e é um múltiplo de 4 e $E = 2e$ e se e é ímpar. Se e é duas vezes ímpar, então $E = e/2$ se todo fator irredutível de f tem ordem par e $E = e$ caso constrário.

Demonstração. Ver [10] p. 88. □

Definição 2.1.23: Um polinômio $f \in \mathbb{F}_q[X]$ de grau $m \geq 1$ é chamado polinômio primitivo sobre $\mathbb{F}_q$ se ele é o polinômio minimal sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^m}$

Consequentemente, um polinômio primitivo sobre $\mathbb{F}_q$ de grau m pode ser descrito como um polinômio mônico que é irredutível sobre $\mathbb{F}_q$ e tem raíz $\alpha \in \mathbb{F}_{q^m}$ que gera o grupo multiplicativo de $\mathbb{F}_{q^m}$. Polinômios primtivos podem também ser caracterizados como segue.

Teorema 2.1.24: 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 $f(0) \neq 0$. Como f é irredutível sobre $\mathbb{F}_q$, temos que $ord(f) = q^m - 1$ pelo Teorema 2.1.6 e do fato que f tem um elemento primitivo de $\mathbb{F}_{q^m}$ como uma raíz.

Reciprocamente, a propriedade $ord(f) = q^m - 1$ implica que $m \geq 1$. Agora, afirmamos que que f é irredutível sobre $\mathbb{F}_q$. Suponha que f é redutível sobre $\mathbb{F}_q$. Então, f é qualquer potência de um polinômio irredutível ou pode ser escrito como um produto de dois polinômios relativamente primos de grau positivo. No primeiro caso temos que $f = g^b$ com $g \in \mathbb{F}_q[X]$ irredutível sobre $\mathbb{F}_q$, $g(0) \neq 0$ e $b \geq 2$. Então, de acordo com o Teorema 2.1.16 temos que $ord(f)$ é divisível pela característica de $\mathbb{F}_q$, mas $q^m - 1$ não, uma contradição. No segundo caso, temos que $f = g_1 g_2$ com g_1, g_2 polinômios mônicos relativamente primos em $\mathbb{F}_q[X]$ e com graus m_1 e m_2, respectivamente. Se $e_i = ord(g_i)$ para $i = 1,2$ então $ord(f) \leq e_1 e_2$. E mais, $e_i \leq q^{m_i} - 1$ para $i = 1,2$ pelo Lema 2.1.1, consequentemente

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

uma contradição. Então, f é irredutível sobre $\mathbb{F}_q$ e, então, segue do Teorema 2.1.6 que f é um polinômio primitivo sobre $\mathbb{F}_q$. □

Exemplo 2.1.25: Seja $f(X) = X^2 + 2X + 2 \in \mathbb{F}_3[X]$ um polinômio irredutível de grau 2. Vamos verificar se f é um polinômio primitivo. Primeiramente vamos identificar a ordem de f. Como f é primitivo, segue que $ord(f) \mid 3^2 - 1 = 8$. Logo, $ord(f) \in \{1,2,4,8\}$. Por uma simples verificação

concluímos que f não divide $X-1, X^2-1$ nem X^4-1. Logo, $f \mid X^8-1$ e, portanto, $ord(f) = 8 = 3^2-1$. Ou seja, f é um polinômio primitivo.

Observemos que a condição de $f(0) \neq 0$ do teorema acima é necessária somente para descartar o polinômio não-primitivo $f(X) = X$ no caso $q = 2$ e $m = 1$. Outra caracterização de polinômios primitivos é baseada no seguinte resultado.

Lema 2.1.26: Seja $f \in \mathbb{F}_q[X]$ um polinômio de grau positivo com $f(0) \neq 0$. Seja r o menor inteiro positivo tal para o qual X^r é congruente módulo $f(X)$ a algum elemento de $\mathbb{F}_q$ e $X^r \equiv a (\text{mod } f(X))$ com a unicamente determinado, $a \in \mathbb{F}_q^*$. Então, $ord(f) = hr$, onde r é a ordem de a no grupo multiplicativo $\mathbb{F}_q^*$.

Demonstração. Ponha $e = ord(f)$. Como $X^e \equiv 1 (\text{mod } f(X))$, temos que $e \geq r$. Consequentemente, podemos escrever $e = sr + t$, com $s \in \mathbb{N}$ e $0 \leq t < r$. Agora,

$$1 \equiv X^e \equiv X^{sr+t} \equiv a^s X^t (mod f(X)), \tag{2.1}$$

então, $X^t \equiv a^{-s} (\text{mod } f(X))$ e, devido a definição de r, isso só é possível se $t = 0$. A congruência 2.1 produz então $a^s \equiv 1 (\text{mod } f(X))$, consequentemente $a^s = 1$ e, então, $s \geq h$ e $e \geq hr$. Por outro lado, $X^{hr} \equiv a^h \equiv 1 (\text{mod } f(X))$ e, assim, $e = hr$. □

Teorema 2.1.27: 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 módulo $f(X)$ a algum elemento de $\mathbb{F}_q$ é $r = (q^m-1)/(q-1)$. No caso, f é primitivo sobre $\mathbb{F}_q$ e temos $X^r \equiv (-1)^m f(0) (\text{mod } f(X))$.

Demonstração. Ver [10] p. 90. □

Exemplo 2.1.28: Considere o polinômio $f(X) = X^2 + 2X + 2 \in \mathbb{F}_3[X]$. Note que f é irredutível sobre $\mathbb{F}_3$. Além disso, pelo Exemplo 2.1.25 vimos que $ord(f) = 8$ e que f é um polinômio primitivo. E mais, temos que $X^4 \equiv 2 \pmod{X^2 + 2X + 2}$ de acordo com o Teorema 2.1.27.

2.2 Polinômios irredutíveis

Relembremos que um polinômio $f \in \mathbb{F}_q[X]$ é irredutível sobre o corpo finito $\mathbb{F}_q$ se f tem grau positivo e, além disso, toda fatorização de f em $\mathbb{F}_q[X]$ deve envolver uma constante polinomial (Ver Definição 1.57 em [10]).

Teorema 2.2.1: Para todo corpo finito $\mathbb{F}_q$ e todo $n \in \mathbb{N}$, o produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujo grau divide n é igual a $X^{q^n} - X$.

Demonstração. Pelo Lema 1.1.2 temos que os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ da fatorização canônica de $g(X) = X^{q^n} - X$ em $\mathbb{F}_q[X]$ são, precisamente, aqueles cujos grau divide n. Como $g'(X) = -1$, o Teorema 1.68 (Ver [10]) implica que g não tem raízes múltiplas em seu corpo de separação sobre $\mathbb{F}_q$ e, então, cada polinômio mônico irredutível sobre $\mathbb{F}_q$ cujo grau divide n ocorre exatamente uma vez na fatorização canônica de g em $\mathbb{F}_q[X]$. □

Exemplo 2.2.2: Considere um polinômio mônico qualquer sobre $\mathbb{F}_2$ e $n = 4$. Primeiramente devemos procurar quais são os polinômios mônicos irredutíveis sobre $\mathbb{F}_{2^4}$ de grau 1, 2 ou 4 (divisores de n=4). Os polinômios irredutíveis nesse caso são: $X, X+1, X^2+X+1, X^4+X+1, X^4+X^3+1$ e $X^4+X^3+X^2+X+1$. Partimos agora para o exemplo propriamente dito:
$X^{2^4} - X = (X)(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1) = X^{16} - X$.

Um consequência do Teorema 2.2.1 é o algoritmo de Rabin, o qual consiste em, basicamente, três passos: primeiramente deve-se gerar um polinômio $g(X)$ qualquer de grau d sobre o corpo finito $\mathbb{F}_q$; posteriormente deve-se verificar se $g(X)$ divide $X^q - X$; por fim, deve ser testado se o mínimo múltiplo comum entre $g(X)$ e $X^{p^{n_i}} - X$ é igual a 1, para todo $n_i = n/k_i$, onde os k_i são todos os divisores primos de n. Se os três passos forem satisfatórios significa que encontramos um polinômio irredutível.

Vamos denotar o número de polinômios mônicos irredutíveis de grau d sobre $\mathbb{F}_q$ por $N_q(d)$. Pelo resultado do teorema anterior tem-se o seguinte.

Corolário 2.2.3: Se $N_q(d)$ é o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau d, então

$$q^n = \sum_{d|n} dN_q(d), \forall n \in \mathbb{N} \tag{2.2}$$

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

Demonstração. Pelo Teorema 2.2.1 sabemos que o produto de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujo grau d divide n é igual a $X^{q^n} - X$. Assim, o produto de todos os polinômios mônicos irredutíveis de grau d, com $d \mid n$, deve ter grau q^n. Logo,

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

□

Exemplo 2.2.4: No exemplo anterior encontramos todos os polinômios irredutíveis de grau no máximo 4 sobre $\mathbb{F}_2$, assim, podemos contar quantos polinômios irredutíveis tem de grau 1, 2 e 4 $\in \mathbb{F}_{2^4}$ e, então, substituir na fórmula do corolário anterior exemplificando-o. Assim,

$$2^4 = \sum_{d|4} dN_{q(d)}.$$

Ou seja,

$$16 = 1.N_q(1) + 2.N_q(2) + 4.N_q(4) = 1.2 + 2.1 + 4.3 = 2 + 2 + 12$$

Contudo, ainda não encontramos uma fórmula explícita que determine o número de polinômios irredutíveis sobre $\mathbb{F}_q$. Para a obtermos precisamos definir, primeiramente, a função de Moebius e a inversão de Moebius.

Definição 2.2.5: A função de Moebius μ é a função em $\mathbb{N}$ definida por:

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

A função anterior foi introduzida por Moebius (1832), mas a notação $\mu(n)$ foi usada primeiramente por Mertens (1874).

Exemplo 2.2.6: Seja $n = 64$, então, $\mu(64) = 0$ pois 64 é divisível por 2^2. Agora, tome $n = 21$, então, $\mu(21) = \mu(3.7) = (-1)^2 = 1$.

Lema 2.2.7: Para $n \in \mathbb{N}$ a função de Moebius μ satisfaz:

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

Demonstração. O caso $n = 1$ é trivial. Assim, para $n > 1$ temos que levar em considereação somente os divisores positivos d de n para o qual $\mu(d) \neq 0$ - ou seja, para $d = 1$ ou para d como produto de primos distintos. Consequentemente, se $p_1, p_2, \ldots, p_k$ são primos distintos divisores de n temos que:

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

□

Exemplo 2.2.8: Seja $n = 12$. Então, os divisores de 12 são: $D(12) = \{1, 2, 3, 4, 6, 12\}$. Assim,

$$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 - 1 - 1 + 0 + 1 + 0 = 0$$

Teorema 2.2.9: (Fórmula da inversão de Moebius)

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

$$H(n) = \sum_{d|n} h(d), \text{para todo } n \in \mathbb{N} \tag{2.3}$$

se, e somente se,

$$h(n) = \sum_{d|n} \mu(n/d)H(d) = \sum_{d|n} \mu(d)H(n/d), \text{para todo } n \in \mathbb{N}. \tag{2.4}$$

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

$$H(n) = \prod_{d|n} h(d), \text{para todo } n \in \mathbb{N} \tag{2.5}$$

se, e somente se,

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} = \prod_{d|n} H(n/d)^{\mu(d)}, \text{para todo } n \in \mathbb{N}. \tag{2.6}$$

Demonstração. Assumindo 2.3 e usando o Lema 2.2.7 temos que

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

para todo $n \in \mathbb{N}$. A volta é derivada por um cálculo análogo. A prova da parte (ii) segue imediatamente da prova da parte (i) se trocarmos os somatórios por produtórios e os múltiplos convenientes por potências. □

Teorema 2.2.10: O número $N_q(n)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau n é dado por,

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

Demonstração. Aplique o caso aditivo da fórmula da inversão de Moebius ao grupo $G = \mathbb{Z}$, o grupo aditivo dos inteiros. Sejam $h(n) = nN_q(n)$ e $H(n) = q^n$ para todo $n \in \mathbb{N}$. Então 2.3 é satisfeito pela identidade 2.2 e, então, a identidade 2.4 nos dá a fórmula desejada. □

Através da fórmula anterior temos que para todo corpo finito $\mathbb{F}_q$ e todo $d \in \mathbb{N}$, existe um polinômio irredutível em $\mathbb{F}_q[X]$ de grau n. De fato, por meio de uma estimativa bruta e usando

$\mu(1) = 1$ e $\mu(d) \geq -1$ para todo $d \in \mathbb{N}$ temos que:

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} \cdots - q) = \frac{1}{n}(q^n - \frac{q^n - 1}{q-1}) > 0.$$

Exemplo 2.2.11: O número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau 20 é dado por:

$$\begin{aligned} N_q(12) &= \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q) \\ &= \frac{1}{12}(q^{12} - q^6 - q^4 + q^2). \end{aligned}$$

Como outra aplicação da fórmula da inversão de Moebius nós estabelecemos a seguir uma fórmula explícita para o $n-$ésimo polinômio ciclotômico Q_n.

Teorema 2.2.12: Para um corpo finito $\mathbb{K}$ de característica p e $n \in \mathbb{N}$ não divisível por p, então, o $n-$ésimo polinômio ciclotômico Q_n sobre $\mathbb{K}$ satisfaz

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

Demonstração. Apliquemos o caso multiplicativo da fórmula da inversão de Moebius ao grupo multiplicativo G de funções racionais diferentes de zero sobre $\mathbb{K}$. Sejam $h(n) = Q_n(X)$ e $H(n) = X^n - 1$ para todo $n \in \mathbb{N}$. Então, o Teorema 1.3.8(i) mostra que 2.5 é satisfeita e, então, 2.6 nos fornece o resultado desejado. □

Exemplo 2.2.13: Para os corpos $\mathbb{K}$ sobre os quais Q_{12} é definido temos que:

$$\begin{aligned} Q_{12}(X) &= \sum_{d|12}(X^{12/d} - 1)^{\mu(d)} \\ &= (X^{12} - 1)^{\mu(1)}(X^6 - 1)^{\mu(2)}(X^4 - 1)^{\mu(3)}(X^3 - 1)^{\mu(4)}(X^2 - 1)^{\mu(6)}(X - 1)^{\mu(12)} \\ &= \frac{(X^{12} - 1)(X^2 - 1)}{(X^6 - 1)(X^4 - 1)} = X^4 - X^2 + 1. \end{aligned}$$

A fórmula explícita do Teorema 2.2.12 pode ser usado para estabelecer as propriedades básicas dos polinômios ciclotômicos. No Teorema 2.2.10 determinamos o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau fixo. Apresentamos agora uma fórmula para o produto de todos os polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau fixado.

Teorema 2.2.14: 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. Segue do Teorema 2.2.1 que

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

Aplicando o caso multiplicativo da fórmula da inversão de Moebius ao grupo multiplicativo G das funções racionais não nulas sobre $\mathbb{F}_q$ e considerando $h(n) = I(q,n;X)$ e $H(n) = X^{q^n} - X$, obtemos a fórmula desejada. □

Exemplo 2.2.15: Para $q = 2$ e $n = 2$ nós temos:

$$\begin{aligned} I(2,2;X) &= (X^4 - X)^{\mu(1)}(X^2 - X)^{\mu(2)} \\ &= \frac{X^4 - X}{X^2 - x} = \frac{X^3 - 1}{X - 1} \\ &= X^2 + X + 1. \end{aligned}$$

Todos o polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau n podem ser determinados fatorando-se $I(q,n;x)$. Para este propósito é vantajoso ter $I(q,n;x)$ disponível em uma forma parcialmente fatorada. Isso é alcançado pelo seguinte resultado.

Teorema 2.2.16: Seja $I(q,n;X)$ como no Teorema 2.2.14. Então, para $n > 1$ temos que

$$I(q,n;X) = \prod_m Q_m(X) \tag{2.7}$$

onde o produto é extendido sobre 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 o conjunto dos elementos de $\mathbb{F}_{q^n}$ que são de grau n sobre $\mathbb{F}_q$. Então, todo $\alpha \in S$ tem um polinômio minimal sobre $\mathbb{F}_q$ de grau n e é, consequentemente, uma raíz de $I(q,n;X)$. Por outro lado, se β é uma raíz de $I(q,n;X)$ então β é raíz de algum polinômio mônico irredutível em $\mathbb{F}_q[X]$ de grau n, o qual implica que $\beta \in S$. Portanto,

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

Se $\alpha \in S$ então $\alpha \in \mathbb{F}_{q^n}^*$ e, então, a ordem de α no grupo multiplicativo é um divisor de $q^n - 1$. Notemos que $\gamma \in \mathbb{F}_{q^n}^*$ é um elemento de um subcorpo próprio de $\mathbb{F}_{q^d}$ de $\mathbb{F}_{q^n}$ se, e somente se, $\gamma^{q^d} = \gamma$ - se, e somente se, a ordem de γ divide $q^d - 1$. Consequentemente, a ordem de m de um elemento α de S deve ser tal que n é o menor inteiro positivo com $q^n \equiv 1 \bmod m$ - tal que n é a ordem multiplicativa de q módulo m. Para um divisor positivo m de $q^n - 1$ com essa propriedade, seja S_m o conjunto dos elementos de S de ordem m. Então, S é a união disjunta dos subconjuntos S_m, então podemos 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 das $m-$ésimas raízes primitivas da unidade sobre $\mathbb{F}_q$. Da definição de polinômios ciclotômicos segue que

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

□

Exemplo 2.2.17: Já determinamos todos os polinômios mônicos irredutíveis em $\mathbb{F}_2[X]$ de grau 4. A identidade 2.7 nos dá que $I(2,4;X) = Q_5(X)Q_{15}(X)$. Note que $Q_5(X) = X^4 + X^3 + X^2 + X + 1$ é irredutível em $\mathbb{F}_2[X]$. Além disso, $Q_{15}(X)$ se fatora em dois polinômios irredutíveis em $\mathbb{F}_2[X]$ de grau 4. Como $Q_5(X+1) = X^4 + X^3 + 1$ é irredutível em $\mathbb{F}_2[X]$, esse polinômio deve dividir $Q_{15}(X)$ e, então

$$Q_{15}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1 = (X^4 + X^3 + 1)(X^4 + X + 1).$$

Então, os polinômios irredutíveis em $\mathbb{F}_2[X]$ de grau 4 são $X^4 + X^3 + X^2 + X + 1, X^4 + X^3 + 1$ e $X^4 + X + 1$.

Teorema 2.2.18: Seja α um elemento da extensão de um corpo $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$. Suponha que o grau de α sobre $\mathbb{F}_q$ é d e que $g \in \mathbb{F}_q[X]$ é o 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 $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ e g é o 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 multilicativo $\mathbb{F}_{q^m}^*$;

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

Demonstração. Ver [10] p. 96. □

2.3 Construção de polinômios irredutíveis

Nessa seção descreveremos, primeiramente, um método geral para obtermos novos polinômios a partir de polinômios já conhecidos. Para isso, utilizaremos um resultado da Teoria dos Números: se n é um inteiro positivo e b é um inteiro relativamente primo a n, então, o menor inteiro positivo k para o qual $b^k \equiv 1 (\text{mod } n)$ é chamado de ordem multiplicativa de b módulo n. Vale observar que essa ordem divide qualquer outro inteiro positivo h para o qual $b^h \equiv 1 (\text{mod } n)$.

Lema 2.3.1: Seja $s \geq 2$ e $e \geq 2$ dois inteiros relativamente primos e, seja m a ordem multiplicativa de s módulo e. Seja $t \geq 2$ um inteiro cujo fator primo divide e mas não divide $(s^m - 1)/e$. Além disso, assuma que $s^m \equiv 1 (\text{mod } 4)$ se $t \equiv 0 (\text{mod } 4)$. Então, a ordem multiplicativa de s módulo et é igual a mt.

Demonstração. Ver [10] p. 97. □

Exemplo 2.3.2: Sejam $s = 3$ e $e = 5$, dois inteiros relativamente primos. Queremos achar m tal que $3^m \equiv 1 (\text{mod } 5)$. Assim, a ordem multiplcativa de 3 módulo 5 é $m = 4$. Seja $t = 20 = 2^2.5$. Note que 5 é fator primo de 20, 5 divide 5 mas não divide $3^4 - 1/5 = 16$. E mais, $20 \equiv 0 (\text{mod } 4)$. Como $3^4 \equiv 1 (\text{mod } 4)$, temos que a ordem multiplicativa de 3 módulo $5 \cdot 20 = 100$ é igual a $4 \cdot 20 = 80$. Ou seja, 80 é o menor inteiro positivo para o qual $3^{80} \equiv 1 (\text{mod } 100)$.

Teorema 2.3.3: Sejam $f_1(X), \ldots, f_N(X)$ todos os polinômios mônicos irredutíveis distintos em $\mathbb{F}_q[X]$ de grau m e ordem e. Seja $t \geq 2$ um inteiro cujo fator primo divide e mas não divide $q^m - 1/e$. Além disso, assuma que $q^m \equiv 1 (\text{mod } 4)$ se $t \equiv 0 (\text{mod } 4)$. Então, $f_1(X^t), \ldots, f_N(X^t)$ são todos os polinômios mônicos irredutíveis distintos em $\mathbb{F}_q[X]$ de grau mt e ordem et.

