Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática

Ednailton Santos Silva

Polinômios de Permutação sobre Corpos Finitos

Juiz de Fora
2018

Ednailton Santos Silva

Polinômios de Permutação sobre Corpos Finitos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Coorientador: Frederico Sercio Feitosa

Juiz de Fora

2018

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Silva, Ednailton Santos.
Polinômios de Permutação sobre Corpos Finitos / Ednailton Santos Silva. – 2018.
60 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Coorientador: Frederico Sercio Feitosa
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2018.

1. Corpos Finitos. 2. Polinômios sobre Corpos Finitos. 3. Polinômios de Permutação. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Feitosa, Frederico Sercio, coorient. III. Título.

Ednailton Santos Silva

Polinômios de Permutação sobre Corpos Finitos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr[a]. Beatriz Casulari da Motta Ribeiro
Orientadora
Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa - Coorientador
Universidade Federal de Juiz de Fora

Prof. Dr. Rafael Peixoto
Universidade Federal do Triângulo Mineiro

Prof. Dr[a]. Joana Darc Antonia Santos da Cruz
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

À minha mãe Ednalva Alves e irmã Taylane Santos, pelo amor e apoio incondicional para que eu pudesse concluir mais uma etapa da minha vida e à minha sobrinha Lohanny Santos pela forma mais pura e genuína, que uma criança tem, de demostrar seu afeto por mim.

À toda minha família, por toda força e apoio.

Ao Armando Júnior, por sempre estar presente, pelo companheirismo, carinho e amor, pelos momentos felizes e tristes, por tudo que vivemos até aqui.

Aos bons e velhos amigos que, mesmo longe, fizeram-se presentes durante toda esta jornada, em especial Juliana, Luana e Marcelo. E aos novos amigos que fiz em Juiz de Fora.

Aos colegas e amigos do Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora pelas experiências trocadas e por todos os momentos de descontração.

À professora Beatriz Casuali Motta Ribeiro e ao professor Frederico Sercio Feitosa, pela orientação, ensinamentos, paciência e confiança.

Aos membros da banca, por aceitar avaliar e contribuir com este trabalho.

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

Enfim, à todos que de alguma forma contribuíram para que eu chegasse até aqui.

RESUMO

O objetivo desse trabalho é apresentar algumas classes clássicas e outras mais recentes de polinômios de permutação sobre corpos finitos. A fim de atingir esse objetivo, apresentamos a construção e uma lista de propriedades de corpos finitos, bem como uma introdução à teoria dos polinômios sobre corpos finitos.

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

ABSTRACT

The main goal of this text is to present some known classes of permutation polynomials over finite fields. With this goal, we begin by presenting the construction and some properties of finite fields, as well as an introduction to the theory of polynomials over finite fields.

Key-words: Finite Fields. Polynomials over Finite Fields. Permutation Polynomials.

SUMÁRIO

1 INTRODUÇÃO

Um polinômio $f \in \mathbb{F}_q[x]$ é dito um polinômio de permutação sobre o corpo finito $\mathbb{F}_q$ se a função polinomial associada $f : \mathbb{F}_q \to \mathbb{F}_q$ dada por $c \mapsto f(c)$ é uma permutação de $\mathbb{F}_q$, ou seja, se f permuta os elementos de $\mathbb{F}_q$. Tal conceito apareceu pela primeira vez ainda no século XIX, em [1], como uma forma de representar permutações, mas o interesse pelo assunto tem sido particularmente maior desde a década de 1980, especialmente pela grande quantidade de aplicações na criptologia e na teoria de códigos.

Em termos gerais, dadas uma mensagem $M \in \mathbb{F}_q$ e um polinômio de permutação $P(x) \in \mathbb{F}_q[x]$, podemos codificá-la fazendo $N = P(M)$. Como $P(x)$ é uma bijeção, podemos recuperar M. Obviamente, para que esse sistema seja seguro e eficiente, é importante que o polinômio apresentado tenha propriedades extras.

Outras questões interessantes foram levantadas por Lidl e Mullen em [7] e [8] e ainda estão completamente ou parcialmente abertas. Por exemplo, um problema imediato seria como determinar se um dado polinômio $f(x) \in \mathbb{F}_q[x]$ é ou não de permutação de forma simples, ou seja, sem precisar verificar se os q valores de $f(a)$, onde $a \in \mathbb{F}_q$ são de fato distintos.

Essa, então, é a questão central do estudo dos polinômos de permutação sobre corpos finitos: embora existam diversos critérios conhecidos para detectá-los, os mesmos não são suficientes para classificar completamente todos os polinômios com essa propriedade. O objetivo principal desse trabalho é fazer um *survey* de famílias clássicas e outras mais recentes de tais polinômios.

A fim de atingir esse objetivo, começamos, no Capítulo 2, relembrando conceitos sobre extensões de corpos e corpos de decomposição, que são essenciais para a construção dos corpos finitos, tema do Capítulo 3. Nesse capítulo, apresentamos ainda a função traço e os caracteres quadráticos que serão utilizados para construção de polinômios de permutação mais adiante.

No Capítulo 4, apresentamos um breve estudo dos polinômios irredutíveis sobre corpos finitos, a fim de tomar familiaridade com os polinômios sobre corpos finitos.

Finalmente, no Capítulo 5, estudamos polinômios de permutação sobre corpos finitos. Começamos com as definições equivalentes e critérios já conhecidos para determinar quando certos polinômios são de permutação. Em seguida, apresentamos algumas classes elementares de polinômios de permutação, como nossos exemplos iniciais, apresentando, inclusive, aplicações de uma dessas classes na criptografia. Encerramos com algumas classes mais recentes, seguindo especialmente os artigos [10], [13] e [14].

2 CONCEITOS BÁSICOS

Neste capítulo apresentamos alguns conceitos e resultados sobre extensões de corpos e corpo de decomposição que nos serão úteis na construção dos corpos finitos que será feita no Capítulo 3. Ao longo desse capítulo K, F e L são corpos. Além disso, $K[x]$ denotará o anel de polinômios na variável x e coeficientes em K. Utilizamos [9] como referência principal.

2.1 EXTENSÕES DE CORPOS

Sejam F um corpo e $K \subset F$ tal que K é um corpo com as operações de F. Dizemos que K é um subcorpo de F. Se $K \neq F$, então K é dito subcorpo próprio de F. Nesse contexto, F é chamado uma extensão (de corpos) de K.

Definição 2.1. *Um corpo que não contém subcorpos próprios é chamado corpo primo.*

Se F é uma extensão de K, então F pode ser visto como um espaço vetorial sobre K. Os elementos (vetores) de F formam um grupo abeliano com a operação de adição e, além disso, cada vetor em F pode ser multiplicado por um escalar $r \in K$ e as leis de multiplicação por escalar são satisfeitas:

$$r(\alpha + \beta) = r\alpha + r\beta,\ (r+s)\alpha = r\alpha + s\alpha,\ (rs)\alpha = r(s\alpha),\ 1\alpha = \alpha$$

onde $r, s \in K$ e $\alpha, \beta \in F$

Definição 2.2. *A dimensão de F como espaço vetorial sobre K é chamada grau da extensão e é denotada por $[F : K]$. F é dito uma extensão finita de K se $[F : K] < \infty$. Caso contrário, dizemos que F é uma extensão infinita.*

Teorema 2.3. *Sejam K um corpo, F uma extensão finita de K e L uma extensão finita de F. Então L é uma extensão finita de K e*

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

Demonstração. Sejam $[L : F] = m$ e $[F : K] = n$. Sejam $\{\alpha_1, ..., \alpha_m\}$ e $\{\beta_1, ..., \beta_n\}$ bases de L sobre F e de F sobre K, respectivamente. Então, cada elemento de $\alpha \in L$ se escreve como $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$ com $a_i \in F$, para todo $i = 1, ..., m$. Além disso, cada $a_i \in F$ pode ser escrito como $a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$, onde $b_{ij} \in K$, para todos $i = 1, ..., m$ $j = 1, ..., n$. Assim, obtemos a seguinte expressão

$$\alpha = \sum_{i=1}^{m} a_i\alpha_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_{ij}\beta_j \right) \alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij}\beta_j\alpha.$$

Assim, basta mostrar que os elementos $\beta_j\alpha_i$, com $1 \leq j \leq n, 1 \leq i \leq m$, são linearmente independentes sobre K. Suponhamos que

$$\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\beta_j\alpha_1 = 0.$$

Então,

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha = 0.$$

Pela independência linear dos elementos α_i sobre F, temos que

$$\sum_{j=1}^{n} b_{ij}\beta_j = 0, \forall\ i \in \{1, ..., m\}$$

E pela independência linear dos elementos β_j sobre K, temos que $b_{ij} = 0$, para todo $i = 1, ...m$ e para todo $j = 1, ...n$. Logo, $\{\alpha_i\beta_j \mid i \in \{1, ..., m\}, j \in \{1, ..., n\}\}$ é uma base de L sobre F com mn elementos, isto é, $[L : K] = mn = [L : K][K : F]$. □

Definição 2.4. *Sejam K um subcorpo de F e M um subconjunto de F. Então, o corpo $K(M)$ é definido pela interseção de todos subcorpos de F que contém K e M e é chamado de extensão de corpo obtido de K adjuntando M.*

(i) Se M for finito, digamos $M = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, escrevemos $K(M) = K(\alpha_1, \alpha_2, ..., \alpha_n)$

(ii) Se M consiste de um único elemento $\alpha \in F$, então $L = K(\alpha)$ é dita uma extensão simples de K e α é chamado elemento definidor de L sobre K.

Definição 2.5. *Sejam K um subcorpo de F e $\alpha \in F$. Se α for raiz de algum polinômio não nulo $p(x) \in F[x]$ dizemos que α é algébrico sobre K. Caso contrário, α é dito transcedente sobre K.*

Exemplo 2.6. *O elemento $\sqrt[3]{4} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$ pois é uma raiz do polinômio $x^3 - 4 \in \mathbb{Q}[x]$. Já $\pi \in \mathbb{R}$ não é algébrico sobre $\mathbb{Q}$ e, portanto, é transcedente.*

Definição 2.7. *Dizemos que o corpo F é uma extensão algébrica de K se todo elemento de F for algébrico sobre K. Se pelo menos um elemento de F for transcedente sobre K a extensão é dita transcendental (ou transcedente).*

Definição 2.8. *Seja $\alpha \in F$ um elemento algébrico sobre K, então existe um único polinômio mônico irredutível $m(x) \in K[x]$, tal que $m(\alpha) = 0$. Tal polinômio é chamado polinômio minimal de α e denotado por $irr(\alpha, K)$.*

Se existe $q(x) \in K[x]$ de modo que $q(\alpha) = 0$, então $irr(\alpha, K)$ divide $q(x)$.

Teorema 2.9. *Toda extensão finita de K é algébrica sobre K.*

Demonstração. Seja L uma extensão finita de K, com $[L : K] = m$. Dado $\alpha \in L$, os $m+1$ elementos $1, \alpha, ..., \alpha^m$ são linearmente dependentes sobre K. Assim, é possível obtermos uma combinação linear $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0$, com $a_i \in K$, para todo $i = 1, ...m$, e com $a_i \neq 0$ para algum $i \in \{1, ..., m\}$. Então, se $p(x) = a_m x^m + \cdots + a_1 x + a_0$, temos que $p(\alpha) = 0$, isto é, α é algébrico sobre K. □

2.2 CORPO DE DECOMPOSIÇÃO

Teorema 2.10. *Um elemento $a \in K$ é uma raiz de um polinômio $f \in K[x]$ se e somente se $x - a$ divide f.*

Demonstração. Pelo algoritmo da divisão, podemos escrever

$$f = q(x - a) + c$$

onde $q \in K[x]$ e $c \in K$. Substituindo $x = a$, temos $f(a) = c$. Logo,

$$f = q(x - a) + f(a).$$

Se a é uma raiz de f, então $f(a) = 0$ e, portanto, $x - a$ divide f. Reciprocamente, se $x - a$ divide f,

$$f = h(x - a),$$

então $f(a) = h(a)(a - a) = 0$ e, portanto, a é uma raiz de $f(x)$. □

Teorema 2.11. *Seja $f \in K[x]$ um polinômio de grau n. O número máximo de raízes de f em K é n.*

Demonstração. Suponhamos que K contenha $n + 1$ raízes distintas $a_1, ..., a_{n+1}$ de f. Pelo Teorema 2.10, podemos escrever

$$f = (x - a_1) \cdots (x - a_{n+1})g,$$

para algum polinômio $g \in K[x]$, não nulo, contradizendo $\deg(f) = n$. □

Definição 2.12. *Seja $a \in F$ uma raiz do polinômio $f \in F[x]$. Se k é um inteiro positivo tal que $f(x)$ é divisível por $(x - a)^k$, mas não por $(x - a)^{k+1}$, então k é chamado de multiplicidade de a. Se $k = 1$, então a é chamado de raiz simples de f e se $k \succ 2$, então a é cahmado de raiz múltipla de f.*

Definição 2.13. *Se $f(x) = a_0 + a_1x_1 + \cdots + a_nx^n \in F[x]$ então a derivada f' de f é definida por $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$.*

Teorema 2.14. *Um elemento $a \in F$ é uma raiz múltipla de $f \in F[x]$ se e somente se é uma raiz de f e f'.*

Demonstração. Suponhamos que $a \in F$ seja uma raiz de f de multiplicidade $m \geq 2$, ou seja, $f(x) = (x-a)^m g(x)$, onde $g(x) \in F[x]$ e $g(a) \neq 0$. Então,

$$f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m g'(x), \text{ com } m-1 \geq 1,$$

e, portanto, $f'(a) = 0$, logo a é raiz de f'. Reciprocamente, suponhamos que $a \in F$ seja raiz de f e de f'. Então, $f(x) = (x-a)q(x)$, onde $q(x) \in F[x]$ e, assim,

$$f'(x) = q(x) + (x-a)q'(x) \Rightarrow f'(a) = q(a) + (a-a)q'(a) \Rightarrow q(a) = 0.$$

Logo, a é raiz de $q(x)$ e portanto, $x-a$ divide $q(x)$ e, então, $q(x) = (x-a)h(x)$, com $h(x) \in F[x]$. Assim,

$$f(x) = (x-a)^2 h(x).$$

Portanto, a é raiz múltipla de f. □

Definição 2.15. *Sejam K um corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ se fatora em $K[x]$ se $f(x)$ pode ser escrito como o produto de fatores lineares*

$$f(x) = c(x-\alpha_1)...(x-\alpha_n)$$

com $c, \alpha_1, ..., \alpha_n \in K$.

Nesse caso, temos que os zeros de $f(x)$ em K são os elementos $\alpha_1, ..., \alpha_n$.

Além disso, se F é uma extensão de K, então $f(x) \in F[x]$ e, portanto, faz sentido falarmos na fatoração de $f(x)$ em F, assim, f pode ser visto como um produto de fatores lineares em $F[x]$.

Definição 2.16. *Seja K um corpo e F uma extensão de K. Então F é um corpo de decomposição para um polinômio $f(x) \in K[x]$ se*

(i) $f(x)$ se fatora em $F[x]$;

(ii) Se existe um corpo F' tal que $K \subset F' \subset F$ e $f(x)$ se fatora em $F'[x]$, então $F = F'$, ou seja, F é o menor corpo que contém K e todas as raízes de $f(x)$.

Teorema 2.17. *Sejam K um corpo e $f(x) \in K[x]$ um polinômio irredutível. Então, existem um corpo F e $\alpha \in F$ tais que $K \subset F$ e $f(\alpha) = 0$.*

Demonstração. Consideremos o anel $F = \dfrac{K[x]}{\langle f \rangle}$, que é um corpo, pois f é irredutível. Os elementos de F são as classes $h(x) + \langle f \rangle$, com $h(x) \in K[x]$. Para todo $a \in K \subset K[x]$ podemos construir as classes $\overline{a}$ determinada pelo polinômio constante a e se $a, b \in K$ são distintos, então $\overline{a} \neq \overline{b}$, pois f possui grau positivo por não ser invertível. A aplicação $a \longmapsto \overline{a}$ fornece um isomorfismo de K sobre um subcorpo K' de F, portanto, F pode ser

visto como uma extensão de K. Para todo $h(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$, usando as regras de operações com classes residuais e da identificação $\overline{a_i} = a_i$, temos que

$$\begin{aligned}\overline{h(x)} &= \overline{a_0 + a_1x + \cdots + a_mx^m} \\ &= \overline{a_0} + \overline{a_1x} + \cdots + \overline{a_mx^m} \\ &= a_0 + a_1\overline{x} + \cdots + a_m\overline{x}^m.\end{aligned}$$

Portanto, todo elemento de F pode ser escrito como um polinômio em $\overline{x}$ com coeficientes em K. Como todo corpo que contém K e $\overline{x}$ deve conter os elementos da forma $h(\overline{x})$, onde $h(x) \in K[x]$, temos que F é uma extensão de K obtida por adjunção de $\overline{x}$. Se $f = b_0 + b_1x + \cdots + b_nx^n$, então,

$$f(\overline{x}) = b_0 + b_1\overline{x} + \cdots + b_n\overline{n}^n = \overline{f(x)} = 0.$$

Portanto, $\overline{x}$ é uma raiz de f em F. □

Teorema 2.18. *Se $f(x) \in K[x]$, então existe uma extensão F de K que é um corpo de decomposição para $f(x)$.*

Demonstração. Vamos mostrar que existe uma extensão L de K sobre a qual $f(x)$ se decompõe completamente em fatores lineares. Faremos a prova por indução sobre o grau n de $f(x)$.

Se $n = 1$, então $L = K$.

Suponhamos que $n > 1$. Se os fatores irredutíveis de $f(x)$ forem de grau 1, então K é um corpo de decomposição para $f(x)$ e $L = K$. Caso contrário, pelo menos um dos fatores irredutíveis, suponha $p(x)$, tem grau ≥ 2. Pelo Teorema 2.17, existe uma extensão L_1 de K contendo uma raiz α de $p(x)$. Logo, sobre L_1, o polinômio $f(x)$ possui o fator linear $x - \alpha$. O grau do fator restante $f_1(x)$ é $n - 1$. Então, por indução, existe uma extensão L de L_1 contendo todas as raízes de $f_1(x)$. Como $\alpha \in L$, L é uma extensão de K contendo todas as raízes de $f(x)$.

