UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE PÓS-GRADUAÇÃO EM MATEMATICA

Fatoração explícita de polinômios de Dickson sobre corpos finitos

Nelcy Esperanza Arévalo Baquero

Belo Horizonte - MG
23 de Fevereiro de 2018

UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Nelcy Esperanza Arévalo Baquero

Orientador: Fabio Enrique Brochero Martinez

Fatoração explícita de polinômios de Dickson sobre corpos finitos

Dissertação submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática do Instituto de Ciências Exatas (ICEX) da Universidade Federal de Minas Gerais, como requisito parcial para obtenção do título de Mestre em Matemática.

Belo Horizonte - MG
23 de Fevereiro de 2018

Dedicatória

Aos meus pais, Arturo e Nelsy.

Agradecimentos

Agradeço primeiramente ao meu orientador Prof. Fabio Enrique Brochero Martinez, por ter acreditado e confiado na minha capacidade, dando-me a oportunidade de desenvolver esta dissertação. Obrigada por toda compreensão, dedicação, ensinamentos e, sobretudo, sua paciência em todos os momentos.

Aos meus pais, Arturo Arévalo Patiño e Nelsy Baquero Ruiz, pelo amor, incentivo e apoio incondicional em todas as minhas escolhas e decisões, em particular durante estes últimos anos. Muitíssimo obrigada.

Ao Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, por me proporcionar a oportunidade de continuar meus estudos em um curso de excelência.

Meus respeitosos agradecimentos aos professores André Contiero e Viktor Bekker pela cortesia em aceitarem integrar a banca examinadora, dispondo de seu tempo e conhecimento para analisar este trabalho.

Por fim, agradeço à CAPES, pelo imprescindível auxílio financeiro.

Resumo

O objetivo deste trabalho é estudar a fatoração em fatores irredutíveis de $D_n(x,a)$ sobre $\mathbb{F}_q$, onde q denota a potência de um primo p, $\mathbb{F}_q$ é um corpo finito de q elementos e $D_n(x,a) \in \mathbb{F}_q[x]$ é um polinômio de Dickson do primeiro tipo de grau n na indeterminada x e com parâmetro a.

Impondo condições sobre n e q determinamos expressões explícitas para os fatores irredutíveis desta família de polinômios. Calculamos a fatoração seguindo as mesmas técnicas usadas no artigo [3], onde são encontrados explicitamente os fatores irredutíveis do polinômio $x^n - 1$ sobre o corpo $\mathbb{F}_q$. Este resultado generaliza os resultados encontrados nos artigos [5],[7] e [12].

Abstract

The objective of this work is to study the factorization in irreducible factors of $D_n(x, a)$ over $\mathbb{F}_q$, where q denotes the power of a prime p, $\mathbb{F}_q$ is a finite field with q elements and $D_n(x, a) \in \mathbb{F}_q[x]$ is a Dickson polynomial of the first type of degree n in the indeterminate x and with parameter a.

Imposing conditions on n and q we determine explicit expressions for the irreducible factors of this family of polynomials. We calculate the factorization by following the same techniques used in article [3], where are found explicitly the irreducible factors of the polynomial $x^n - 1$ over the field $\mathbb{F}_q$. This result generalizes the results find in [5],[7] e [12].

Sumário

Introdução

O estudo de corpos finitos teve seu início no século 19 com os trabalhos de Gauss e Hermite, e o interesse era essencialmente teórico. A propriedade de permutação em corpos finitos é uma das propriedades que atraem muita atenção, com o avanço da era digital, seu estudo teve aplicações práticas em criptografia, desenhos combinatórios, códigos corretores de erros, assim como na implementação em hardware de *turbo decoders, feedback shift-register, linear-feedback shift register*, etc, além de interesses puramente teóricos.