Demonstração. A condição sobre e implica que $e \geq 2$. Pelo Teorema 2.1.10, polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau m e ordem $e \geq 2$ existem se, e somente se, m é a ordem multiplicativa de q módulo e e, então, $N = \phi(e)/m$. Do Lema 2.3.1 temos que a ordem multiplicativa de q módulo et é igual a mt e, como $\phi(et)/mt = \phi(e)/m$ segue que o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau mt e ordem et é igual a N. Assim, resta mostrar que cada um dos polinômios $f_j(X^t), 1 \leq j \leq N$ é irredutível em $\mathbb{F}_q[X]$ e de ordem et. Como as raízes de cada $f_j(X)$ são $n-$ésimas raízes primitivas da unidade sobre $\mathbb{F}_q$ segue que $f_j(X)$ divide o polinômio ciclotômico $Q_e(X)$ sobre $\mathbb{F}_q$. Então, $f_j(X^t)$ divide $Q_e(X^t)$ e assim $Q_e(X^t) = Q_{et}(X)$. Consequentemente, $f_j(X^t)$ divide $Q_{et}(X)$. Dessa forma, o grau de cada fator irredutível de $Q_{et}(X)$ em $\mathbb{F}_q[X]$ é igual à ordem multiplicativa de q módulo et, o qual é mt. Como $f_j(X^t)$ tem grau mt, segue então que $f_j(X^t)$ é irredutível em $\mathbb{F}_q[X]$. Além disso, como $f_j(X^t)$ divide $Q_{et}(X)$, a ordem de $f_j(X^{et})$ é igual a et. □

Teorema 2.3.4: Sejam $f_1(X), \ldots, f_N(X)$ todos os polinômios mônicos irredutíveis e distintos em $\mathbb{F}_q[X]$ de grau ímpar m e de ordem e. Seja $q = 2^a u - 1$, $t = 2^b v$ com $a, b \geq 2$, u, v ímpares e todo fator primo de t divide e mas não divide $(q^m - 1)/e$. Seja k o menor entre a e b. Então, cada um dos polinômios $f_j(X^t)$ se fatora como produto de 2^{k-1} polinômios mônicos irredutíveis $g_{ij}(X)$ em $\mathbb{F}_q[X]$ de grau $2^{1-k}mt$. Os $2^{k-1}N$ polinômios $g_{ij}(X)$ são todos os polinômios mônicos irredutíveis distintos em $\mathbb{F}_q[X]$ de grau $2^{1-k}mt$ e ordem et.

Demonstração. Ver [10] p. 98. □

A seguir, mostraremos que para um dado polinômio irredutível de ordem e todos os polinômios irredutíveis cuja ordem divide e podem ser obtidos. Uma vez que em todos os casos $g(X) = X$ estará entre os últimos polinômios, vamos considerar somente polinômios g com $g(0) \neq 0$. Assim, seja f um polinômio mônico irredutível sobre $\mathbb{F}_q[X]$ de grau m, ordem e e $f(0) \neq 0$. Seja $\alpha \in \mathbb{F}_{q^m}$ uma raíz de f e, para todo $t \in \mathbb{N}$ seja $g_t \in \mathbb{F}_q[X]$ o polinômio minimal de α^t sobre $\mathbb{F}_q$. Seja $T = \{t_1, \ldots, t_n\}$ um conjunto de inteiros positivos tal que para cada $t \in \mathbb{N}$ existe um único e determinado i, $1 \leq i \leq n$,

com $t \equiv t_i q^b (\text{mod } e)$ para algum inteiro $b \geq 0$. Tal conjunto T pode, por exemplo, ser construído da seguinte forma: Ponha $t_1 = 1$ e, quando $t_1, t_2, \ldots, t_{j-1}$ tiver sido construído, seja t_j o menor inteiro positivo tal que $t_j \not\equiv t_i q^b (\text{mod } e)$ para $1 \leq i \leq j$ e todo inteiro $b \geq 0$. Este procedimento para após um número finito de etapas.

Assim, com a notação recém introduzida temos o seguinte resultado geral.

Teorema 2.3.5: Os polinômios $g_{t_1}, \ldots, g_{t_n}$ são todos os polinômios mônicos irredutíveis e distintos em $\mathbb{F}_q[X]$ cujas ordens dividem e e cujos termos constantes são não-nulos.

Demonstração. Cada g_{t_i} é mônico e irredutível me $\mathbb{F}_q[X]$, por definição, e satisfaz $g_{t_i}(0) \neq 0$. Além disso, como cada g_{t_i} tem raízes α^{t_i} cujas ordens no grupo $\mathbb{F}_{q^m}^*$ divide a ordem de α, segue que $ord(g_{t_i})$ divide e.

Seja g um polinômio mônico irredutível arbitrário em $\mathbb{F}_q[X]$ de ordem d dividindo e e com $g(0) \neq 0$. Se β é uma raíz de g, então, $\beta^d = 1$ implica que $\beta^e = 1$ e, então, β é uma $n-$ésima raíz da unidade sobre $\mathbb{F}_q$. Como α é uma $n-$ésima raíz primitiva da unidade de $\mathbb{F}_q$, segue que $\beta = \alpha^t$ para algum $t \in \mathbb{N}$. Então, a definição de T implica que $t \equiv t_i q^b (\text{mod } e)$ para algum i, $1 \leq i \leq n$, e algum $b \geq 0$. Consequentemente, $\beta = \alpha^t = (\alpha^{t_i})^{q^b}$ e, então, β é uma raíz de g_{t_i}. Segue então que g é o polinômio minimal de β sobre $\mathbb{F}_q$ e daí $g = g_{t_i}$.

Agora, nos resta mostrar que os polinômios g_{t_i}, $1 \leq i \leq n$, são distintos. Suponha que $g_{t_i} = g_{t_j}$ para $i \neq j$. Então, α^{t_i} e α^{t_j} são raízes de g_{t_i} e, então, $\alpha^{t_j} = (\alpha^{t_i})^{q^b}$ para algum $b \geq 0$. Isso implica que $t_j \equiv t_i q^b (\text{mod } e)$, mas, como também temos que $\alpha^{t_j} \equiv t_j q^0 (\text{mod } e)$, obtemos uma contradição com a definição do conjunto T. Portanto, os polinômios g_{t_i}, $1 \leq i \leq n$ são todos distintos. □

Teorema 2.3.6: Seja f um polinômio mônico irredutível em $\mathbb{F}_q[X]$ de grau m. Seja $\alpha \in \mathbb{F}_{q^m}$ uma raíz de f e, para todo $t \in \mathbb{N}$, seja f_t o polinômio característico de $\alpha^t \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Então,

$$f_t(X^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j X),$$

onde $\omega_1, \ldots, \omega_t$ são as $t-$ésimas raízes da unidade sobre $\mathbb{F}_q$ contadas de acordo com a multiplicidade.

Demonstração. Sejam $\alpha = \alpha_1, \ldots, \alpha_m$ todas as raízes de f. Então, $\alpha_1^t, \ldots, \alpha_m^t$ são as raízes de f_t contadas de acordo com a multiplicidade. Consequentemente,

$$\begin{aligned} f_t(X^t) &= \prod_{i=1}^{m} (X^t - \alpha_i^t) \\ &= \prod_{i=1}^{m} \prod_{j=1}^{t} (X - \alpha_i \omega_j) \\ &= \prod_{i=1}^{m} \prod_{j=1}^{t} \omega_j (\omega_j^{-1} X - \alpha_j). \end{aligned}$$

Uma comparação dos coeficientes na identidade

$$X^t - 1 = \prod_{j=1}^{t}(X - \omega_j)$$

mostra que

$$\prod_{j=1}^{t}\omega_j = (-1)^{t+1},$$

e então,

$$\begin{aligned} f_t(X^t) &= (-1)^{m(t+1)}\prod_{j=1}^{t}\prod_{i=1}^{m}(\omega_j^{-1}X - \alpha_i) \\ &= (-1)^{m(t+1)}\prod_{j=1}^{t}f(\omega_j^{-1}) = (-1)^{m(t+1)}\prod_{j=1}^{t}f(\omega_j x) \end{aligned}$$

uma vez que $\omega_1^{-1}, \ldots, \omega_t^{-1}$ percorre todas as $t-$ésimas raízes da unidade sobre $\mathbb{F}_q$, □

Exemplo 2.3.7: Considere o polinômio $f(X) = X^4 + X + 1$ irredutível sobre $\mathbb{F}_2$. Para calcularmos f_4, observemos que as quartas raízes da unidade sobre $\mathbb{F}_2$ são 1, -1, ω e $-\omega$, onde ω é raíz de X^2+1 em $\mathbb{F}_2$. Então,

$$\begin{aligned} f_4(X^4) &= (-1)^{20}f(X)f(-x)f(\omega x)f(-\omega x) \\ &= (X^4+X+1)(X^4-X+1)(\omega X^4+\omega x+1)(-\omega X^4-\omega X+1) \\ &= X^{16}+X^4+1. \end{aligned}$$

Logo, $f_4(X) = X^4 + X + 1$

Vejamos agora outro método para calcular f_t, que é baseado na Teoria de Matrizes. Assim, sejam $f(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_1X - a_0$ e A a matriz companheira de f, a qual é definida pela matriz $m \times m$

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{m-1} \end{bmatrix}.$$

Então, f é o polinômio característico de A na álgebra linear, o qual é dado por $f(X) = det(xI - A)$ onde I é a matriz identidade $m \times m$ sobre $\mathbb{F}_q$. Para cada $t \in \mathbb{N}$, f_t é o polinômio característico de A^t (a $t-$ésima potência de A). Ou seja, calculando as potências de A obtemos os polinômios f_t.

Exemplo 2.3.8: Queremos determinar os polinômios f_t que são irredutíveis em $\mathbb{F}_q[X]$. Da discussão do Teorema 2.3.6 temos que f_t é irredutível em $\mathbb{F}_q[X]$ se, se somente se $k = m$ o qual ocorre se, e somente se m é a ordem multiplicativa de q módulo $d = e/mdc(t,e)$. Considere, por exemplo,

$q = 2, m = 8$ e $e = 45$. Assim, queremos achar os valores de k para o qual $q^k \equiv 1 (\mathrm{mod}\, d)$, onde d é um divisor positivo de e, e k divide m. Assim, as únicas possibilidades para a ordem multiplicativa além de m são $k = 1, 2, 4$. Logo, $2^k - 1 = 1, 3, 15$ e $2^k \equiv 1 (\mathrm{mod}\, d)$ só é possível quando $d = 1, 3, 5, 15$. Consequentemente, f_t é irredutível em $\mathbb{F}_2[X]$ se $mdc(t, 45) = 3, 9, 15, 45$. Como é suficiente considerar valores de t com $1 \leq t \leq 45$, segue que f_t é irredutível em $\mathbb{F}_2[X]$ exceto quando $t = 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 40, 42, 45$.

Na prática, polinômios irredutíveis geralmente surgem como polinômios minimais de elementos em uma extensão de corpos. Se na discussão acima considerarmos f como sendo um polinômio primitivo sobre $\mathbb{F}_q$, de modo que $e = q^m - 1$, então, as potências α percorrem por todos os elementos não nulos de $\mathbb{F}_{q^m}$. Portanto, os métodos descritos acima podem ser usados para calcular os polinômios minimais sobre $\mathbb{F}_q$ de cada elemento de $\mathbb{F}_{q^m}^*$.

Um método mais direto para determinar polinômios minimais é o seguinte: Seja θ um elemento de definição de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, então, o conjunto $\{1, \theta, \ldots, \theta^{m-1}\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Assim, com a finalidade de encontrar o polinômio minimal g de $\beta \in \mathbb{F}_{q^m}^*$ sobre $\mathbb{F}_q$, expressamos as potências $\beta^0, \beta^1, \ldots, \beta^m$ em termos dos elementos da base. Com isso, seja

$$\beta^{i-1} = \sum_{j=1}^{m} b_{ij} \theta^{j-1}$$

para $1 \leq i \leq m+1$. Escreva g como $g(X) = c_m X^m + \cdots + c_1 X + c_0$. Queremos que g seja o polinômio minimal de menor grau positivo com $g(\beta) = 0$. Assim, a condição $g(\beta) = 0$ nos leva ao sistema linear homogêneo dado por

$$\sum_{i=1}^{m+1} c_{i-1} b_{ij} = 0, 1 \leq j \leq m \tag{2.8}$$

onde $c_0, c_1, \ldots, c_m$ são desconhecidos. Seja B a matriz dos coeficientes do sistema - isto é, B é a $(m+1) \times m$ matriz cuja entrada (i, j) é b_{ij}- e seja r o posto dessa matriz. Então, a dimensão do espaço solução dos sistema é $s = m + 1 - r$ e, como $1 \leq r \leq m$ temos que $1 \leq s \leq m$. Então, podemos assumir valores para s dos coeficientes desconhecidos $c_0, c_1, \ldots, c_m$ e, então, os elementos restantes serão unicamente determinados. Agora, se $s = 1$, ponha $c_m = 1$, se $s > 1$, defina $c_m = c_{m-1} = \cdots = c_{m-s+2} = 0$ e $c_{m-s+1} = 1$.

Exemplo 2.3.9: Seja $\theta \in \mathbb{F}_{16}$ uma raíz do polinômio irredutível $X^4 + X + 1$ em $\mathbb{F}_2[X]$. Para $\beta = 1 + \theta$ temos que

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= 1 + \theta \\
\beta^2 &= 1 + 0\theta + \theta^2 \\
\beta^3 &= 1 + \theta + \theta^2 + \theta^3 \\
\beta^4 &= 0 + \theta
\end{aligned}$$

Então, a matriz B é dada por

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

e seu posto é $r = 4$. Daí, $s = m + 1 - r = 1$ e, então, $c_4 = 1$. Para encontrar os demais coeficientes, usaremos a identidade 2.9. Dela obtemos o seguinte sistema:

$$\begin{cases} c_0 + c_1 + c_2 + c_3 = 0 \\ c_1 + c_3 + 1 = 0 \\ c_2 + c_3 = 0 \\ c_3 = 0 \end{cases}$$

Assim, temos que $c_0 = 1, c_1 = 1, c_2 = 0, c_3 = 0, c_4 = 1$. Consequentemente, o polinômio minimal de $\beta \in \mathbb{F}_2[X]$ é $g(X) = 1 + X + X^4$.

Além do exposto acima, outro método para determinar polinômios minimais é baseado no Teorema 2.2.18(v). Ou seja, se quisermos encontrar o polinômio minimal g de $\beta \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, devemos calcular as potências $\beta, \beta^q, \beta^{q^2}, \ldots$ até encontrarmos o menor inteiro positivo d para o qual $\beta^{q^d} = \beta$. Esse inteiro d é o grau de g e, esse é dado por

$$g(X) = (X - \beta)(X - \beta^q) \ldots (X - \beta^{q^{d-1}}).$$

Os elementos $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$ são conjugados distintos de β com respeito a $\mathbb{F}_q$ e, g é o polinômio minimal sobre $\mathbb{F}_q$ de todos esses elementos.

Exemplo 2.3.10: Vamos computar os polinômios minimais sobre $\mathbb{F}_2$ de todos os elementos de $\mathbb{F}_8$. Seja $\theta \in \mathbb{F}_8$ uma raíz do polinômio primitivo $X^3 + X + 1$ sobre $\mathbb{F}_2$, então, todo elemento não nulo de $\mathbb{F}_8$ pode ser escrito como potências de θ. Segue abaixo a tabela dos índices para $\mathbb{F}_8$:

Tabela 3: índices de 0 a 6

i	θ^i
0	1
1	θ
2	θ^2
3	$1 + \theta$
4	$\theta + \theta^2$
5	$1 + \theta + \theta^2$
6	$1 + \theta^2$

Assim, os polinômios minimais dos elementos $\beta \in \mathbb{F}_8$ sobre $\mathbb{F}_2$ são:

$\beta = 0 \rightarrow g_1(X) = X.$

$\beta = 1 \rightarrow g_2(X) = X + 1.$

$\beta = \theta \rightarrow$ Os conjugados distintos de θ com respeito a $\mathbb{F}_2$ são $\theta, \theta^2, \theta^4$ e o polinômio minimal é:
$g_3(X) = (X-\theta)(X-\theta^2)(X-\theta^4) = X^3 + X + 1$

$\beta = \theta^3 \rightarrow$ Os conjugados distintos de θ^3 com respeito a $\mathbb{F}_2$ são $\theta^3, \theta^5, \theta^6$ com polinômio minimal:
$g_4(X) = (X-\theta^3)(X-\theta^5)(X-\theta^6) = X^3 + X^2 + 1.$

Um problema também interessante é determinar os polinômios primitivos. Um dos métodos é baseado no fato de que o produto de todos os polinômios primitivos sobre $\mathbb{F}_q$ de grau m é igual ao polinômio ciclotômico Q_e com $e = q^m - 1$. Então, todos os polinômios primitivos sobre $\mathbb{F}_q$ de grau m pode ser determinado aplicando um dos algoritmos de fatorização que veremos no próximo capítulo ao polinômio ciclotômico Q_e.

Outro método depende da construção de um elemento primitivo de $\mathbb{F}_{q^m}$ e, então, determinar o polinômio minimal desse elemento sobre $\mathbb{F}_q$ usando um dos métodos vistos anteriormente. Assim, para encontrar um elemento primitivo de $\mathbb{F}_{q^m}$ primeiro partimos de um elemento de $\mathbb{F}_{q^m}^*$ de ordem $q^m - 1$ e fatoramos essa ordem da forma $q^m - 1 = h_1 \dots h_k$, onde os inteiros positivos $h_1, \dots, h_k$ são relativamente primos dois a dois. Se para cada i, $1 \leq i \leq k$, pode-se encontrar um elemento $\alpha_i \in \mathbb{F}_{q^m}^*$ de ordem h_i, então, o produto $\alpha_1 \dots \alpha_k$ tem ordem $q^m - 1$ e, consequentemente, é um elemento primitivo de $\mathbb{F}_{q^m}$.

Exemplo 2.3.11: Vamos determinar um polinômio primitivo sobre $\mathbb{F}_3$ de grau 4. Como $3^4 - 1 = 16 \cdot 5$, primeiro construiremos dois elementos de $\mathbb{F}_{81}^*$ de ordem 16 e 5, respectivamente. Note que, o elemento de ordem 16 são as raízes da unidade do polinômio ciclotômico $Q_{16}(X) = X^8 + 1 \in \mathbb{F}_3[X]$. Como a ordem multiplicativa de 3 módulo 16 é igual a 4, então, Q_{16} fatora-se em dois polinômios em $\mathbb{F}_3[X]$ de grau 4. Assim,

$$\begin{aligned} X^8 + 1 &= (X^4 - 1)^2 - X^4 \\ &= (X^4 - 1 + X^2)(X^4 - 1 - X^2), \end{aligned}$$

e então, $f(X) = X^4 - X^4 - 1$ é irredutível sobre $\mathbb{F}_3$ e, sendo θ uma raíz de f temos que $\mathbb{F}_{81} = \mathbb{F}_3(\theta)$. Além disso, θ é um elemento de $\mathbb{F}_{81}^*$ de ordem 16. Encontremos agora um elemento α de ordem 5.

Assim, escreva $\alpha = a+b\theta+c\theta^2+d\theta^3$ com $a,b,c,d \in \mathbb{F}_3$ e observe que $\alpha^{10}=1$, então

$$\begin{aligned} 1 &= \alpha^9\alpha \\ &= (a+b\theta^9+c\theta^{18}+d\theta^{27})(a+b\theta+c\theta^2+d\theta^3) \\ &= (a-b\theta+c\theta^2-d\theta^3)(a+b\theta+c\theta^2+d\theta^3) \\ &= (a+c\theta^2)^2-(b\theta+d\theta^3)^2 \\ &= a^2+(2ac-b^2)\theta^2+(c^2-2bd)\theta^4-d^2\theta^6 \\ &= a^2+c^2-d^2+bd+(c^2+d^2-b^2-ac+bd)\theta^2. \end{aligned}$$

Comparando os coeficientes temos $a^2+c^2-d^2+bd=1$ e $c^2+d^2-b^2-ac+bd=0$. Fazendo $a=d=0$ temos $b^2=c^2=1$. Tomando $b=c=1$, segue que $\alpha=\theta+\theta^2$ tem ordem 5. Então, $\zeta=\theta\alpha=\theta^2+\theta^3$ tem ordem 80 e, consequentemente, é um elemento primitivo de $\mathbb{F}_{81}$. Assim, o polinômio minimal g de ζ sobre $\mathbb{F}_3$ é

$$\begin{aligned} g(X) &= (X-\zeta)(X-\zeta^3)(X-\zeta^9)(X-\zeta^{27}) \\ &= (X-\theta^2-\theta^3)(X-1+\theta+\theta^2)(X-\theta^2+\theta^3)(X-1-\theta+\theta^2) \\ &= X^4+X^3+X^2-X-1. \end{aligned}$$

e temos, consequentemente, um polinômio primitivo sobre $\mathbb{F}_3$ de grau 4.