Finalmente, tome F a interseção de todos os subcorpos de L contendo K quem também contém todas as raízes de $f(x)$. Então F é um corpo de decomposição de $f(x)$. □

Exemplo 2.19. *O corpo de decomposição de $f(x) = x^2 - 2$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt{2})$ pois as duas raízes de $f(x)$, que são $\pm\sqrt{2}$, pertencem à $\in \mathbb{Q}(\sqrt{2})$.*

Exemplo 2.20. *O corpo de decomposição de $g(x) = (x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$ é o corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ gerado sobre $\mathbb{Q}$ por $\sqrt{2}$ e $\sqrt{3}$, uma vez que as raízes de g são $\pm\sqrt{2}$ e $\pm\sqrt{3}$.*

Exemplo 2.21. *Sejam p um número primo e $f(x) = x^p - 1 \in \mathbb{Q}[x]$. Temos que o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\xi)$, onde $\xi = e^{2\pi i/p}$. Ainda, o polinômio minimal de ξ é $x^{p-1} + x^{p-2} + \cdots + x + 1$, donde a extensão $\mathbb{Q} \subset \mathbb{Q}(\xi)$ tem grau $p - 1$.*

3 CORPOS FINITOS

Nesse capítulo, estudamos corpos finitos, começando com resultados que nos levarão a prova da existência e unicidade de corpos finitos de cardinalidade q para todo q potência de um número primo. Em seguida, estudamos raízes de polinômios irredutíveis, raízes da unidade e polinômios ciclotômicos, relacionando os corpos ciclotômicos com os corpos finitos. Por fim, introduzimos duas importantes funções: traços e normas; além dos caracteres, funções que serão utilizadas em um dos critérios para polinômios de permutação apresentados no capítulo final. Novamente, utilizamos [9] como referência principal.

3.1 DEFINIÇÕES E PROPRIEDADES

Começamos o capítulo com a noção de característica de um anel com unidade, passando pela característica de um domínio de integridade a fim de estudar o corpo primo de um corpo de característica não nula.

Definição 3.1. *Um anel R tem característica p se p é o menor inteiro positivo tal que para todo elemento não nulo $\alpha \in R$, temos que $p\alpha = 0$. Se não existe tal inteiro, então R tem característica zero.*

Teorema 3.2. *A característica de um domínio de integridade é um número primo ou zero.*

Demonstração. Seja D um domínio de integridade e suponhamos que sua característica seja $n \neq 0$. Se n não é primo, então $n = ab$, onde $1 < a < n$ e $1 < b < n$. Assim, $0 = n1 = (ab)1 = (a1)(b1)$. Como não há divisores de zero em D, então $a1 = 0$ ou $b1 = 0$. Segue que, ou $ar = (a1)r = 0$ para todo $r \in D$ ou $br = (b1)r = 0$ para todo $r \in D$, o que contradiz a definição da característica n. □

Teorema 3.3. *Se K é um corpo finito, então a característica de K é p, onde p é primo.*

Demonstração. Pelo Teorema 3.2, basta mostrar que todo corpo finito possui característica positiva. Assim, consideremos K um corpo finito e sejam $1, 2\cdot1, 3\cdot1, ...$ os múltiplos inteiros da unidade de K. Como K possui somente um número finito de elementos distintos, temos que existem inteiros $m, n \in \mathbb{Z}$ tais que $1 < m < n$ e $m1 = n1$, ou seja, $n1 - m1 = 0$. Então, $(n - m)1 = 0$ e, assim, K possui característica positiva. □

Para um primo p, seja $\mathbb{F}_p = \{0, 1, ..., p-1\}$. Consideremos a aplicação $\varphi : \mathbb{Z}_p \longrightarrow \mathbb{F}_p$ definida por $\varphi(\overline{a}) = a$, para $a = 0, 1, ..., p - 1$. Notemos que, se $\overline{a} = \overline{b} \in \mathbb{Z}_p$, existe $k \in \mathbb{Z}$ tal que $a - b = pk$. Assim,

$$\varphi(\overline{a - b}) = \varphi(\overline{pk}) \Rightarrow a - b = 0 \Rightarrow \varphi(\overline{a}) - \varphi(\overline{b}) = 0 \Rightarrow \varphi(\overline{a}) = \varphi(\overline{b}).$$

Portanto, φ está bem definida. Além disso, φ é um homomorfismo sobrejetor. De fato, para todos $\overline{a}, \overline{b} \in \mathbb{Z}_p$, temos que:

$$\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = a + b = \varphi(\overline{a}) + \varphi(\overline{b});$$

$$\varphi(\overline{a} \cdot \overline{b}) = \varphi(\overline{ab}) = ab = \varphi(\overline{a})\varphi(\overline{b}).$$

E ainda,

$$\forall\, a \in \mathbb{F}_p \;\exists\, \overline{a} \in \mathbb{Z}_p \text{ tal que } \varphi(\overline{a}) = a$$

Assim, pelo Primeiro Teorema de Isomorfismos, $\mathbb{F}_p$ é isomorfo a $\mathbb{Z}_p$, ou seja, o corpo finito $\mathbb{F}_p$ tem a mesma estrutura do corpo $\dfrac{\mathbb{Z}}{\langle p \rangle}$.

Então, $\mathbb{F}_p$ dotado da estrutura de corpo induzida por φ é um corpo finito, chamado corpo de Galois de ordem p.

Exemplo 3.4. *Consideremos o corpo $\mathbb{F}_2$: os elementos desse corpo são 0 e 1. Suas tabelas de operações são:*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Exemplo 3.5. *O corpo $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ é isomorfo a $\mathbb{Z}_5$, onde o isomorfismo é dado por $\overline{0} \longmapsto 0, ..., \overline{4} \longmapsto 4$. As tabelas de operações são:*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Seja p primo. Se K é um subcorpo de um corpo finito $\mathbb{F}_p$, então K contém os elementos 0 e 1 e, portanto, contém também todos os demais elementos de $\mathbb{F}_p$, uma vez que a operação adição é fechada em K. Assim, pela definição 2.1, $\mathbb{F}_p$ é um corpo primo. Os corpos $\mathbb{F}_p$ desempenham um papel importante na teoria geral de corpos, conforme mostra a Proposição 3.6.

Proposição 3.6. *Seja p um número primo. O subcorpo primo de um corpo F de característica p é isomorfo a $\mathbb{F}_p$.*

Demonstração. Consideremos a aplicação $\varphi : \mathbb{Z}_p \longrightarrow F$ dada por $\varphi(\overline{n}) = n \cdot 1$. Temos que a aplicação está bem definida. De fato, se $\overline{n} = \overline{m}$ em $\mathbb{Z}_p$, com m, n inteiros, então existe $\lambda \in \mathbb{Z}$ tal que $n = m + \lambda p$, de modo que

$$n1 = (m + \lambda p)1 = m1 + \lambda p1 = m1.$$

Além disso, φ é homomorfismo. De fato, para todos $\overline{m}, \overline{n} \in \mathbb{Z}_p$, temos que

$$\varphi(\overline{m} + \overline{n}) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1 = \varphi(\overline{m}) + \varphi(\overline{n})$$

$$\varphi(\overline{m} \cdot \overline{n}) = (m \cdot n) \cdot 1 = (m \cdot 1)(n \cdot 1) = \varphi(\overline{m}) \cdot \varphi(\overline{n}).$$

Logo, sendo $\mathbb{Z}_p$ e F corpos, temos que φ é homomorfismo injetor e assim $\varphi(\mathbb{Z}_p)$ é um subcorpo de F isomorfo a $\mathbb{Z}_p$. Como qualquer subcorpo de F contém 0 e 1, temos que qualquer subcorpo também irá conter $\varphi(\mathbb{Z}_p)$. Logo, $\varphi(\mathbb{Z}_p)$ é o subcorpo primo de F e é isomorfo a $\mathbb{F}_p$. □

Lema 3.7. *Sejam p um primo e F um corpo finito de característica p. Então,*

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

para todo inteiro positivo n.

Demonstração. Vamos provar usando indução em n.
Para $n = 1$, usando o teorema binomial, temos

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}. \tag{3.1}$$

Se $0 < k < p$, então

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

deve ser divisível por p, uma vez que p não divide $k!(p-k)!$. Como F é um corpo finito de característica p, então todos, exceto o primeiro e o último termos de (3.1), devem ser zero. Portanto, $(a + b)^p = a^p + b^p$. Agora, suponhamos que o resultado seja válido para todo h, onde $1 \leq h \leq n$. Pela hipótese de indução,

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

Logo, o resultado é válido para $n + 1$ e, então, a prova está completa. □

3.2 CARACTERIZAÇÃO DOS CORPOS FINITOS

Nessa seção, fixada uma potência q de um número primo, estudamos a existência e unicidade dos corpos finitos de cardinalidade q.

Lema 3.8. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então, F tem q^m elementos, onde $m = [F : K]$.*

Demonstração. Temos que F é um espaço vetorial sobre K, então a dimensão do espaço vetorial F sobre o corpo K é finita, pois F é finito. Se $[F : K] = m$, então F possui uma base sobre K com m elementos, digamos $b_1, b_2, ..., b_m$. Portanto, todo elemento de F pode ser unicamente representado na forma $a_1b_1 + a_2b_2 + \cdots + a_mb_m$, onde $a_1, a_2, ..., a_m \in K$. Mas, como K possui q elementos, F possui exatamente q^m elementos. □

Teorema 3.9. *Seja F um corpo finito. Então, F possui p^n elementos onde p é a característica de F e n a dimensão de F sobre seu corpo primo.*

Demonstração. Como F é finito então a característica p de F é um número primo. Portanto, o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ e, assim, possui p elementos. Então, pelo Lema 3.8, F tem p^n elementos com $n = [F : K]$. □

Lema 3.10. *Se F é um corpo finito com q elementos, então $a^q = a$ para todo $a \in F$.*

Demonstração. Se $a = 0$, segue a igualdade. Por outro lado, temos que os elementos não nulos de F formam um grupo de ordem $q - 1$ com a operação produto. Então, $a^{q-1} = 1$, para todo $a \in F$, com $a \neq 0$. Logo, $a^{q-1} \cdot a = 1 \cdot a$, ou seja, $a^q = a$ para todo $a \in F^*$. □

Proposição 3.11. *Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $x^q - x \in K[x]$ é fatorado em $F[x]$ na forma $x^q - x = \prod_{a \in F} (x - a)$ e F é um corpo de decomposição de $x^q - x$ sobre K.*

Demonstração. O polinômio $x^q - x$ de grau q possui no máximo q raízes em F. Ainda, pelo Lema 3.10, temos que todos os elementos de F são raízes de $x^q - x$. Logo, $x^q - x$ fatora-se em F e não pode fatorar-se em nenhum corpo menor que F. Portanto, F é um corpo de decomposição para o polinômio $x^q - x$ sobre K. □

Com isto, podemos provar o principal teorema de caracterização para corpos finitos.

Teorema 3.12 (Existência e Unicidade de Corpos Finitos)**.** *Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. Além disso, corpos finitos com $q = p^n$ elementos são isomorfos ao corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. (*Existência*) Para $q = p^n$ consideremos $x^q - x \in \mathbb{F}_p[x]$. Seja F o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Esse polinômio possui q raízes distintas em F, já que sua derivada é $qx^{q-1} - 1 = -1$ em $\mathbb{F}_p[x]$. Seja $S = \{a \in F; a^q - a = 0\}$. Então, S é um subcorpo de F pois:

- S contém os elementos 0 e 1;

- $a, b \in S$ implica em $(a-b)^q = a^q - b^q = a - b$ e assim $a - b \in S$;
- dados $a, b \in S, b \neq 0$ temos $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ e assim $ab^{-1} \in S$.

Por outro lado, $x^q - x$ deve se decompor em S já que S contém todas as suas raízes. Portanto, $F = S$ e, como S contém q elementos, F é um corpo finito com q elementos.

(*Unicidade*) A Proposição 3.11 mostra que dois corpos de ordem p^n são corpos de decomposição de $x^{p^n} - x$ sobre $\mathbb{F}_p$, portanto o resultado segue do Teorema da Extensão do Isomorfismo (ver [11], Teorema 3.20). □

Segundo o Teorema 3.12, passaremos a considerar então $\mathbb{F}_q$ o corpo finito com q elementos, onde q é uma potência de um primo p.

Teorema 3.13 (Critério de 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 tal que m divide n. Por outro lado, se m divide n, então há um único subcorpo de $\mathbb{F}_p$ com p^m elementos.*

Demonstração. Seja F um subcorpo de $\mathbb{F}_q$. Vamos assumir que F contém p^m elementos. Então, pelo Lema 3.9, temos $q = p^n = (p^m)^k = p^{mk}$, onde $k = [\mathbb{F}_q : F]$. Logo, $n = mk$ e, portanto, m divide n. Por outro lado, suponhamos que m divide n para algum $m > 0$. Então, $p^m - 1$ divide $p^n - 1$. Consequentemente, $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$. Portanto, $x^{p^m} - x$ divide $x^{p^n} - x$ e toda raiz de $x^{p^m} - x$ é raiz de $x^{p^n} - x = x^q - x$. Logo, $\mathbb{F}_q$ deve conter como subcorpo um corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$ e, pelo Teorema 3.12, tal corpo de decomposição deve ter ordem p^m. Agora suponhamos que existem dois subcorpos F e K de ordem p^m em $\mathbb{F}_q$. Então, existe pelo menos um elemento de K que é diferente de todos os elementos de F e, como F possui todas as raízes de $x^{p^m} - x$, esses subcorpos juntos contém mais de p^m raízes de $x^{p^m} - x$ em $\mathbb{F}_q$, que é uma contradição. □

Exemplo 3.14. *Os subcorpos do corpo finito $\mathbb{F}_{2^{24}}$ são $\mathbb{F}_{2^{24}}, \mathbb{F}_{2^{12}}, \mathbb{F}_{2^8}, \mathbb{F}_{2^6}, \mathbb{F}_{2^4}, \mathbb{F}_{2^3}, \mathbb{F}_{2^2}, \mathbb{F}_2$.*

Teorema 3.15. *O grupo multiplicativo $\mathbb{F}_q^*$ formado por todos os elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Podemos assumir $q \geq 3$. Sejam $h = q - 1$ a ordem do grupo $\mathbb{F}_q^*$ e $h = p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$ a decomposição de h em fatores primos. Para todo i, com $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes em $\mathbb{F}_q$. Como $h/p_i < h$ segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes deste polinômio. Sejam a_i um tal elemento e $b_i = a_i^{h/p_i^{r_i}}$. Assim, $b_i^{p_i^{r_i}} = 1$ e, então, a ordem de b_i é um divisor de $p_i^{r_i}$. Logo, a ordem de b_i é da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Por outro lado, temos que $(a_i^{h/p_i^{r_i}})^{p_i^{r_i}} = a^h = 1$ e, portanto,

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

e, então, a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 ... b_m$ tem ordem h. Suponhamos que a ordem de b seja um divisor próprio de h, e, portanto, um divisor de pelo menos um dos m inteiros $h_i, 1 \leq i \leq m$. Digamos que este inteiro seja h_1. Então, temos que

$$1 = b^{h_1} = b_1^{h_1} b_2^{h_1} ... b_m^{h_1}.$$

Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h_1 e, assim, $b_i^{h_1} = 1$. Portanto $b_1^{h_1} = 1$. Isto implica que a ordem de b_1 deve dividir h_1, que é impossível, pois a ordem de b_1 é $p_1^{r_1}$. Portanto, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 3.16. *Um elemento $\alpha \in \mathbb{F}_q$ é dito um elemento primitivo se α é um gerador do grupo cíclico $\mathbb{F}_q^*$, ou seja, $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, ..., \alpha^{q-2}\}$.*

Teorema 3.17. *Seja $\mathbb{F}_r$ uma extensão de $\mathbb{F}_q$. Então, $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ é um gerador de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja α um elemento primitivo de $\mathbb{F}_r$. Temos que $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. Por outro lado, $\mathbb{F}_q(\alpha)$ contém 0 e todas as potências de α e, portanto, todos os elementos de $\mathbb{F}_r$. Logo $\mathbb{F}_r = \mathbb{F}_q(\alpha)$. □

Corolário 3.18. *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 de $\mathbb{F}_q$ de ordem q^n, de modo que $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 3.17, $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ para algum $\alpha \in \mathbb{F}_q$. Então, o polinômio minimal de α sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n. □

3.3 RAÍZES DE POLINÔMIOS IRREDUTÍVEIS

Nessa seção, apresentamos informações sobre o conjunto de raízes de um polinômio irredutível sobre um corpo finito.

Lema 3.19. *Sejam $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ e α uma raiz de f em uma extensão de $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$ temos que $h(\alpha) = 0$ se e somente se f divide h.*

Demonstração. Sejam a o coeficiente líder de f e $g(x) = a^{-1} f(x)$. Então g é um polinômio mônico irredutível em $\mathbb{F}_q[x]$ com $g(\alpha) = 0$ e, portanto, é o polinômio minimal de α sobre $\mathbb{F}_q$. Como $h(\alpha) = 0$, pela definição de polinômio minimal, segue que $g(x)$ divide $h(x)$. Portanto, $f(x)$ divide $h(x)$. □

Lema 3.20. *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. Suponhamos que $f(x)$ divide $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, de modo que $\alpha \in \mathbb{F}_{q^n}$. Logo, $\mathbb{F}_q(\alpha)$ é subcorpo de $\mathbb{F}_{q^n}$. Mas como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e, pelo Lema 3.8, $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, então, pelo Teorema 2.3, temos que m divide n.

Por outro lado, se m divide n então, do Teorema 3.13, temos que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como subcorpo. Se α é uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e, então, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Assim, $\alpha \in \mathbb{F}_{q^m}$ e, então, $\alpha^{q^n} = \alpha$. Portanto, α é raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$ e, pelo Lema 3.19, $f(x)$ divide $x^{q^n} - x$. □

Teorema 3.21. *Se f é um polinômio irredutível de $\mathbb{F}_q[x]$ de grau m, então f possui uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e são os m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Em particular, $\alpha \in \mathbb{F}_{q^m}$. Agora, mostremos que se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f então β^q é também uma raiz de f. Escrevendo $f(x) = a_m x^m + \cdots + a_1 x + a_0$ com $a_i \in \mathbb{F}_q$, para todo $i = 0, 1, ..., m$, então, usando o Lema 3.10 e o Lema 3.7, temos que

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

Portanto, os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são raízes de f. Resta mostrar que esses elementos são distintos. Suponhamos o contrário: que $\alpha^{q^j} = \alpha^{q^k}$ para alguns inteiros j e k com $0 \leq j < k \leq m-1$. Ao elevar ambos os lados desta igualdade à potência q^{m-k}, temos

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

Assim, segue do Lema 3.19 que $f(x)$ divide $x^{q^{m-k+j}} - x$. Mas, pelo Lema 3.20, isto só é possível se m dividir $m-k+j$. Como $0 < m-k+j < m$ chegamos a uma contradição. □

Corolário 3.22. *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m. Então, o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.*

Demonstração. O Teorema 3.21 mostra que f se decompões em $\mathbb{F}_{q^m}$. Ainda,

$$\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$$

para uma raiz α de f em $\mathbb{F}_{q^m}$, onde a segunda igualdade é tomada da prova do Teorema 3.21. □

Podemos introduzir uma terminologia conveniente para os elementos que aparecem no Teorema 3.21, independentemente se $\alpha \in \mathbb{F}_{q^m}$ é uma raiz de um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m ou não.