Os polinômios de Dickson sobre corpos finitos foram introduzidos por Leonard Eugene Dickson (1874-1954) há mais de cem anos como parte da sua tese de doutorado [6] em 1897 na Universidade de Chicago. Os polinômios de Dickson têm várias aplicações e propriedades interessantes, sendo principalmente exemplos de famílias de polinômios de permutação. Estes são agora chamados de polinômios de Dickson do primeiro tipo $D_n(x;a) \in \mathbb{F}_q[x]$, para distingui-los de suas variações introduzidas por Schur em 1923 [11], que agora são chamados de polinômios Dickson do segundo tipo $E_n(x;a) \in \mathbb{F}_q[x]$.

Quando $a = 0$, $D_n(x,0) = x^n$, que induz uma permutação de $\mathbb{F}_q$, isto é, é um *polinômio de permutação* (PP) em $\mathbb{F}_q$, se e somente se $(n, q-1) = 1$. Quando $0 \neq a \in \mathbb{F}_q$, sabe-se que o polinômio de Dickson $D_n(x,a)$ induz uma permutação de $\mathbb{F}_q$ se e somente se $(n, q^2-1) = 1$; veja [10, Teorema 7.16] ou [9, Teorema 3.2]. Esta condição simples fornece um teste muito eficaz para determinar quais polinômios $D_n(x;a)$ induzem permutações de $\mathbb{F}_q$, e além disso, uma vez satisfeita a condição, obtemos $q-1$ permutações diferentes, uma para cada um dos elementos $a \in \mathbb{F}_q^*$.

Sobre os números complexos, os polinômios de Dickson são essencialmente equivalentes aos polinômios clássicos de Chebyshev, $T_n(x)$, com uma mudança simples de variável e, de fato, os polinômios de Dickson às vezes são referidos como polinômios de Chebyshev na literatura.

Nos últimos anos, esses polinômios receberam um estudo intenso. Em particular o problema de fatoração destes polinômios tem sido estudado por vários autores. Eles foram redescobertos por Brewer (1961), fatorações explícitas de certos polinômios de Dickson do primeiro tipo têm sido usadas para calcular somas de Brewer e às vezes, embora raramente, foram referidos como polinômios de

Brewer. Por exemplo Chou [5] e logo de forma simplificada Bhargava e Zieve [2] estudam uma fatoração dos polinômios de Dickson do primeiro tipo sobre $\mathbb{F}_q$ usando métodos muito mais longos do que usamos aqui, embora as fatorações são feitas sobre $\mathbb{F}_q$, os fatores contêm elementos fora de $\mathbb{F}_q$. Fitzgerald e Yucas [7] obtém fatorações explícitas como produto de polinômios irredutíveis de polinômios ciclotômicos de ordem 2^m e generaliza esses resultados para obter fatorações explícitas como produto de polinômios irredutíveis de polinômios de Dickson do primeiro tipo de ordem 2^m sobre $\mathbb{F}_q$. Tosun [12] amplia o anterior obtendo fatorações explícitas de polinômios de Dickson do primeiro tipo de ordem $3 \cdot 2^m$ e de polinômios de Dickson do segundo tipo de ordem $3 \cdot 2^m - 1$ sobre $\mathbb{F}_q$.

Neste trabalho estudamos o problema de encontrar a fatoração em fatores irredutíveis de $D_n(x, a)$ e $E_n(x, a)$ sobre $\mathbb{F}_q$, onde q denota a potencia de um primo p, $\mathbb{F}_q$ é um corpo finito de q elementos e $D_n(x, a)$, $E_n(x, a) \in \mathbb{F}_q[x]$ são polinômios de Dickson do primeiro e segundo tipo respectivamente de grau n na indeterminada x e com parâmetro a.

O primeiro capítulo consiste numa introdução a Álgebra e Teoria dos Números, fazemos um breve estudo sobre corpos finitos, polinômios ciclotômicos e fatores irredutíveis.