Exemplo 2.3.12: Determinemos agora um polinômio primitivo sobre $\mathbb{F}_2$ de grau 4. Como $2^2-1=15=5\cdot 3$, vamos construir primeiramente dois elementos de $\mathbb{F}_{16}^*$ de ordem 5 e 3, respectivamente. O elemento de ordem 5 são as raízes do poliômio ciclotômico $Q_5(X)=1+X+X^2+X^3+X^4$ irredutível sobre $\mathbb{F}_2[X]$. Uma raíz θ de Q_5 tem ordem 5 e $\mathbb{F}_{16}=\mathbb{F}_2(\theta)$. Um elemento $\alpha\in\mathbb{F}_{16}^*$ de ordem 3 satisfaz $\alpha^4=\alpha$, pondo $\alpha=\sum_{i=0}^{3}a_i\theta^i$ com $a_i\in\mathbb{F}_2$, $0\le i\le 5$ temos que

$$\begin{aligned} \sum_{i=0}^{3}a_i\theta^i &= (\sum_{i=0}^{3}a_i\theta^i)^8 \\ &= \sum_{i=0}^{3}a_i\theta^{8i} \\ &= a_0+a_1\theta^4+a_2\theta^8+a_3\theta^{12} \\ &= a_0+a_1+a_1\theta+(a_1+a_3)\theta^2+(a_1+a_2)\theta^3. \end{aligned}$$

Comparando os coeficiente temos que $a_0\in\mathbb{F}_2$ e $a_2=a_3$. Escolhendo $a_0=0$ e $a_2=a_3=1$ temos que $\alpha=\theta+\theta^3$ é um elemento de ordem 3. Consequentemente, $\zeta=\theta\alpha=1+\theta+\theta^2$ é um elemento primitivo de $\mathbb{F}_{16}$. Então, $\zeta^2=\theta+\theta^3$, $\zeta^3=\theta^3$, $\zeta^4=\theta+\theta^2$. Aplicando o método do Exemplo 2.3.9 temos que $g(X)=1+X+X^4$ é o polinômio minimal de ζ sobre $\mathbb{F}_2$ e, consequentemente, é o polinômio primitivo sobre $\mathbb{F}_2$ de grau 4.

Observamos que, se um polinômio primitivo g sobre $\mathbb{F}_q$ de grau m é conhecido, então, todos os demais polinômios primitivos podem ser obtidos considerando uma raíz θ de g em $\mathbb{F}_{q^m}$ e determinando

os polinômios minimais sobre $\mathbb{F}_q$ de todos os elementos θ^t, onde t percorre todos os inteiros positivos menores ou iguais a q^m-1 que são relativamente primos a q^m-1. O calculo desses polinômios minimais é realizado por meio dos métodos já descritos anteriormente.

É útil ser capaz de decidir se um polinômio irredutível sobre um corpo finito permanece irredutível sobre uma certa extensão de um corpo finito. Os seguintes resultados abordam esta questão.

Teorema 2.3.13: Sejam f um polinômio irredutível sobre $\mathbb{F}_q$ de grau n e $k \in \mathbb{N}$. Então, f se fatora em d polinômios irredutíveis em $\mathbb{F}_{q^k}$ de mesmo grau n/d, onde $d = mdc(k,n)$.

Demonstração. Como o caso $f(0) = 0$ é trivial, vamos assumir que $f(0) \neq 0$. Seja g um fator irredutível de f em $\mathbb{F}_{q^k}$. Se $ord(g) = e$, então, as raízes de g também são as raízes de f. Como a ordem multiplicativa de q módulo e é n e o grau de g é igual à ordem multiplicativa de q^k módulo e, então, as potências q^j, $j = 0,1,\ldots$ consideradas módulo e formam um grupo de ordem n. Consequentemente, a ordem multiplicativa de q^k módulo e é n/d e, então, o grau de g é n/d. □

Exemplo 2.3.14: Consideremos o polinômio primitivo $g(X) = 1+X+X^4$ sobre $\mathbb{F}_2$ do Exemplo 2.3.12 como um polinômio sobre $\mathbb{F}_{16}$. Então, na notação do Teorema 2.3.13 temos que $n = 4$, $k = 4$ e, então, $d = 4$, então, g se fatora em 4 polinômios irredutíveis de grau 1.

Corolário 2.3.15: Um polinômio irredutível sobre $\mathbb{F}_q$ de grau n permanece irredutível sobre $\mathbb{F}_{q^k}$ se, e somente se, k e n são relativamente primos.

Demonstração. Consequência imediata do teorema anterior. □

Exemplo 2.3.16: Segue do Corolário 2.3.15 que o polinômio irredutível $X^3+X+1 \in \mathbb{F}_2[X]$ sobre $\mathbb{F}_2$ permanece irredutível sobre $\mathbb{F}_{2^2}$ pois $mdc(2,3) = 1$.

2.4 Polinômios linearizados

Tanto na teoria quanto nas aplicações, a classe especial de polinômios a ser introduzida abaixo é importante. Uma característica útil desses polinômios é a estrutura do conjunto de raízes, que facilita a determinação das raízes. Como anteriormente, seja q a potência de um primo.

Definição 2.4.1: Um polinômio da forma

$$L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i}$$

com coeficientes em uma extensão $\mathbb{F}_{q^m}$ do corpo $\mathbb{F}_q$ é chamado polinômio linearizado, ou $q-$polinômio, sobre $\mathbb{F}_{q^m}$.

Exemplo 2.4.2: Seja a um elemento gerador de $\mathbb{F}_8$. O polinômio $L(X) = X + aX^2 + a^2X^4$ é um polinômio linearizado (ou $2-$polinômio) e pode ser representado por $L(X) = \sum_{i=0}^{4} \alpha_i X^{2^i}$, com $\alpha_i = a^i \in$

$\mathbb{F}_8$.

Observamos que a terminologia polinômio linearizado segue da propriedade de linearização dos polinômios. Isto é, se F é uma extensão arbitrária do corpo $\mathbb{F}_{q^m}$ e $L(X)$ é um polinômio linearizado (isto é, um $q-$polinômio) sobre $\mathbb{F}_{q^m}$, então,

$$L(\beta+\gamma) = L(\beta)+L(\gamma) \text{ para todo } \beta,\gamma \in F, \tag{2.9}$$

$$L(c\beta) = cL(\beta) \text{ para todo } c \in \mathbb{F}_q \text{ e todo } \beta \in F. \tag{2.10}$$

Se F é considerado como um espaço vetorial sobre $\mathbb{F}_q$, então, o polinômio linearizado $L(X)$ induz um operador linear em F. Uma característica especial do conjunto de raízes de um polinômio linearizado é mostrada no resultado abaixo.

Teorema 2.4.3: Seja $L(X)$ um polinômio linearizado não-nulo sobre $\mathbb{F}_{q^m}$ e seja $\mathbb{F}_{q^s}$ uma extensão do corpo $\mathbb{F}_{q^m}$ contendo todas as raízes de $L(X)$. Então, cada raíz de $L(X)$ têm a mesma multiplicidade, a qual é 1 ou uma potência de q e, as raízes formam um subespaço de $\mathbb{F}_{q^s}$, onde $\mathbb{F}_{q^s}$ é considerado como um espaço vetorial sobre $\mathbb{F}_q$.

Demonstração. Segue das identidades 2.9 e 2.10 que qualquer combinação linear das raízes com coeficientes em $\mathbb{F}_q$ é também uma raíz e, então, as raízes de $L(X)$ formam um subespaço linear de $\mathbb{F}_{q^s}$. Se

$$L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i},$$

então, $L'(X) = \alpha_0$, logo, $L(X)$ tem somente raízes simples no caso $\alpha_0 \neq 0$. Por outro lado, temos que $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$, mas, $a_k \neq 0$ para algum $k \geq 1$ e, então,

$$L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i} = \sum_{i=k}^{n} \alpha_i^{q^{mk}} X^{q^i} = (\sum_{i=k}^{n} \alpha_i^{q^{(m-1)k}} X^{q^{i-k}})^{q^k}$$

o qual é a q^k-ésima potência de um polinômio linearizado tendo somente raízes simples. Nesse caso, cada raíz de $L(X)$ tem multiplicidade q^k. □

Observemos que a reciproca do teorema anterior não é verdadeira. Para isso, considere o polinômio $f(X) = X^2 - X$ sobre $\mathbb{F}_3$. Note que f só tem raízes simples, mas não é um $3-$polinômio. Porém, podemos encontrar uma “recíproca parcial"para o teorema anteirior, que será apresentada após o seguinte lema.

Lema 2.4.4: Sejam $\beta_1, \beta_2, \ldots, \beta_n$ elementos de $\mathbb{F}_{q^m}$. Então,

$$\begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_n & \beta_n^q & \beta_n^{q^2} & \ldots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} (\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k) \tag{2.11}$$

e, então, o determinante é diferente de 0 se, e somente se, $\beta_1, \beta_2, \ldots, \beta_n$ são linearmente independentes sobre $\mathbb{F}_q$.

Demonstração. Seja D_n o determinante do lado esquerdo da identidade 2.11. Faremos a prova por indução sobre n.

Note que, para $n = 1$ o resultado é trivial se o produto vazio do lado direito for considerado como 1. Agora, suponha que a identidade vale para $n \geq 1$. Assim, considere o polinômio

$$D(X) = \begin{vmatrix} \beta_1 & \beta_1^q & \ldots & \beta_1^{q^{n-1}} & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \ldots & \beta_2^{q^{n-1}} & \beta_2^{q^n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_n & \beta_n^q & \ldots & \beta_n^{q^{n-1}} & \beta_n^{q^n} \\ X & X^q & \ldots & X^{q^{n-1}} & X^{q^n} \end{vmatrix}$$

Por expansão ao longo da última linha temos que

$$D(X) = D_n X^{q^n} + \sum_{i=0}^{n-1} \alpha_i X^{q^i} \tag{2.12}$$

com $\alpha_i \in \mathbb{F}_{q^m}$ para $0 \leq i \leq n-1$. Assuma primeiro que $\beta_1, \ldots, \beta_n$ são linearmente independentes sobre $\mathbb{F}_q$. Assim, temos que $D(\beta_k) = 0$ para $1 \leq k \leq n$ e, como $D(X)$ é um $q-$polinômio sobre $\mathbb{F}_{q^m}$ todas as combinações lineares $c_1\beta_1 + \cdots + c_n\beta_n$ com $c_k \in \mathbb{F}_q$ para $1 \leq k \leq n$ são raízes de $D(X)$. Consequentemente, $D(X)$ tem q^n raízes distintas, então, obtemos a seguinte fatorização

$$D(X) = D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} (X - \sum_{k=1}^{n} c_k\beta_k).$$

Se $\beta_1, \ldots, \beta_n$ são linearmente independentes sobre $\mathbb{F}_q$, então, $D_n = 0$ e $\sum_{k=1}^{n} b_k\beta_k = 0$ para algum $b_1, \ldots, b_n \in \mathbb{F}_q$ não todos nulos. Segue daí que

$$\sum_{k=1}^{n} b_k\beta_k^{q^j} = (\sum_{k=1}^{n} b_k\beta_k)^{q^j} = 0 \text{ para } j = 0, 1, \ldots, n,$$

e, então, os primeiros vetores de n linhas no determinante que define $D(X)$ são linearmente dependentes sobre $\mathbb{F}_q$. Consequentemente, $D(X) = 0$ e, a identidade 2.12 é satisfeita em todos os casos. Consequentemente, temos que

$$D_{n+1} = D(\beta_{n+1}) = D_n \prod_{c_1,\ldots,c_n \in \mathbb{F}_q} (\beta_{n+1} - \sum_{k=1}^{n} c_k\beta_k)$$

e 2.11 está estabelecido. □

Teorema 2.4.5: Seja U um subespaço linear de $\mathbb{F}_{q^m}$, considerado como um espaço vetorial sobre $\mathbb{F}_q$.

Então, para cada inteiro não negativo k o polinômio

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

é um polinômio linearizado sobre $\mathbb{F}_{q^m}$.

Demonstração. Como a q^k-ésima potência de um polinômio linearizado sobre $\mathbb{F}_{q^m}$ é também um polinômio, é suficiente considerar o caso $k = 0$. Assim, seja $\{\beta_q, \ldots, \beta_n\}$ uma base de U sobre $\mathbb{F}_q$. Então, o determinante D_n do lado esquerdo da identidade 2.11 é diferente de 0 e, então,

$$\begin{aligned} L(X) &= \prod_{\beta \in U} (X - \beta) \\ &= \prod_{c_1, \ldots, c_n \in \mathbb{F}_q} (X - \sum_{k=1} n c_k \beta_k) = D_n^{-1} D(X) \end{aligned}$$

pela identidade 2.12, o que mostra que $L(X)$ é um polinômio linearizado sobre $\mathbb{F}_{q^m}$. □

As propriedades dos polinômios linearizados nos leva ao seguinte método de determinar as raízes desses polionômios. Seja

$$L(X) = \sum_{i=0}^{n} \alpha_i X^{q^i}$$

um polinômio linearizado sobre $\mathbb{F}_{q^m}$ e suponha que queremos encontrar todas as raízes de $L(X)$ na extensão finita F de $\mathbb{F}_{q^m}$. Como observamos anteriormente, a aplicação $L : \beta \in F \mapsto L(\beta) \in F$ é um operador linear no espaço vetorial F de $\mathbb{F}_q$. Então, L pode ser representado na forma de uma matriz sobre $\mathbb{F}_q$. Ou seja, tome uma base $\{\beta_1, \ldots, \beta_s\}$ de F sobre $\mathbb{F}_q$, então, todo $\beta \in F$ pode ser escrito como

$$\beta = \sum_{j=1}^{s} c_j \beta_j \text{ com } c_j \in \mathbb{F}_q \text{ para } 1 \leq j \leq s,$$

então,

$$L(\beta) = \sum_{j=1}^{s} c_j L(\beta_j).$$

Agora, seja

$$L(\beta_j) = \sum_{k=1}^{s} b_{jk} \beta_k \text{ para } 1 \leq j \leq s,$$

onde $b_{jk} \in \mathbb{F}_q$ para $1 \leq j,k \leq s$ e seja B a matriz $s \times s$ sobre $\mathbb{F}_q$ cuja entrad (j,k) é b_{jk}. Então, se

$$(c_1, \ldots, c_s)B = (d_1, \ldots, d_s),$$

temos que

$$L(\beta) = \sum_{k=1}^{s} d_k \beta_k.$$

Assim, a equação $L(\beta) = 0$ equivale a dizer que

$$c_1, \ldots, c_s)B = (0, \ldots, 0). \tag{2.13}$$

Ou seja, obtemos um sistema linear homogêneo de s equações para $c_1, \ldots, c_s$. Se r é o posto da matriz B, então a identidade 2.13 nos dá q^{r-s} vetores-solução $(c_1, \ldots, c_s)$. Cada vetor solução produz uma raíz $\beta = \sum_{j=1}^{s} c_j \beta_j$ de $L(X)$ em F. Dessa forma, o problema de encontrar raízes de $L(X)$ é reduzido ao simples problema de resolver sistemas de equações lineares homogêneas.

Capítulo 3

Polinômios de permutação

Um polinômio $f \in \mathbb{F}_q[X]$ é chamado **polinômio de permutação** se a aplicação $f : a \longmapsto f(a)$ de $\mathbb{F}_q$ em $\mathbb{F}_q$ induz uma permutação sobre $\mathbb{F}_q$, isto é, se a função polinomial associada ao polinômio f for uma bijeção em $\mathbb{F}_q$. Neste capítulo apresentaremos alguns resultados sobre polinômios de permutação. Observemos que toda aplicação de $\mathbb{F}_q$ em $\mathbb{F}_q$ admite uma representação polinomial. Assim, estaremos interessados nessas aplicações e na sua bijetividade.

Determinar polinômios de permutação não é um problema trivial. Na Seção 3.1 apresentaremos alguns critérios mais gerais que garantem que um polinômio é de permutação. Fornecer condições para que polinômios arbitrários sejam de permutação é algo bem difícil, por isso estudos são feitos para certos tipos ou famílias de polinômios, sendo em muitos casos sobre corpos com característica fixada. Na Seção 3.2 apresentaremos alguns exemplos mais simples desses estudos para certos tipos de polinômios. Exemplos mais complexos serão apresentados no Capítulo 4.

3.1 Critérios para polinômios de permutação

Começamos observando que, se f é um polinômio de permutação, então, para cada $c \in \mathbb{F}_q$, a equação $f(X) = c$ tem exatamente uma solução em $\mathbb{F}_q$. Usando a finitude de $\mathbb{F}_q$ obtemos algumas definições equivalentes para polinômios de permutação.

Lema 3.1.1: O polinômio $f \in \mathbb{F}_q[X]$ é de permutação se, e somente se, pelo menos uma das seguintes condições acontece:

(i) a função $f : a \longmapsto f(a)$ é sobrejetiva;

(ii) a função $f : a \longmapsto f(a)$ é injetiva;

(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 $a \in \mathbb{F}_q$.

Note que as duas últimas condições nos remete a determinar o número de raízes do polinômio $f(X) - a$ para cada $a \in \mathbb{F}_q$.

Exemplo 3.1.2: Seja $f(X) = X^3 + 1 \in \mathbb{F}_5[X]$. Note que $f(0) = 1, f(1) = 2, f(2) = 4, f(3) = 3$ e $f(4) = 0$. Logo, $f(X)$ é um polinômio injetivo. Como $\mathbb{F}_5$ é finito segue que $f(X)$ é bijetivo, ou seja, $f(X)$ é uma permutação sobre $\mathbb{F}_5$ e podemos representá-lo pelo produto de ciclos $(3)(0124)$.

Agora, observemos que se $\phi : \mathbb{F}_q \longmapsto \mathbb{F}_q$ é uma função arbitrária, então, existe um único polinômio $g \in \mathbb{F}_q[X]$ de grau menor que q representando ϕ, nesse caso, $g(a) = \phi(a)$ para todo $a \in \mathbb{F}_q$. Assim, podemos encontrar g pela seguinte fórmula

$$g(X) = \sum_{a \in \mathbb{F}_q} \phi(a)(1 - (X - a)^{q-1}). \tag{3.1}$$

Veja que, se ϕ é uma função polinomial, digamos $\phi : a \longmapsto f(a)$ com $f \in \mathbb{F}_q[X]$, então podemos obter g por meio de uma redução módulo $X^q - X$, como nos mostra o seguinte resultado.

Lema 3.1.3: Para $f, g \in \mathbb{F}_q[X]$ temos que $f(a) = g(a)$ para todo $a \in \mathbb{F}_q$ se, e somente se, $f(X) \equiv g(X) \bmod (X^q - X)$.

Demonstração. Segue do algoritmo da divisão que $f(X) - g(X) = h(X)(X^q - X) + r(X)$ onde $h, r \in \mathbb{F}_q[X]$ e $deg(r) < q$. Assim, $f(a) = g(a)$ para todo $a \in \mathbb{F}_q$ se, e somente se, $r(a) = 0$ para todo $a \in \mathbb{F}_q$ o que equivale a dizer que $r = 0$. Assim, $f(X) - g(X) = h(X)(X^q - X)$ como queríamos. □

Exemplo 3.1.4: Sejam $f(X) = X^8 - 1$ e $g(X) = X^4 - 1$ polinômios em $\mathbb{F}_5[X]$. Note que

$$\frac{X^8 - 1}{X^5 - X} = X^3(X^5 - X) + X^4 - 1$$

ou seja, $f(X) \equiv g(X) \pmod{X^5 - X}$. Logo, pelo Lema 3.1.3 segue que $f(x) = g(x)$ para todo $x \in \mathbb{F}_5[X]$.

Observamos que o número de bijeções em um conjunto com n elementos é $n!$. Assim, existem $q!$ polinômios de permutação sobre $\mathbb{F}_q$ de grau menor do que q e que podem ser construídos por meio da equação (3.1).

A seguir, veremos um critério bastante útil para polinômios de permutação, o chamado *Critério de Hermite*. Porém, antes apresentaremos um lema que nos será bastante útil.