Definição 3.23. *Sejam $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$. Então, os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são chamados conjugados de α com respeito a $\mathbb{F}_q$.*

Observação 3.24. *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, se o grau do polinômio minimal é d, então d é um divisor próprio de m e os conjugados de α com respeito a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$, repetindo $\frac{m}{d}$ vezes.*

Para demosntrar o seguinte teorema, relembremos um resultado que segue da teoria de grupo: em um grupo finito cíclio $\langle a \rangle$ de ordem m o elemento a^k gera um subgrupo de ordem $\frac{m}{\text{mdc}(k,m)}$, ([9], Teorema 1.15).

Teorema 3.25. *Os conjugados de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ têm a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Pelo Teorema 3.15, $\mathbb{F}_q^*$ é um grupo cíclico e pelo fato de que toda potência da característica de $\mathbb{F}_q$ é relativamente prima à ordem $q-1$ de $\mathbb{F}_q^*$, segue o resultado. □

3.4 TRAÇOS E NORMAS

Nessa seção iremos considerar uma extensão $F = \mathbb{F}_{q^m}$ de um corpo finito $K = \mathbb{F}_q$ como um espaço vetorial sobre K. Introduzimos a seguir uma importante função de F para K.

Definição 3.26. *Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o traço $Tr_{F/K}(\alpha)$ de α sobre K é definido por*

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

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

Seja $f \in K[x]$ o polinômio minimal de α sobre K de grau d. Então d é um divisor de m e $g(x) = f(x)^{m/d}$ é chamado de polinômio característico de α sobre K. Pelo Teorema 3.21, as raízes de f em F são dadas por $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$ e, da Observação 3.24, temos que as raízes de g em F são precisamente os conjugados de α com respeito a K. Consequentemente,

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + ... + a_0 \\ &= (x-\alpha)(x-\alpha^q)...(x-\alpha^{q^{m-1}}) \end{aligned} \tag{3.2}$$

e uma comparação de coeficientes mostra que

$$Tr_{F/K}(\alpha) = -a_{m-1}. \tag{3.3}$$

Em particular, $Tr_{F/K}(\alpha)$ é sempre um elemento de K.

Teorema 3.27. *A função $Tr_{F/K}$ satisfaz as seguintes propriedades:*

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

(ii) $Tr_{F/K}(c\,\alpha) = c\,Tr_{F/K}(\alpha)$, *para todos* $c \in K, \alpha \in F$;

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

(iv) $Tr_{F/K}(a) = ma$, *para todo* $a \in K$;

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

Demonstração. (i) Para todo $\alpha, \beta \in F$, usando o Lema 3.7, temos que

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

(ii) Para todo $c \in K$ temos que $c^{q^j} = c$, para todo $j \geq 0$, pelo Lema 3.10. Assim, obtemos, para todo $\alpha \in F$:

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

(iii) As propriedades (i) e (ii), juntamente com o fato de $Tr_{F/K}(\alpha) \in K$, para todo $\alpha \in F$, mostram que $Tr_{F/K}$ é uma transformação linear.

(iv) Para todo $a \in K$, pelo Lema 3.10, temos que $a^{q^j} = a, j \geq 0$. Assim,

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

(v) Se $\alpha \in F$ temos, pelo Lema 3.10, $\alpha^{q^m} = \alpha$ e então

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

□

A função traço $Tr_{F/K}$ não é apenas uma transformação linear de F para K, mas também serve para descrever todas as transformações lineares de F em K (ou, numa terminologia equivalente, de todos os funcionais lineares em F). Tal descrição que tem a vantagem de ser independente de uma base pré-fixada.

Teorema 3.28. *Seja F uma extensão finita do corpo finito K. Então, as transformações lineares de F em K são exatamente as funções L_β dadas por $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ para todo $\alpha \in F$ e β fixo em F. Além disso, temos que $L_\beta \neq L_\gamma$ sempre que β e γ são elementos distintos de F.*

Demonstração. Pelo item (iii) do Teorema 3.27, cada função L_β é uma transformação linear de F em K. Para $\beta, \gamma \in F$ com $\beta \neq \gamma$, temos

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

para algum $\alpha \in \mathbb{F}$, pois $Tr_{F/K}$ leva F para K. Portanto, as funções L_β e L_γ são diferentes. Se $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$ então a função L_β produz q^m diferentes transformações lineares de F em K. Por outro lado, toda transformação linear de F em K pode ser obtida atribuindo elementos arbitrários de K aos m elementos de uma determinada base de F sobre K. Como isto pode ser feito de q^m maneiras diferentes, as funções L_β já esgotam todas as possíveis transformações lineares. □

Teorema 3.29 (Transitividade do Traço)**.** *Sejam K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então, para todo $\alpha \in E$, temos*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$$

Demonstração. Sejam $K = \mathbb{F}_q$, $[F : K] = m$ e $[E : F] = n$. Pelo Teorema 2.3, $[E : K] = mn$. Então, para $\alpha \in E$, temos

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

□

Outra função interessante de um corpo finito para um subcorpo é obtida pelo produto dos conjugados de um elemento do corpo em relação ao subcorpo.

Definição 3.30. *Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, a norma $N_{F/K}(\alpha)$ de α sobre K é definida por*

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

Comparando os termos constantes em (3.2), temos que $N_{F/K}(\alpha)$ pode ser lida a partir do polinômio característico g de α sobre K como

$$N_{F/K}(\alpha) = (-1)^m a_0, \text{ onde } a_0 \text{ é o termo independente de } g(x)$$

Segue, em particular, que $N_{F/K}$ é também um elemento de K.

Teorema 3.31. *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a 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 todos* $\alpha, \beta \in F$;

(ii) $N_{F/K}$ *uma função sobrejetora de* F *em* K *e de* F^* *em* K^*;

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

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

Demonstração. (i) Para todo $\alpha, \beta \in F$, temos

$$\begin{aligned} N_{F/K}(\alpha\beta) &= (\alpha\beta)(\alpha\beta)^q ... (\alpha\beta)^{q^{m-1}} \\ &= \alpha\beta\alpha^q\beta^q ... \alpha^{q^{m-1}}\beta^{q^{m-1}} \\ &= (\alpha\alpha^q ... \alpha^{q^{m-1}})(\beta\beta^q ... \beta^{q^{m-1}}) \\ &= N_{F/K}(\alpha)N_{F/K}(\beta) \end{aligned} \tag{3.4}$$

(ii) Já observamos $N_{F/K}$ é uma função de F em K. Como $N_{F/K}(\alpha) = 0$ se e somente se $\alpha = 0$, $N_{F/K}$ leva F^* em K^*. Vamos mostrar que $N_{F/K}$ é sobrejeora. Da primeira propriedade, segue que $N_{F/K}$ é um homomorfismo entre grupos multiplicativos. Como os elementos do núcleo de $N_{F/K}$ são exatamente as raízes do polinômio $x^{(q^m-1)/(q-1)} - 1 \in K[x]$ em F, a ordem d do núcleo satisfaz $d \leq \frac{q^m-1}{q-1}$. Pelo Primeiro Teorema do isomorfismo de grupos, a imagem de $N_{F/K}$ tem ordem $\dfrac{q^m-1}{d}$ que é por sua vez, pelo menos $q-1$. Portanto, $N_{F/K}$ leva, sobrejetivamente, F^* em K^* e, portanto, F em K.

(iii) Para todo $a \in K$, temos, pelo Lema 3.10, que $a^{q^j} = a$, para todo $j \geq 0$. Assim,

$$\begin{aligned} N_{F/K}(a) &= a \cdot a^q \cdot ... \cdot a^{q^{m-1}} \\ &= \underbrace{a \cdot a \cdot ... \cdot a}_{m \text{ vezes}} = a^m \end{aligned}$$

(iv) Se $\alpha \in F$, então

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

Como $N_{F/K}(\alpha) \in K$, usando o Lema 3.10, temos que

$$N_{F/K}(\alpha^q) = N_{F/K}(\alpha).$$

□

Teorema 3.32 (Transitividade da Norma)**.** *Sejam K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então*

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha)), \text{ para todo } \alpha \in E.$$

Demonstração. Sejam $K = \mathbb{F}_q$, $[F : K] = m$ e $[E : F] = n$. Pelo Teorema 2.3, $[E : K] = mn$. Então, para $\alpha \in E$, temos

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

□

3.5 RAÍZES DA UNIDADE E POLINÔMIO CICLOTÔMICO

Definição 3.33. *Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre K é chamado de n-ésimo corpo ciclotômico sobre K e é denotado por $K^{(n)}$. As raízes de $x^n - 1$ em $K^{(n)}$ são chamadas de raízes n-ésimas da unidade sobre K e o conjunto dessas raízes será denotado por $E^{(n)}$.*

Teorema 3.34. *Sejam n um inteiro positivo e K um corpo de característica p. Então:*

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

(ii) Se p divide n, digamos $n = mp^e$, onde m e e são inteiros positivos com $mdc(m, p) = 1$, 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. (i) O caso $n = 1$ é trivial. Para $n \geq 2$, $x^n - 1$ e sua derivada nx^{n-1} não possuem raízes em comum, com nx^{n-1} possuíndo 0 como raiz em $K^{(n)}$. Assim, pelo Teorema 2.14, temos que $x^n - 1$ não pode ter es múltiplas e, portanto, $E^{(n)}$ possui n elementos. Agora, se $\gamma, \eta \in E^{(n)}$, então $(\gamma\eta^{-1})^n = \gamma^n(\eta^{-1})^n = 1$, logo $\gamma\eta^{-1} \in E^{(n)}$. Segue que $E^{(n)}$ é um grupo multiplicativo. Seja $n = p_1^{e_1}p_2^{e_2}...p_t^{e_t}$ a decomposição de n em fatores primos. Então, usando os mesmos argumentos da prova do Teorema 3.15, mostramos que

para cada $j, 1 \leq j \leq t$, existe um elemento $\alpha_j \in E^{(n)}$ que não é raiz do polinômio $x^{n/p_j} - 1$, que $\beta_j = \alpha_j^{n/p_j^{e_t}}$ tem ordem $p_j^{e_t}$ e que $E^{(n)}$ é um grupo cíclico com gerador $\beta = \beta_1\beta_2...\beta_t$.

(ii) A prova segue de $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$ e da parte (i). □

Definição 3.35. *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 n-ésima raiz primitiva da unidade sobre K.*

Definição 3.36. *Sejam K um corpo de característica p, n um inteiro positivo não divisível por p e γ uma n-ésima raiz primitiva da unidade sobre K. Então o polinômio*

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

é chamado n-ésimo polinômio ciclotômico sobre K.

Observação 3.37. *O polinômio $Q_n(x)$ é independente da escolha de γ. De fato, como γ uma n-ésima raiz primitiva da unidade sobre K e estamos tomando todas as potências s de γ com $mdc(s, n) = 1$, segue que o polinômio pode ser escrito como o produto de fatores $x - \gamma_i$, onde γ_i são todas as n-ésimas raízes primitivas da unidade.*

Exemplo 3.38. *Sejam $n = 3$, K um corpo com característica diferente de 3 e ζ uma raiz cúbica primitiva cúbica da unidade sobre K. Então,*

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

Usamos o símbolo de produto $\prod_{d|n}$ para denotar um produto estendido sobre todos os divisores positivos d de um inteiro positivo n.

Teorema 3.39. *Sejam K um corpo de característica p e n um inteiro positivo não divisível por p. Então:*

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

(ii) os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K.

Demonstração. Cada n-ésima raiz da unidade sobre K é uma d-ésima raiz primitiva da unidade sobre K para um divisor positivo d de n. Em detalhes, se γ for uma n-ésima raiz primitiva da unidade sobre K e γ^s for uma n-ésima raiz da unidade sobre K, então $d = n/\text{mdc}(s, n)$, isto é, d é a ordem de γ^s em $E^{(n)}$. Como

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

a fórmula em (i) é obtida coletando esses fatores $(x-\gamma^s)$ para os quais γ^s é uma d-ésima raiz primitiva da unidade sobre K.

(ii) Provaremos por indução em n. Notemos que $Q_n(x)$ é um polinômio mônico. Para $n=1$ temos $Q_1(x)=x-1$, que é obviamente válido. Agora, seja $n>1$ e suponha válido para todo $Q_d(x)$ com $1\leq d<n$. Então, por (i), temos

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

onde $f(x)=\prod_{d|n,\, d<n} Q_d(x)$. A hipótese de indução implica que $f(x)$ é um polinômio com coeficiente no subcorpo primo de K. Fazendo a divisão entre x^n-1 e o polinômio mônico $f(x)$ temos que os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K. □

Exemplo 3.40. *Sejam r um número primo e $k\in\mathbb{N}$. Pelo Teorema 3.39 (i),*

$$Q_{r^k}=\frac{x^{r^k}-1}{Q_1(x)Q_r(x)\cdots Q_{r^{k-1}}(x)}=\frac{x^{r^k}-1}{x^{r^{k-1}}-1}=1+x^{r^{k-1}}+x^{2r^{k-1}}+\cdots+x^{(r-1)r^{k-1}}.$$

Para $k=1$, temos por exemplo $Q_r(x)=1+x+x^2+\cdots+x^{r-1}$.

Lema 3.41. *Se h é um divisor positivo da ordem de um grupo cíclico $\langle a\rangle$, então $\langle a\rangle$ contém $\phi(h)$ elementos de ordem h, onde $\phi(h)$ é a função de Euler, isto é, o número de inteiros $1\leq n\leq h$ que são relativamente primos a h.*

Demonstração. Seja $m=|\langle a\rangle|$. Como h divide m, existe $d\in\mathbb{N}$ tal que $m=dh$. Temos que um elemento a^k tem ordem h se e somente se $\mathrm{mdc}(k,m)=d$. Então, o número de elementos de ordem h é igual ao número de inteiros k com $1\leq k\leq m$ e $\mathrm{mdc}(k,m)=d$, assim, podemos escrever $k=dn$ com $1\leq n\leq h$ e, portanto, $\mathrm{mdc}(k,m)=d$ é equivalente a $\mathrm{mdc}(n,h)=1$. O número de elementos de ordem h que satisfazem essa igualdade é igual a $\phi(h)$. □

Teorema 3.42. *O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K. Além disso, se $K=\mathbb{F}_q$ com $mdc(q,n)=1$ e d é o menor inteiro positivo tal que $q^d\equiv 1 \pmod n$, então Q_n se fatora em $\dfrac{\phi(n)}{d}$ polinômios mônicos irredutíveis distintos em $K[x]$ de mesmo grau d, $K^{(n)}$ é o corpo de decomposição de qualquer fator irredutível de Q_n sobre K e o grau da extensão $K^{(n)}$ sobre K é d.*

Demonstração. Se existe uma raiz n-ésima primitiva da unidade γ sobre K é claro que $K^{(n)}=K(\gamma)$. Além disso, se $K=\mathbb{F}_q$ com $\mathrm{mdc}(q,n)=1$, seja η uma n-ésima raiz primitiva da unidade sobre $\mathbb{F}_q$. Então $\eta\in\mathbb{F}_{q^k}$ se e somente se $\eta^{q^k}=\eta$ e esta igualdade é equivalente a $q^k\equiv 1 \pmod n$. O menor inteiro positivo para o qual isto é válido é $k=d$, e assim η está em $\mathbb{F}_{q^d}$, mas não está em nenhum de seus subcorpos próprios. Portanto, o polinômio minimal de η sobre $\mathbb{F}_q$ tem grau d, e como η é uma raiz arbitrária de Q_n, seguem os resultados desejados. □

Uma conexão entre o corpos ciclotômicos e corpos finitos é dada pelo seguinte resultado.

Teorema 3.43. *O corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um dos seus subcorpos.*

Demonstração. Como todos os $q-1$ elementos não nulos de $\mathbb{F}_q$ são raízes do polinômio $x^{q-1}-1$, esse polinômio de decompões em $\mathbb{F}_q$. Obviamente, o polinômio não pode se decompor em qualquer subcorpo próprio de $\mathbb{F}_q$, portanto, $\mathbb{F}_q$ é o corpo de decomposição de $x^{q-1}-1$ sobre qualquer um de seus subcorpos. □

Exemplo 3.44. *O corpo $\mathbb{F}_9$ é o oitavo corpo ciclotômico sobre $\mathbb{F}_3$, isto é, $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$. Como no exemplo 3.40,*

$$Q_8(x) = Q_{2^3}(x) = \frac{x^8-1}{x^4-1} = x^4+1 \in \mathbb{F}_3[x].$$

A decomposição de $Q_8(x)$ em fatores irredutíveis em $\mathbb{F}_3[x]$ é

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

3.6 CARACTERES

Nessa seção, apresentamos de maneira sucinta algumas definições e propriedades sobre o caracter de um grupo finito abeliano G. Tais conceitos serão usados em um dos critérios para polinômios de permutação que apresentaremos na seção 5.1.

Definição 3.45. *Seja G um grupo finito abeliano de ordem $|G|$ com elemento identidade 1_G. Um caracter χ de G é um homomorfismo de G no grupo multiplicativo U dos números complexos de valor absoluto unitário, isto é, uma função de G em U com $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ para todo $g_1, g_2 \in G$.*

Como $\chi(1_G) = \chi(1_G)\chi(1_G)$, temos que $\chi(1_G) = 1_G$.

Além disso,

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1_G$$

para todo $g \in G$, portanto os valores de χ são as $|G|$-ésimas raízes da unidade. Note também que

$$\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1_G$$

e, portanto,

$$\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$$

para todo $g \in G$, onde a barra denota o conjugado complexo.

Dentre os caracteres de G temos o caracter trivial χ_0, que é definido por $\chi_0(g) = 1_G$ para todo $g \in G$; qualquer outro caracter é dito não trivial. Para cada caracter χ há

associado o caracter conjugado $\overline{\chi}$ definido por $\overline{\chi}(g) = \overline{\chi(g)}$, para todo $g \in G$. Dado um número finito de caracteres $\chi_1, \chi_2, ..., \chi_n$ de G pode-se formar o caracter produto $\chi_1\chi_2 \cdots \chi_n$ dado por

$$(\chi_1\chi_2 \cdots \chi_n)(g) = \chi_1(g)\chi_2(g) \cdots \chi_n(g),$$

para todo $g \in G$. Se $\chi_1 = \chi_2 = \cdots = \chi_n = \chi$ podemos escrever χ^n para $\chi_1\chi_2 \cdots \chi_n$. Temos que o conjunto $G^\wedge$ dos caracteres de G forma um grupo abeliano com a multiplicação de caracteres. Além disso, como os valores dos caracteres de G só podem ser as $|G|$-ésimas raízes da unidade, $G^\wedge$ é finito.