No segundo capítulo introduzimos a noção de polinômios de Dickson do primeiro e segundo tipo sobre corpos finitos $\mathbb{F}_q$ e estudamos propriedades básicas de tipo algébricas, aritméticas e algumas analíticas desta família de polinômios. Também são introduzidos e caracterizados os polinômios a-auto-recíprocos e sua relação com a fatoração dos polinômios de Dickson. Referimos o leitor à monografia [9] de Lidl, Mullen e Turnwald para uma pesquisa de muitas propriedades aritméticas e algébricas dos polinômios de Dickson sobre corpos finitos e sobre os anéis comutativos finitos. Veja também Lidl e Niederreiter [10] para uma série de resultados em polinômios Dickson sobre corpos finitos.

Por fim, no capítulo 3, para completar o estudo dos polinômios de Dickson do primeiro e segundo tipo damos novas fatorações em polinômios irredutíveis sobre $\mathbb{F}_q[x]$, exibimos uma abordagem mais simples seguindo as mesmas técnicas usadas no artigo [3], onde são encontrados explicitamente os fatores irredutíveis de $x^n - 1$ no caso que todo fator primo de n divide $q - 1$. De interesse, é como essas fatorações demonstram que os polinômios de Dickson do primeiro tipo aparecem na fatoração dos polinômios do primeiro tipo quanto aqueles do segundo tipo. Os resultados ainda inéditos a serem exibidos neste texto generalizam de forma mais simples aqueles apresentados em [5],[7] e [12].

O texto termina com algumas considerações, onde apresentamos perspectivas de continuidade do tema estudado e trabalhos relacionados a esta área.

Capítulo 1

Preliminares

Incluímos neste capítulo conceitos e resultados básicos para o desenvolvimento de nosso trabalho, muitos dos quais consagrados pelo constante uso em trabalhos nesta área. Apesar de quase todos estes resultados serem enunciados sem prova, o leitor pode consultar [4] e [10] para mais informações.

1.1 Corpos

Um *corpo* é um anel unitário e comutativo $(K, +, \cdot)$ tal que $(K, +)$ $(K^*, \cdot)$ são grupos abelianos, onde $K^* = K \setminus \{0\}$ e $0 \in K$ é o elemento neutro com relação à primeira operação $+$ e $\cdot$ é distributiva respeito à operação $+$. No que segue $(K, +, \cdot)$ será um corpo, e 1 o elemento neutro com relação a segunda operação $\cdot$.

Se L um subconjunto não vazio de K tal que é um corpo com as operações induzidas de $(K, +, \cdot)$, dizemos que L é um *subcorpo* de K. Neste contexto K é dito um corpo extensão de L e essa extensão de corpos é notada por K/L. A dimensão do L-espaço vetorial K é chamada de *grau* da extensão e denotada por $[K : L]$.

Exemplo 1.1. *O conjunto* $\mathbb{R}$ *dos números reais é um corpo com relação a soma e produto usuais e* $\mathbb{Q}$ *o conjunto dos números racionais, é um subcorpo de* $\mathbb{R}$.

Exemplo 1.2. *Se* p *é primo, então todo inteiro positivo menor que* p *é relativamente primo com* p *e assim* $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$, *onde* $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ *o anel de inteiros módulo* p. *Em particular* $\mathbb{Z}_p$ *é um corpo com a suma e produto induzido dos inteiros.*

Sendo $1 \in K$ o elemento neutro de K com relação ao produto, por abuso de notação, escreveremos $n = 1 + \cdots + 1$ onde a soma possui $n > 0$ parcelas. Se existe $n > 0$ tal que a soma $n = 1 + \cdots + 1$ é igual a $0 \in K$ o elemento neutro da adição, e se n é o menor inteiro positivo com esta propriedade, dizemos que K possui característica n. Entretanto, se não houver tal n, dizemos que K possui característica 0.