Lema 3.1.5: Sejam $a_0, a_1, \ldots, a_{q-1}$ elementos de $\mathbb{F}_q$. Então, são equivalentes:

(i) $a_0, a_1, \ldots, a_{q-1}$ são distintos;

(ii) Além disso,

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0, & \text{para } t = 0, 1, \ldots, q-2 \\ -1, & \text{para } t = q-1 \end{cases}$$

Demonstração. Considere o polinômio

$$g_i(X) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} X^j,$$

para i fixo com $0 \leq i \leq q-1$. Note que $g_i(a_i) = 1$ e $g_i(b) = 0$ para $b \in \mathbb{F}_q$ com $b \neq a_i$. Assim, o polinômio

$$g(X) = \sum_{i=1}^{q-1} g_i(X) = -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j} \right) X^j$$

transforma cada elemento de $\mathbb{F}_q$ em 1 se, e somente se, $\{a_0, \ldots, a_{q-1}\} = \mathbb{F}_q$. Como $deg(g) < q$, segue do Lema 3.1.3 que o polinômio g transforma cada elemento de $\mathbb{F}_q$ em 1 se, e somente se, $g(X) = 1$, o qual equivale à condição (ii). □

Teorema 3.1.6: (Critério de Hermite) Seja $\mathbb{F}_q$ de característica p. Então, $f \in \mathbb{F}_q[X]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, são válidas as seguintes condições:

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

(ii) para cada inteiro t com $1 \leq t \leq q-2$ e $t \not\equiv 0 \pmod{p}$, a redução de $f(X)^t \pmod{X^q - X}$ tem grau menor ou igual a $q-2$.

Demonstração. Seja f um polinômio de permutação de $\mathbb{F}_q$, então o item (i) é trivial. Assim, a redução de $f(X)^t \pmod{X^q - X}$ é algum polinômio da forma $\sum_{j=0}^{q-1} b_j^{(t)} X^j$, onde $b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^t$ pela identidade (3.1). Pelo Lema 3.1.5 temos que $b_{q-1}^{(t)} = 0$ para $t = 1, 2, \ldots, q-2$, e segue (ii).

Reciprocamente, considere que (i) e (ii) são satisfeitos. Então, (i) implica que $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1$, enquanto (ii) implica que $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para $1 \leq t \leq q-2$, $t \not\equiv 0 \pmod{p}$. Considerando o fato que

$$\sum_{c \in \mathbb{F}_q} f(c)^{tp^j} = \left(\sum_{c \in \mathbb{F}_q} f(c)^t \right)^{p^j},$$

temos que $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para $1 \leq t \leq q-2$ e essa identidade é trivial para $t = 0$. Pelo Lema 3.1.5 temos que f é um polinômio de permutação de $\mathbb{F}_q$. □

Exemplo 3.1.7: Seja $f(X) = X^3 + 1 \in \mathbb{F}_5[X]$. Vimos no Exemplo 3.1.2 que 4 é a única raíz de $f(X)$. Agora, tome $1 \leq t \leq 3 = 5-2$, com $t \not\equiv 0 \pmod{5}$. Assim,

- Para $t = 1$ temos que $f(X) \equiv f(X) \pmod{X^5 - X}$ e $\deg(f(X)) = 3 = 5-2$;
- Para $t = 2$ temos que $f(X)^2 = X^6 + 2X^3 + 1 \equiv 2X^3 + X^2 + 1 \pmod{X^5 - X}$ com $\deg(2X^3 + X^2 + 1) = 3 = 5-2$;
- Para $t = 3$ temos que $f(X)^3 = X^9 + 3X^6 + 3X^3 + 1 \equiv 3X^3 + 3X^2 + X + 1 \pmod{X^5 - X}$ e $\deg(3X^3 + 3X^2 + X + 1) = 3 = 5-2$.

Portanto, as duas condições do Critério de Hermite são satisfeitas e, consequentemente, temos que f é um polinômio de permutação sobre $\mathbb{F}_5$.

Corolário 3.1.8: 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 $deg(f) = d$, então o grau de $f^{q-1/d}$ é igual a $q-1$. Como $\mathbb{F}_q$ tem característica p, então, p divide q mas não divide $q-1$, assim, $\frac{q-1}{d} \not\equiv 0 (\text{mod } p)$. Assim, o item (ii) do Critério de Hermite não é satisfeita para $t = \frac{q-1}{d}$. □

Teorema 3.1.9: Seja $\mathbb{F}_q$ de característica p. Então, $f \in \mathbb{F}_q[X]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, as seguintes condições 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 $t \not\equiv 0 \pmod{p}$, a redução de $f(X)^t \pmod{X^q - X}$ tem grau menor ou igual a $q-2$.

Demonstração. Note que o item (ii) segue do Teorema 3.1.6. Usando a notação desse teorema temos que $b_{q-1}^{(q-1)} = -\sum_{c \in \mathbb{F}_q} f(c)^{q-1}$, consequentemente, f é um polinômio de permutação de $\mathbb{F}_q$, logo, $b_{q-1}^{(q-1)} = 1$ e segue (i).

Reciprocamente, considere que (i) e (ii) são satisfeitas. Então, como na prova do Teorema 3.1.6(ii) temos que $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para $0 \leq t \leq q-2$, enquanto (i) implica que $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} \neq 0$. Consequentemente, 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 constante diferente de zero. Se f não é um polinômio de permutação de $\mathbb{F}_q$, então, o argumento utilizado na prova do Lema 3.1.5 nos mostra que $g(b) = 0$ para algum $b \in \mathbb{F}_q$, donde temos uma contradição. □

3.2 Certos tipos especiais de polinômios de permutação

Nesta subseção apresentaremos alguns resultados que nos permitirão obter exemplos simples de polinômios de permutação.

Teorema 3.2.1: Temos que:

(i) Todo polinômio linear de $\mathbb{F}_q[X]$ é um polinômio de permutação sobre $\mathbb{F}_q$.

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

Demonstração. Veja que:

(i) Seja $f(X) = aX + b \in \mathbb{F}_q[X]$ com $a \neq 0$. Para todos $x_1, x_2 \in \mathbb{F}_q$ temos que:

$$f(x_1) = f(x_2) \Leftrightarrow ax_1 + c = ax_2 + c \Leftrightarrow a(x_1 - x_2) = 0$$

como $a \neq 0$ temos que $x_1 - x_2 = 0$. Logo, $f(X) = c$ tem uma única solução para cada $c \in \mathbb{F}_q$. Segue do Lema 3.1.1 que f é um polinômio de permutação.

(ii) Note que, X^n é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, a função $x \in \mathbb{F}_q \mapsto x^n$ é sobrejetiva em $\mathbb{F}_q$. Seja t um elemento primitivo do grupo $\mathbb{F}_q^*$, assim, a imagem de $\mathbb{F}_q^*$ por f é o subgrupo cíclico gerado por t^n. Veja que, esse subgrupo é o próprio $\mathbb{F}_q^*$ se, e somente se, t^n é um elemento primitivo de $\mathbb{F}_q^*$, mas isso equivale a dizer que $mdc(q, n-1) = 1$, o que é claro, pois em um grupo cíclico finito de ordem m temos que o elemento c^k gera um subgrupo de ordem $\frac{m}{mdc(k,m)}$.

□

Teorema 3.2.2: Seja $\mathbb{F}_q$ de caractrística p. Então, o $q-$polinômio

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

é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $L(X)$ tem somente 0 como raíz em $\mathbb{F}_q$.

Demonstração. Claramente 0 é uma raíz de $L(X)$. Assim, supondo que $L(X)$ é um polinômio de permutação não pode haver outra solução para $L(X) = 0$ além do próprio 0.

Reciprocamente, se 0 é a única raíz de $L(X)$ em $\mathbb{F}_q$, então

$$L(a) = L(b) \Rightarrow L(a) - L(b) = 0 \Rightarrow L(a-b) = 0 \Rightarrow a - b = 0.$$

Logo, a função $X \mapsto L(X)$ é injetora e, assim, $L(X)$ é um polinômio de permutação. □

Exemplo 3.2.3: Considere o $2-$polinômio $f(X) = X + X^2 + X^4$ em $\mathbb{F}_2[X]$. Note que $f(0) = 0$ e $f(1) = 1$. Como a única raíz de $f(X)$ é 0, segue do Teorema 3.2.2 que $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_2$.

Podemos obter outros exemplos a partir do exposto acima observando que o conjunto de polinômios de permutação é fechado com relação à composição, o que ocorre se, e somente se, $f(X)$ e $g(X)$ são polinômios de permutação de $\mathbb{F}_q$, assim, $f(g(X))$ também é um polinômio de permutação de $\mathbb{F}_q$. O teorema a seguir nos fornecerá outras classes de polinômios de permutação.

Teorema 3.2.4: Seja $r \in \mathbb{N}$ com $mdc(r, q-1) = 1$ e seja s um divisor positivo de $q-1$. Seja $g \in \mathbb{F}_q[X]$ tal que $g(X^s)$ não tem raíz não nula em $\mathbb{F}_q$. Então, $f(X) = X^r(g(X^s))^{\frac{q-1}{s}}$ é um polinômio de permutação de $\mathbb{F}_q$.

Demonstração. Mostremos que f satisfaz as condições (i) e (ii) do Critério de Hermite. Assim, note

que a única raíz possível para f é 0, já que $g(X^s)$ não possui raíz não nula.

Agora, tome $t \in \mathbb{Z}$ com $1 \leq t \leq q-2$ e suponha que t não seja divisível por s. Dessa forma, todos os expoentes de $f(X)^t$ são da forma $rt+ks$, onde k é um inteiro positivo. Considerando que s é um divisor positivo de $q-1$ e $mdc(r,q-1)=1$, segue que $mdc(r,s)=1$. Ou seja, nenhum dos expoentes de $f(X)^t$ é divisível por s e, consequentemente, nenhum desses expoentes é divisível por $q-1$. Logo, não devem existir termos da forma $X^{i(q-1)}$ na expressão de $f(X)^t$, na qual a redução de $f(X)^t \pmod{X^q-X}$ tem grau menor ou igual a $q-2$.

Para a segunda condição, suponhamos quer $t=ks$, onde k é um inteiro positivo. Assim,

$$f(X)^t = X^{rt}(g(X^s))^{(\frac{q-1}{s})ks} = X^{rt}(g(X^s))^{(q-1)k}.$$

Considere $h(X)=X^{rt}$. Então, $f(c)^t = h(c)$ para todo $c \in \mathbb{F}_q^*$ desde que $g(c^s)=1$ se $c \neq 0$ e $f(0)^t = h(0)$. Então,

$$f(X)^t \equiv X^{rt} \pmod{X^q-X}$$

e, como rt não é divisível por $q-1$ temos que a redução $f(X)^t \pmod{X^q-X}$ tem grau menor ou igual a $q-2$. □

Exemplo 3.2.5: Seja $r=3$, $s=2$ e $q=3$. Note que $mdc(3,2)=1$ e $s|q-1=2$. Considere $g(X)=X+X^3 \in \mathbb{F}_3[X]$. Note que $g(X^2)=h(X)=X^2+X^6 \in \mathbb{F}_3[X]$ e $h(0)=0, h(1)=2$ e $h(2)=2$, ou seja, h não possui raíz não nula em $\mathbb{F}_3$. Então, segue do Teorema 3.2.4 que o polinômio

$$f(X) = X^3(g(X)^2)^{\frac{3-1}{2}} = X^3(X^2+X^6) = X^5+X^9$$

é um polinômio de permutação sobre $\mathbb{F}_3$.

Do Teorema 3.2.2 temos 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 também um polinômio de permutação de $\mathbb{F}_q$. Escolhendo b,c,d adequadamente podemos obter f_1 na forma normalizada, ou seja, f_1 mônico, $f_1(0)=0$ e, quando o grau n de f não for divisível pela característica de $\mathbb{F}_q$, o coeficiente de X^{n-1} é 0. É suficiente, então, estudar polinômios de permutação normalizados. Por meio do Critério de Hermite é possível construir uma tabela de todos os polinômio de permutação normalizados de grau menor ou igual a 5 (Ver [10] Tabela 7.1).

Para q ímpar podemos caracterizar os polinômios de permutação de $\mathbb{F}_q$ da forma $X^{(q+1)/2}+aX \in \mathbb{F}_q[X]$. Seja η o caracter quadrático de $\mathbb{F}_q$ definido por:

$$\eta(a) := \begin{cases} 1, & \text{se } a \text{ é um quadrado em } \mathbb{F}_q^* \\ -1, & \text{se } a \text{ não é um quadrado em } \mathbb{F}_q^* \\ 0, & \text{se } a=0 \end{cases}$$

Teorema 3.2.6: Para q ímpar, o polinômio $X^{(q+1)/2}+aX \in \mathbb{F}_q[X]$ é um polinômio de permutação de $\mathbb{F}_q$ se, e somente se, $\eta(a^2-1)=1$.

Demonstração. Mostremos que a função $X \mapsto f(X)$ não é injetiva se, e somente se, $\eta(a^2-1) \neq 1$. Assim, se existir $c \in \mathbb{F}_q^*$ tal que $f(c) = f(0) = 0$, então,

$$c^{\frac{q+1}{2}} + ac = 0 \Leftrightarrow a = -c^{\frac{q-1}{2}}.$$

Logo,

$$a^2 = (-c^{\frac{q-1}{2}})^2 = c^{q-1} = 1$$

e, portanto, $\eta(a^2-1) = 0$. Agora, se existirem $b, c \in \mathbb{F}_q^*$ distintos tais que $f(b) = f(c) \neq 0$ então,

$$\begin{aligned}(b^{\frac{q+1}{2}} + ab) = (c^{\frac{q+1}{2}} + ac) \Rightarrow 1 &= (c^{\frac{q+1}{2}} + ac)(b^{\frac{q+1}{2}} + ab)^{-1} \Rightarrow \\ 1 &= c(c^{\frac{q-1}{2}} + a)b^{-1}(b^{\frac{q-1}{2}} + a)^{-1} \\ \Rightarrow bc^{-1} &= (c^{\frac{q-1}{2}} + a)(b^{\frac{q-1}{2}} + a)^{-1}.\end{aligned}$$

Se tivéssemos $\eta(b) = \eta(c)$ então $b^{\frac{q-1}{2}} = c^{\frac{q-1}{2}}$ e, assim, $\frac{b}{c} = \zeta$ onde ζ é uma $\frac{q-1}{2}$ raíz primitiva da unidade, e isso implica que $b = c$, o que nos dá uma contradição. Logo, $\eta(b) \neq \eta(c)$. Sem perda de generalidade, vamos supor que $\eta(b) = -1$ e $\eta(c) = 1$. Então, $b^{\frac{q-1}{2}} = -1, c^{\frac{q-1}{2}} = 1$ e, assim,

$$-1 = \eta(bc^{-1}) = \eta((a+1)(a-1)^{-1}) = \eta((a+1)(a-1)) = \eta(a^2-1).$$

Por outro lado, suponhamos que $\eta(a^2-1) \neq 1$. Então, $a^2-1 = 0$ ou $\eta(a^2-1) = -1$. Para o primeiro caso temos que $a = \pm 1$ e, daí, existe $c \in \mathbb{F}_q^*$ tal que $c^{\frac{q-1}{2}} = -a$. Logo, $f(c) = f(0)$. Se $\eta(a^2-1) = -1$, tome $b = (a+1)(a-1)^{-1}$, então, $\eta(b) = -1$ e $b^{\frac{q-1}{2}} = -1$. Dessa forma,

$$f(b) = ab + b^{\frac{q+1}{2}} = (a + b^{\frac{q-1}{2}})b = (a-1)(a+1)(a-1)^{-1} = a+1 = f(1),$$

com $b \neq 1$. Em ambos os casos temos que $X \mapsto f(X)$ não é injetiva, como queríamos. □

Vale observar que $\eta(a^2-1) = 1$ se, e somente se $a = (c^2+1)(c^2-1)^{-1}$ para algum $c \in \mathbb{F}_q^*$ com $c^2 \neq 1$. Agora, se $\eta(a^2-1) = 1$, então, $a^2-1 = b^2$ para algum $b \in \mathbb{F}_q^*$ e, então, para $c = (a+1)b^{-1}$ temos que $c \neq 0$, $c^2 \neq 1$ e

$$(c^2+1)(c^2-1)^{-1} = \left[(a+1)^2 + b^2\right]\left[(a+1)^2 - b^2\right]^{-1} = 1.$$

Reciprocamente, se $a = (c^2+1)(c^2-1)^{-1}$, com $c \in \mathbb{F}_q^*$, $c^2 \neq 1$, então, $a^2-1 = 4c^2(c^2-1)^{-2}$, consequentemente, $\eta(a^2-1) = 1$.

Teorema 3.2.7: Sejam $a \in \mathbb{F}_q^*$ e q ímpar, então, $X^{\frac{q+1}{2}} + aX$ não é um polinômio de permutação de qualquer $\mathbb{F}_{q^r}$ com $r > 1$.

Demonstração. Ver [10] p. 353. □

Exemplo 3.2.8: Seja $q = 3$. Então, pelo Teorema 3.2.7 temos que o polinômio $X^2 + aX$ não permuta nenhuma extensão $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$ para $r > 1$. Seja $a = 1$ e $r = 2$. Vejamos se $f(X) = X^2 + X$ permuta $\mathbb{F}_{3^2}$.

Note que $f(1) = 2 = f(4)$, ou seja, $f(X)$ não é injetor. Logo, $f(X)$ não é um polinômio de permutação sobre $\mathbb{F}_{3^2}$.

O teorema anterior nos sugere que polinômios sobre $\mathbb{F}_q$ que são polinômios de permutação de todas as extensões finitas de $\mathbb{F}_q$ são, provavelmente, raros. Claramente, visto que os polinômios com essa propriedade podem ser classificados completamente e tem, de fato, uma forma especial. A seguir, enunciaremos um resultado que nos será bastante útil, sua demonstração pode ser encontrada em [10] no Lema 6.39.

Lema 3.2.9: Para quaisquer inteiro positivo m e p primo temos que

$$E_p(m) = \sum_{i=1}^{m} \lfloor \frac{m}{p^i} \rfloor = \frac{m-s}{p-1}.$$

onde s é a soma dos dígitos na representação de m para a base p.

Teorema 3.2.10: Um polinômio $f \in \mathbb{F}_q[X]$ é um polinômio de permutação de todas as extensões finitas de $\mathbb{F}_q$ se, e somente se é da forma $f(X) = aX^{p^h} + b$, onde $a \neq 0$, p é a característica de $\mathbb{F}_q$ e h é um inteiro não negativo.

Demonstração. Notemos que se f é um polinômio de permutação de $\mathbb{F}_q$, então, para todo $c \in \mathbb{F}_q$ temos que a equação $f(X) = c$ tem uma única solução $d \in \mathbb{F}_q$. Assim,

$$f(X) - c = (X-d)^k g(X)$$

onde $k \in \mathbb{N}, g \in \mathbb{F}_q[X]$n e deg $g = 0$ ou g é um produto de polinômios irredutíveis g_i em $\mathbb{F}_q[X]$ com deg $g_i \geq 2$. Dessa forma, supondo que g é um produto de polinômios irredutíveis g_i em $\mathbb{F}_q[X]$ com grau de g maior ou igual a 2 temos que se r é um múltiplo do grau de algum g_i, então, g_i tem uma raíz em $\mathbb{F}_{q^r}$ e, portanto, f não é um polinômio de permutação em $\mathbb{F}_{q^r}$. Assim, devemos ter que deg $g = 0$ e, portanto, $f(X) - c = a(X-d)^k$ com $a \neq 0$, isto é, para cada $c \in \mathbb{F}_q$ existe $d \in \mathbb{F}_q$ que depende de c tal que torne a identidade válida. Tomando $c = 0$, temos que $f(X) = a(X-d_0)^k$ e, escolhendo $c = 1$ segue que $f(X) = a(X-d_1)^k + 1$. Assim, obtemos que $a(X-d_0)^k - a(X-d_1)^k = 1$; Substituindo X por $X + d_1$ temos $a(X + d_1 - d_0)^k + aX^k = 1$. Expandindo, temos que $\binom{k}{j} \equiv 0 (\text{mod } p)$ para $0 < j < k$. Assim, $p^h \leq k < p^{h+1}$ para algum $h \in \mathbb{Z}, h \geq 0$. Se $k \neq p^h$, então, temos que $j = p^h$ e $E_p\left(\binom{k}{j}\right) = \frac{1}{p-1}(s_j + s_{k-j} - s_k) = 0$, onde s_n denota a soma dos dígitos na representação de n na base p. Como isso contradiz o fato que $\binom{k}{j} \equiv 0 (\text{mod } p)$ devemos ter $k = p^h$ e o restante segue do fato que $f(X) - c = a(X-d)^k$.

Por outro lado, seja $\mathbb{F}_{q^r}$ uma extensão finita de $\mathbb{F}_q$. Se $c = a^{-1}b$ então temos que

$$f(X) = aX^{p^h} + b = a(X^{p^h} + c) = a(X+c)^{p^h}.$$

Então, $f(X) = h \circ g(X)$, onde $g(X) = X + c$ é um polinômio de permutação de $\mathbb{F}_{q^r}$ e $h(X) = aX^{p^h}$ é um polinômio de permutação de $\mathbb{F}_{q^r}$. Portanto, $f(X)$ é um polinômio de permutação de $\mathbb{F}_{q^r}$. □

Exemplo 3.2.11: Seja $a = 1 = b, h = 2$, e $p = 3$. Então, pelo Teorema 3.2.10 temos que o polinômio $f(X) = X^{3^2} + 1 = X^9 + 1 \in \mathbb{F}_3[X]$ é um polinômio de permutação de todas as extensões finitas de $\mathbb{F}_3$.