Teorema 3.46. *Se χ é um caracter não trivial de um grupo abeliano finito G, então*

$$\sum_{g \in G} \chi(g) = 0. \tag{3.5}$$

Por outro lado, para cada $g \in G$ com $g \neq 1_G$, temos

$$\sum_{\chi \in G^\wedge} \chi(g) = 0. \tag{3.6}$$

Demonstração. Como χ é um caracter não trivial, existe $h \in G$ com $\chi(h) \neq 1$. Então

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

pois, se g percorre todos os elementos de G, o mesmo ocorre com hg. Assim, temos

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0 \ \Rightarrow \ \sum_{g \in G} \chi(g) = 0,$$

pois $\chi(h) \neq 1$.

Para a segunda parte, consideremos a função $\hat{g}$ definida por $\hat{g}(\chi) = \chi(g)$ para $\chi \in G^\wedge$. Como o caracter é não trivial, existe $\chi \in G^\wedge$ de modo que $\chi(g) \neq 1 = \chi(1_G)$. Assim, aplicando (3.5) ao grupo $G^\wedge$, temos

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

□

Teorema 3.47. *O número de caracteres de um grupo finito abeliano G é igual a $|G|$.*

Demonstração. Segue de

$$|G^\wedge| = \sum_{g \in G} \sum_{\chi \in G^\wedge} \chi(g) = \sum_{\chi \in G^\wedge} \sum_{g \in G} \chi(g) = |G|,$$

onde usamos (3.6) na primeira identidade e (3.5) na última identidade. □

Sejam χ e ψ caracteres de G. Então

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} 0, & \text{se } \chi \neq \psi \\ 1, & \text{se } \chi = \psi \end{cases}, \tag{3.7}$$

onde a primeira parte segue ao aplicarmos (3.5) ao caracter $\chi\overline{\psi}$ e a segunda parte é trivial pois, se $\chi = \psi$, temos que $\chi\overline{\psi} = \chi\overline{\chi} = \chi_0$.

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

$$\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)} = \begin{cases} 0, & \text{se } g \neq h \\ 1, & \text{se } g = h \end{cases}, \tag{3.8}$$

onde obtemos a primeira parte aplicando (3.6) ao elementos gh^{-1}. Para a segunda parte usamos o Teorema 3.47 e o fato que, se $g = h$, então, $\chi(g)\overline{\chi(g)} = \chi(1_G) = 1_G$, para todo $g \in G$.

Temos então, de (3.7) e (3.8), as relações de ortogonalidade para caracteres.

De acordo com [9], a teoria de caracteres é frequentemente usada para obter expressões para o número de soluções de equações em um grupo abeliano finito. Seja f uma função arbitrária do produto cartesiano $G^n = G \times \cdots \times G$ em G. Então para $h \in G$ fixo, o número $N(h)$ de n-uplas $(g_1, ..., g_n) \in G^n$ com $f(g_1, ..., g_n) = h$ é dado por

$$N(h) = \frac{1}{|G|}\sum_{g_1\in G}\cdots\sum_{g_n\in G}\sum_{\chi\in G^\wedge}\chi(f(g_1, ..., g_n))\overline{\chi(h)}, \tag{3.9}$$

por conta de (3.8).

Em um corpo finito $\mathbb{F}_q$ existem dois grupos finitos abelianos que são muito importantes: o grupo aditivo e o grupo multiplicativo do corpo. Caracteres dos grupos aditivo e multiplicativo de $\mathbb{F}_q$ são chamados, respectivamente, de caracteres aditivos e caracteres multiplicativos de $\mathbb{F}_q$.

Para caracteres aditivos χ_a e χ_b, aplicando as relações de ortogonalidade para caracteres (3.7), temos

$$\sum_{c\in\mathbb{F}_q}\chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0, & \text{para } a \neq b \\ q, & \text{para } a = b \end{cases}. \tag{3.10}$$

Em particular

$$\sum_{c\in\mathbb{F}_q}\chi_a(c) = 0 \text{ para } a \neq 0. \tag{3.11}$$

4 POLINÔMIOS SOBRE CORPOS FINITOS

Nesse capítulo intruduzimos, na seção 4.1, a noção de ordem de um polinômio e apresentamos alguns resultados sobre polinômios irredutíveis, na seção 4.2, a fim de compreendermos melhor o funcionamento dos polinômios sobre corpos finitos. Em particular, estudamos a quantidade de polinômios irredutíveis de dado grau sobre um corpo finito fixo.

4.1 ORDEM DE UM POLINÔMIO

Além do grau, outro inteiro não nulo relacionado a um polinômio sobre um corpo finito que também é importante é sua ordem. A definição de ordem de um polinômio é baseada no Lema 4.1 a seguir.

Lema 4.1. *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. O anel de classes residuais $\dfrac{\mathbb{F}_q[x]}{\langle f \rangle}$ contém $q^m - 1$ classes residuais não nulas. As q^m classes residuais $x^j + < f >, j = 0, 1, ..., q^m - 1$, são todas não nulas e então existem inteiros r e s com $0 \leq r < s \leq q^m - 1$ tais que $x^s \equiv x^r \pmod{f(x)}$. Como x e $f(x)$ são relativamente primos, segue que $x^{r-s} \equiv 1 \pmod{f(x)}$, isto é, $f(x)$ divide $x^{r-s} - 1$ onde $0 < r - s \leq q^m - 1$. □

Definição 4.2. *Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo. Se $f(0) \neq 0$, então o menor inteiro positivo e para o qual $f(x)$ divide $x^e - 1$ é chamado ordem de f (ou período ou expoente de f) e é denotado por $ord(f(x))$, ou simplesmente, $ord(f)$. Se $f(0) = 0$, então $f(x) = x^h g(x)$, onde $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$ com $g(0) \neq 0$ e $ord(f)$ é então definida como sendo $ord(g)$.*

A ordem de um polinômio irredutível f pode ser caracterizada na forma alternativa do Teorema 4.3 a seguir.

Teorema 4.3. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m tal que $f(0) \neq 0$. Então, $ord(f)$ é igual à ordem de qualquer raiz de f no grupo multiplicativo $\mathbb{F}_q^*$.*

Demonstração. Pelo Corolário 3.22, $\mathbb{F}_{q^m}$ é o corpo de decomposição de f sobre $\mathbb{F}_q$. As raízes de f têm a mesma ordem no grupo $\mathbb{F}_{q^m}^*$ pelo Teorema 3.25. Então, pelo Lema 3.19, obtemos que $\alpha^e = 1$ se e somente se $f(x)$ divide $x^e - 1$. O resultado segue então da definição de ordem de f e de ordem de α no grupo $\mathbb{F}_{q^m}^*$. □

Corolário 4.4. *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 4.3 e do fato de que $\mathbb{F}_{q^m}^*$ é um grupo de ordem $q^m - 1$. □

O Teorema 4.3 nos leva a uma fórmula para o número de polinômios mônicos irredutíveis de determinados grau e ordem. Usaremos ϕ para denotar a função de Euler, como no Lema 3.41. A seguinte terminologia será conveniente: se n é um inteiro positivo e o inteiro b é relativamente primo a n, então o menor inteiro positivo k para qual $b^k \equiv 1 \pmod{n}$ é chamado ordem multiplicativa de b módulo n.

Teorema 4.5. *O número de polinômios irredutíveis mônicos em $\mathbb{F}_q[x]$ de grau m e ordem e é igual a:*

(i) $\dfrac{\phi(e)}{m}$, *se $e \geq 2$ e m é a ordem multiplicativa de q módulo e;*

(ii) 2, *se $m = e = 1$, e igual a 0 em todos os demais 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. (i) Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ com $f(0) \neq 0$. Então, pelo Teorema 4.3, temos $ord(f) = e$ se e somente se todas raízes de f são raízes primitivas da unidade de ordem e sobre $\mathbb{F}_q$. Em outras palavras, temos $ord(f) = e$ se e somente se f divide o polinômio ciclotômico Q_e. Pelo Teorema 3.42, qualquer fator mônico irredutível de Q_e tem o mesmo grau m, o menor inteiro positivo tal que $q^m \equiv 1 \pmod{e}$. Além disso e há $\dfrac{\phi(e)}{m}$ fatores.

(ii) Para $m = e = 1$ o resultado segue de (i) juntamente com o polinômio mônico irredutível $f(x) = x$. □

4.2 POLINÔMIOS IRREDUTÍVEIS

Teorema 4.6 (Fatoração Única)**.** *Seja K um corpo. Qualquer polinômio $f \in K[x]$ de grau positivo pode ser escrito na forma*

$$f = ap_1^{n_1} \cdots p_k^{n_k} \tag{4.1}$$

onde $a \in K$, $p_1, ..., p_k$ são polinômios mônicos distintos de $K[x]$ e $n_1, \cdots, n_k$ são inteiros positivos. Além disso, tal fatoração é única a menos da ordem em que os fatores ocorrem.

Demonstração. Ver [9], (Teorema 1.59, p. 23). □

A fatoração definida no teorema 4.6 é chamada fatoração canônica de f em $K[x]$.

Teorema 4.7. *Para todo corpo finito $\mathbb{F}_q$ e todo $n \in \mathbb{N}$, o produto de todos polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujos graus dividem n é igual a $x^{q^n} - x$.*

Demonstração. De acordo com o Lema 3.20, todo polinômio mônico irredutível cujo grau divide n é um fator de $x^{q^n} - x$. Ainda, a fatoração de $f(x) = x^{q^n} - x$ em irredutíveis é livre de quadrados pois $f'(x) = -1$. Agora, seja $p(x)$ um fator mônico irredutível de $f(x)$ de grau d. Usando novamente o Lema 3.20, temos que d divide n. □

Seja $N_q(d)$ o número de polinômios mônicos irredutíveis de grau d sobre $\mathbb{F}_q$.

Corolário 4.8. *Fixado $\mathbb{F}_q$, para todo $n \in \mathbb{N}$ temos*

$$q^n = \sum_{d|n} dN_q(d)\,, \tag{4.2}$$

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

Demonstração. A identidade (4.2) segue do Teorema 4.7 comparando o grau de $x^{q^n} - x$ com o grau total da fatoração canônica de $x^{q^n} - x$. □

Ainda, é possível determinar uma fórmula que nos dá o número de polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ de grau fixo. Para isto, precisamos primeiramente definir a função de Möebius.

Definição 4.9. *Para $n \in \mathbb{N}$, a função μ de Möebius é definida por*

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

Lema 4.10. *Para $n \in \mathbb{N}$, a função de Möebius μ satisfaz*

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

Demonstração. O caso $n = 1$ é trivial. Para $n > 1$, devemos levar em conta apenas os divisores positivos d de n para os quais $\mu(d) \neq 0$, isto é, para os quais $d = 1$ ou d é um produto de primos distintos. Portanto se $p_1, p_2, ..., p_k$ são os divisores primos distintos de n, temos

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

□

Exemplo 4.11. *Os divisores positivos de* 16 *são* $\{1, 2, 4, 8, 16\}$. *Assim,*

$$\sum_{d|16} \mu(d) = \mu(1) + \mu(2) + \mu(4) + \mu(8) + \mu(16) = 1 - 1 + 0 + 0 + 0 = 0$$

Teorema 4.12 (Fórmula de Inversão de Möebius)**.** *Sejam* h *e* H *duas funções de* $\mathbb{N}$ *em um grupo abeliano aditivo* G. *Então*

$$H(n) = \sum_{d|n} h(d) \text{ para todo } n \in \mathbb{N} \tag{4.3}$$

se e somente se

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \text{ para todo } n \in \mathbb{N}. \tag{4.4}$$

Demonstração. Suponhamos que $H(m) = \sum_{e|m} h(e)$ para todo $m \in \mathbb{N}$. Fazendo $m = \frac{n}{d}$, temos

$$H\left(\frac{n}{d}\right) = \sum_{e|\frac{n}{d}} h(e) \Rightarrow H\left(\frac{n}{d}\right) = \sum_{ed|n} h(e).$$

Então, temos que

$$\sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{ed|n} h(e) = \sum_{e|n} h(e) \sum_{d|\frac{n}{e}} \mu(d) = h(n).$$

Para o inverso, suponhamos que $h(n) = \sum_{e|n} \mu(e) H\left(\frac{n}{e}\right)$ para todo $n \in \mathbb{N}$. Fazendo $n = d$, temos

$$h(d) = \sum_{e|d} \mu(e) H\left(\frac{d}{e}\right)$$

Daí,

$$\sum_{d|n} h(d) = \sum_{d|n} \sum_{e|d} \mu(e) H\left(\frac{d}{e}\right).$$

Podemos escrever $n = kd$ e $d = le$, e então, $n = kle$. Assim,

$$\sum_{d|n} \sum_{e|d} \mu(e) H\left(\frac{d}{e}\right) = \sum_{kle=n} \mu(e) H(l) = \sum_{l|n} H(l) \sum_{e|\frac{n}{l}} \mu(e) = H(n).$$

□

Teorema 4.13. *O número* $N_q(n)$ *de polinômios mônicos irredutíveis em* $\mathbb{F}_q[x]$ *de grau* n *é dado por*

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

Demonstração. Pelo Corolário 4.8, temos que

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

Fazendo, $H(n) = q^n$ e $h(n) = nN_q(n)$, $\forall n \in \mathbb{N}$, obtemos

$$H(n) = \sum_{d|n} dN_q(d) = \sum_{d|n} h(d).$$

Aplicando a Inversão de Möebius, temos

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right).$$

Portanto,

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

E então,

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

Exemplo 4.14. *O número de polinômios mônicos irredutíveis em* $\mathbb{F}_q[x]$ *de grau* 20 *é dado por*

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

Se $q = 2$*, por exemplo, esse número é*

$$N_2(20) = \frac{1}{20}(2^{20} - 2^{10} - 2^4 + 2^2) = 52377.$$

□

5 POLINÔMIOS DE PERMUTAÇÃO

Nesse capítulo, estudamos, primeiramente, alguns critérios gerais para polinômios de permutação, tendo como referência principal [9]. Em seguida, passamos a apresentar classes específicas de polinômios de permutação, incluindo famílias mais novas apresentadas em [10], [13] e [14]. Ao longo do capítulo, q é uma potência de um número primo p.

5.1 DEFINIÇÃO E CRITÉRIOS

Definição 5.1. *Um polinômio $f \in \mathbb{F}_q[x]$ é chamado um polinômio de permutação de $\mathbb{F}_q$ se a função polinomial associada $f : \mathbb{F}_q \to \mathbb{F}_q$ dada por $c \mapsto f(c)$ é uma permutação de $\mathbb{F}_q$.*

O Lema a seguir apresenta outras equivalências para a Definição 5.1, que também estão baseadas no fato de $\mathbb{F}_q$ ser finito.

Lema 5.2. *O polinômio $f \in \mathbb{F}_q[x]$ é um polinômio de permutação se e somente se uma das seguintes condições é válida:*

(i) a função $c \mapsto f(c)$ é sobrejetora.

(ii) a função $c \mapsto f(c)$ é injetora.

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

Demonstração. Por definição, se $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ então f é uma permutação de $\mathbb{F}_q$ que, por sua vez, é uma bijeção. Portanto, $f(x) = a$ tem uma solução em $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$ e esta solução é única.

Por outro lado, pela finitude do corpo $\mathbb{F}_q$, note que estas condições são equivalentes, logo $f : c \longmapsto f(c)$ é uma bijeção de $\mathbb{F}_q$ em $\mathbb{F}_q$ e, portanto, uma permutação. Portanto f é um polinômio de permutação. □

Exemplo 5.3. *Consideramos o polinômio $f(x) \in \mathbb{F}_7[x]$ dado por $f(x) = x^4 + 3x$. Na tabela a seguir, temos os valores de $f(c)$ para cada $c \in \mathbb{F}_7$ e observamos que f é um polinômio de permutação em $\mathbb{F}_7$, pode ser representado pela permutação* $(1\,4\,2)(3\,6\,5)$.

c	0	1	2	3	4	5	6
$f(c)$	0	4	1	6	2	3	5

Exemplo 5.4. *Consideramos o polinômio $f(x) = x^2 + 2x + 1 \in \mathbb{F}_7[x]$. Observamos que $f(2) = 2 = f(3)$, logo $f(x) = x^2 + 2x + 1 \in \mathbb{F}_7$ não é um polinômio de permutação.*

Observação 5.5. *Fixados $\mathbb{F}_q$, n um inteiro positivo e $f \in \mathbb{F}_q[x]$ de grau n, o processo de calcular $f(a)$ para todo $a \in \mathbb{F}_q$ e checar se os q valores encontrados são de fato distintos é da ordem de nq operações em $\mathbb{F}_q$, ou seja, se q e n crescem, esse processo não faz sentido.*

Lema 5.6. *O conjunto de polinômios de permutação de $\mathbb{F}_q$ é fechado para composição, isto é, se $f, g \in \mathbb{F}_q[x]$ são polinômios de permutação de $\mathbb{F}_q$, então $f \circ g$ também é.*

Demonstração. Sejam $f, g \in \mathbb{F}_q[x]$ polinômios de permutação de $\mathbb{F}_q$. Temos que f, g são injetoras, assim $f \circ g$ também é injetora e, portanto, $f \circ g$ é um polinômio de permutação de $\mathbb{F}_q$. □

Sabemos que dada $\Phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ uma função arbitrária injetiva de $\mathbb{F}_q$ em $\mathbb{F}_q$, então existe um único polinômio $g \in \mathbb{F}_q$ com $\deg(g) < q$ representando Φ no sentido de que $g(c) = \Phi(c)$ para todo $c \in \mathbb{F}_q$. O polinômio g pode ser encontrado calculando o polinômio de interpolação de Lagrange para a dada função Φ ou pela seguinte fórmula:

$$g(x) = \sum_{c \in \mathbb{F}_q} \Phi(c)(1 - (x - c)^{q-1}). \tag{5.1}$$

Se Φ já é dado como uma função polinomial, digamos $c \mapsto f(c)$ com $f \in \mathbb{F}_q$, então g pode ser obtido de f pela redução módulo $x^q - x$ de acordo com o lema a seguir.