Exemplo 1.3. *O corpo $\mathbb{Z}_p$ possui característica p para cada primo p e os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ possuem característica 0.*

Se K é um corpo que possui característica zero, é necessariamente infinito, pois os elementos $1, 1+1, 1+1+1, \ldots$ devem ser todos distintos. Os corpos de característica prima podem ser finitos ou infinitos.

Teorema 1.4. *A característica de um corpo K é 0 ou um número primo p.*

Observação 1.5. *Em particular, se K é finito, então existe $p > 0$ primo tal que K possui característica p.*

É fácil verificar que a intersecção de qualquer família de subcorpos de um corpo K é ainda um subcorpo de K. Em particular a intersecção de todos os subcorpos de K é um subcorpo P de K.

Definição 1.6. *Seja K um corpo. Chamamos subcorpo primo de K à interseção de todos os subcorpos de K.*

Teorema 1.7. *O subcorpo primo de um corpo K é isomorfo a $\mathbb{Z}_p$ ou a $\mathbb{Q}$, consoante a característica de K seja p ou 0.*

Apresentamos uma identidade especial que se satisfaz em qualquer corpo de característica p.

Definição 1.8 (Aplicação de Frobenius)**.** *Seja K um corpo de característica p. Definimos a aplicação de Frobenius do corpo K como sendo a função*

$$\begin{aligned} \tau_p : K &\to K \\ a &\mapsto a^p. \end{aligned}$$

O teorema a seguir é basicamente uma generalização do Teorema de Fermat para corpos de característica não nula.

Teorema 1.9. *Se K é um corpo de característica p, então para quaisquer $a, b \in K$ temos que τ_p é aditiva, isto é,*

$$(a+b)^p = a^p + b^p.$$

Ainda mais, podemos provar que a aplicação τ_p é um homomorfismo injetivo de corpos.

Corolário 1.10. *Seja K um corpo de característica p. Então todo elemento de K é uma potencia p-ésima de um elemento de K. Ou bem, a aplicação de Frobenius é um automorfismo.*

1.1.1 Polinômios sobre um corpo

Dado K um corpo e uma variável x, consideramos o conjunto S de todas as expressões da forma $a_0 + a_1x + \cdots + a_nx^n$ onde $a_i \in K$ e n é um inteiro não negativo. Cada elemento de S é chamado de polinômio em uma variável. Podemos induzir naturalmente as operações de K em S e, com estas operações, vemos que o conjunto S é um anel. Dizemos que S é o *anel de polinômios* em uma variável sobre K e escrevemos $S = K[x]$. Por indução, podemos definir o anel de polinômios em k variáveis sobre K do modo seguinte: $K[x_1, \ldots, x_k] = (K[x_1, \ldots, x_{k-1}])[x_k]$.

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio sobre K que não é o polinômio zero, isto é, podemos supor que $a_n \neq 0$. Então dizemos que os elementos a_i são os *coeficientes* de $f(x)$, a_n é o *coeficiente líder* de $f(x)$ e a_0 o *termo constante*, enquanto n é o *grau* de $f(x)$; denotamos por $\deg f(x)$, o grau de $f(x)$. Se o coeficiente líder de $f(x)$ é 1, então $f(x)$ é dito *polinômio mônico*. Temos $f \equiv 0$ o *polinômio identicamente nulo* se, e somente se, $a_i = 0$, para $i = 0, 1, \ldots, n$, nesse caso, convencionamos que o seu grau é $-\infty$. Polinômios de grau $\leqslant 0$ são chamados de *polinômios constantes*. Se identificamos os polinômios constantes com elementos de K, então podemos ver K como um subanel de $K[x]$.