Como consequência do teorema anterior enunciamos o seguinte resultado.

Corolário 3.2.12: Se $f \in \mathbb{F}_q[X]$ não é da forma $aX^{p^h} + b$, então, existem infinitas extensões $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$ de tal forma que f não é um polinômio de permutação de $\mathbb{F}_{q^r}$.

Capítulo 4

Alguns tipos de polinômios de permutação

Nesse capítulo apresentaremos alguns resultados preliminares e investigaremos as relação entre os dois tipos de polinômios de permutação apresentados abaixo:

$$cX - X^s + X^{qs}; \tag{4.1}$$

$$(X^{q^k} - X + \delta)^s + cX. \tag{4.2}$$

O estudo desses tipos de polinômios de permutação foi feito por Zheng, Yuan e Yu em [18].

Começamos este capítulo apresentando um resultados muito importante para o estudo de polinômios de permutação, o *Critério AGW*, apresentado por A. Akbary, D. Ghioca e Q. Wang em [1].

Lema 4.0.1: (Critério AGW) Sejam A, S e $\overline{S}$ conjuntos finitos com $\#S = \#\overline{S}$ e, sejam $f : A \to A$, $h : S \to \overline{S}$, $\lambda : A \to \overline{S}$ aplicações tais que $\overline{\lambda} \circ f = h \circ \lambda$. Se ambas λ e $\overline{\lambda}$ forem sobrejetivas, então as seguintes condições são equivalentes.

(1) f é uma bijeção; e

(2) h é uma bijeção de S em $\overline{S}$ e f é injetiva em $\lambda^{-1}(t)$ para cada $t \in S$.

Demonstração. $(1) \Rightarrow (2)$: Suponhamos que f seja uma bijeção. Assim, por definição, f será injetora em $\lambda^{-1}(t)$ para cada $t \in S$. Como f e $\overline{\lambda}$ são sobrejetivas e $\overline{\lambda} \circ f = h \circ \lambda$ então h é uma sobrejeção de S em $\overline{S}$, consequentemente h é uma bijeção de S em $\overline{S}$, pois ambos os conjuntos têm o mesmo número de elementos.

$(2) \Rightarrow (1)$: Considere agora que h seja uma bijeção em $\overline{S}$ e que f é injetiva em $\lambda^{-1}(t)$ para cada $t \in S$. Assim, sejam $x_1, x_2 \in A$ tais que $f(x_1) = f(x_2)$. Dessa forma, temos que

$$h(\lambda(x_1)) = \overline{\lambda}(f(x_1)) = \overline{\lambda}(f(x_2)) = h(\lambda(x_2))$$

Por hipótese h é bijetora, logo, $\lambda(x_1) = \lambda(x_2)$, isto é, $x_1, x_2 \in \lambda^{-1}(t)$ para algum $t \in S$. Assim, usando o fato que f é injetora em cada $\lambda^{-1}(t)$ temos que $x_1 = x_2$. Logo, f é injetora e, portanto, é uma bijeção,

visto que A é um conjunto finito. □

Este critério é muito útil para explicar algumas construções anteriores e para construir novas classes de polinômios de permutação. A chave do Critério AGW está em transformar o problema de construir permutações f de um conjunto finito A em encontrar bijeções g de S a $\overline{S}$, cujas cardinalidades são menores do que o tamanho de A.

Agora, seja $\mu_d = \{X \in \mathbb{F}_q^*; X^d = 1\}$, isto é, o conjunto das $d-$ésimas raízes da unidade, onde $d|(q-1)$. Tomando, por meio das notações do teorema anterior, $A = \mathbb{F}_q$, $S = \overline{S} = \mu_d$, $f(X) = X^r g(X^{(q-1)/d})$, $\lambda = \overline{\lambda} = X^{(q-1)/d}$ e $h(X) = X^r g(X)^{(q-1)/d}$ obtermos o resultado seguinte que nos será bastante útil, visto que sob certas condições ele nos permite estudar a bijeção de um polinômio apenas em um subconjunto de $\mathbb{F}_q$, não nele todo.

Lema 4.0.2: Sejam d, r inteiros positivos com $d|(q-1)$ e, seja, $h(X) \in \mathbb{F}_q[X]$. Então, o polinômio $X^r h(X^{(q-1)/d})$ permuta $\mathbb{F}_q$ se, e somente se, ambas afirmações abaixo são satisfeitas

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

(2) $X^r h(X)^{(q-1)/d}$ permuta μ_d.

Demonstração. Tome $s := (q-1)/d$. Assim, para $\varphi \in \mu_d$ temos que $f(\varphi) = \varphi^r f(X)$. Logo, se f permuta em $\mathbb{F}_q$ então $mdc(r,s) = 1$.

Reciprocamente, se $mdc(r,s) = 1$ então os valores de f em $\mathbb{F}_q$ consistem de todas as $s-$ésimas raízes dos valores de $f(X)^s = X^{rs} h(X^s)^s$. Mas, note que os valores de $f(X)^s$ em $\mathbb{F}_q$ consistem de $f(0)^s = 0$ e os valores de $g(X) := X^r h(X)^s$ em $(\mathbb{F}_q^*)^s$. Consequentemente, f permuta em $\mathbb{F}_q$ se, e somente se, g é uma bijeção em $(\mathbb{F}_q^*)^s = \mu_d$. □

A proposição a seguir nos fornecerá uma relação restrita entre dois polinômios de permutação.

Proposição 4.0.3: Sejam m,k inteiros com $0 < k < m$ e $l = mdc(k,m)$. Seja $c \in \mathbb{F}_{q^l}^*$ e $g(X) \in \mathbb{F}_{q^m}[X]$. Então, $f(X) = g(X^{q^k} - X + \delta) + cX$ permuta $\mathbb{F}_{q^m}$ para cada $\delta \in \mathbb{F}_{q^m}$ se, e somente se, $h(X) = g(X)^{q^k} - g(X) + cX$ permuta $\mathbb{F}_{q^m}$.

Demonstração. Sejam $\varphi(X) = X^{q^k} - X + \delta$ e $S_\delta = \{x^{q^k} - x + \delta; x \in \mathbb{F}_{q^m}\}$. Claramente temos que $S_\delta \subset \mathbb{F}_{q^m}$ e $\cup_{\delta \in \mathbb{F}_{q^m}} S_\delta = \mathbb{F}_{q^m}$ (tomando $X = 0$ vemos que $\delta \in S_\delta$). Agora, considere $\overline{h}(X) = g(X)^{q^k} - g(X) + cX + (1-c)\delta = h(X) + (1-c)\delta$. Observe que $\overline{h} : S_\delta \to S_\delta$. De fato, seja $y = x^{q^k} - x - \delta \in S_\delta$ para algum $x \in \mathbb{F}_{q^m}$. Então,

$$\begin{aligned}
\overline{h}(y) &= g(y)^{q^k} - g(y) + c(y) + (1-c)\delta \\
&= g(y)^{q^k} - g(y) + c(X^{q^k} - X + \delta) + \delta - c\delta \\
&= \underbrace{(g(y) + cX)}_{r}^{q^k} - (g(y) + cX) + c\delta + \delta - c\delta \\
&= r^{q^k} - r + \delta \in S_\delta
\end{aligned}$$

E mais,

$$\begin{aligned}(\varphi\circ f)(y) &= (g(\varphi(x))+cx)^{q^k}-(g(\varphi(x))+cx)+\delta\\ &= g(\varphi(x))^{q^k}-g(\varphi(x))+c(x^{q^k}-x)+\delta\end{aligned}$$

$$\begin{aligned}(\overline{h}\circ\varphi)(y) &= g(\varphi(x))^{q^k}-g(\varphi(x))+c(\varphi(x))+(1-c)\delta\\ &= g(\varphi(x))^{q^k}-g(\varphi(x))+c(x^{q^k}-x+\delta)+\delta-c\delta\\ &= g(\varphi(x))^{q^k}-g(\varphi(x))+c(x^{q^k}-x)+\delta.\end{aligned}$$

concluímos assim que $\varphi\circ f=\overline{h}\circ\varphi$.

Note que, para $\beta\in S_\delta$ temos que $f(X)=g(\beta)+cX$, o que nos fornece que f é injetora em $\varphi^{-1}(\beta)$. Assim, pelo Lema 4.0.1 temos que $f(X)$ permuta $\mathbb{F}_{q^m}$ se, e somente se, $\overline{h}(X)$ permuta S_δ para cada $\delta\in\mathbb{F}_{q^m}$. Mas, note que $\overline{h}=h+(1-c)\delta$, então, $\overline{h}$ permuta S_δ se, e somente se, h for uma bijeção entre S_δ e $S_{c\delta}$ para cada $\delta\in\mathbb{F}_{q^m}$.

Agora, observemos que $\cup_{\delta\in\mathbb{F}_{q^m}}S_\delta=\cup_{\delta\in\mathbb{F}_{q^m}}S_{c\delta}=\mathbb{F}_{q^m}$. Logo, se h for uma bijeção entre S_δ e $S_{c\delta}$ para cada $\delta\in\mathbb{F}_{q^m}$ então h será uma sobrejeção de $\mathbb{F}_{q^m}$ em si mesmo, e como $\mathbb{F}_{q^m}$ é finito então h será uma bijeção de $\mathbb{F}_{q^m}$. Agora, se h for uma bijeção de $\mathbb{F}_{q^m}$ então h será uma bijeção de S_δ e $S_{c\delta}$. Portanto, $\overline{h}$ permuta S_δ para cada $\delta\in\mathbb{F}_{q^m}$ se, e somente se, h for uma bijeção em $\mathbb{F}_{q^m}$. □

Vale observar que a Proposição 4.0.3 nos fornece a relação entre dois tipos de polinômios de permutação e não envolve subconjuntos e sua bijeções, então, é um resultado mais forte para encontrar encontrar polinômios de permutação da forma generalizada $((X^{q^k}-X+\delta)^s+cX)$ sem restrição a δ.

Se tomarmos, usando a notação da proposição anterior, $m=2$, $k=1$ e $g(X)=X^s$ teríamos que $c\in\mathbb{F}_q^*$. E daí $ccXX^s+X^{qs}$ permuta $\mathbb{F}_{q^2}$ se, e somente se, $(X^q-X+\delta)^s+cX$ permuta $\mathbb{F}_{q^2}$. O corolário a seguir é um exemplo derivado de que $h(X)$ é um polinômio de permutação do tipo quadrático.

Corolário 4.0.4: Sejam k,m,l inteiros positivos com $\frac{m}{mdc(m,kl)}$ ímpar. Sejam $s_1=\frac{1}{2^{kl}+1}$ e $s_{i+1}=2^k s_i$, ou seja, $s_i=\frac{2^{k(i-1)}}{2^{kl}+1}$ para $1\leq i\leq l$. Então, o polinômio

$$f(X)=\sum_{i=1}^{l}(X^{2^k}+X+\delta)^{s_i}+x$$

permuta $\mathbb{F}_{2^m}$ para $\delta\in\mathbb{F}_{2^m}$.

Demonstração. Considere $g(X)=\sum_{i=1}^{l}X^{s_i}$. Por hipótese $\frac{m}{mdc(m,kl)}$ é ímpar, logo, $mdc(2^{kl}+1,2^m+1)=1$. Dessa forma,

$$h(X)=g(X)^{2^k}-g(X)+x=(X^{\frac{1}{2^{kl}+1}}+1)^{2^{kl}+1}-1$$

permuta $\mathbb{F}_{2^m}$. Da Proposição 4.0.3 segue que $f(X)$ permuta $\mathbb{F}_{2^m}$. □

Exemplo 4.0.5: Sejam $m=2=k,l=3$ e $\delta=3\in\mathbb{F}_4$. Seja $s_i=\frac{2^{2(i-1)}}{2^6+1}=\frac{2^{2(i-1)}}{65}$ para $1\leq i\leq 3$. Então,

o polinômio

$$f(X)=\sum_{i=1}^{3}(X^4+X+3)^{s_i}+x=(X^4+X+3)^{\frac{1}{65}}+(X^4+X+3)^{\frac{4}{65}}+(X^4+X+3)^{\frac{16}{65}}+3x$$

é um polinômio de permutação sobre $\mathbb{F}_4$.

Vale observar que o caso $l=1$ e alguns casos específicos de $l=2$ do corolário anterior foram provados, respectivamente, por [15] e [17]. A prova do corolário a seguir pode ser encontrada em [9] Proposição 4.

Corolário 4.0.6: Sejam m um inteiro positivo e $\delta \in \mathbb{F}_{2^{3m}}$ fixo. Então, o polinômio

$$f(X)=(X^{2^m}+X+\delta)^s+X$$

é de permutação em $\mathbb{F}_{2^{3m}}$ se uma das seguintes condições acontece:

(1) $s=2^{2m}+1$;

(2) $s=2^{im-1}+2^{m-1}$, $mdc((i-1)m-1,3m)=1$, $i\in\{2,3\}$.

Exemplo 4.0.7: Sejam $m=2$, $s=65$ e $\delta=5\in\mathbb{F}_{2^6}$. Então, o polinômio $f(X)=(X^8+X+5)^{65}+X$ permuta $\mathbb{F}_{2^6}$.

Corolário 4.0.8: Sejam m e e inteiros positivos. Seja $s=2^{2e-1}+2^{m-1}$ com $mdc(e-1,3e)=1$ ou $s=2^{3e-1}+2^{m-1}$ com $mdc(2e-1,3e)=1$. Então, o polinômio $X^{2^m s}+X^s+X$ permuta $\mathbb{F}_{2^{3m}}$.

Demonstração. Seja $g(X):=X^s\in\mathbb{F}_{2^{3m}}$. Pelo Corolário 4.0.6 sabemos que o polinômio $f(X)=g(X^{2^m}+X+\delta)+X=(X^{2^m}+X+\delta)^s+X$ permuta $\mathbb{F}_{2^{3m}}$ para cada $\delta\in\mathbb{F}_{2^{3m}}$. Assim, considerando $q=2,k=m$ segue da Proposição 4.0.3 que o polinômio $h(X)=g(X)^{2^m}+g(X)+X=X^{2^m s}+X^s+X$ permuta $\mathbb{F}_{2^{3m}}$, como queríamos. □

Exemplo 4.0.9: Sejam $m=10,e=6$ e $s=544$. Então, o polinômio $f(X)=X^{557056}+X^{544}+X$ permuta $\mathbb{F}_{2^{30}}$.

4.1 Polinômios de permutação com a forma $cX-X^s+X^{sq}$

A seguir, apresentaremos mais quatro tipos de polinômios de permutação que terão a forma $cX-X^s+X^{sq}$ para algum s indexado e parâmetro $c\in\mathbb{F}_{q^2}^*$.

Teorema 4.1.1: Seja $s=\frac{3q^2+2q-1}{4}$ e $c\in\mathbb{F}_{q^2}^*$. O polinômio $f(X)=cX-X^s+X^{qs}$ permuta $\mathbb{F}_{q^2}$ em cada um dos seguintes casos:

(i) $q\equiv 1 \pmod 8$ e $\left(\frac{-2}{c}\right)^{\frac{q+1}{2}}=1$;

(ii) $q \equiv 5 \pmod 8$ e $\left(\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$.

Demonstração. Provaremos somente o item (i). A prova do caso (ii) segue de forma análoga.

Como $q \equiv 1 \pmod 8$ então $4 \mid (3q+5)$. Assim, podemos reescrever o polinômio $f(X)$ como

$$f(X) = cX - X^{\frac{3q+5}{4}(q-1)+1} + X^{\left(\frac{3q+5}{4}q+1\right)(q-1)+1}.$$

Seja $u = \frac{3q+5}{4}$. Então, pelo Lema 4.0.2 temos que $f(X)$ permuta $\mathbb{F}_{q^2}$ se, e somente se,

$$g(X) = X(c + X^{1-u} - X^u)^{q-1}$$

permuta μ_{q+1}.

Seja $\mu_{\frac{q+1}{2}}$ o subgrupo cíclico de μ_{q+1} de ordem $\frac{q+1}{2}$. Por uma simples verificação temos que $\mu_{\frac{q+1}{2}}$ é formado pelos quadrados dos elementos de μ_{q+1}. Como $q \equiv 1 \pmod 8$ temos que -1 é um elemento não quadrado de μ_{q+1}. Então, $-\mu_{\frac{q+1}{2}}$ é o conjunto de todos os elementos não-quadrados de μ_{q+1}. A seguir mostraremos que $g(X)$ permuta $\mu_{\frac{q+1}{2}}$ e $-\mu_{\frac{q+1}{2}}$, respectivamente.

Como $q \equiv 1 \pmod 8$ temos que o quadrado é uma bijeção em $\mu_{\frac{q+1}{2}}$. Assim, para $x \in \mu_{\frac{q+1}{2}}$ existe um único $y \in \mu_{\frac{q+1}{2}}$ tal que $x = y^2$. Então,

$$x^u = (y^2)^u = y^{2\frac{3q+5}{4}} = y^{\frac{3q+5}{2}} = y, x^{1-u} = x.x^{-u} = y^2.y^{-1} = y.$$

Ou seja, $g(X) = c^{q-1}X$ e permuta $\mu_{\frac{q+1}{2}}$.

Agora, tome $x \in -\mu_{\frac{q+1}{2}}$. Então, existe um único $y \in \mu_{\frac{q+1}{2}}$ tal que $x = -y^2$ pelo mesmo motivo dado acima. Devido a $(-2/c)^{\frac{q+1}{2}} = 1$, isto é, $c/2 \in -\mu_{\frac{q+1}{2}}$ e $y \in \mu_{\frac{q+1}{2}}$, temos que $c - 2y \neq 0$. Daí,

$$\begin{aligned} g(x) &= g(-y^2) = -y^2(c + (-1)^{1-u}y - (-1)^u y)^{q-1} \\ &= -y^2\frac{(c-2y)^q}{2-2y} = -y^2\frac{c^q - 2y^{-1}}{c-2y} \\ &= \frac{2}{c}y. \end{aligned}$$

Como $\frac{c}{2} \in -\mu_{\frac{q+1}{2}}$ e $y \in \mu_{\frac{q+1}{2}}$ temos que $\frac{2}{c}y \in -\mu_{\frac{q+1}{2}}$. Logo, $g(X)$ permuta $-\mu_{\frac{q+1}{2}}$. Combinando os dois casos acima temos que $g(X)$ permuta μ_{q+1}. □

Exemplo 4.1.2: Seja $q = 9$ e $c = -2 \in \mathbb{F}_{81}^*$. Note que $9 \equiv 1 \pmod 8$ e $\left(\frac{-2}{-2}\right)^{\frac{9+1}{2}} = 1^5 = 1$. Além disso, $s = \frac{3.9^2+2.9-1}{4} = 65$. Logo, pelo Teorema 4.1.1 temos que o polinômio $f(X) = -2X - X^{65} + X^{585}$ permuta $\mathbb{F}_{81}$.

De modo análogo ao teorema anterior, pode-se obter outra família de infinitas classes de polinômios de permutação sobre $\mathbb{F}_{q^2}$, como segue abaixo.

Teorema 4.1.3: Seja $s = \frac{(q+1)^2}{4}$ e $c \in \mathbb{F}_{q^2}^*$. O polinômio $f(X) = cX - X^s + X^{qs}$ permuta $\mathbb{F}_{q^2}$ em cada

um dos casos abaixo:

(i) $q \equiv 5 \pmod 8$ e $\left(\frac{-2}{c}\right)^{\frac{q+1}{2}} = 1$;

(ii) $q \equiv 1 \pmod 8$ e $\left(\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$.

O teorema a seguir nos fornece outra família de classes infinitas de polinômios de permutação sobre $\mathbb{F}_{q^2}$.

Teorema 4.1.4: Seja q uma potência de um primo com $q \equiv 1 \pmod 3$ e $s = \frac{q^2+q+1}{3}$. Então, $f(X) = X - X^s + X^{qs}$ é um polinômio de permutação sobre $\mathbb{F}_{q^2}$.

Demonstração. Como $q \equiv 1 \pmod 3$ temos que $3 \mid (q+2)$, Assim, o polinômio $f(X)$ é reescrito como

$$f(X) = X - X^{\frac{q+2}{3}(q-1)+1} + X^{\left(\frac{q(q+2)}{3}+1\right)(q-1)+1}.$$

Seja $u = \frac{q+2}{3}$. Pelo Lema 4.0.2 temos que $f(X)$ permuta $\mathbb{F}_{q^2}$ se, e somente se,

$$g(X) = X(1 + X^{1-u} - X^u)^{q-1}.$$

permuta μ_{q+1}. Mostremos primeiro que $1 + X^{1-u} - X^u = 0$ não tem raízes em μ_{q+1}. Para isso, assuma que existe $x \in \mu_{q+1}$ tal que

$$1 + x^{1-u} - x^u = 0, x^{q+1} = 1. \tag{4.3}$$

Isso implica que $x^{2u-1} - x^{u-1} = x^{q+1}$, ou seja, $x^{2u-2} - x^{u-2} = x^q$. Isso implica que $x^{2-2u} - x^{2-u} = x$, então, $x^{1-2u} = x^{1-u} = 1$, isto é, $x^{2u-1} + x^u = 1$. Essa igualdade juntamente com (4.3) implica que $x^{u-1} + x^u = 0$, ou seja, $x = -1$. Por outro lado, é fácil ver que $x = -1$ não satisfaz (4.3) pois $3 \nmid q$. Logo, temos uma contradição.