Lema 5.7. *Sejam $f, g \in \mathbb{F}_q[x]$. Temos que $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$ se e somente se $f(x) \equiv g(x) \pmod{x^q - x}$.*

Demonstração. Pelo algoritmo da divisão em $\mathbb{F}_q[x]$, podemos escrever

$$f(x) - g(x) = h(x)(x^q - x) + r(x)$$

com $h, r \in \mathbb{F}_q[x]$ e $r = 0$ ou $\deg(r) < q$. Então, $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$ se e somente se $r(c) = 0$ para todo $c \in \mathbb{F}_q$, que é equivalente a $r = 0$. □

Observação 5.8. *O conjunto de todos os polinômios de permutação em $\mathbb{F}_q$ é um grupo com a operação de composição módulo $x^q - x$. Esse grupo é isomorfo ao grupo simétrico S_q de ordem $q!$.*

Em seguida, vamos estabelecer um critério útil para decidir se um polinômios é de permutação. Primeiramente, relembremos a fórmula para a soma dos n primeiros termos de uma série geométrica. Sejam F um corpo e $a \in F, a \neq 1$. Então, temos a seguinte identidade

$$\sum_{i=0}^{n-1} a^i = \frac{(1 - a^n)}{1 - a}. \tag{5.2}$$

Lema 5.9. *Sejam $a_0, a_1, ..., a_{q-1} \in \mathbb{F}_q$. Então as seguintes condições são equivalentes:*

(i) $a_0, a_1, ..., a_{q-1}$ *são distintos.*

(ii) $\sum_{k=0}^{q-1} a_k^t = \begin{cases} 0, & \text{se } t = 0, 1, ..., q-2 \\ -1, & \text{se } t = q-1 \end{cases}$.

Demonstração. Para k fixo com $0 \leq k \leq q-1$, consideramos o polinômio

$$g_k(x) = 1 - \sum_{j=0}^{q-1} a_k^{q-1-j} x^j \tag{5.3}$$

Temos que $g_k(a_k) = 1$ para todo $0 \leq k \leq q-1$. Note que $g_k(b) = 0$ para cada $b \in \mathbb{F}_q$ com $b \neq a_k$. De fato, se $b \neq 0$, por (5.2) obtemos:

$$g_k(b) = 1 - \sum_{j=0}^{q-1} a_k^{q-1-j} b^j = \sum_{j=0}^{q-1} (a_k b^{-1})^j = 1 - \frac{1 - (a_k b^{-1})^q}{1 - (a_k b^{-1})} = 1 - 1 = 0.$$

Além disso, $g_k(0) = 0$ sempre que $a_k \neq 0$. Assim, o polinômio

$$g(x) = \sum_{k=0}^{q-1} g_k(x) = -\sum_{k=0}^{q-1} \left(\sum_{j=0}^{q-1} a_k^{q-1-j} x^j \right) = -\sum_{j=0}^{q-1} \left(\sum_{k=0}^{q-1} a_k^{q-1-j} \right) x^j \tag{5.4}$$

identifica cada elemento de $\mathbb{F}_q$ com 1 se e somente se $\{a_0, a_1, ..., a_{q-1}\} = \mathbb{F}_q$. Como $\deg(g) < q$, o Lema 5.7 mostra que o polinômio g leva cada elemento de $\mathbb{F}_q$ em 1 se e somente se $g(x) = 1$, que é equivalente à condição (ii). □

Teorema 5.10 (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 as duas condições seguintes são válidas.*

(i) f tem exatamente uma raiz 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 $\mathbb{F}_q$. Temos que (i) é satisfeito pelo Lema 5.2. Para (ii), notamos que:

$$f(x)^t \pmod{x^q - x} = \sum_{j=0}^{q-1} b_j^{(t)} x^j \quad \text{onde} \quad b_{q-1}^{(t)} = -\sum_{c \in \mathbb{F}_q} f(c)^t$$

por (5.1). Como $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$, então $\{f(c) \,|\, c \in \mathbb{F}_q\} = \mathbb{F}_q$ e, pelo Lema 5.9, $b_{q-1}^{(q-1)} = 1$ e $b_{q-1}^{(t)} = 0$ para todo $t = 1, ..., q-2$. Logo, a redução de $f(x)^t \pmod{x^q - x}$ tem grau menor ou igual a $q-2$.

Por outro lado, suponhamos que as condições (i) e (ii) sejam satisfeitas. Se f tem exatamente j raízes em $\mathbb{F}_q$, então podemos escrever $\mathbb{F}_q = A \cup (\mathbb{F}_q - A)$ onde A é o conjunto das j raízes de f em $\mathbb{F}_q$, então

$$b_{q-1}^{(q-1)} = -\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -\sum_{b \in A} f(c)^{q-1} - \sum_{c \in \mathbb{F}_q - A} f(c)^{q-1}$$

Para todo $b \in A$ temos que $f(b) = 0$ e, então, $\sum_{b \in A} f(c)^{q-1} = 0$. Além disso, para todo $c \in \mathbb{F}_q - A$ temos que $f(c)^{q-1} = 1$, donde $\sum_{c \in \mathbb{F}_q - A} = q - j$. Logo,

$$b_{q-1}^{(q-1)} = -(q-j) = j$$

com $0 \leq j \leq q-1$. Assim, temos que $b_{q-1}^{(q-1)} = 1$ se e somente se $j = 1$. Então, (i) implica $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1$ e, pela condição, (ii) temos que $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para $1 \leq t \leq q-2$, $t \not\equiv 0 \pmod{p}$. Agora, usando o seguinte fato

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

temos que $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ para todo $1 \leq t \leq q-2$, e essa identidade é trivial para $t = 0$. Segue então do Lema 5.9 que f é um polinômio de permutação de $\mathbb{F}_q$. □

Veremos aplicações desse critério nas seções subsequentes.

Corolário 5.11. *Seja $d > 1$ um divisor de $q-1$. Não existe polinômio de permutação de $\mathbb{F}_q$ de grau d.*

Demonstração. Se $f \in \mathbb{F}_q[x]$ tem grau d, então $\deg(f^{(q-1)/d}) = q-1$ e, assim, a condição (ii) do Critério de Hermite não é satisfeita para $t = (q-1)/d$. □

Observação 5.12. *Na seção 4.2, nos debruçamos sobre o problema de contagem do número de polinômios irredutíveis de certo grau em um corpo finito $\mathbb{F}_q$. Em [7], Lidl e Mullen propuseram 9 problemas e conjecturas sobre polinômios de permutação sobre corpos finitos. Um desse problemas era: fixados $\mathbb{F}_q$ e $d > 0$, determinar $P_q(d)$ o número de polinômios de permutação de grau d sobre $\mathbb{F}_q$. Para alguns valores de d esse número é trivial. Por exemplo, claro que $P_q(1) = q(q-1)$ e, pelo Corolário 5.11, $P_q(d) = 0$ se $d > 1$ é um divisor de $q-1$. Além disso*

$$\sum_{\substack{1 \leq d < q-1 \\ d \nmid q-1}} P_q(d) = q!.$$

No entanto, não existe, até o momento, uma fórmula fechada para o número de polinômios de permutação de $\mathbb{F}_q$ de grau fixo d. Alguns resultados para graus específicos podem ser encontrados em [2] e [5].

Um critério para polinômios de permutação também pode ser dado usando caracteres aditivos dos corpos finitos, apresentados no Capítulo 5.

Teorema 5.13. *O polinômio $f \in \mathbb{F}_q[x]$ permuta $\mathbb{F}_q$ se e somente se*

$$\sum_{c\in\mathbb{F}_q} \chi(f(c)) = 0\,. \tag{5.5}$$

para todo caracter aditivo não trivial χ de $\mathbb{F}_q$.

Demonstração. Se f é um polinômio de permutação de $\mathbb{F}_q$ e χ é um caracter aditivo não trivial de $\mathbb{F}_q$, então

$$\sum_{c\in\mathbb{F}_q} \chi(f(c)) = \sum_{c\in\mathbb{F}_q} \chi(c) = 0\,.$$

Por outro lado, seja χ_0 o caracter aditivo trivial de $\mathbb{F}_q$. Como (3.4) é válido para todo $\chi \neq \chi_0$, então, por (3.9), para qualquer $a \in \mathbb{F}_q$ o número N de soluções de $f(x) = a$ em $\mathbb{F}_q$ é dado por

$$N = \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\chi}\chi(f(c))\overline{\chi(a)} = 1 + \frac{1}{q}\sum_{\chi\neq\chi_0}\overline{\chi(a)}\sum_{c\in\mathbb{F}_q}\chi(f(c)) = 1.$$

Portanto, f é um polinômio de permutação de $\mathbb{F}_q$ pelo Lema 5.2. □

Para encerrar essa seção, notamos que a noção de polinômio de permutação em $\mathbb{F}_q$ pode passar de forma análoga para os anéis $\mathbb{Z}_m$. Nesse caso, dizemos que $f(x)$ é um polinômio de permutação módulo m se $f(x)$ permuta $\mathbb{Z}_m$. Tendo isso em mente, apresentamos um critério que será usado na seção 5.4.

Teorema 5.14. *O polinômio $g(x)$ é um polinômio de permutação módulo p^e para $e > 1$ se e somente se é um polinômio de permutação módulo p e $g'(x)$ não se anula módulo p.*

Demonstração. Vamos proceder por indução em e. Suponhamos que $g(x)$ seja um polinômio de permutação módulo p^{e-1}. Então para cada λ, $g(x) - \lambda \equiv 0 \pmod{p^{e-1}}$ tem exatamente uma solução s módulo p^{e-1}. Como todas as soluções de $g(x) - \lambda \equiv 0 \pmod{p^{e-1}}$ são do tipo $x = s + yp^{e-1}$, temos pela fórmula de Taylor

$$p^{e-1}y(g'(s) - \lambda) \equiv \lambda - g(s) \pmod{p^e}\,,$$

que é satisfeito se e somente se

$$y(g'(s) - \lambda) \equiv (\lambda - g(s))/p^{e-1} \pmod{p} \tag{5.6}$$

Como $g(s) - \lambda \equiv 0 \pmod{p^{e-1}}$, segue que $\lambda \equiv g(s) \pmod{p}$, donde, por hipótese, $g'(s) - \lambda \equiv g'(s) - g(s) \not\equiv 0 \pmod{p}$. Assim, (5.6) tem exatamente uma solução y módulo p e, consequentemente, $g(x) - \lambda \equiv 0 \pmod{p^e}$ tem exatamente uma solução módulo p^e.

Por outro lado, se $g(x)$ é um polinômio de permutação módulo p^e, então também é módulo p e p^{e-1}. Suponhamos que $g'(s) - g(s) \equiv 0 \pmod{p}$ para algum s. Escolhendo

$\lambda = g(s)$, temos que s é a única solução de $g(x) - \lambda \equiv 0 \pmod{p^{e-1}}$, donde todas as soluções de $g(x) - \lambda \equiv 0 \pmod{p^{e-1}}$ são $x = s + yp^{e-1}$. Assim, (5.6) deve ter exatamente p soluções módulo p e, então, $g(x) - \lambda \equiv 0 \pmod{p^e}$ tem exatamente p soluções módulo p^e, o que é uma contradição. □

5.2 CLASSES ELEMENTARES DE POLINÔMIOS DE PERMUTAÇÃO

Nessa seção, veremos alguns exemplos de polinômios de permutação utilizando a definição 5.1, o lema 5.2 e o Critério de Hermite (Teorema 5.10). Nossa principal referência aqui é, novamente, [9].

Teorema 5.15. *Todo polinômio linear $ax + b \in \mathbb{F}_q[x]$ com $a \neq 0$ é um polinômio de permutação de $\mathbb{F}_q$.*

Demonstração. Seja $f(x) = ax + b \in \mathbb{F}_q[x]$, onde $a \neq 0$. Para todos $c_1, c_2 \in \mathbb{F}_q$, temos que

$$f(c_1) = f(c_2) \Leftrightarrow ac_1 + b = ac_2 + b \Leftrightarrow ac_1 = ac_2 \Leftrightarrow ac_1 - ac_2 = 0 \Leftrightarrow a(c_1 - c_2) = 0$$

Como $a \neq 0$, segue que $c_1 - c_2 = 0$. Logo, $f(x) = c$ tem uma única solução para cada $c \in \mathbb{F}_q$ e o resultado segue do Lema 5.2. □

Observação 5.16. *Segue do Lema 5.6 e do Teorema 5.15 que se $f \in \mathbb{F}_q[x]$ é um polinômio de permutação de $\mathbb{F}_q$ e $a, b, c \in \mathbb{F}_q$, então $g(x) = a\,f(x + c) + b$ ainda é um polinômio de permutação de $\mathbb{F}_q$.*

Teorema 5.17. *O monômio x^n é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $mdc(n, q - 1) = 1$.*

Demonstração. x^n é um polinômio de permutação de $\mathbb{F}_q$ se e somente se a função $f : \mathbb{F}_q^* \to \mathbb{F}_q^*$ dada por $x \mapsto x^n$ é sobrejetora. Seja g um elemento primitivo do grupo $\mathbb{F}_q^*$, então a imagem de $\mathbb{F}_q^*$ pela função f é o subgrupo cíclico gerado por g^n. Esse subgrupo é o próprio $\mathbb{F}_q^*$ se e somente se g^n é um elemento primitivo de $\mathbb{F}_q^*$, o que é equivalente a $\text{mdc}(n, q - 1) = 1$. De fato, em um grupo cíclico finito de ordem m, o elemento a^k gera um subgrupo de ordem $\dfrac{m}{\text{mdc}(k, m)}$. □

Definição 5.18. *Um polinômio da forma*

$$L(x) = \sum_{i=0}^{m} a_i x^{q^i} = a_0 x + a_1 x^q + \cdots + a_n x^{q^n}$$

com coeficientes em uma extensão $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ é chamado um $q-$polinômio sobre $\mathbb{F}_{q^m}$.

Tais polinômios são também conhecidos como polinômios linearizados, cujo nome deriva de suas propriedades:

1. $L(\beta+\gamma) = L(\beta) + L(\gamma)$ para todos $\beta, \gamma \in \mathbb{F}_{q^m}$.

2. $L(c\beta) = cL(\beta)$ para todos $c \in \mathbb{F}_q$ e $\beta \in \mathbb{F}_{q^m}$.

Considerando $\mathbb{F}_{q^m}$ como um espaço vetorial sobre $\mathbb{F}_q$, então essas propriedades mostram que $L(x)$ é um operador linear em $\mathbb{F}_{q^m}$.

Teorema 5.19. *Seja $\mathbb{F}_q$ de característica p. Então o $p-$polinômio*

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

é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $L(x)$ só possui o 0 como raiz em $\mathbb{F}_q$.

Demonstração. Temos que 0 é uma raiz de $L(x)$. Assim, se $L(x)$ é um polinômio de permutação, não pode existir uma outra solução para $L(x) = 0$ além do 0. Por outro lado, se $L(x)$ possui somente 0 como raiz em $\mathbb{F}_q$, então

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

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

Uma aplicação direta do Critério de Hermite (Teorema 5.10) é utilizada para estudar a seguinte classe de polinômios de permutação:

Teorema 5.20. *Sejam $r \in \mathbb{N}$ com $mdc(r, q-1) = 1$ e s um divisor positivo de $q-1$. Seja $g \in \mathbb{F}_q[x]$ tal que $g(x^s)$ não tem raiz 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. Vamos mostrar que f satisfaz as condições (i) e (ii) do Critério de Hermite.

Primeiro, temos que a única raiz possível para f é 0, uma vez que $g(x^s)$ não possui raiz não nula.

Agora, seja $t \in \mathbb{Z}$ com $1 \leq t \leq q-2$ e suponhamos que t não seja divisível por s. Assim, todos expoentes de $f(x)^t$ são da forma $rt + ms$, para algum inteiro positivo m. Como s é um divisor positivo de $q-1$ e $\text{mdc}(r, q-1) = 1$, então $\text{mdc}(r, s) = 1$. Logo, nenhum dos expoentes de $f(x)^t$ é divisível por s e, consequentemente, nenhum desses expoentes é divisível por $q-1$. Então, não existem termos da forma $x^{i(q-1)}$ na expressão de $f(x)^t$, donde a redução de $f(x)^t \pmod{x^q - x}$ tem grau $\leq q-2$.

Como segundo caso, suponhamos agora que $t = ks$ para algum inteiro positivo k. Temos que

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

Seja $h(x) = x^{rt}$. Temos que $f(c)^t = h(c)$ para todo $c \in \mathbb{F}_q^*$, pois $g(c^s) = 1$ se $c \neq 0$ e $f(0)^t = h(0)$. Então, pelo Lema 5.7,

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

e, como rt não é divisível por $q-1$, a redução de $f(x)^t \pmod{x^q - x}$ tem grau $\leq q-2$. □

Exemplo 5.21. *Pelo Teorema 5.20, temos que o polinômio* $f(x) = x^3(3x^4 + x^2)^2 = 4x^{11} + x^9 + x^7$ *é um polinômio de permutação de* $\mathbb{F}_5$. *De fato, tomamos no teorema* $r = 3$, $q = 5$ *e* $s = 2$. *Além disso,* $g(x) = 3x^2 + x$ *é tal que* $g(x^2) = 3x^4 + x^2$ *não possui raiz não nula em* $\mathbb{F}_5$.

5.3 POLINÔMIOS DA FORMA $x^{\frac{q+1}{2}} + ax$ E OUTROS RELACIONADOS

Nessa seção, consideramos q ímpar e apresentamos uma classificação completa dos polinômios de permutação de $\mathbb{F}_q$ da forma $x^{\frac{q+1}{2}} + ax$.

Seja η o caracter quadrático de $\mathbb{F}_q$:

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

Lema 5.22. *Para* q *ímpar e* $c \in \mathbb{F}_q^*$ *temos*

$$c^{\frac{q-1}{2}} = \begin{cases} 1, & \textit{se } c \textit{ é um quadrado} \\ -1, & \textit{se } c \textit{ é um não quadrado} \end{cases}.$$

Demonstração. Para todo $c \in \mathbb{F}_q^*$, temos que $c^{q-1} - 1 = 0$. Assim,

$$0 = c^{q-1} - 1 = (c^{\frac{q-1}{2}} - 1)(c^{\frac{q-1}{2}} + 1)\,,$$

donde

$$c^{\frac{q-1}{2}} = 1 \text{ ou } c^{\frac{q-1}{2}} = -1$$

Agora, se $c = x^2$ para algum $x \in \mathbb{F}_q^*$, segue que

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

Ainda, notamos que o único subgrupo de ordem $(q-1)/2$ de $\mathbb{F}_q^*$ é o formado pelos quadrados não nulos de $\mathbb{F}_q^*$. Dessa forma, se c não é um quadrado em $\mathbb{F}_q^*$, devemos ter $c^{\frac{q-1}{2}} = -1$. □

Teorema 5.23. *Seja* q *ímpar. O polinômio* $f(x) = x^{\frac{q+1}{2}} + ax \in \mathbb{F}_q[x]$ *é um polinômio de permutação de* $\mathbb{F}_q$ *se e somente se* $\eta(a^2 - 1) = 1$.