Exemplo 1.11. *Se $K = \mathbb{Z}_5$, então os elementos de $K[x]$ só possuem coeficientes 0,1,2,3 ou 4. Por exemplo, $g(x) = 3x^2 + 1$ e $f(x) = 2x^5 + x^4 + 4x + 3$ são elementos de $K[x]$ de graus 2 e 5 respectivamente.*

Se K é corpo, o anel $K[x]$ apresenta importantes semelhanças algébricas com o anel $\mathbb{Z}$ dos números inteiros. Assim, temos uma noção de divisibilidade em $K[x]$: dizemos que $f(x)$ *divide* $g(x)$ se existe $h(x) \in K[x]$ tal que $g(x) = f(x)h(x)$, isto é, $g(x)$ é um múltiplo de $f(x)$ em $K[x]$. Os polinômios $f(x)$ e $h(x)$ são ditos *divisores* de $f(x)$. Por exemplo, em $\mathbb{Z}_2[x]$ temos que $x + 1$ divide $x^2 + 1$ pois $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1$.

Os *polinômios irredutíveis* sobre um corpo K satisfazem certas propriedades semelhantes aos números primos nos números inteiros. Apresentamos a seguir um conceito bastante simples, mas muito poderoso e que contribui para o foco do presente trabalho.

Definição 1.12 (Irredutibilidade)**.** *Seja $f(x) \in K[x]$ tal que $\deg f(x) \geqslant 1$. Dizemos que $f(x)$ é um polinômio irredutível sobre K se toda vez que $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in K[x]$ então temos $g(x) =$ a constante em K ou $h(x) = b$ constante em K. Se $f(x)$ for não irredutível sobre K dizemos que f é redutível sobre K. De forma análoga, podemos definir um polinômio $f(x_1, \ldots, x_k)$ em k variáveis irredutível sobre K.*

Exemplo 1.13. *Todo polinômio de grau 1 sobre um corpo K é irredutível.*

Exemplo 1.14. *Se $K = \mathbb{Z}_2$, então o único polinômio irredutível em $K[x]$ de grau 2 é $f(x) = x^2 + x + 1$, e os polinômios irredutíveis em $K[x]$ de grau 3 são $f_1(x) = x^3 + x + 1$ e $f_2(x) = x^3 + x^2 + 1$.*

Observação 1.15. *Se um polinômio é irredutível sobre um corpo, então é irredutível sobre todos os subcorpos deste corpo, ou seja, se L é um subcorpo de K e $f(x) \in L[x]$ é irredutível sobre K, então $f(x)$ é irredutível sobre L.*

1.1.2 Polinômios simétricos

Uma ferramenta bastante útil emerge naturalmente quando estudamos a resolução de problemas de fatoração sobre um corpo, uma classe especial de polinômios em k variáveis, os *polinômios simétricos*.

Definição 1.16 (Polinômio Simétrico)**.** *Um polinômio $p(x_1, \ldots, x_k) \in K[x_1, \ldots, x_k]$ é chamado de polinômio simétrico se ele é invariante quando as variáveis $x_1, \ldots, x_k$ permutam arbitrariamente entre si, isto é, se para qualquer $\pi \in S_k$,*

$$p(x_{\pi(1)}, \ldots, x_{\pi(k)}) = p(x_1, \ldots, x_k).$$

Observação 1.17. *O conjunto dos polinômios simétricos é um subanel de $K[x_1, \ldots, x_k]$ que contem ao corpo K.*

En especial, entre os polinômios simétricos, temos os mais simples possíveis.

Exemplo 1.18. *Os seguintes polinômios e_m, somas de todos os produtos de m variáveis, são simétricos.*

$$\begin{aligned}
e_1 = e_1(x_1, \ldots, x_k) &= x_1 + x_2 + \cdots + x_k = \sum_{i=1}^{k} x_i, \\
e_2 = e_2(x_1, \ldots, x_k) &= x_1x_2 + x_1x_3 + \cdots + x_{k-1}x_k = \sum_{1 \leqslant i < j < \leqslant n} x_ix_j, \\
e_3 = e_3(x_1, \ldots, x_k) &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{k-2}x_{k-1}x_k = \sum_{1 \leqslant i < j < l \leqslant n} x_ix_jx_l, \\
&\vdots \\
e_k = e_k(x_1, \ldots, x_k) &= x_1x_2 \cdots x_k.
\end{aligned}$$