Agora, observe que para algum $x \in \mu_{q+1}$ temos que $x^{3u} = X$ desde que $u = \frac{q+2}{3}$ e

$$g(x) = x\frac{1 + x^{u-1} - x^{-u}}{1 + x^{1-u} - x^u} = \frac{x + x^u - x^{1-u}}{1 + x^{1-u} - x^u} = \frac{x^u + x^{3u} - x^{2u}}{1 + x^{2u} - x^u} = x^u.$$

Então, $g(X)$ permuta μ_{q+1} desde que $mdc(u, q+1) = 1$. □

Exemplo 4.1.5: Seja $q = 4 = 2^2$ e observe que $4 \equiv 1 \pmod 3$. Dado $s = \frac{4^2+4+1}{3} = \frac{21}{3} = 7$ temos, pelo Teorema 4.1.4, que o polinômio $f(X) = X - X^7 + X^{28}$ permuta $\mathbb{F}_{16}$.

A principal técnica para provar o teorema acima vem do Lema 4.0.2. Este método não se aplica ao próximo teorema. Usando os métodos fornecidos por [3], [5], foi proposto uma série de polinômios de permutação de classes infinitas em $\mathbb{F}_{q^4}$. Em [5], o autor eliminou algumas variáveis computando a base de Grobner para alguns ideais, já o processo em [18] baseou-se em eliminar algumas variáveis através do processo de encontrar o resultado de dois polinômios. Mas, primeiro, vamos apresentar dois lemas preliminares.

Lema 4.1.6: Existe $x \in \mathbb{F}_{q^4}$ tal que $x^{2q^2} + x^{q^2+1} + x^2 = 0$ se, e somente se, $3|q$ e $x^{q^2-1} = 1$.

Demonstração. Assuma que $x \in \mathbb{F}_{q^4}$ satisfaz

$$x^{2q^2} + x^{q^2+1} + x^2 = 0.$$

Assim, seja $y = x^{q^2-1}$,então, $y \in \mu_{q^2+1}$ e $y^2+y+1 = 0$. Segue daí que $y^3 = 1$. Como $mdc(3, q^2+1) = 1$, devemos ter que $y = 1$ e $3|q$.

Agora, suponha que $3 \mid q$ e $x^{q^2-1} = 1$. Note que,

$$x^{2q^2} + x^{q^2+1} + x^2 = x^2(x^{2(q^2-1)} + x^{q^2-1} + 1).$$

Como $x^{q^2-1} = 1$, segue que $x^2(x^{2(q^2-1)} + x^{q^2-1} + 1) = x^2(1+1+1)$, e como $3 \mid q$ temos que $1+1+1 = 0$, e segue o resultado. □

Exemplo 4.1.7: Seja $q = 3$. Note que $80 \equiv -1 \pmod{81}$, então, $80^8 \equiv 1 \pmod{81}$. Logo, considerando $x = 80$ temos que $80^8 = 1$. Segue do Lema 4.1.6 que $x = 80$ é raíz de $X^{18} + X^{10} + X^2$ sobre $\mathbb{F}_{81}$.

A demonstração do lema a segir é análoga à do lema que vimos anteriormente.

Lema 4.1.8: Existe $x \in \mathbb{F}_{q^4}$ tal que $x^{2q^2} - x^{q^2+1} + x^2 = 0$ se, e somente se, $3|q$ e $x^{q^2-1} = -1$.

Teorema 4.1.9: Seja q uma potência de um primo ímpar e $s = q^3 + q^2 - q$. Então, o polinômio $f(X) = X - X^s + X^{q^2 s}$ permuta $\mathbb{F}_{q^4}$;

Demonstração. Vamos provar que $f(X) = \alpha$ tem somente uma raíz em $\mathbb{F}_{q^4}$ para qualquer $\alpha \in \mathbb{F}_{q^4}$. Para isso, vamos separar a prova em casos.

Caso 1: $\alpha = 0$ e $f(X) = 0$. Claramente a equação tem uma solução $x = 0$. A seguir vamos mostrar que não existe $x \in \mathbb{F}_{q^4}^*$ satisfazendo $f(x) = 0$. Seja $x \in \mathbb{F}_{q^4}$ tal que

$$1 - x^{q^3+q^2-q-1} + x^{-q^3+q} = 0.$$

Denote por $y = x^{q^2-1}$, então, $y \in \mu_{q^2+1}$. Da equação acima obtemos

$$y^{q+1} - y^{-q} = 1 \tag{4.4}$$

Calculando $(4.4)^q - (4.4)^{q^3}$ juntamente com $y^{q^2} = y^{-1}$ obtemos

$$\begin{aligned} 0 &= y^{q^2+q} - y^{-q^2} - y^{q^3+1} = y^{-1} \\ &= y^{q-1} - y - y^{-q+1} + y^{-1} \\ &= (y^{q-1} - y)(y^{-q} + 1). \end{aligned}$$

Segue daí que $y^{q-2}=1$ pois $y\neq -1$. Esse fato juntamente com $y^{q^2+1}=1$ implica que

$$y^{mdc(q-2,q^2+1)}=y^{mdc(q-2,5)}=1.$$

Então, temos que $y^5=1$. Por outro lado, substituindo $y^{q-2}=1$ em (4.4) temos que $y^5=y^2+1$. Isso, junto com o fato que $y^5=1$ implica que $y=0$, uma contradição. Então, $f(X)=0$ tem somente uma solução $x=0$ em $\mathbb{F}_{q^4}$.

Para discutirmos o caso em que $\alpha\neq 0$ vamos definir dois conjuntos, como segue,

$$S_{\pm}=\{x\in\mathbb{F}_{q^4}; x^{2q^2}\pm x^{q^2+1}+x^2=0\}.$$

Caso 2: $\alpha\in S_+$ e $f(X)=\alpha$. Pelo Lema 4.1.6 temos que $3|q$ e $\alpha^{q^2}-\alpha=0$. Nesse caso temos que

$$\begin{aligned}
0 &= \alpha^{q^2}-\alpha=f(X)^{q^2}-f(X)\\
&= X^{q^2}-X^{-q^3+q+1}+X^{q^3+q^2-q}-(X-X^{q^3+q^2}-q+X^{-q^3+q+1})\\
&= X^{q^2}-X-X^{q^3+q^2-q}+X^{-q^3+q+1}\\
&= X^{-q^3-q}(X-X^{q^2})^q(X^{q^2+q^3}+X^{1+q}).
\end{aligned}$$

Se $X-X^{q^2}=0$ então $f(X)=X=\alpha$. Se $X^{q^2+q^3}=-X^{1+q}$ então $X^{(q+1)(q^2-1)}=-1$. Como $x\in\mathbb{F}_{q^4}$ temos que $X^{mdc(2(q+1)(q^2-1),q^4-1)}=X^{2(q+1)}=1$. Isso implica que $X^{(1+q)(q^2-1)}=1$. O que nos leva a uma contradição. Consequentemente, $f(X)=\alpha$ tem somente uma raíz $x=\alpha$.

Caso 3: $\alpha\in S_-$ e $f(X)=\alpha$. Por uma prova análoga à do Caso 2 temos que $f(X)=\alpha$ tem somente uma solução $x=\alpha$.

Agora, denote por $T=\mathbb{F}_{q^4}^*\setminus(S_+\cup S_-)$. Das provas dos Casos 1 e 2 sabemos que $f(X)$ é uma permutação sobre S_+ e S_- respectivamente. Além disso, $f(T)\subseteq T$. Isso nos leva a mostrar que $f(X)$ também é um polinômio de permutação sobre o conjunto T.

Caso 4: $\alpha\in T$. Vamos mostrar que $f(X)=\alpha$ tem somente um $x\in T$ satisfazendo a equação. Assim, denote por

$$y=x^q, z=x^{q^2}, w=x^{q^3}, \beta=\alpha^q, \gamma=\alpha^{q^2}, \delta=\alpha^{q^3}.$$

Com isso, a equação $f(X)=\alpha$ é reduzida a

$$x+\frac{xy}{w}-\frac{zw}{y}=\alpha. \tag{4.5}$$

Tomando $q-$ésima, q^2-ésima e q^3-ésima potência em ambos os lados de (4.5) respectivamente, obtemos:

$$y+\frac{yz}{x}-\frac{wx}{z}=\beta, \tag{4.6}$$

$$z+\frac{zw}{y}-\frac{yx}{w}=\gamma, \tag{4.7}$$

$$w+\frac{wx}{z}-\frac{yz}{x}=\delta, \tag{4.8}$$

respectivamente. Somando (4.5) e (4.7) obtemos $z=\alpha+\gamma-x$. Analogamente, obtemos $w=\beta+\delta-y$ de (4.6) e (4.8). Substituindo as duas igualdades em (4.5) e (4.6) respectivamente, obtemos

$$\begin{cases} (-\gamma+x)y^2+((\alpha+2\gamma-x)(\beta+\delta))y+(-\alpha-\gamma+x)(\beta+\delta)^2=0 \\ (x^2-(\alpha+\gamma)x+(\alpha+\gamma)^2)y-\delta x^2-\beta(\alpha+\gamma)x=0. \end{cases} \tag{4.9}$$

Como $x\in T$, segue do Lema 4.1.6 que

$$x^2-(\alpha+\gamma)x+(\alpha+\gamma)^2=x^2+xz+z^2\neq 0.$$

Da segunda equação em (4.9) temos que

$$y=\frac{x(\beta\alpha+\beta\gamma+\delta x)}{\alpha^2+2\alpha\gamma+\gamma^2-(\alpha+\gamma)x+x^2}:=H(x). \tag{4.10}$$

Substituindo y na primeira equação de (4.9) obtemos uma igualdade $A(X)=0$, onde $A(X)\in \mathbb{F}_{q^4}^*[\alpha,\beta,\gamma,\delta][X]$ e seu grau em X é 5.

Agora, suponha que $f(X)=\alpha$ tem outra raíz $X\in T$ diferente de x, então, $A(X)=0$. Substituindo $\alpha,\beta,\gamma,\delta$ em coeficientes de $A(X)$ pela esquerda de (4.5, (4.6), (4.7) e (4.8) respectivamente e, multiplicando wx^2yz^2 em ambos os lados de $A(X)=0$ nós obtemos

$$(X-x)B(X)C(X)=0 \tag{4.11}$$

onde

$B(X)=yw(X^2+xz+z^2)X^2+wxz(z+x)^2(w+y)-(z+x)(w^2xz+wX^2y+wxyz+wyz^2-xy^2z)X$

$C(X)=(w^2X^2-wxyz+y^2z^2)X^2+yz(z+x)^3(w+y)+(z+x)(w^2xz+wX^2y+wxyz-xy^2z-2y^2z^2)X.$

Consequentemente, $B(X)=0$ ou $C(X)=0$. Isso pode ser verificado acima vendo que $yw(X^2+xz+z^2)\neq 0$. Assuma que $w^2X^2-wxyz+y^2z^2=0$. Então,

$$0=w^2X^2-wxyz+y^2z^2=(yz)^{2q^2}-(yz)^{q^2+1}+(yz)^2. \tag{4.12}$$

Pelo Lema 4.1.8 temos que $(yz)^{q^2-1}=-1$, isto é, $y^{(q^2-1)(q+1)}=-1$. Como $mdc(2(q^2-1)(q+1),q^4-1)=2(q^2-1)$, temos que $y^2(q^2-1)=1$. Uma contradição com $y^{(q^2-1)(q+1)}=-1$. Então, o grau de $B(X)$ e $C(X)$ em X é 2, respectivamente.

(i) Quando $B(X)=0$ em (4.11). Tomando a $q-$ésima potência em ambos os lados da igualdade temos que $B'(X^q)=0$, onde os coeficientes de $B'(X)$ são as $q-$ésimas potências dos coeficientes correspondentes de $B(X)$. Substituindo $Y=X^q$ com $H(X)$ em (4.10) nós obtemos

$$0=B'(H(X))=C(X)D(X), \tag{4.13}$$

onde

$D(X)=(w^2X^2+w^2xz+zxwy+xy^2z+y^2z^2)X^2+wX^2(z+x)^2(w+y)-(z+x)(2w^2X^2+w^2xz+wX^2y+zxwy-wyz^2xy^2z)X$. Se $C(X)=0$ de (4.13) temos que X é uma raíz comum de $B(X)$ e

$C(X)$. Então, o resultante desses dois polinômios poderia ser 0. Assim,

$$\begin{aligned} 0 = Res(B(X),C(X),X) = zx(z+x)^4(w+y)^2\times \\ \times(w^2X^2 - zxwy + y^2z^2)\times \\ \times(w^2xz + w^2z^2 + wxyz + X^2y^2 + xy^2z)^{q+1} \end{aligned} \tag{4.14}$$

Foi verificado acima que $w^2X^2 - zxwy + y^2z^2 \neq 0$. Além disso, temos que $(z+x)(w+y) \neq 0$. De fato, se $X+z=0$ ou $w+y=0$ podíamos dizer que $B(X) = D(X) = X^2y^2X^2 = 0$. De (4.14) temos que

$$w^2xz + w^2z^2 + wxyz + X^2y^2 + xy^2z = 0. \tag{4.15}$$

combinando (4.15) e $B(X) = 0$ obtemos que

$$yw(X^2 + xz + z^2)(X-x)^2 = 0.$$

Uma contradição com o fato de que $X^2 + xz + z^2 \neq 0$ e $X \neq x$. Então, de (4.13) temos que $D(X) = 0$. Se o coeficiente líder de $D(X)$ é diferente de zero, isto é, $w^2X^2 + w^2xz + zxwy + xy^2z + y^2z^2 \neq 0$ então

$$0 = Res(B(X),D(X),X) = xwyz(z+x)^6(w+y)^2(w^2X^2 - zxwy + y^2z^2)^{q+1}.$$

Isso é impossível de acordo com as discussões feitas nos parágrafos anteriores. Consequentemente, o coeficiente líder de $D(X)$ é zero, ou seja,

$$L(X) = w^2X^2 + w^2xz + zxwy + xy^2z + y^2z^2 = 0.$$

O fato que $wX^2(z+x)^2(w+y) \neq 0$ implica que o grau de $D(X)$ é 1. O resultante entre $B(X)$ e $D(X)$ é zero. Então,

$$0 = Res(B(X),D(X),X) = (z+x)^4xw(w+y)U(X), \tag{4.16}$$

onde

$U(X) = -yw^3X^5 + (2zw^4 + yzw^3 + 2y^2zw^2X^4)X^4 + (3z^2w^4 + 3yz^2w^3 + 6y^2z^2w^2 + 2y^3z^2w + y^4z^2)X^3 + (z^3w^4 - 2yz^3w^3 + y^2z^3w^2 + y^4z^3)X^2 - (2yz^4w^3 + y^2z^4w^2 + 2y^3z^4w)X + y^2z^5w^2$.
De (4.16) temos que $U(X) = 0$. Calculando o resultante de $L(X)$ e $U(X)$ temos

$$0 = Res(L(X),U(X),x) = (w^2 + y^2)(w+y)^6w^4z^{10}y^4 \tag{4.17}$$

Nesse caso, fica verificado acima que $y+w \neq 0$. De (4.17) temos que $w^2 = -y^2$, ou seja,$y^{2(q^2-1)} = -1$ e $y^{4(q^2-1)} = 1$. Então, $y^{mdc(4(q^2-1),q^4-1)} = y^{2(q^2-1)} = 1$. O que nos dá uma contradição. Então, provamos que $B(X)$ não pode ser zero.

(ii) Analogamente, podemos provar que $C(X)$ em (4.11) não é zero. Consequentemente, $f(X) = \alpha$ tem somente uma raíz em T e $f(X)$ permuta T.

□

Exemplo 4.1.10: Sejam $q = 3^2$ e $s = (3^2)^3 + (3^2)^2 - 3^2 = 801$. Então, pelo teorema anterior, temos que $f(X) = X - X^{801} + X^{7209}$ é um polinômio de permutação sobre $\mathbb{F}_{9^4}$.

4.2 Polinômios de permutação com a forma $(X^{q^k} - X + \delta)^s + cX$

Nessa seção apresentaremos algumas classes de polinômios de permutação com a forma (4.2) sem restrições a δ. Esses polinômios são derivados de trinômios de permutação conhecidos com a forma (4.1) por meio da Proposição 4.0.3.

Proposição 4.2.1: Sejam $\delta \in \mathbb{F}_{q^2}$ e $c \in \mathbb{F}_q^*$. O polinômio

$$f(X) = (X^q - X + \delta)^{\frac{3q^2+2q-1}{4}} + cX$$

é de permutação sobre $\mathbb{F}_{q^2}$ em cada um dos seguintes casos:

(i) $q \equiv 1 \pmod 8$ e $c = -2$;

(ii) $q \equiv 5 \pmod 8$ e $c = 2$.

Demonstração. A demonstração é análoga à do Teorema 4.1.1. No item (i) basta obsevar que como $c = -2$ temos que $-\frac{2}{c} = 1$ e daí $(-\frac{2}{c})^{\frac{q+1}{2}} = 1$. Para o item (ii) segue-se o mesmo raciocínio. □

Exemplo 4.2.2: Sejam $q = 13$, $c = 2$ e $\delta = 11 \in \mathbb{F}_{13}^*$. Então, pela Proposição 4.2.1 segue que o polinômio $f(X) = (X^{13} - X + 11)^{133} + 2x$ permuta $\mathbb{F}_{13^2}$.

A demonstração da proposição abaixo é análoga à do Teorema 4.1.1, para isso basta perceber que o polinômio $f(X) = (X^q - X + \delta)^{\frac{(q+1)^2}{4}} + cX$ permuta $\mathbb{F}_{q^2}$ se, e somente se, $g(X) = X^{q\frac{(q+1)^2}{4}} - X^{\frac{(q+1)^2}{4}} + cX$ permuta $\mathbb{F}_{q^2}$.

Proposição 4.2.3: Sejam $\delta \in \mathbb{F}_{q^2}$ e $c \in \mathbb{F}_q^*$. O polinômio

$$f(X) = (X^q - X + \delta)^{\frac{(q+1)^2}{4}} + cX$$

permuta $\mathbb{F}_{q^2}$ em cada um dos seguintes casos:

(i) $q \equiv 1 \pmod 8$ e $c = 2$;

(ii) $q \equiv 5 \pmod 8$ e $c = -2$

Exemplo 4.2.4: Sejam $q = 9$, $c = 2$ e $\delta = 7 \in \mathbb{F}_9^*$. Então, pela Proposição 4.2.3 segue que o polinômio $f(X) = (X^9 - X + 7)^{25} + 2x$ permuta $\mathbb{F}_{9^2}$.

Proposição 4.2.5: Seja q uma potência de um primo ímpar com $q \equiv 1 \pmod 3$. Para $\delta \in \mathbb{F}_{q^2}$, o polinômio

$$f(X) = (X^q - X + \delta)^{\frac{q^2+q+1}{3}} + x$$

permuta $\mathbb{F}_{q^2}$.

Demonstração. Pela Proposição 4.0.3 temos que o polinômio $f(X) = (X^q - X + \delta)^{\frac{q^2+q+1}{3}} + x$ permuta $\mathbb{F}_{q^2}$ se, e somente se, $g(X) = X^{q\frac{q^2+q+1}{3}} - X^{\frac{q^2+q+1}{3}} + x$ permuta $\mathbb{F}_{q^2}$. O restante da demonstração é análoga à do Teorema 4.1.4. □

Exemplo 4.2.6: Sejam $q = 25 = 5^2$ e $\delta = 79 \in \mathbb{F}_{25^2}$. Então, pela Proposição 4.2.5 segue que o polinômio $f(X) = (X^{25} - X + 79)^{217} + x$ permuta $\mathbb{F}_{25^2}$.

Proposição 4.2.7: Sejam q uma potência de um primo ímpar e $\delta \in \mathbb{F}_{q^4}$. O polinômio

$$f(X) = (X^{q^2} - X + \delta)^{q^3+q^2-q} + X$$

é de permutação sobre $\mathbb{F}_{q^4}$.

Demonstração. Segue da Proposição 4.0.3 que o polinômio $f(X) = (X^{q^2} - X + \delta)^{q^3+q^2-q} + X$ permuta $\mathbb{F}_{q^4}$ se, e somente se, $g(X) = X^{q^2(q^3+q^2-q)} - X^{q^3+q^2-q} + X$ permuta $\mathbb{F}_{q^4}$. O restante da demonstração é análoga à do Teorema 4.1.9. □

Exemplo 4.2.8: Sejam $q = 9$ e $\delta = 11 \in \mathbb{F}_{9^4}$. Então, pela Proposição 4.2.7 segue que o polinômio $f(X) = (X^{81} - X + 11)^{801} + X$ permuta $\mathbb{F}_{9^4}$.