Demonstração. Vamos mostrar que a função $x \mapsto f(x)$ não é injetiva se e somente se $\eta(a^2-1) \neq 1$.

Se existe $c \in \mathbb{F}_q^*$ 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, $\eta(a^2-1) = 0$.

Se existem $b, c \in \mathbb{F}_q^*$ distintos tais que $f(b) = f(c) \neq 0$, então

$$(b^{\frac{q+1}{2}} + ab) = (c^{\frac{q+1}{2}} + ac)$$

$$\Rightarrow 1 = (c^{\frac{q+1}{2}} + ac)(b^{\frac{q+1}{2}} + ab)^{-1}$$

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

$$\Rightarrow bc^{-1} = (c^{\frac{q-1}{2}} + a)(b^{\frac{q-1}{2}} + a)^{-1}$$

Pelo Lema 5.22, se tivéssemos $\eta(b) = \eta(c)$, então $b^{\frac{q-1}{2}} = c^{\frac{q-1}{2}}$ e, assim, $b = c$, o que é uma contradição. Portanto, $\eta(b) \neq \eta(c)$. Sem perda de generalidade suponhamos $\eta(b) = -1$ 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 $\eta(a^2-1) = -1$. No primeiro caso, temos $a = \pm 1$ e, assim, existe $c \in \mathbb{F}_q^*$ tal que $c^{\frac{q-1}{2}} = -a$. Logo, $f(c) = f(0)$. Se $\eta(a^2-1) = -1$, seja $b = (a+1)(a-1)^{-1}$. Então, $\eta(b) = -1$ e $b^{\frac{q-1}{2}} = -1$. Portanto

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

com $b \neq 1$. Em ambos os caso, $x \mapsto f(x)$ não é injetiva. □

Para que possamos demonstrar o próximo teorema são necessários a definição e o Lema a seguir:

Definição 5.24. *Seja p um número primo. Definimos $E_p(r)$ como o maior expoente j tal que p^j divide $r \in \mathbb{N}$. Além disso, dado $t \in \mathbb{R}$, denotamos por $\lfloor t \rfloor$ o maior inteiro menor ou igual a t.*

Lema 5.25. *Sejam $m \in \mathbb{Z}_+$ e p primo. Então:*

$$E_p(m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor = \frac{m-s}{p-1}$$

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

Demonstração. Ver [9] (Lema 6.39, p.296). □

Teorema 5.26. *Sejam q ímpar e $r > 1$. O polinômio $f(x) = x^{\frac{q+1}{2}} + ax \in \mathbb{F}_q^*[x]$ não é um polinômio de permutação de $\mathbb{F}_{q^r}$.*

Demonstração. Se r é par, então

$$q^r - 1 = k\left(\frac{q+1}{2}\right),$$

onde $k = 2(q^r - 1 + q^r - 2 + ... + q + 1)$, ou seja, $\dfrac{q+1}{2}$ divide $q^r - 1$ e daí o resultado segue do Cololário 5.11.

Se r é ímpar, definindo $m = \frac{q-1}{2}$, temos que $q^r \equiv -1 \pmod{m+1}$, de modo que existe $k \in \mathbb{Z}_+$ tal que $q^r = k(m+1) + m$, pois $m \equiv 1 \pmod{m+1}$. Notamos ainda que

$$k(m+1) \equiv m+1 \pmod{q} \quad \text{e} \quad \text{mdc}(m+1, q) = 1,$$

o que implica $k \equiv 1 \pmod{q}$. Pelo Critério de Hermite, devemos mostrar que existe t com $1 \leq t \leq q^r - 2, t \not\equiv 0 \pmod{p}$ tal que a redução

$$(x^{m+1} + ax)^t \pmod{x^{q^r} - x}$$

tem grau $q^r - 1$. Seja $t = k + m - 1$, temos

$$(x^{m+1} + ax)^{k+m-1} \pmod{x^{q^r} - x}$$

Agora, pelo desenvolvimento do binômio de Newton, temos que

$$\begin{aligned}
(x^{m+1} + ax)^{k+m-1} &= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} (ax)^j (x^{(m+1)})^{(k+m+j-1)} \\
&= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{(m+1)(k+m-j-1)+j} \\
&= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{mk+m^2-mj-m+k+m-j-1+j} \\
&= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{k(m+1)+m^2-jm-1+m-m} \\
&= \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{q^r+m^2-jm-1-m}
\end{aligned}$$

Para $j \geq m$, os expoentes correspondentes de x são $\leq q^r - 2$. Para $j \leq m-2$, os expoentes correspondentes de x são $\geq q^r$ e $\leq 2q^r - 3$, de modo que após a redução desses termos $(\text{mod } x^{q^r} - x)$ obtemos monômios de grau $\leq q^r - 2$. O único termo restante é o mesmo para $j = m - 1$, a saber

$$\binom{k+m-1}{m-1} a^{m-1} x^{q^r-1}.$$

Basta então mostrar que o coeficiente binomial acima não é divisível pela característica p de $\mathbb{F}_q$. Se s_n denota a soma de dígitos na representação de n na base p, então

$$k \equiv 1 \pmod{q}, \quad m < q \quad \text{e} \quad m \not\equiv q \pmod{p}$$

implicam que $s_{k+m-1} = s_{m-1} + s_k$. Então, pelo Lema 5.25

$$E_p\left(\binom{k+m-1}{m-1}\right) = \frac{1}{p-1}(s_{m-1} + s_k - s_{k+m-1}) = 0$$

que é o que desejávamos. □

O Teorema 5.26 sugere que polinômios sobre $\mathbb{F}_q$ que são polinômios de permutação de todas as extensões finitas de $\mathbb{F}_q$ provavelmente são raros. De fato, os polinômios com essa propriedade podem ser classificados completamente e tem, de fato, uma forma especial.

Teorema 5.27. *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 for 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. Primeiramente, notamos que se f é um polinômio de permutação de $\mathbb{F}_q$, então para todo $c \in \mathbb{F}_q$ a equação $f(x) = c$ tem uma única solução $d \in \mathbb{F}_q$. Portanto

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

onde $k \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ e $\deg g = 0$ ou g é um produto de polinômios irredutíveis g_i em $\mathbb{F}_q[x]$ com $\deg g_i \geq 2$. Assim, supondo que g é um produto de polinômios irredutíveis g_i em $\mathbb{F}_q[x]$ com $\deg g_i \geq 2$ temos que se r é um múltiplo do grau de algum g_i, então g_i tem uma raiz em $\mathbb{F}_{q^r}$ e, portanto, f não é um polinômio de permutação em $\mathbb{F}_{q^r}$. Então, devemos ter $\deg g = 0$, e portanto,

$$f(x) - c = a(x - d)^k \tag{5.7}$$

com $a \neq 0$, isto é, para cada $c \in \mathbb{F}_q$ existe $d \in \mathbb{F}_q$ dependendo de c tal que essa identidade é válida. Escolhendo $c = 0$, temos $f(x) = a(x - d_0)^k$ e, escolhendo $c = 1$, temos $f(x) = a(x - d_1)^k + 1$. Assim, obtemos

$$a(x - d_0)^k - a(x - d_1)^k = 1$$

e substituindo x por $x + d_1$, obtemos

$$a(x + d_1 - d_0)^k + ax^k = 1\,.$$

Expandindo, temos

$$\binom{k}{j} \equiv 0 \pmod{p} \tag{5.8}$$

para $0 < j < k$. Temos $p^h \leq k < p^{h+1}$ para algum $h \in \mathbb{Z}, h \geq 0$. Se $k \neq p^h$, então pelo Lema 5.25, temos $j = p^h$ e

$$E_p\left(\binom{k}{j}\right) = \frac{1}{p-1}(s_j + s_{k-j} - s_k) = 0\,, \tag{5.9}$$

onde s_n denota a soma dos dígitos na representação de n na base p. Como isso contradiz (5.8), devemos ter $k = p^h$ e o restante segue de (5.7).
Por outro lado, seja $\mathbb{F}_{q^r}$ uma extensão finita de $\mathbb{F}_q$. Se $c = a^{-1}b$ então temos

$$f(x) = ax^{p^h} + b = a(x^{p^h} + c) = a(x + c)^{p^h}.$$

Então, $f(x) = h \circ g(x)$, onde $g(x) = x + c$ é um polinômio de permutação de $\mathbb{F}_{q^r}$ pelo Teorema 5.15 e $h(x) = ax^{p^h}$ é um polinômio de permutação de $\mathbb{F}_{q^r}$ pelo Teorema 5.19. Portanto, $f(x)$ é um polinômio de permutação de $\mathbb{F}_{q^r}$. □

Corolário 5.28. *Se $f \in \mathbb{F}_q[x]$ não é da forma $f(x) = ax^{p^h} + b$, então existem infinitas extensões $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ tais que f não é um polinômio de permutação de $\mathbb{F}_{q^m}$.*

5.4 POLINÔMIOS DE DICKSON

Vamos introduzir agora uma classe especial de polinômios chamados polinômios de Dickson, que possui algumas propriedades interessantes e também produz novos exemplos de polinômios de permutação.

Sejam x_1, x_2 indeterminadas e $k \in \mathbb{N}$. Então, em [9] (ver Teorema 5.46) temos a Fórmula de Waring:

$$x_1^k + x_2^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-x_1x_2)^j(x_1 + x_2)^{k-2j}\,. \tag{5.10}$$

Isso é válido para qualquer anel comutativo R com identidade. Para $a \in R$ definimos o polinômio de Dickson $g_k(x, a)$ sobre R por

$$g_k(x, a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j}\,. \tag{5.11}$$

Se considerarmos o polinômio de Dickson sobre um corpo K, então no corpo das funções racionais sobre K em y temos a identidade

$$g_k\left(y + \frac{a}{y}, a\right) = y^k + \frac{a^k}{y^k} \tag{5.12}$$

a qual segue de (5.10) substituindo $x_1 = y, x_2 = \dfrac{a}{y}$. De fato,

$$\begin{aligned} y^k + \frac{a^k}{y^k} &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}\left(-y\frac{a}{y}\right)^j\left(y + \frac{a}{y}\right)^{k-2j} \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-a)^j\left(y + \frac{a}{y}\right)^{k-2j} = g_k\left(y + \frac{a}{y}, a\right)\,. \end{aligned}$$

A definição de polinômios de Dickson gera também a fórmula

$$\begin{aligned} g_k(x, ab^2) &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-ab^2)^j x^{k-2j} \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-ab^{k-k+2})^j x^{k-2j} \\ &= \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j b^k b^{-(k-2j)} x^{k-2j} \\ &= b^k \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j (b^{-1}x)^{k-2j} \\ &= b^k g_k(b^{-1}x, a). \end{aligned} \tag{5.13}$$

para quaisquer $a, b \in F$ com $b \neq 0$. Portanto, se $F = \mathbb{F}_q$, q par, então todo polinômio $g_k(x, a)$ com $a \in \mathbb{F}_q^*$ pode ser expressado em termos de $g_k(x, 1)$. Se $F = \mathbb{F}_q$, q ímpar, então todo polinômio de Dickson $g_k(x, a), a \in \mathbb{F}_q^*$, pode ser expressado em termos de $g_k(x, 1)$ ou $g_k(x, c)$, sendo c um não quadrado fixo.

Teorema 5.29. *O polinômio de Dickson $g_k(x, a), a \in \mathbb{F}_q^*$, é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $mdc(k, q^2 - 1) = 1$.*

Demonstração. Suponha $g_k(b, a) = g_k(c, a)$ para algum $b, c \in \mathbb{F}_q$. Assim como em 5.12, existem $\beta, \gamma \in \mathbb{F}_q^*$ tais que $\beta + a\beta^{-1} = b$ e $\gamma + a\gamma^{-1} = c$. Então, temos que

$$g_k(\beta + a\beta^{-1}, a) = g_k(\gamma + a\gamma^{-1}) \Leftrightarrow \beta^k + a^k\beta^{-k} = \gamma^k + a^k\gamma^{-k}.$$

Portanto,

$$\begin{aligned} &\beta^k + a^k\beta^{-k} - \gamma^k - a^k\gamma^{-k} = 0 \\ \Rightarrow\ &\beta^k\gamma^k(\beta^k + a^k\beta^{-k} - \gamma^k - a^k\gamma^{-k}) = 0 \\ \Rightarrow\ &\beta^k\beta^k\gamma^k + a^k\gamma^k - \beta^k\gamma^k\gamma^k - a^k\beta^k = 0 \\ \Rightarrow\ &(\beta^k - \gamma^k)(\beta^k\gamma^k - a^k) = 0 \end{aligned}$$

donde $\beta^k = \gamma^k$ ou $\beta^k = (a\gamma^{-1})^k$. Se $\text{mdc}(k, q^2 - 1) = 1$, então x^k é um polinômio de permutação de $\mathbb{F}_{q^2}$ pelo Teorema 5.17, o que implica $\beta = \gamma$ ou $\beta = a\gamma^{-1}$. Em ambos os casos, segue que $b = c$, e portanto $g_k(x, a)$ é um polinômio de permutação de $\mathbb{F}_q$.
Agora, suponhamos que $\text{mdc}(k, q^2 - 1) = d > 1$. Se d é par, então q é ímpar e k é par. Como (5.11) mostra que $g_k(x, a)$ contém somente potências pares de x, temos que $g_k(c, a) = g_k(-c, a)$ para $c \in \mathbb{F}_q^*$. Mas $c \neq -c$, logo $g_k(x, a)$ não pode ser um polinômio de permutação de $\mathbb{F}_q$. Se d é ímpar, então existe um primo ímpar r dividindo d. Então r divide k e $q - 1$ ou $q + 1$ é divisível por r. No primeiro caso, a equação $x^r = 1$ tem r

soluções em $\mathbb{F}_q$, portanto existe $b \in \mathbb{F}_q, b \neq 1, a$, com $b^r = 1$. Ainda, $b^k = 1$ e, então, (5.12) implica que

$$g_k(b + ab^{-1}, a) = 1 + a^k = g_k(1 + a, a).$$

Como $b + ab^{-1}$ implicaria $b = 1$ ou $b = a$, temos que $b + ab^{-1} \neq 1 + a$ e, assim, $g_k(x, a)$ não é um polinômio de permutação de $\mathbb{F}_q$. No segundo caso, seja $\gamma \in \mathbb{F}_q$ uma solução de $x^{q+1} = a$. Como $x^r = 1$ tem r soluções em $\mathbb{F}_{q^2}$, existe $\beta \in \mathbb{F}_{q^2}$ com $\beta \neq 1, a\gamma^{-2}$ e $\beta^r = 1$. Então, temos também $\beta^{q+1} = 1$ e $\beta^k = 1$. Consequentemente,

$$g_k(\gamma + a\gamma^{-1}, a) = g_k(\beta\gamma + a(\beta\gamma)^{-1}, a)$$

por (5.12). Além disso, $\gamma + a\gamma^{-1} = \gamma + \gamma^q \in \mathbb{F}_q$ e $\beta\gamma + a(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^q \in \mathbb{F}_q$. Assim, como $\beta\gamma + a(\beta\gamma)^{-1} \neq \gamma + a\gamma^{-1}$, para o contrário $\beta = 1$ ou $\beta = a\gamma^{-2}$. Portanto, $g_k(x, a)$ não é um polinômio de permutação. □

Exemplo 5.30. *Pelo Teorema 5.29, como* $mdc(5, 48) = 1$*, temos que* $g_5(x, 2) = x^5 + 4x^3 + 6x$ *é um polinômio de permutação de* $\mathbb{F}_7$*.*

Exemplo 5.31. *O polinômio de Dickson* $g_4(x, 1) = x^4 + x^2$ *não é um polinômio de permutação de* $\mathbb{F}_5$*. De fato,* $mdc(4, 24) \neq 1$ *e, ainda,* $g_4(0, 1) = g_4(2, 1) = 0$*, donde a função polinomial não é injetora.*

Observação 5.32. *Uma questão interessante dos polinômios de Dickson é que eles generalizam os polinômios do tipo* x^k*. De fato,* $g_k(x, 0) = x^k$*, que é, pelo Teorema 5.17, um polinômio de permutação de* $\mathbb{F}_q$ *se e somente se* $mdc(k, q-1) = 1$*. Por outro lado, se* $a \neq 0$*, então* $g_k(x, a)$ *é um polinômio de permutação de* $\mathbb{F}_q$ *se e somente se* $mdc(k, q^2 - 1) = 1$*.*

Lema 5.33. *O polinômio de Dickson* $g_k(x, a), a \in R$*, satisfaz a seguinte propriedade:*

$$g_{k\ell}(x, a) = g_k(g_\ell(x, a), a^\ell).$$

Demonstração. Seja $x = y + \frac{a}{y}$, então

$$g_{k\ell}(x, a) = y^{k\ell} + \left(\frac{a}{y}\right)^{k\ell} = g_k\left(y^\ell + \left(\frac{a}{y}\right)^\ell, a^\ell\right) = g_k(g_\ell(x, a), a^\ell).$$

□

Lema 5.34. *Sejam* $a \neq 0$ *e* $g_k(x, a)$ *um polinômio de Dickson que é um polinômio de permutação em* $\mathbb{F}_q$*. Então, a derivada* $g'_k(x, a)$ *não se anula em* $\mathbb{F}_q$ *se e somente se* $mdc(k, q) = 1$*.*

Demonstração. Começamos supondo $\text{mdc}(k, q) = 1$ e $k > 1$. Seja $x = y + a/y$, onde $y \in \mathbb{F}_{q^2}^*$. Então:

$$g'_k(y + a/y, a) = \frac{k(y^{2k} - a^k)}{y^{k-1}(y^2 - a)}. \tag{5.14}$$

Basta então provar que $\dfrac{y^{2k}-a^k}{y^2-a}$ não tem raízes em F_{q^2}. Seja $h(y)=y^{2k}-a^k$. Se existe uma raiz de $h(y)$, como $h'(y)=2ky^{2k-1}$, vamos provar que essa raiz é simples e também satisfaz $y^2-a=0$. Se q é ímpar, $\text{mdc}(h'(y),h(y))=1$, donde $h(y)$ só tem raízes simples. O mesmo ocorre com y^2-a. Como $g_k(x,a)$ é um polinômio de permutação, segue do Teorema 5.29 que $\text{mdc}(k,q^2-1)=1$, donde y^k permuta $\mathbb{F}_{q^2}$ pelo Teorema 5.17. Isso significa que se $\beta^{2k}=a^k$, então $\beta^2=a$, ou seja, β é raiz de $\dfrac{y^{2k}-a^k}{y^2-a}$. Agora, se q é par, temos

$$\frac{y^{2k}-a^k}{y^2-a}=\left(\frac{y^k-\beta^k}{y-\beta}\right)^2,$$

onde $\beta^2=a$. Como $\text{mdc}(k,q^2-1)=1$, a única raiz de $t(y)=y^k-\beta^k$ é $y=\beta$, que é uma raiz simples pois $t'(y)=ky^{k-1}$.