Em geral o polinômio simétrico

$$e_m = e_m(x_1, \ldots, x_k) = \sum_{1 \leqslant i_1 < \cdots < i_m \leqslant k} x_{i_1}x_{i_2} \cdots x_{i_m},$$

onde $m = 1, 2, \ldots, k$ é chamado de *m-ésimo polinômio simétrico elementar* nas variáveis $x_1, \ldots, x_k$ sobre K. Notemos que $e_0 = 1$, $e_m(x_1, \ldots, x_k) = 0$ se $m > k$

e o número de termos em $e_m(x_1, \ldots, x_k)$ é $\binom{k}{m}$. Além disso, $deg(e_m) = m$ para $1 \leqslant m \leqslant k$.

Observação 1.19. *Se K é um corpo de característica zero, os polinômios simétricos elementares em k variáveis são elementos do subanel $\mathbb{Z}[x_1, \cdots, x_k] \subset K[x_1, \cdots, x_k]$.*

Exemplo 1.20. *Temos que o polinômio $x_1^2 + \cdots + x_k^2 \in \mathbb{Q}[x_1, \ldots, x_k]$ é simétrico, e pode ser expresso como $e_1^2 - 2e_2$.*

De fato os polinômios simétricos elementares fornecem uma estrutura básica, são os blocos na construção de todos os polinômios simétricos e geram um subanel do anel dos polinômios simétricos.

O principal resultado sobre polinômios simétricos diz que todo polinômio simétrico em k variáveis sobre um corpo, é, de modo único, um polinômio em polinômios elementares simétricos sobre essas k variáveis. Exibimos, sem demonstração, o seguinte.

Teorema 1.21 (Teorema fundamental dos polinômios simétricos ([10], Teorema 6.25))**.** *Todo polinômio simétrico $p(x_1, \ldots, x_k)$ pode ser escrito como um polinômio em termos dos polinômios simétricos elementares $e_m(x_1, \ldots, x_k)$.*

Para cada $n \geqslant 1$ a n-ésima soma de potencias é

$$S_n = S_n(x_1, \ldots, x_k) = \sum_{i=1}^{k} x_i^n.$$

A fórmula a seguir expressa explicitamente S_n em termos de funções simétricas elementares e_m.

Teorema 1.22 (Fórmula de Waring ([10], Teorema 1.76))**.** *Sejam $e_1, \ldots, e_k$ polinômios simétricos elementares nas variáveis $x_1, \ldots, x_k$ sobre um anel R e $S_n = S_n(x_1, \ldots, x_k) = x_1^n + \cdots + x_k^n \in R[x_1, \ldots, x_k]$ para $n \geq 1$. Então temos*

$$S_n = \sum (-1)^{i_2+i_4+i_6+\cdots} \frac{(i_1 + i_2 + \cdots + i_k - 1)!n}{i_1! i_2! \cdots i_k!} \, e_1^{i_1} \, e_2^{i_2} \cdots \, e_k^{i_k},$$

para $n \geq 1$, onde estendemos a somatória sobre todas as tuplas $(i_1, \ldots, i_n)$ de inteiros não negativos com $i_1 + 2i_2 + \cdots + ki_k = n$. Os coeficientes de $e_1^{i_1} \, e_2^{i_2} \cdots \, e_k^{i_k}$ são inteiros.

No caso particular em que temos duas indeterminadas, i.e. $k = 2$, a fórmula de Waring nos diz que

$$x_1^n + x_2^n = \sum_{i_1 + 2i_2 = n} (-1)^{i_2} \frac{(i_1 + i_2 - 1)!n}{i_1! i_2!} (x_1 + x_2)^{i_1} (x_1 x_2)^{i_2},$$

e fazendo a substituição de variável $i_1 = n - 2i_2$, obtemos

$$x_1^n + x_2^n = \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^i \frac{n}{n-i} \binom{n-i}{i} (x_1 + x_2)^{n-2i} (x_1 x_2)^i.$$

1.2 Corpos finitos

Iniciaremos o nosso estudo sobre polinômios com coeficientes em corpos finitos conhecendo um pouco da estrutura destes corpos. Agora traremos algumas definições e teoremas importantes da teoria de corpos finitos que nos serão muito úteis nos capítulos subsequentes.