Observe que a condição $k|n$ para polinômios com a forma (4.2) é satisfeita nos quatro casos anteriores. A proposição a seguir nos fornece uma classe de polinômios com a forma (4.2) no qual essa condição não é satisfeita. Mas antes apresentaremos um trinômio com a forma (4.1). Vale observar que a demonstração do resultado a seguir pode ser encontrado em [13].

Lema 4.2.9: Sejam m, k inteiros positivos com $m = 3k$ e $k \not\equiv 1 \pmod 3$. Então,

$$f(X) = X^{3^{2k}+3^k-1} - X^{3^{2k}-3^k+1} + X$$

é um polinômio de permutação sobre $\mathbb{F}_{3^m}$.

Exemplo 4.2.10: Sejam $k = 2 \not\equiv 1 \pmod 3$ e $m = 3k = 6$. Então, o polinômio

$$f(X) = X^{3^4+3^2-1} - X^{3^4-3^2+1} + X = X^{89} - X^{73} + X$$

é de permutação sobre $\mathbb{F}_{3^m}$.

Proposição 4.2.11: Sejam m,k inteiros positivos com $m = 3k$ e $k \not\equiv 1 \pmod 3$. Então,

$$f(X) = (X^{3^{2k}} - X + \delta)^{3^{2k}-3^k+1} + X$$

é um polinômio de permutação sobre $\mathbb{F}_{3^m}$ para qualquer $\delta \in \mathbb{F}_{3^m}$.

Demonstração. Segue da Proposição 4.0.3 que o polinômio $f(X) = (X^{3^{2k}} - X + \delta)^{3^{2k}-3^k+1} + X$ permuta $\mathbb{F}_{3^m}$ se, e somente se,

$$g(X) = X^{3^{2k}(3^{2k}-3^k+1)} - X^{3^{2k}-3^k+1} + X = X^{3^{4k}-3^{3k}+3^{2k}} - X^{3^{2k}-3^k+1} + X$$

permuta $\mathbb{F}_{3^m}$. Mas note que $4k \equiv k \pmod 3, 3k \equiv 0 \pmod 3$, então,

$$g(X) = X^{3^{2k}+3^k-1} - X^{3^{2k}-3^k+1} + X.$$

Pelo Lema 4.2.9 temos que $g(X)$ é um polinômio de permutação sobre $\mathbb{F}_{3^m}$. E segue o resultado. □

A seguir, estudaremos polinômios de permutação com a forma (4.2) sobre corpos finitos de característica par. Começamos com o seguinte lema.

Lema 4.2.12: ([2], [7], [9]) Sejam k um inteiro positivo e $q = 2^k$. Os trinômios $f(X) = X^{qs} + X^s + cX$ são polinômios de permutação sobre $\mathbb{F}_{q^2}$ em cada um dos seguintes casos.

(i) $s = 2q-1$. O inteiro positivo k e $c \in \mathbb{F}_{q^2}$ satisfaz uma das seguintes condições:

  a) k é par e $c = 1$;

  b) k é ímpar e $c^3 = 1$.

(ii) $s = \frac{(3q-2)(q^2+q+1)}{3}$, k é par e $c \in \mathbb{F}_{q^2}$ satisfaz $c^3 = 1$.

(iii) $s = \frac{q+4}{5}$, k é ímpar e $c \in \mathbb{F}_{q^2}$ satizfaz $c^3 = 1$.

(iv) $s = \frac{3q+1}{4}$ e $c \in \mathbb{F}_{q^2}$ satisfaz que $X^3 + X + c = 0$ não tem solução em $\mathbb{F}_q$.

(v) $s = \frac{q+6}{7}$ e $c = 1$.

(vi) $s = \frac{q^2+3q+2}{6}$, k é ímpar e $c \in \mathbb{F}_{q^2}$ satisfaz $c^{\frac{q+1}{3}} = 1$.

(vii) $s = \frac{q^2-2q+4}{3}$, k é par e $c = 1$.

(viii) $s = \frac{Q^3+Q^2-Q+1}{2}$ onde $Q = 2^{\frac{k}{2}}$ para algum k par e, $c \in \mathbb{F}_Q^*$.

(ix) $s = \frac{-1}{2^{k'}-1}(2^k-1)+1$, onde k' é um inteiro positivo com $mdc(2^{k'}-1, 2^k+1) = 1$ e $c \in \mathbb{F}_{2^{k'}}^* \cap \mathbb{F}_q$.

(X) $s = \frac{1}{2^{k'}-1}(2^k-1)+1$, onde k' é um inteiro positivo com $mdc(2^{k'}+1, 2^k+1) = 1$ e $c \in \mathbb{F}_{2^{k'}}^* \cap \mathbb{F}_q$.

O resultado a seguir é consequência imediata da Proposição 4.0.3 e do Lema 4.2.12.

Proposição 4.2.13: Sejam k um inteiro positivo e $q = 2^k$. Sejam $\delta \in \mathbb{F}_{q^2}$ e $\overline{s} = s$ ou qs. Então, $f(X) = (X^q + X + \delta)^{\overline{s}} + cX$ é um polinômio de permutação em cada um dos seguintes casos:

(i) $s = 2q - 1$ e $c = 1$.

(ii) $s = \frac{(3q-2)(q^2+q+1)}{3}$, k é par e $c \in \mathbb{F}_q$ satisfaz $c^3 = 1$.

(iii) $s = \frac{q+4}{5}$, $c = 1$ e k é ímpar.

(iv) $s = \frac{3q+1}{4}$ e $c \in \mathbb{F}_q$ satisfaz que $X^3 + X + c = 0$ não tem solução em $\mathbb{F}_q$.

(v) $s = \frac{q+6}{7}$ e $c = 1$.

(vi) $s = \frac{q^2+3q+2}{6}$ e k é ímpar.

(vii) $s = \frac{q^2-2q+4}{3}$, $c = 1$ e k é par.

(viii) $s = \frac{Q^3+Q^2-Q+1}{2}$ e $Q = 2^{\frac{k}{2}}$ para algum k par e, $c \in \mathbb{F}_Q^*$.

(ix) $s = \frac{-1}{2^{k'}-1}(2^k - 1) + 1$, onde k' é um inteiro positivo com $mdc(2^{k'} - 1, 2^k + 1) = 1$ e $c \in \mathbb{F}_{2^{k'}} \cap \mathbb{F}_q$.

(X) $s = \frac{1}{2^{k'}-1}(2^k - 1) + 1$, onde k' é um inteiro positivo com $mdc(2^{k'} + 1, 2^k + 1) = 1$ e $c \in \mathbb{F}_{2^{k'}} \cap \mathbb{F}_q$.

Na tabela a seguir apresentaremos os polinômios de permutação da forma $(X^{2^k} + X + \delta)^s + cX$ sem restrição a δ sobre $\mathbb{F}_{2^{2k}}$, em que $\omega = \{c \in \mathbb{F}_q; X^3 + X + c = 0 \text{ não tem raízes em } \mathbb{F}_q\}$.

Número	k	$s = i(2^k - 1) + 1$	c	Referências
1	k é par	$i = 2$ ou -1	$c = 1$	[11][12]
2	todo k	$i = 0$ ou 1	$c = 1$	[11][15]
3	todo k	$i = 1/2$	$c = 1$	[11]
4	k é par	$i = 1/3$ ou $2/3$	$c = 1$	[14]
5	k é ímpar	$i = 1/5$ ou 4/5	$c = 1$	[4]
6	um inteiro positivo	$i = 1/4$ ou 3/4	$c \in \omega$	[16][12]
7	k é par	$i = \frac{1}{2^k-2}$ ou $\frac{-4}{2^k-2}$	$c^3 = 1$	Proposição 4.2.13
8	um inteiro positivo	$i = 1/7$ ou 6/7	$c = 1$	Proposição 4.2.13
9	k é ímpar	$i = \frac{2^k+4}{6}$ ou $\frac{2-2^k}{6}$	$c^{\frac{q+1}{3}} = 1$	Proposição 4.2.13
10	k é par	$i = \frac{2^k-1}{3}$ ou $\frac{4-2^k}{3}$	$c = 1$	Proposição 4.2.13
11	k é par	$i = \frac{2^{k/2}+1}{2}$ ou $\frac{1-2^{k/2}}{2}$	$c \in \mathbb{F}_{2^{k/2}}^*$	Proposição 4.2.13
12	$mdc(2^{k'} - 1, 2^k + 1) = 1$	$i = \frac{-1}{2^{k'}-1}$ ou $\frac{2^{k'}}{2^{k'}-1}$	$c \in \mathbb{F}_{2^k}^* \cap \mathbb{F}_{2^{k'}}$	Proposição 4.2.13
13	$mdc(2^{k'} + 1, 2^k + 1) = 1$	$i = \frac{1}{2^{k'}+1}$ ou $\frac{2^{k'}}{2^{k'}+1}$	$c \in \mathbb{F}_{2^k}^* \cap \mathbb{F}_{2^{k'}}$	Proposição 4.2.13

Capítulo 5

Trinômios de permutação sobre corpos finitos de característica par

Os tipos mais simples de polinômios, como já sabemos, são os monômios. Vimos no Teorema 3.2.1 que um monômio X^n permuta $\mathbb{F}_q$ se, e somente se, $mdc(n, q-1) = 1$. Porém, para binômios e trinômios a situação é mais complicada. Somente algumas classes de binômios e trinômios de permutção são conhecidas, no capítulo anterior apresentamos alguns exemplos. Nesse capítulo nosso interesse será nos trinômios de permutação sobre corpos finitos com característica par, onde apresentaremos quatro classes de trinômios de permutação com a forma $X^r h(X^{\frac{q-1}{3}})$, em que $q = 2^{2m}$ e $d = 2^m + 1$. Observamos que este capítulo está baseado nos resultados obtidos por Gupta e Sharma [4].

A seguir, apresentamos um resultado que será importante no decorrer deste capítulo.

Lema 5.0.1: Para $m, n \in \mathbb{N}$, cada um dos polinômios $1+X+X^3$, $1+X^2+X^3$, $1+X+X^4$ e $1+X^3+X^4$ não possuem raízes em μ_{2^m+1}.

Demonstração. Vamos supor inicialmente que existe $\alpha \in \mu_{2^m+1}$ tal que α seja uma raíz de $1+X+X^3$, ou seja,

$$1 + \alpha + \alpha^3 = 0. \tag{5.1}$$

Elevando ambos os lados de (5.1) à potência 2^m e multiplicando por α^3 temos que

$$1 + \alpha^2 + \alpha^3 = 0. \tag{5.2}$$

Somando (5.1) a (5.2) obtemos $\alpha + \alpha^2 = 0$, o que nos dá que $\alpha = 1$. Mas $\alpha = 1$ não satisfaz (5.1), uma contradição. Logo, $1+X+X^3$ não possui raízes em μ_{2^m+1}.

De modo análogo se mostra que os outros três polinômios também não possuem raízes em μ_{2^m+1}. □

Teorema 5.0.2: O polinômio $f_1(X) := X^4 + X^{2^m+3} + X^{3.2^m+1} \in \mathbb{F}_{2^{2m}}[X]$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, $mdc(m, 3) = 1$.

Demonstração. Podemos reescrever o polinômio $f_1(X)$ como sendo $f_1(X) = X^4 h_1(X^{2^m-1})$, com

$h_1(X) := 1+X+X^3 \in \mathbb{F}_{2^{2m}}[X]$. Como $mdc(4, 2^m-1) = 1$, pelo Lema 4.0.2 temos que $f_1(X)$ permuta $\mathbb{F}_{2^{2m}}$ se, e somente se, o polinômio $g_1(X) = X^4 h_1(X)^{2^m-1}$ permuta μ_{2^m+1}.

Vamos assumir que $mdc(m,3) = 1$. Pelo Lema 5.0.1 temos que $h_1(X)$ não possui raízes em μ_{2^m+1}, o que implica que $h_1(\mu_{2^m+1}) \subseteq \mathbb{F}^*_{2^{2m}}$ e, consequentemente, $g_1(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$. Como μ_{2^m+1} é um conjunto finito, $g_1(X)$ permuta μ_{2^m+1} se, e somente se, $g_1(X)$ é injetiva em μ_{2^m+1}. Daí, para $\alpha \in \mu_{2^m+1}$, temos

$$\begin{aligned} g_1(\alpha) &= \alpha^4(1+\alpha+\alpha^3)^{2^m-1} \\ &= \frac{\alpha^4(1+\alpha+\alpha^3)^{2^m}}{1+\alpha+\alpha^3} \\ &= \frac{\alpha^4(1+\alpha^{2^m}+(\alpha^{2^m})^3)}{1+\alpha+\alpha^3} \\ &= \frac{\alpha^4(1+\alpha^{-1}+(\alpha^{-1})^3)}{1+\alpha+\alpha^3} \\ &= \frac{\alpha+\alpha^3+\alpha^4}{1+\alpha+\alpha^3}. \end{aligned}$$

Consequentemente, $g_1(X)$ é injetivo em μ_{2^m+1} se, e somente se,

$$G_1(X) = \frac{X+X^3+X^4}{1+X+X^3}$$

é injetivo em μ_{2^m+1}. Suponha agora que $G_1(X) = G_1(y)$ para alguns $X, y \in \mu_{2^m+1}$. Vamos considerar dois casos.

Caso 1: X ou y é igual a 1. Vamos assumir que $y = 1$, então

$$\frac{X+X^3+X^4}{1+X+X^3} = 1$$

o que nos dá que $X^4+1 = 0$. E então $x = y = 1$;

Caso 2: Nem X nem y é igual a 1. Então, $G_1(X) = G_1(y)$ implica que

$$\frac{X+X^3+X^4}{1+X+X^3} = \frac{y+y^3+y^4}{1+y+y^3}.$$

Somando 1 de ambos os lados temos

$$\begin{aligned} \frac{1+X^4}{1+X+X^3} &= \frac{1+y^4}{1+y+y^3} \\ \Rightarrow \frac{(X+1)^3+X^2}{(X+1)^4} &= \frac{(y+1)^3+y^2}{(y+1)^4} \\ \Rightarrow \frac{1}{1+X} + \left(\frac{X}{1+X}\right)^2\left(\frac{1}{1+X}\right)^2 &= \frac{1}{1+y} + \left(\frac{y}{1+y}\right)^2\left(\frac{1}{1+y}\right)^2 \end{aligned}$$

Substituindo $a = \frac{1}{X+1}$ e $b = \frac{1}{y+1}$ na equação acima, obtemos

$$(a+b)^4 + (a+b)^2 + (a+b) = 0. \tag{5.3}$$

Observe que $a = b$ se, e somente se, $x = y$. Se considerarmos $x \neq y$ então a equação (5.3) implica que

$$(a+b)^3 + (a+b) + 1 = 0,$$

ou seja, $a+b \in \mathbb{F}_{2^{2m}}$ e é uma raíz de $X^3 + X + 1 \in \mathbb{F}_{2^{2m}}[X]$. O que não é possível, pois, $1 + X + X^3$ é irredutível sobre $\mathbb{F}_2$ e $mdc(3, 2m) = 1$ implica que $1 + X + X^3$ é irredutível sobre $\mathbb{F}_{2^{2m}}$.

Suponha agora que $f_1(X)$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$. Seja $\alpha \in \mathbb{F}_{2^3}$ uma raíz de $1 + X + X^3 \in \mathbb{F}_2[X]$ e seja β uma raíz de $X^{2^m} + X + 1 \in \mathbb{F}_{2^{2m}}[X]$ em alguma extensão desse corpo. Note que $\beta^{2^{2m}} = (\beta^{2^m})^{2^m} = (\beta+1)^{2^m} = \beta^{2^m} + 1 = \beta$, ou seja, $\beta \in \mathbb{F}_{2^{2m}}$. Se $mdc(m, 3) = 3$, então $\alpha \in \mathbb{F}_{2^{2m}}$ e

$$\begin{aligned} f_1(\alpha+\beta) &= (\alpha+\beta)^4 + (\alpha+\beta)^{2^m}(\alpha+\beta)^3 + ((\alpha+\beta)^{2^m})^3(\alpha+\beta) \\ &= (\alpha+\beta)^4 + (\alpha+\beta+1)(\alpha+\beta)^3 + (\alpha+\beta+1)^3(\alpha+\beta) \\ &= (\beta^4 + \beta^2 + \beta) + (\alpha^4 + \alpha^2 + \alpha) \\ &= f_1(\beta) \end{aligned}$$

o que contradiz nossa hipótese. □

Exemplo 5.0.3: Seja $m = 5$ e note que $mdc(5, 3) = 1$. Então, pelo Teorema 5.0.2 temos que o polinômio $f(X) = X^4 + X^{2^5+3} + X^{3.2^5+1} = X^4 + X^{35} + X^{97}$ permuta $\mathbb{F}_{2^{10}} = \mathbb{F}_{1024}$.

O resultado a seguir é consequência imediata do Teorema 5.0.2 e foi obtido por K. Li *et al* em [6].

Corolário 5.0.4: O polinômio $f(X) = X + X^{2^m} + X^{2^{2m-1}-2^{m-1}+1} \in \mathbb{F}_{2^{2m}}[X]$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, $mdc(m, 3) = 1$.

Demonstração. O polinômio $f(X)$ pode ser reescrito como $f(X) = Xh(X^{2^m-1})$, onde $h(X) := 1 + X + X^{2^m-1} \in \mathbb{F}_{2^{2m}}[X]$. Pelo Lema 4.0.2 temos que $f(X)$ permuta $\mathbb{F}_{2^{2m}}$ se, e somente se, $g(X) := Xh(X)^{2^m-1}$ permuta μ_{2^m+1}.

Como $mdc(2, 2^m + 1) = 1$, $g(X)$ permuta μ_{2^m+1} se, e somente se, $g(X)^2$ permuta μ_{2^m+1}. Assim, para $X \in \mu_{2^m+1}$ temos

$$\begin{aligned} g(X)^2 &= X^2(1 + X^2 + X^{2^m})^{2^m-1} \\ &= X^2\left(1 + X^2 + \frac{1}{x}\right)^{2^m-1} \\ &= X^4(1 + X + X^3)^{2^m-1} \\ &= g_1(X). \end{aligned}$$

Da prova do Teorema 5.0.2 temos que $g_1(X)$ permuta μ_{2^m+1} se, e somente se, $mdc(m,3)=1$, o que completa a demonstração. □

Exemplo 5.0.5: Seja $m=7$. Como $mdc(7,3)=1$ temos, pelo Corolário 5.0.4, que o polinômio

$$f(X)=X+X^{2^7}+X^{2^{2.7-1}-2^{7-1}+1}=X+X^{128}+X^{8129}$$

é um polinômio de permutação sobre $\mathbb{F}_{2^{14}}$.

Teorema 5.0.6: O polinômio $f_2(X):=X^2+X^{2.2^m}+X^{3.2^m-1}\in\mathbb{F}_{2^{2m}}[X]$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, $mdc(m,3)=1$.

Demonstração. Podemos reescrever o polinômio $f_2(X)$ como $f_2(X)=X^2h_2(X^{2^m-1})$, onde $h_2(X):=1+X^2+X^3\in\mathbb{F}_{2^{2m}}[X]$. Como $mdc(2,2^{m-1})=1$, pelo Lema 4.0.2 temos que $f_2(X)$ permuta $\mathbb{F}_{2^{2m}}$ se, e somente se, o polinômio $g_2(X):=X^2h(X)^{2^m-1}$ permuta μ_{2^m+1}.

Vamos assumir inicialmente que $mdc(m,3)=1$. Pelo Lema 5.0.1 segue que $h_2(X)$ não possui raízes em μ_{2^m+1}, o que implica que $h_2(\mu_{2^m+1})\subseteq\mathbb{F}_{2^{2m}}^*$ e, consequentemente, $g_2(\mu_{2^m+1})\subseteq\mu_{2^m+1}$. Assim, $g_2(X)$ permuta μ_{2^m+1} se, e somente se, $g_2(X)$ é injetivo em μ_{2^m+1}. Seja $\alpha\in\mu_{2^m+1}$. Podemos simplificar $g_2(\alpha)$ como sendo

$$g_2(\alpha)=\frac{1+\alpha+\alpha^3}{\alpha+\alpha^3+\alpha^4}$$

e, então, $g_2(X)$ é injetivo em μ_{2^m+1} se, e somente se,

$$G_2(X):=\frac{1+X+X^3}{X+X^3+X^4}=\frac{1}{G_1(X)}$$

é injetivo em μ_{2^m+1}. Como $mdc(m,3)=1$, da prova do Teorema 5.0.2 segue que $G_1(X)$ e, consequentemente, $G_2(X)$ são injetivos em μ_{2^m+1}.