Por outro lado, se $\text{mdc}(k,q)\neq 1$, segue de (5.14) que $g_k'(x,a)$ é zero em todo elemento de $\mathbb{F}_q$. □

Usando o Teorema 5.14 e o Lema 5.34, temos o seguinte resultado

Teorema 5.35. *Sejam $p_1,\ldots,p_r$ primos distintos, $m>1$ com fatoração $m=p_1^{e_1}p_2^{e_2}\ldots p_r^{e^r}$ e $a\neq 0$ tal que $mdc(a,m)=1$. O polinômio $g_k(x,a)$ é um polinômio de permutação módulo m se e somente se $mdc(k,p_i^{e_i-1}(p_i^2-1))=1$ para todos $i=1,\ldots,r$.*

5.4.1 Aplicações em criptografia

Nessa subseção, apresentamos aplicações dos polinômios de Dickson como extensão de protocolos estabelecidos da criptografia RSA. Para isso, utilizamos a referência [6].

A criptologia é a ciência das comunicações seguras, tendo como áreas a criptografia e a criptoanálise: criptografia está preocupada, principalmente, em projetar criptossistemas e cifras; equanto a criptanálise preocupa-se com ataques e quebra de cifras.

O criptossistema de chave pública mais conhecido é a criptografia RSA devido a Ronald Rivest, Adi Shamir e Leonard Adleman. Aqui, A quer enviar a B uma mensagem $m\in\mathbb{Z}_n$ através de um canal de comunicação inseguro. O módulo n é conhecido publicamente e é o produto de dois primos grandes p e q, que são mantidos em segredo. O expoente de codificação e_B de B é conhecido publicamente e satisfaz $\text{mdc}(e_B,\phi(n))=1$, onde ϕ denota a função de Euler. A codifica a mensagem calculando $c\equiv m^{e_B}\pmod n$ e envia isto para B. B conhece os fatores primos p e q de n, então é capaz de encontrar $\phi(n)$ e resolver a congruência linear $e_Bd_B\equiv 1\pmod{\phi(n)}$ para d_B, que é o expoente de decodificação de B. Então, B obtém a mensagem usando d_B, já que

$$c^{d_B}\equiv(m^{e_B})^{d_B}\equiv m\pmod n.$$

Exponenciação em RSA pode ser interpretada como aplicando a função polinomial potência, ou simplemente função potência,

$$x \longmapsto x^k \pmod{n}.$$

Quando considerada como uma função de $\mathbb{Z}_n$ ou de $\mathbb{F}_p$, temos que

(*i*) Valores de x^k para $x \in \mathbb{Z}_n$ ou $x \in \mathbb{F}_p$ podem ser facilmente calculados.

(*ii*) As funções potências são fechadas em relação à composição:

$$x^r \circ x^s = x^{rs} = x^{sr} = x^s \circ x^r,$$

isto é, o conjunto $\{x \longmapsto x^k | k \in \mathbb{N}\}$ é um semigrupo comutativo com a operação de composição de funções.

(*iii*) Pelo Teorema 5.17, a função $x \longmapsto x^k$ é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $\text{mdc}(k, q-1) = 1$. Portanto, o semigrupo comutativo

$$\{x \longmapsto x^k | k \in \mathbb{N},\ mdc(k, q-1) = 1\}$$

é um grupo comutativo com a operação de composição. Similarmente, $x \longmapsto x^k$ é uma permutação de $\mathbb{Z}_n$ se e somente se $\text{mdc}(k, \phi(n)) = 1$. A permutação inversa é definida pela função $x \mapsto x^m$ onde $km \equiv 1 \pmod{\phi(n)}$.

Vimos na seção 5.4, que os polinômios de Dickson generalizam algumas propriedades de x^k. Assim, podemos generalizar o sistema RSA usando tais polinômios. Pelo Teorema 5.35, se $n = \prod_{i=1}^{r} p_i^{e_i}$, $a = 1$ e $v(n) = \text{mmc}\{p_i^{e_i-1}(p_i^2 - 1)\}$ para todo $1 = 1, ..., r$, então $g_k(x, a)$ induz uma permutação de $\mathbb{Z}_n$ se e somente se $\text{mdc}(k, v(n)) = 1$. A permutação inversa, nesse caso, é induzida por $g_\ell(x, a)$ onde $k\ell \equiv 1 \pmod{v(n)}$. Notamos que, com a teoria existente, os módulos $v(n)$ só podem ser calculados se a fatoração de n for conhecida, donde a única forma viável conhecida de encontrar o inverso de uma permutação de Dickson módulo $v(n)$ é encontrar a fatoração de n. Se os fatores primos de n são suficientemente grandes, digamos maiores que 10^{100}, essa tarefa é computacionalmente inviável.

Exemplo 5.36 (Criptossistema de Dickson)**.** *Seja $a = 1$ ou -1 em $\mathbb{Z}_n$. Se A quer enviar uma mensagem m para B, A usa a chave pública de codificação e_B de B, com a propriedade $mdc(e_B, v(n)) = 1$, e calcula $c \equiv g_{e_B}(m, a) \pmod{n}$. Para decifrar c, B calcula a chave de decodificação d_B através da congruência linear $e_B d_B \equiv 1 \pmod{v(n)}$ e encontra $g_{d_B}(c, a) \pmod{n}$ que é a mensagem m, pois pelo Lema 5.33*

$$g_{d_B}(c, a) \equiv g_{d_B}(g_{e_B}(m, a), a) \equiv g_{d_B e_B}(m, a) \equiv g_1(m, a) \equiv m \pmod{n}.$$

Observemos que para $n = p_1p_2$, com p_1 e p_2 primos, podemos tomar $v(n)^* = (p_1^2 - 1)(p_2^2 - 1)$ em vez de $v(n)$ como um módulo para encontrar d_B e, nesse caso, o criptossistema Dickson é muito similar à criptografia RSA. Para $a = 0$ e $n = p_1p_2$, obtemos a criptografia RSA.

RSA é uma das poucas criptografias de chave pública que permite o uso de assinatura digital, isto é: o utilizador que possua uma chave privada d poderá assinar uma dada mensagem para dar certeza ao destinatário de que foi enviada pelo remetente correto. Para isso, o remetente usa $s \equiv m^d \pmod{n}$. Assinatura digital também pode ser estabelecida quando a função $x \longrightarrow x^k$ em RSA é substituída por $x \longrightarrow g_k(x, a)$, com $a = \pm 1$.

Exemplo 5.37 (Assinatura Digital)**.** *Sejam n o produto de primos grandes, e_A a chave pública de codificação de A e d_A a chave secreta de decodificação de A. Se A quer enviar uma mensagem m, A envia $g_{d_A}(m, a) \pmod{n} = s$ como uma assinatura para B. B calcula $g_{e_A}(s, a) \equiv g_{e_A}(g_{d_A}(m, a), a) \equiv m \pmod{n}$ e reconhece que isso foi enviado por A, já que apenas A poderia ter conhecimento da chave secreta d_A.*

Alternativamente, A poderia usar o expoente de codificação público e_B de B da seguinte maneira: como antes, A calcula s e envia $g_{e_B}(s, a)$ para B. O receptor conhece a chave secreta d_B, recupera s de $g_{d_B}(g_{e_B}(s, a)) \equiv s \pmod{n}$ e usa a chave pública de A para recuperar m pelo cálculo de $g_{e_A}(s, a) \equiv g_{e_A}(g_{d_A}(m, a)) \equiv m \pmod{n}$.

Encerramos as aplicações com o protocolo de três passagens. A estrutura de um protocolo de três passagens permite que uma parte envie mensagens com segurança para uma segunda parte sem precisar trocar ou distribuir chaves de criptografia e recebe esse nome pois troca três vezes para autenticar o remetente e o destinatário do primeiro protocolo. Foi desenvolvido por Adi Shamir por volta de 1980 (veja [12]).

Na formulação original isso é alcançado usando exponenciação módulo p, que pode ser generalizada da forma a seguir.

Exemplo 5.38. *Em um algoritmo generalizado do protocolo de três passagens A que enviar uma mensagem $m \in \mathbb{F}_p$, p primo, para B. Os seguintes passão são executados:*

(i) A escolhe um inteiro a tal que $mdc(a, p^2 - 1) = 1$, a é mantido em segredo, e envia $y = g_a(m, 1) \pmod{p}$ para B.

(ii) B escolhe um inteiro b tal que $mdc(b, p^2 - 1) = 1$, mantendo b em segredo, e envia $z = g_b(y, 1) \pmod{p}$ para A.

(iii) A calcula a' de modo que $aa' \equiv 1 \pmod{p^2 - 1}$ e envia $g_{a'}(z, 1) \pmod{p}$ para B.

(iv) B obtém $m \pmod{p}$ calculando b' tal que $bb' \equiv 1 \pmod{p^2 - 1}$ e

$$g_{b'}(g_{a'}(g_b(g_a(m, 1), 1), 1), 1) \equiv m \pmod{p}.$$

5.5 POLINÔMIOS DA FORMA $x^r h(x^{(q-1)/d})$

Nessa seção, apresentamos polinômios de permutação de $\mathbb{F}_q$ da forma $x^r h(x^{(q-1)/d})$, onde d é um divisor de $(q-1)$. Esses polinômios foram estudados em [10], [14] e [13].

No que segue, fixamos a seguinte notação:

- μ_d o conjunto das $d-$ésimas raízes da unidade em $\mathbb{F}_q$;
- $(\mathbb{F}_q^*)^s$ o conjunto da $s-$ésimas potências dos elementos de $\mathbb{F}_q^*$;
- para $d \geq 2$, $h_d(x) = x^{d-1} + x^{d-2} + \cdots + x + 1 \in \mathbb{F}_q[x]$.

O seguinte critério, apresentado por Park e Lee em [13] e Zieve em [14] determina se um polinômio dessa forma induz uma permutação em $\mathbb{F}_q$.

Lema 5.39. *Sejam $d, r \in \mathbb{Z}_+^*$, com $d|(q-1)$, e $h \in \mathbb{F}_q[x]$. Fixemos $s = \frac{q-1}{d}$. Então, $f(x) = x^r h(x^s)$ é um polinômio de permutação de $\mathbb{F}_q$ se e somente se as condições a seguir são satisfeitas:*

(i) $mdc\,(r, s) = 1$;

(ii) $g(x) = x^r h(x)^s$ *permuta* μ_d.

Demonstração. Fixado $\zeta \in \mu_s$, então $\zeta^s = 1$, e assim, temos que

$$f(\zeta x) = \zeta^r x^r h(\zeta^s x^s) = \zeta^r x^r h(x^s) = \zeta^r f(x).$$

Portanto, se f permuta $\mathbb{F}_q$ então $\text{mdc}(r, s) = 1$. De fato, suponhamos que f seja um polinômio de permutação de $\mathbb{F}_q$ e seja $\text{mdc}(r, s) = k, k > 1$, então existem $u, v \in \mathbb{Z}_+^*$ tais que $r = uk$ e $s = vk$, e portanto,

$$f(\zeta x) = \zeta^r f(x) = \zeta^{uk} f(x) = \zeta^{\frac{su}{v}} f(x) = (\zeta^s)^{\frac{u}{v}} f(x) = 1 f(x) = f(x),$$

o que é uma contradição pois f é injetivo, logo $\text{mdc}(r, s) = 1$.

Por outro lado, se $\text{mdc}(r, s) = 1$, 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, os valores de $f(x)^s$ em $\mathbb{F}_q$ consistem de $f(0)^s = 0$ e dos valores de $g(x)$ em $(\mathbb{F}_q^*)^s$. Portanto, f permuta $\mathbb{F}_q$ se e somente se g é bijetiva em $(\mathbb{F}_q^*)^s$. Porém, notamos ainda que $(\mathbb{F}_q^*)^s = \mu_d$, pois note que $(\mathbb{F}_q^*)^s = \{x^s | x \in \mathbb{F}_q\}$, temos que $\mu_d \subseteq (\mathbb{F}_q^*)^s$ e, além disso, para todo $x^s \in (\mathbb{F}_q^*)^s$ temos que

$$(x^s)^d = (x^{\frac{q-1}{d}})^d = x^{q-1} = 1,$$

logo $(\mathbb{F}_q^*)^s \subseteq \mu_d$. □

A dificuldade de aplicar o Lema 5.39 é a verificação da condição (ii). A seguir temos uma situação onde isto não é difícil.

Corolário 5.40. *Sejam $d, r, n \in \mathbb{Z}_+^*$, com $d|(q-1)$, e $h \in \mathbb{F}_q[x]$. Fixemos $s = \frac{q-1}{d}$ e suponhamos que $h(\zeta)^s = \zeta^n$ para todo $\zeta \in \mu_d$. Então, $f(x) = x^r h(x^s)$ é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $mdc(r+n, d) = mdc(r, s) = 1$.*

Demonstração. Pelo Lema 5.39, temos que $f(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se e somente se $\text{mdc}(r, s) = 1$ e $g(x) = x^r h(x)^s$ permuta μ_d. Agora, fixado $\zeta \in \mu_d$, temos que

$$g(\zeta) = \zeta^r h(\zeta)^s = \zeta^r \zeta^n = \zeta^{r+n} \in \mu_d \Leftrightarrow \text{mdc}(r+n, d) = 1$$

Assim, o resultado segue pois concluimos que $g(x) = x^r h(x)^s$ permuta μ_d se e somente se $\text{mdc}(r+n, d) = 1$. □

O Lema 5.39 foi usado por Marcos em [10] para estudar outra classe de polinômios de permutação. Apresentamos o resultado a seguir.

Teorema 5.41. *Sejam $3 \leq d < q-1$, com $d|(q-1)$, e $s = (q-1)/d$. Sejam ainda $r \geq 1$, $0 \leq k \leq d-1$ e $b \in \mathbb{F}_q$. O polinômio*

$$g(x) = x^r(h_d(x^s) + bx^{ks}) \in \mathbb{F}_q[x]$$

é um polinômio de permutação de $\mathbb{F}_q$ se e somente se as quatro condições seguintes são satisfeitas:

(i) $b \neq 0$ *e* $d + b \neq 0$ *em* $\mathbb{F}_q$.

(ii) $mdc\,(r, s) = 1$.

(iii) $mdc(r + ks, d) = 1$.

(iv) $\dfrac{d+b}{b}$ *é uma d-ésima potência em $\mathbb{F}_q$.*

Demonstração. Primeiro, notamos que a condição (ii) é a condição (i) do Lema 5.39.

Ainda, pelo mesmo Lema, o polinômio $g(x)$ é um polinômio de permutação de $\mathbb{F}_q$ se e somente se o polinômio

$$\lambda(x) = x^r(h_d(x) + bx^k)^s\,,$$

permuta μ_d. Seja $\omega \in \mu_d$ uma d-ésima raiz primitiva da unidade, ou seja, um gerador de $\mu_d = \{1, \omega, \omega^2, \ldots, \omega^{d-1}\}$.

Suponhamos que as quatro condições são satisfeitas. Para cada $1 \leq i \leq d-1$ temos que

$$\lambda(\omega^i) = \omega^{ir}(b\omega^{ik})^s = b^s(\omega^i)^{r+ks} \tag{5.15}$$

Segue então da condição (iii) que o número de valores assumidos por $\lambda(\omega^i)$ com $1 \leq i \leq d-1$ é exatamente $d-1$. Por outro lado, temos que

$$\lambda(1) = 1^r(h_d(1) + 1^k b)^s = (d+b)^s.$$

Agora, se $\lambda(1) = \lambda(\omega^i)$ para algum $1 \leq i \leq d-1$, então de (5.15) temos a igualdade

$$\left(\frac{d+b}{b}\right)^s = (\omega^i)^{r+ks}. \tag{5.16}$$

Pela condição (iv), o lado esquedo de (5.16) vale 1. Mas, pela condição (iii), o lado direito de (5.16) é diferente de 1. Portanto, $\lambda(1) \neq \lambda(\omega^i)$ para todo $1 \leq i \leq d-1$. Assim, $\lambda(x)$ induz uma permutação no conjunto μ_d.

Agora devemos mostrar que as quatro condições são necessárias para $g(x)$ ser um polinômio de permutação. A condição (ii) é necessária pelo Lema 5.39. A condição (i) é necessária pois se $b = 0$, então $g(\omega) = 0 = g(0)$, e se $d + b = 0$, então $g(1) = 0 = g(0)$. Agora, se $\text{mdc}(r + ks, d) = t > 1$, então $1 < 1 + \dfrac{d}{s} < d$ e $\lambda(\omega) = \lambda(\omega^{1+d/t})$. Ou seja, $\lambda(x)$ não permuta μ_d, o que contradiz o Lema 5.39. Sendo assim, a condição (iii) é necessária.

Finalmente, se as três primeiras condições são satisfeitas mas $\dfrac{d+b}{b}$ não é uma d-ésima potência em $\mathbb{F}_q$, temos que

$$\left(\frac{d+b}{b}\right)^s = \omega^h, 1 \leq h \leq d-1.$$

Seja $1 \leq i \leq d-1$ tal que $h \equiv i(ks + r) \pmod{d}$. Então,

$$\left(\frac{d+b}{b}\right)^s = (\omega^i)^{ks+r},$$

e, portanto, $\lambda(1) = (d+b)^s = \lambda(\omega^i)$. Isto é, $\lambda(x)$ não permuta μ_d. Assim, a condição (iv) também é necessária. □

Exemplo 5.42. *Sejam $d = 6, b = -2, k = 0$ e $r = 1$. Então o polinômio*

$$g(x) = x(x^{15} + x^{12} + x^9 + x^6 + x^3 - 1) \in \mathbb{F}_{19}[x]$$

é um polinômio de permutação de $\mathbb{F}_{19}$. De fato, claramente as três primeiras condições do Teorema 5.41 são satisfeitas e, além disso, $\dfrac{d+b}{b} = \dfrac{6-2}{-2} = -2 \equiv 17 \pmod{19}$ que é uma quarta potência em $\mathbb{F}_{19}$ pois $5^4 \equiv 17 \pmod{19}$.

Notamos que no Teorema 5.41 foi exigido que $3 \leq d < q-1$. Se $d = 2$, as quatro condições do Teorema 5.41 são suficientes para $g(x)$ ser um polinômio de permutação de $\mathbb{F}_q$, mas não são necessárias. O seguinte resultado mostra este fato.