Um *corpo finito* é um corpo com um número finito de elementos, o número de elementos de um corpo finito é dito de *ordem* do corpo.

Lema 1.23. *Seja p primo. Todos os corpos de ordem p são isomorfos a $\mathbb{Z}_p$.*

No seguinte teorema temos uma descrição da estrutura de um corpo finito.

Teorema 1.24. *Seja K um corpo finito de característica p para algum primo p. Então existe $n \geqslant 1$ tal que $|K| = p^n$.*

Demonstração.

Note que K possui um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular podemos encarar K como um $\mathbb{Z}_p$-espaço vetorial de dimensão finita, pois $\mathbb{Z}_p$ é finito. Denotemos esta dimensão por n, então K tem uma base sobre $\mathbb{Z}_p$ consistente de n elementos, digamos $\{v_1, \ldots, v_n\}$. Cada elemento de K pode ser unicamente representado na forma $c_1 v_1 + \cdots + c_n v_n$, onde $c_1, \ldots, c_n \in \mathbb{Z}_p$. Como cada $c_i \in \mathbb{Z}_p$ pode tomar p valores, K deve ter exatamente p^n elementos. ■

O próximo teorema caracteriza os corpos finitos, garantindo a existência e unicidade de tais corpos.

Teorema 1.25 (Existência e unicidade de corpos finitos ([10], Teorema 2.5))**.** *Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Observação 1.26. *Em virtude da parte da unicidade do Teorema 1.25, podemos falar do corpo finito com q elementos, ou do corpo finito de ordem q. De agora em diante, vamos denotar este corpo por $\mathbb{F}_q$, onde $q = p^n$ é uma potencia da característica prima p de $\mathbb{F}_q$.*

Teorema 1.27 (Critério para Subcorpos ([10], Teorema 2.6))**.** *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 divisor positivo de n. Reciprocamente, se m é um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Exemplo 1.28. *Os subcorpos do corpo finito $\mathbb{F}_{2^{30}}$ podem ser determinados, após listarmos todos os divisores positivos de 30. Pelo Teorema 1.27, as relações de inclusão são equivalentes às relações de divisibilidade entre os divisores positivos de 30. Assim os subcorpos de $\mathbb{F}_{2^{30}}$ são:*

$$\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^5}, \mathbb{F}_{2^6}, \mathbb{F}_{2^{10}}, \mathbb{F}_{2^{15}}, \mathbb{F}_{2^{30}}.$$

Observação 1.29. *Os corpos intermediários de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ são linearmente ordenados por inclusão, isto é, se F e K são corpos tais que $\mathbb{F}_q \subseteq F \subseteq \mathbb{F}_{q^n}$ e $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ então $F \subseteq K$ ou $K \subseteq F$.*

O teorema seguinte nos será muito útil na próxima seção para demostrarmos diversas propriedades acerca de polinômios ciclotômicos.

Teorema 1.30. *([10], Teorema 2.8) Para todo corpo finito $K = \mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ de elementos diferentes de zero de $\mathbb{F}_q$, é cíclico.*

Demonstração.

No caso $q = 2$ o resultado é trivial, assim assumiremos que $q \geqslant 3$ e seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para todo i, $1 \leqslant i \leqslant m$, o polinômio $x^{h/p_i} - 1$ tem no máximo $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Como $\frac{h}{p_i} \leqslant h$, segue que existem elementos diferentes de zero em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um desses elementos e defina $b_i = a_i^{h/p_i^{r_i}}$. Temos que $b_i^{p_i^{r_i}} = 1$, onde segue que a ordem de b_i é um divisor de $p_i^{r_i}$ e além disso é da forma $p_i^{s_i}$ com $0 \leqslant s_i \leqslant r_i$.