Agora, se $mdc(m,3)\neq 1$, da prova do Teorema 5.0.2 segue que $f_1(X)$ não é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$. Como $mdc(2,2^m-1)=1$, a condição (i) do Lema 4.0.2 é válida e, então, $g_1(X)$ não permuta μ_{2^m+1}. Consequentemente, $G_1(X)$ e $G_2(X)=\frac{1}{G_1(X)}$ não permutam μ_{2^m+1}, o que implica que $f_2(X)$ não é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$, o que completa essa demonstração. □

Teorema 5.0.7: O polinômio $f_3(X):=X^5+X^{2^m+4}+X^{4.2^m+1}\in\mathbb{F}_{2^{2m}}[X]$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, m é ímpar.

Demonstração. O polinômio $f_3(X)$ pode ser reescrito como $f_3(X)=X^5h_3(X)^{2^m-1}$, com $h_3(X):=1+X+X^4\in\mathbb{F}_{2^{2m}}[X]$. Pelo Lema 4.0.2 temos que $f_3(X)$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, $mdc(5,2^m-1)=1$ e o polinômio $g_3(X):=X^5h_3(X)^{2^m-1}$ permuta μ_{2^m+1}.

Vamos assumir inicialmente que m é ímpar. Então, $mdc(5,2^m-1)=1$. Pelo Lema 5.0.1 temos que $h_3(\alpha)\neq 0$ para todo $\alpha\in\mu_{2^m+1}$, então, $g_3(\mu_{2^m+1})\subseteq\mu_{2^m+1}$. Agora, para $\alpha\in\mu_{2^m+1}$ podemos simplificar $g_3(\alpha)$ como sendo

$$g_3(\alpha)=\frac{\alpha+\alpha^4+\alpha^5}{1+\alpha+\alpha^4}.$$

Segue daí que $g_2(X)$ é injetivo em μ_{2^m+1} se, e somente se,

$$G_3(X) := \frac{X+X^4+X^5}{1+X+X^4} \tag{5.4}$$

é injetivo em μ_{2^m+1}. Suponha que $G_3(X) = G_3(y)$ para algum $x, y \in \mu_{2^m+1}$ com $x \neq y$. Da equação (5.4) segue que

$$\begin{aligned} (X+X^4+X^5)(1+y+y^4)+(y+y^4+y^5)(1+X+X^4) &= 0 \\ \Rightarrow (X^5+y^5)+xy(X^4+y^4)+X^4y^4(X+y)+(X^4+y^4)+(X+y) &= 0. \end{aligned}$$

Usando o fato de que $X^5+y^5 = (X+y)^5+X^2y^2(X+y)+xy(X+y)^3$ e dividindo a equação acima por $(X+y)^5$, obtemos

$$\frac{1}{(X+y)^4}+\left(\frac{xy}{X+y}\right)^4+\frac{1}{X+y}+\frac{xy}{X+y}+\left(\frac{xy}{(X+y)^2}\right)^2+\frac{xy}{(X+y)^2}+1=0.$$

Substituindo $a = \frac{1}{X+y}$ e $b = a^{2^m} = \frac{xy}{X+y}$ na equação acima e simplificando, obtemos

$$(a+b)^4+a+b+a^2b^2+ab+1=0. \tag{5.5}$$

Note que a e b não podem pertencer a $\mathbb{F}_{2^{2m}}$, mas $a+b, ab \in \mathbb{F}_{2^{2m}}$. Aplicando $Tr_1^m(.)$ em ambos os lados da equação (5.5) e usando a linearidade da função traço obtemos

$$Tr_1^m((a+b)^4)+Tr_1^m(a+b)+Tr_1^m((ab)^2)+Tr_1^m(ab)+1=0. \tag{5.6}$$

Como $Tr_1^m((a+b)^4) = Tr_1^m(a+b)$ e $Tr_1^m((ab)^2) = Tr_1^m(ab)$, a equação (5.6) implica que $1=0$, o que é uma contradição.

Agora, se considerarmos m par, então $5|2^{2m}-1$, o que significa que 2^m-1 ou 2^m+1 é divisível por 5. Se $5|2^m-1$, então, pelo Lema 4.0.2 temos que $f_3(X)$ não é um polinômio de permutação. Se $5|2^m+1$, então, para uma raíz quinta primitiva da unidade $\zeta \in \mu_{2^m+1}$ temos que $g_3(\zeta) = (1+\zeta+\zeta^4)^{2^m-1} = g_3(\zeta^4)$ e $g_3(\zeta^2) = (1+\zeta^2+\zeta^3)^{2^m-1} = g_3(\zeta^3)$. Então, $g_3(X)$ não permuta μ_{2^m+1} e, consequentemente, $f_3(X)$ não permuta $\mathbb{F}_{2^{2m}}$, o que completa nossa demonstração. □

Exemplo 5.0.8: Seja $f(X) = X^5+X^{2^3+4}+X^{4.2^3+1} = X^5+X^{12}+X^{33}$. Pelo Teorema 5.0.7 temos que $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_{2^6}$, pois $m=3$ é ímpar.

Teorema 5.0.9: O polinômio $f_4(X) := X^3+X^{3.2^m}+X^{2^{m+2}-1} \in \mathbb{F}_{2^{2m}}[X]$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, m é ímpar.

Demonstração. Vamos reescrever o polinômio $f_4(X)$ como sendo $f_4(X) = X^3h_4(2^m-1)$, com $h_4(X) := 1+X^3+X^4 \in \mathbb{F}_{2^{2m}}[X]$. Pelo Lema 4.0.2 temos que $f_4(X)$ é um polinômio de permutação sobre $\mathbb{F}_{2^{2m}}$ se, e somente se, $mdc(3,2^m-1)=1$ e o polinômio $g_4(X) = X^3h_4(X)^{2^m-1}$ permuta μ_{2^m+1}. Como $mdc(3,2^m-1)=1$ se, e somente se, m é ímpar, precisamos somente mostrar que $g_4(X)$ permuta μ_{2^m+1} se m é ímpar.

Vamos assumir que m é ímpar. Pelo Lema 5.0.1 sabemos que $h_4(X)$ não possui raízes em μ_{2^m+1}. Para $\alpha \in \mu_{2^m+1}$ podemos simplificar $g_4(\alpha)$ como

$$g_4(\alpha) = \frac{1+\alpha+\alpha^4}{\alpha+\alpha^4+\alpha^5}$$

e, então, $g_4(X)$ é injetivo em μ_{2^m+1} se, e somente se,

$$G_4(X) := \frac{1+X+X^4}{X+X^4+X^5} = \frac{1}{G_3(X)}$$

é injetivo em μ_{2^m+1}. Como m é ímpar, da prova do Teorema 5.0.7 segue que $G_3(X)$ e, consequentemente, $G_4(X)$ são injetivos em μ_{2^m+1}, o que conclui nossa demonstração. □

Referências Bibliográficas

[1] AKBARY, A.; GHIOCA, D.; WANG, Q. *On constructing permutations of finite fields*. Finite Fields and Their Applications, v. 17, p. 51-67, 2011. Disponível em:<https://doi.org/10.1016/j.ffa.2010.10.002>. Acesso em: 20/02/2022.

[2] BARTOLI, D.; QUOOS, L. *Permutation polynomials of the type $X^r g(X^s)$ over $\mathbb{F}_{q^{2n}}$*. Designs, Codes and Cryptograph, v. 86, p. 1589-1599, 2018. Disponível em: <https://doi.org/10.1007/s10623-017-0415-8>. Acesso em: 20/02/2022.

[3] DOBBERTIN, H. *Uniformly Representable Permutation Polynomials, Sequence and Their Applications*. Springer, p. 1-22, 2002. Disponível em: <https://doi.org/10.1007/978-1-4471-0673-9_1>. Acesso em: 20/02/2022.

[4] GUPTA, R.; SHARMA, R. K. *Some new classes of permutation trinomials over finite fields with even characteristic*. Finite Fields and Their Applications, v. 41, p. 89-96, 2016. Disponível em: <https://doi.org/10.1016/j.ffa.2016.05.004>. Acesso em: 20/02/2022.

[5] KYUREGHYAN, G.; ZIEVE, M. *Permutation polynomials of the form $X + \gamma T_{r_{F/K}}(X^k)$*. Contemporary Developments in Finite Fields and Applications, p. 178-194, 2016. Disponível em: <https://doi.org/10.1142/9789814719261_0011>. Acesso em: 20/02/2022.

[6] LI, K.; QU, L.; CHEN, X. *New classes of permutation binomials and permutation trinomials over Finite Fields*. Finite Fields and Their Applications, v. 43, p. 69-85, 2017. Disponível em: <https://doi.org/10.1016/j.ffa.2016.09.002>. Acesso em: 20/02/2022.

[7] LI, K.; QU, L.; CHEN, X.; LI, C. *Permutation polynomials of the form $cX + T_{r_{F/K}}(X^a)$ and permutation trinomials over finite fields with even characteristic*. Cryptography and Communications, v. 10, p. 531-554, 2018. Disponível em: <https://dl.acm.org/doi/abs/10.5555/3190794.3190828>. Acesso em: 21/02/2022.

[8] LI, L.; WANG, S.; ZENG, X. *Permutation polynomials $(X^{p^m} - X + \delta)^{s_1} + (X^{p^m} - X + \delta)^{s_2} + X$ over $\mathbb{F}_{p^n}$*. Finite Fields and Their Applications, v. 51, p. 31-61, 2018. Disponível em: <https://doi.org/10.1016/j.ffa.2018.01.003>. Acesso em: 21/02/2022.

[9] LI, N.; HELLESETH, T. *New permutation trinomials from Niho expoents over finite fields with even characteristic*. Cryptography and Communications, v. 11, p. 129-136, 2019. Disponível em: <https://link.springer.com/article/10.1007/s12095-018-0321-6>. Acesso em: 21/02/2022.

[10] LIDL, R.; NIEDERREITER, H. *Finite Fields*. Cambridge University Press, 1997. Disponível em: <https://doi.org/10.1017/CBO9780511525926>. Acesso em: 21/02/2022.

[11] TU, Z.; ZENG, X.; JIANG, X. *Two classes of permutation polynomials having the form* $(X^{2^m}+X+\delta)^s+X$. Finite Fields and Their Applications, v. 31, p. 12-24, 2015. Disponível em: <https://doi.org/10.1016/j.ffa.2014.09.005>. Acesso em: 21/02/2022.

[12] WANG, L.; WU, B.; LIU, Z. *Further results on permutation polynomials of the form* $(X^p-X+\delta)^s+X$ *over* $\mathbb{F}_{p^{2m}}$. Journal of Algebra and Its Applications, v. 15, p. 92-112, 2016. Disponível em: <https://doi.org/10.1142/S0219498816500985>. Acesso em: 21/02/2022.

[13] WANG, Y.; ZHA, Z.; ZHANG, W. *Six new classes of permutation trinomials over* $\mathbb{F}_{3^{3k}}$. Applicable Algebra in Engineering, Communication and Computing, v. 29, p. 479-499, 2018. Disponível em: <https://doi.org/10.1007/s00200-018-0353-3>. Acesso em: 21/02/2022.

[14] XU, G.; CAO, X.: XU, S. *Further results on permutation polynomials of the form* $(X^{p^m}-X+\delta)^s+L(X)$ *over* $\mathbb{F}_{p^{2m}}$. Journal of Algebra and Its Applications, v. 15, p. 1650098 (13 páginas), 2016. Disponível em: <http://dx.doi.org/10.1142/S0219498816500985>. Acesso em: 21/02/2022.

[15] YUAN, P.; DING, C. *Permutation polynomials over finite fields from a powerful lemma*. Finite Fields and Their Applications, v.17, p. 560-574, 2011. Disponível em: <http://dx.doi.org/10.1016/j.ffa.2011.04.001>. Acesso em: 21/02/2022.

[16] ZHA, Z.; HU, L. *Some classes of permutation polynomials of the form* $(X^{p^m}-X+\delta)^s+X$ *over* $\mathbb{F}_{p^{2m}}$. Finite Fields and Their Applications, v. 40, p. 150-162, 2016. Disponível em: <http://dx.doi.org/10.1016/j.ffa.2016.04.003>. Acesso em: 21/02/2022.

[17] ZENG, X.; ZHU, X.; LI, N.; LIU, X. *Permutation polynomials over* $\mathbb{F}_{2^n}$ *of the form* $(X^{2^i}+X+\delta)^{s_1}+(X^{2^i}+X+\delta)^{s_2}+X$. Finite Fields and Their Applications, v. 47, p. 256-268, 2017. Disponível em: <https://doi.org/10.1016/j.ffa.2017.06.012>. Acesso em: 21/02/2022.

[18] ZHENG, D.; YUAN, M.; YU, L. *Two types of permutation polynomials with special forms*. Finite Fields and Their Applications, v. 56, p. 1-16, 2019. Disponível em: <https://doi.org/10.1016/j.ffa.2018.10.008>. Acesso em: 21/02/2022.

Apêndice A

Resultado	Polinômio de permutação	Condições necessárias
Corolário 3.1.8	Não existe $p(X)$ com $\deg(p(X)) = d$ que permuta $\mathbb{F}_q$	$d > 1$ e $d \mid q-1$
Teorema 3.2.1	$aX + b$ permuta $\mathbb{F}_q$	$a \neq 0$
Teorema 3.2.1	X^n permuta $\mathbb{F}_q$	$mdc(n, q-1) = 1$
Teorema 3.2.2	$L(X) = \sum_{i=0}^{m} a_i X^{p^i}$ permuta $\mathbb{F}_q$	$char(\mathbb{F}_q) = p$ e $L(X) = 0$ somente se $x = 0$
Teorema 3.2.4	$f(X) = X^r(g(X^s))^{\frac{q-1}{s}}$ permuta $\mathbb{F}_q$	$r, s \in \mathbb{N}$, $s \mid q-1$, $mdc(r, q-1) = 1$ e $g \in \mathbb{F}_q[X]$ é tal $g(X^s) = 0$ somente se $x = 0$
Teorema 3.2.6	$X^{\frac{q+1}{2}} + ax$ permuta $\mathbb{F}_q$	q ímpar e $\eta(a^2 - 1) = 1$
Teorema 3.2.7	$X^{\frac{q+1}{2}} + ax$ não permuta nenhuma extensão $\mathbb{F}_{q^r}$ de $\mathbb{F}_q$	$r > 1, a \in \mathbb{F}_q^*$ e q ímpar
Teorema 3.2.10	$f(X) = aX^{p^h} + b$ permuta todas as extensões finitas de $\mathbb{F}_q$	$a \neq 0$, $char(\mathbb{F}_q) = p$ e $h \in \mathbb{Z}_+$
Teorema **??**	$g_k(x, a)$ permuta $\mathbb{F}_q$	$a \in \mathbb{F}_q^*$ e $mdc(k, q^2 - 1) = 1$
Lema 4.0.2	$f(X) = X^r h(X^{\frac{q-1}{d}})$ permuta $\mathbb{F}_q$	$d, r \in \mathbb{Z}$, $d \mid q-1, h(X) \in \mathbb{F}_q[X]$, $mdc(r, (q-1)/d) = 1$ e $X^r h(X)^{\frac{q-1}{d}}$ permuta μ_d
Proposição 4.0.3	$f(X) = g(X^{q^k} - X + \delta) + cX$ permuta $\mathbb{F}_{q^m}$	$m, k \in \mathbb{Z}$, $0 < k < m, mdc(k, m) = l, c \in \mathbb{F}_{q^l}^*, \delta \in \mathbb{F}_{q^m}$, $g(X) \in \mathbb{F}_{q^m}$ e $h(X) = g(X)^{q^k} - g(X) + cX$ permuta $\mathbb{F}_{q^m}$
Corolário 4.0.4	$f(X) = \sum_{i=1}^{l} (X^{2^k} + X + \delta)^{s_i} + x$ permuta $\mathbb{F}_{2^m}$	$k, m, l \in \mathbb{N}$, $\frac{m}{mdc(m,kl)}$ ímpar, $s_i = \frac{2^{k(i-1)}}{2^{kl}+1}$, $1 \leq i \leq l$ e $\delta \in \mathbb{F}_{2^m}$

Corolário 4.0.6	$f(X) = (X^{2^m} + X + \delta)^s + x$ permuta $\mathbb{F}_{2^{3m}}$	m inteiro positivo, $\delta \in \mathbb{F}_{2^{3m}}$, $s = 2^{2m} + 1$ ou $s = 2^{im-1} + 2^{m-1}$ com $mdc((i-1)m - 1, 3m) = 1, i = 2, 3$
Corolário 4.0.8	$f(X) = X^{2^m s} + X^s + x$ permuta $\mathbb{F}_{2^{3m}}$	$m, e \in \mathbb{N}$, $s = 2^{2e-1} + 2^{m-1}$ com $mdc(e-1, 3e) = 1$ ou $s = 2^{3e-1} + 2^{m-1}$ com $mdc(2e-1, 3e) = 1$
Teorema 4.1.1	$f(X) = cX - X^s + X^{qs}$ permuta $\mathbb{F}_{q^2}$	$s = \frac{3q^2+2q-1}{4}$, $c \in \mathbb{F}_{q^2}^*$, $q \equiv 1 \pmod 8$ e $(-2/c)^{\frac{q+1}{2}}$ ou $q \equiv 5 \pmod 8$ e $(2/c)^{\frac{q+1}{2}} = 1$
Teorema 4.1.3	$f(X) = cX - X^s + X^{qs}$	$s = \frac{(q+1)^2}{4}$, $c \in \mathbb{F}_{q^2}^*$, $q \equiv 5 \pmod 8$ e $(-2/c)^{\frac{q+1}{2}} = 1$ ou $q \equiv 1 \pmod 8$ e $(2/c)^{\frac{q+1}{2}} = 1$
Teorema 4.1.4	$f(X) = X - X^s + X^{qs}$ permuta $\mathbb{F}_{q^2}$	q potência de um primo, $q \equiv 1 \pmod 3$ e $s = \frac{q^2+q+1}{3}$
Teorema 4.1.9	$f(X) = X - X^s + X^{q^2 s}$ permuta $\mathbb{F}_{q^2}$	q potência de um primo ímpar, $s = q^3 + q^2 - q$
Proposição 4.2.1	$f(X) = (X^q - X + \delta)^{\frac{3q^2+2q-1}{4}} + cX$ permuta $\mathbb{F}_{q^2}$	$\delta \in \mathbb{F}_{q^2}$, $c \in \mathbb{F}_q^*$, $q \equiv 1 \pmod 8$ e $c = -2$ ou $q \equiv 5 \pmod 8$ e $c = 2$
Proposição 4.2.3	$f(X) = (X^q - X + \delta)^{\frac{(q+1)^2}{4}} + cX$ permuta $\mathbb{F}_{q^2}$	$\delta \in \mathbb{F}_{q^2}$, $c \in \mathbb{F}_q^*$, $q \equiv 1 \pmod 8$ e $c = 2$ ou $q \equiv 5 \pmod 8$ e $c = -2$
Proposição 4.2.5	$f(X) = (X^q - X + \delta)^{\frac{q^2+q+1}{3}} + x$ permuta $\mathbb{F}_{q^2}$	q potência de um primo ímpar, $q \equiv 1 \pmod 3$ e $\delta \in \mathbb{F}_{q^2}$
Proposição 4.2.7	$f(X) = (X^{q^2} - X + \delta)^{q^3+q^2-q} + x$ permuta $\mathbb{F}_{q^4}$	q potência de primo ímpar, $\delta \in \mathbb{F}_{q^4}$
Lema 4.2.9	$f(X) = X^{3^{2k}+3^k-1} - X^{3^{2k}-3^k+1} + X$ permuta $\mathbb{F}_{3^m}$	$m, k \in \mathbb{Z}$, $m = 3k$, $k \not\equiv 1 \pmod 3$
Proposição 4.2.11	$f(X) = (X^{3^{2k}} - X + \delta)^{3^{2k}-3^k+1} + X$ permuta $\mathbb{F}_{3^m}$	$m, k \in \mathbb{Z}_+$, $m = 3k$, $k \not\equiv 1 \pmod 3$, qualquer $\delta \in \mathbb{F}_{3^m}$

Teorema 5.0.2	$f_1(X) = X^4 + X^{2^m+3} + X^{3.2^m+1}$ permuta $\mathbb{F}_{2^{2m}}$	$mdc(m,3) = 1$
Corolário 5.0.4	$f(X) = X + X^{2^m} + X^{2^{2m-1}-2^{m-1}+1}$ permuta $\mathbb{F}_{2^{2m}}$	$mdc(m,3) = 1$
Teorema 5.0.6	$f_2(X) = X^2 + X^{2.2^m} + X^{3.2^m-1}$ permuta $\mathbb{F}_{2^{2m}}$	$mdc(m,3) = 1$
Teorema 5.0.7	$f_3(X) = X^5 + X^{2^m+4} + X^{4.2^m+1}$ permuta $\mathbb{F}_{2^{2m}}$	m ímpar
Teorema 5.0.9	$f_4(X) = X^3 + X^{3.2^m} + X^{2^{m+2}-1}$ permuta $\mathbb{F}_{2^{2m}}$	m ímpar