Proposição 5.43. *Seja* $q \equiv 3 \pmod 4$. *O polinômio*

$$g(x) = x^2(x^{(q-1)/2} + 1 + b) \in \mathbb{F}_q[x]$$

é um polinômio de permutação se e somente se $(1+b)^2 - 1$ *não é um quadrado em* $\mathbb{F}_q$, *ou seja, se e somente se* $\dfrac{2+b}{b}$ *não é um quadrado em* $\mathbb{F}_q$.

Demonstração. Pelo Lema 5.39, $g(x)$ é um polinômio de permutação se e somente se

(*i*) $\text{mdc}(2, (q-1)/2) = 1$;

(*ii*) $x^2(x+1+b)^{(q-1)/2}$ permuta $\mu_2 = \{\pm 1\}$.

Temos que $x^2(x+1+b)^{(q-1)/2}$ pemuta $\mu_2 = \pm 1$ se e somente se

$$\{(2+b)^{(q-1)/2}, b^{(q-1)/2}\} = \{\pm 1\}$$

e assim,

$$(2+b)^{(q-1)/2}b^{(q-1)/2} = -1 \Leftrightarrow (2b+b^2)^{(q-1)/2} = -1 \Leftrightarrow ((1+b)^2-1)^{(q-1)/2} = -1.$$

Suponha $(1+b)^2 - 1 = x^2$, onde $x \in \mathbb{F}_q$, então $x^{q-1} = (x^2)^{(q-1)/2} = ((1+b)^2-1)^{(q-1)/d} = -1$. Como $x \in \mathbb{F}_q$ então $x^{q-1} = 1$, donde temos uma contradição. Logo, $(1+b)^2 - 1$ não é um quadrado em $\mathbb{F}_q$. Além disso, $(1+b)^2 - 1$ não é um quadrado em $\mathbb{F}_q$ se e somente se $\dfrac{(1+b)^2-1}{b^2} = \dfrac{2b+b^2}{b} = \dfrac{2+b}{b}$ não é um quadrado em $\mathbb{F}_q$. □

Teorema 5.44. *Sejam* $d, r \in \mathbb{Z}_+^*$ *com* $d|(q-1)$ *e* $s = (q-1)/d$. *Consideramos* $q = q_0^m$ *onde* $q_0 \equiv 1 \pmod d$ *e* $d|m$. *Seja ainda* $h \in \mathbb{F}_{q_0}[x]$. *Então,* $f(x) = x^r h(x^s)$ *é um polinômio de permutação de* $\mathbb{F}_q$ *se e somente se* $mdc(r,s) = 1$ *e* h *não tem raízes em* μ_d.

Demonstração. Se f é um polinômio de permutação de $\mathbb{F}_q$, pelo Lema 5.39, temos que $\text{mdc}(r,s) = 1$. Agora, como para todo $\zeta \in \mathbb{F}_{q_0}$ temos que $\zeta^{q_0-1} = 1$. Além disso, $d|q_0 - 1$, por hipótese, e assim se $\zeta \in \mu_d$, então $\zeta^d = 1$. Portanto $\zeta^{q_0-1} = \zeta^{dk} = 1$. Logo, se $\zeta \in \mu_d$ então $\zeta \in \mathbb{F}_{q_0}$, donde $h(\zeta) \in \mathbb{F}_{q_0}$. Como $f(0) = 0$, então $h(\zeta) \neq 0$, pois f permuta $\mathbb{F}_q$.

Por outro lado, suponhamos que $\text{mdc}(r,s) = 1$ e h não possui raízes em μ_d. Como $q_0 \equiv 1 \pmod d$, temos

$$\frac{q_0^d - 1}{q_0 - 1} = \frac{(q_0-1)(q_0^{d-1} + q_0^{d-2} + q_0 + 1)}{q_0 - 1} = \sum_{i=0}^{d-1} q_0^i \equiv 0 \pmod d$$

Consequentemente, $q_0 - 1$ divide $\dfrac{q_0^d - 1}{d}$, que divide s. Como $d|(q_0-1)$, segue que d divide $\dfrac{q-1}{d}$ e como $\text{mdc}\left(r, \dfrac{q-1}{d}\right) = 1$, temos que $\text{mdc}(r, q-1) = 1$. De fato, se

$\text{mdc}(r, q-1) = n$, então n divide tanto r quanto $(q-1)$. Mas, como $\text{mdc}\left(r, \frac{q-1}{d}\right) = 1$, existem a, b tais que

$$1 = ar + b\frac{q-1}{d},$$

isto é, $d = ard + b(q-1)$. Como d divide $\frac{q-1}{d}$, então n divide $\frac{q-1}{d}$, ou seja, n divide $\text{mdc}\left(r, \frac{q-1}{d}\right)$. Dessa forma, $n = 1$.

Agora, como $h(\zeta) \neq 0$ para todo $\zeta \in \mu_d$ e $q_0 - 1$ divide $\frac{q-1}{d}$, obtemos

$$h(\zeta)^{(q-1)/d} = 1.$$

Dessa forma, o resultado segue do Corolário 5.40 fazendo $n = d$. □

5.6 POLINÔMIOS RELACIONADOS COM A FUNÇÃO TRAÇO

Seja $Tr(x)$ o traço absoluto de $\mathbb{F}_{p^n}$ em $\mathbb{F}_p$, isto é,

$$Tr(x) = x + x^p + x^{p^2} + ... + x^{p^{n-1}}.$$

Ao longo desta seção vamos assumir $n > 1$ e estudar uma classe de polinômios de permutação envolvendo a função traço apresentada por Marcos em [10].

Usaremos o seguinte fato para demonstrar o principal resultado desta seção.

Lema 5.45. *Sejam $L(x) = a_0x + a_1x^p + \cdots + a_{n-1}x^{p^{n-1}} \in \mathbb{F}_p[x]$ um polinômio linearizado e $Tr(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ o polinômio traço. Então para cada $\alpha \in \mathbb{F}_{p^n}$, temos*

$$L(Tr(\alpha)) = Tr(L(\alpha)) = (a_0 + a_1 + \cdots + a_{n-1})Tr(\alpha)$$

Demonstração. Pelas propriedade do traço, temos que $(Tr(\alpha))^{p^i} = Tr(\alpha)$ para todo $0 \leq i \leq n-1$. Assim

$$\begin{aligned} L(Tr(\alpha)) &= a_0Tr(\alpha) + a_1(Tr(\alpha))^p \cdots + a_{n-1}(Tr(\alpha))^{p^{n-1}} \\ &= a_0Tr(\alpha) + a_1Tr(\alpha) \cdots + a_{n-1}(Tr(\alpha)) \\ &= (a_0 + a_1 + ... + a_{n-1})Tr(\alpha). \end{aligned}$$

Por outro lado

$$\begin{aligned} Tr(L(\alpha)) &= Tr(a_0\alpha + a_1\alpha^p + \cdots + a_{n-1}\alpha^{p^{n-1}}) \\ &= Tr(a_0\alpha) + Tr(a_1\alpha^p) + \cdots + Tr(a_{n-1}\alpha^{p^{n-1}}) \\ &= a_0Tr(\alpha) + a_1Tr(\alpha^p) + \cdots + a_{n-1}Tr(\alpha^{p^{n-1}}) \\ &= a_0Tr(\alpha) + a_1Tr(\alpha) + \cdots + a_{n-1}Tr(\alpha) \\ &= (a_0 + a_1 + \cdots + a_{n-1})Tr(\alpha). \end{aligned}$$

Portanto, segue o resultado. □

Agora podemos provar o resultado principal.

Teorema 5.46. *Seja* $L(x) = a_0x + a_1x^p + \cdots + a_{n-1}x^{p^{n-1}} \in \mathbb{F}_p[x]$ *um polinômio linearizado que permuta* $\mathbb{F}_{p^n}$*. Sejam* $h(x) \in \mathbb{F}_p[x], \gamma \in \mathbb{F}_{p^n}$ *e* $k = Tr(\gamma) \in \mathbb{F}_p$*. O polinômio*

$$f(x) = L(x) + \gamma h(Tr(x))$$

permuta $\mathbb{F}_{p^n}$ *se e somente se o polinômio*

$$(a_0 + a_1 + \cdots + a_{n-1})x + kh(x)$$

permuta $\mathbb{F}_p$*.*

Demonstração. Suponhamos que o polinômio $(a_0 + a_1 + \cdots + a_{n-1})x + kh(x)$ permuta $\mathbb{F}_p$. Sejam $\alpha \in \mathbb{F}_{p^n}$ e $i = Tr(\alpha) \in \mathbb{F}_p$. Então $f(\alpha) = L(\alpha) + \gamma h(i)$. É claro que $f(x)$ é injetiva no conjunto

$$T_i = \{\alpha \in \mathbb{F}_{p^n} : Tr(\alpha) = i\}.$$

Agora, sejam $\beta \in \mathbb{F}_{p^n}$ e $j = Tr(\beta) \in \mathbb{F}_p$. Vamos assumir que $f(\alpha) = f(\beta)$, isto é

$$L(\alpha) + \gamma h(i) = L(\beta) + \gamma h(j).$$

Aplicando o traço em ambos os lados da equação acima, temos

$$Tr(L(\alpha) + \gamma h(i)) = Tr(L(\beta) + \gamma h(j))$$

$$Tr(L(\alpha)) + Tr(\gamma h(i)) = Tr(L(\beta)) + Tr(\gamma h(j))$$

$$Tr(L(\alpha)) + h(i)Tr(\gamma) = Tr(L(\beta)) + h(j)Tr(\gamma)$$

$$Tr(L(\alpha)) + kh(i) = Tr(L(\beta)) + kh(j)$$

E, usando o Lema 5.45, obtemos

$$(a_0 + a_1 + \cdots + a_{n-1})Tr(\alpha) + kh(i) = (a_0 + a_1 + \cdots + a_{n-1})Tr(\beta) + kh(j)$$

$$(a_0 + a_1 + \cdots + a_{n-1})i + kh(i) = (a_0 + a_1 + \cdots + a_{n-1})j + kh(j).$$

Por hipótese, temos que $i = j$ uma vez que o polinômio $(a_0 + a_1 + \cdots + a_{n-1})x + kh(x)$ permuta $\mathbb{F}_p$, e, usando o fato de $f(x)$ ser injetiva no conjunto T_i, concluímos que $\alpha = \beta$.

Para o contrário, suponhamos que $f(x)$ permuta $\mathbb{F}_{p^n}$. Se $(a_0+a_1+\cdots+a_{n-1})x+kh(x)$ não é injetivo, então $f(x)$ aplica dois conjuntos T_i e T_j em um conjunto T_a do mesmo tipo, o que é uma contradição, pois $f(x)$ é injetiva. Portanto, $(a_0 + a_1 + \cdots + a_{n-1})x + kh(x)$ deve ser injetivo. □

Corolário 5.47. *Seja* $h(x) \in \mathbb{F}_p[x]$*. O polinômio* $f(x) = x + h(Tr(x))$ *permuta* $\mathbb{F}_{p^n}$ *se e somente se o polinômio x+nh(x) permuta* $\mathbb{F}_p$*.*

Demonstração. Temos que

$$f(x) = x + h(Tr(x)) = L(x) + \gamma h(Tr(x)),$$

onde $L(x) = x$ e $\gamma = 1$. Assim, pelo Teorema 5.20, $f(x)$ permuta $\mathbb{F}_{p^n}$ se e somente se o polinômio $x + Tr(1)h(x)$ permuta $\mathbb{F}_p$. Como $Tr(1) = 1 + 1^p + \cdots + 1^{p^{n-1}} = n$, segue o resultado. □

Corolário 5.48. *Sejam $h(x) \in \mathbb{F}_p[x]$ e $\gamma \in \mathbb{F}_{p^n}$ tal que $Tr(\gamma) = 0$. Então, o polinômio $f(x) = x + \gamma h(Tr(x))$ permuta $\mathbb{F}_{p^n}$.*

Demonstração. Temos que $f(x)$ permuta $\mathbb{F}_{p^n}$ se e somente se $x+0h(x) = x$ é um polinômio de permutação em $\mathbb{F}_p$, o que é verdade pelo do Teorema 5.15. □

A seguir, introduzimos uma outra classe de polinômios de permutação semelhante à que vimos no Teorema 5.46.

Teorema 5.49. *Seja $L(x) = a_0x+a_1x^p+\cdots+a_{n-1}x^{p^{n-1}} \in \mathbb{F}_p[x]$ um polinômio linearizado que permuta $\mathbb{F}_{p^n}$. Sejam $h(x) \in \mathbb{F}_p[x], \gamma \in \mathbb{F}_{p^n}$, $k = Tr(\gamma) \in \mathbb{F}_p$ e $b \in \mathbb{F}_p$. O polinômio*

$$f(x) = bL(x) + h(Tr(x))(L(x) + \gamma)$$

permuta $\mathbb{F}_{p^n}$ se e somente se as duas condições seguintes são válidas:

(i) $b + h(i) \neq 0$ para todo $i \in \mathbb{F}_p$.

(ii) O polinômio $g(x) = (b + h(x))(a_0 + a_1 + \cdots + a_{n-1})x + h(x)k$ permuta $\mathbb{F}_p$.

Demonstração. Começamos supondo que duas condições são válidas. Sejam $\alpha \in \mathbb{F}_{p^n}$ e $i = Tr(\alpha) \in \mathbb{F}_p$. Então

$$f(\alpha) = bL(\alpha) + h(i)(L(\alpha) + \gamma) = (b + h(i))L(\alpha) + h(i)\gamma.$$

Pela primeira condição, vemos que $f(x)$ é injetiva no conjunto

$$T_i = \{\alpha \in \mathbb{F}_{p^n} : Tr(\alpha) = i\}.$$

Agora, sejam $\beta \in \mathbb{F}_{p^n}$ e $j = Tr(\beta) \in \mathbb{F}_p$. Supondo que $f(\alpha) = f(\beta)$, temos que

$$(b + h(i))L(\alpha) + h(i)\gamma = (b + h(j))L(\beta) + h(j)\gamma.$$

Aplicando o traço em ambos os lados da equação obtemos

$$Tr((b + h(i))L(\alpha) + h(i)\gamma) = Tr((b + h(j))L(\beta) + h(j)\gamma)$$

$$Tr((b + h(i))L(\alpha)) + Tr(h(i)\gamma) = Tr((b + h(j))L(\beta)) + Tr(h(j)\gamma)$$

$$(b+h(i))Tr(L(\alpha))+h(i)Tr(\gamma)=(b+h(j))Tr(L(\beta))+h(j)Tr(\gamma)$$

$$(b+h(i))Tr(L(\alpha))+h(i)k=(b+h(j))Tr(L(\beta))+h(j)k.$$

E aplicando o Lema 5.45, obtemos

$$(b+h(i))(a_0+a_1+\cdots+a_{n-1})i+h(i)k=(b+h(j))(a_0+a_1+\cdots+a_{n-1})j+h(j)k$$

Da segunda condição, temos que $i=j$ e, como $f(x)$ é injetiva em T_i, $\alpha=\beta$. Para o contrário, notamos que o polinômio $f(x)$ leva cada conjunto T_i bijetivamente em um conjunto T_a do mesmo tipo. □

O corolário a seguir é um caso particular do Teorema 5.49, no qual consideramos $b=0$, $\gamma=0$ e $L(x)=x$.

Corolário 5.50. *Seja $h(x)\in\mathbb{F}_p[x]$. O polinômio $f(x)=xh(Tr(x))$ permuta $\mathbb{F}_{p^n}$ se e somente se as duas condições seguintes são satisfeitas:*

(i) $h(i)\neq 0$.

(ii) O polinômio $g(x)=xh(x)$ permuta $\mathbb{F}_p$.

O seguinte exemplo ilustra o Corolário 5.50.

Exemplo 5.51. *Seja $p\equiv\pm 2 \pmod 5$. Seja $h(x)=x^4-5x^3+5x\in\mathbb{F}_p[x]$. Então, o polinômio*

$$xh(x)=x^5-5x^3+5x=g_5(x,1),$$

é um polinômio de Dickson. Pelo Teorema 5.29, segue que $xh(x)$ é um polinômio de permutação se e somente se $mdc(5,p^2-1)=1$. Dessa forma, esse polinômio permuta $\mathbb{F}_p$ para todo primo $p\equiv\pm 2 \pmod 5$. Portanto, o polinômio

$$f(x)=x(Tr(x)^4-5Tr(x)^5+5)$$

permuta $\mathbb{F}_{p^5}$.

REFERÊNCIAS

[1] BETTI, E. *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*. Annali di Scienze Matematiche e Fisiche 2, p. 5–19 (1851).

[2] DAS, P. *The number of permutation polynomials of a given degree over a finite field*, Finite Fields Appl., n. 8, p. 478–490 (2002).

[3] DUMMIT, D. S.; FOOTE, R. M. *Abstract Algebra*. Jhon Wiley & Sons (2004).

[4] HUCZYNSKA, S.; NEUNHÖFFER, M. *Finite Fields*. Disponível em `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf`.

[5] KIM, K.; KIM, R; KIM, J. *On the number of permutation polynomials over a finite field*. International Journal of Number Theory, v. 12, n. 06, p. 1519–1528 (2016)

[6] LIDL, R.; MULLEN, G. L.; TURNWALD, G. *Dickson Polynomials*. Jhon Wiley & Sons (1993).

[7] LIDL, R.; MULLEN, G. *When Does a Polynomial Over a Finite Field Permute the Elements of the Field?*. The American Mathematical Monthly, v. 95, n. 3, p. 243–246 (1988).

[8] LIDL, R.; MULLEN, G. *When Does a Polynomial Over a Finite Field Permute the Elements of the Field? II*. The American Mathematical Monthly, v. 100, n. 1, p. 71–74 (1993).

[9] LIDL, R.; NIEDERREITER, H. *Finite Fields (Enciclopedia of Mathematics and its Applications)*. Reading: Addison-Wesley (1983).

[10] MARCOS, J. E. *Specific permutation polynomials over finite fields*. Finite Fields and Their Applications n. 17, p. 105–112 (2011).

[11] MORANDI, P. *Field and Galois Theory*. Springer-Verlag, New York (1996).

[12] OKTAVIANA,B.; SIAHAAN, A. P. U. *Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography*. IOSR Journal of Computer Engineering, v. 18, p. 26–29 (2016).

[13] PARK, Y. H.; LEE, J. B. *Permutation polynomials and group permutation polynomials*. Bull. Austral. Math. Soc. n. 63, p. 67–74 (2001).

[14] ZIEVE, M. *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$*. Proceedings of the American Mathematical Society n. 137, v. 7, p. 2209–2216 (2009).