Por outro lado

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

então a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. De fato, se denotamos por k a ordem de b, e k fosse um divisor próprio de h, para algum inteiro $1 \leqslant i \leqslant m$ teríamos que k divide $\frac{h}{p_i}$, podemos supor sem perda de generalidade que $i = 1$. Então

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

Agora, se $2 \leqslant j \leqslant m$, então $p_j^{r_j}$ divide $\frac{h}{p_1}$ e assim $b_j^{h/p_1} = 1$. Isso implica $b_1^{h/p_1} = 1$, de onde temos que a ordem de b_1 deve dividir $\frac{h}{p_1}$, o que não é possível uma vez que a ordem de b_1 é $p_1^{r_1}$. Portanto, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. ■

Definição 1.31. *Um gerador de um grupo cíclico $\mathbb{F}_q^*$ é chamado um elemento primitivo de $\mathbb{F}_q$.*

Observação 1.32. *Temos provado que qualquer corpo finito tem um elemento primitivo. A questão de achar um elemento primitivo, é importante para a construção do corpo finito. Segue da definição que um elemento primitivo α de um corpo $\mathbb{F}_q$ tem ordem $q-1$. Portanto $\alpha^{q-1} = \alpha^0 = 1$, e vemos que o exponente é calculado módulo $q-1$.*

1.2.1 Raízes de Polinômios Irredutíveis

Nesta seção vamos listar algumas informações acerca do conjunto das raízes de um polinômio irredutível sobre um corpo finito.

Lema 1.33 ([10], Lema 2.12)**.** *Sejam $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre um corpo finito $\mathbb{F}_q$ e α uma raiz de f em uma extensão de $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$, $h(\alpha) = 0$, se, e somente se, $f \mid h$.*

Lema 1.34 ([10], Lema 2.13)**.** *Sejam $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então, f divide $x^{q^n} - x$ se, e somente se, m divide n.*

O próximo teorema nos fala sobre as raízes de polinômios em $\mathbb{F}_q[x]$.

Teorema 1.35 ([10], Teorema 2.14)**.** *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m, então f tem uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e dadas por m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração.

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

Devemos mostrar agora, que se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f, então β^q também é uma raiz de f. Seja $f = a_m x^m + \cdots + a_1 x + a_0$, com $a_i \in \mathbb{F}_q$ para $0 \leqslant i \leqslant m$. Então

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

Portanto, os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ são raízes de f. Falta agora mostrar que estes elementos são todos distintos. Para tanto, vamos supor o contrário, isto é,

$$\alpha^{q^j} = \alpha^{q^k}, \tag{1}$$

para alguns inteiros j e k com $0 \leqslant j < k \leqslant m-1$. Elevando ambos os membros da identidade (1) à potencia q^{m-k}, obtemos

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

Segue do Lema 1.33, que f divide $x^{q^{j+m-k}} - x$, e isto só é possível se m divide $j+m-k$, de acordo com o Lema 1.34. Mas isto é uma contradição, pois temos que $0 < j+m-k < m$, uma vez que $j < k < m$ implica $j-k < m-k$. ■

Corolário 1.36 ([10], Corolário 2.15). *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível de grau m, então o corpo de decomposição de f sobre $\mathbb{F}_q$ é $\mathbb{F}_{q^m}$.*

Corolário 1.37 ([10], Corolário 2.16). *Quaisquer dois polinômios irredutíveis em $\mathbb{F}_q[x]$ de mesmo grau, têm corpos de decomposição isomorfos.*

Vamos agora introduzir uma terminologia conveniente para os elementos que aparecem no Teorema 1.35 independentemente de $\alpha \in \mathbb{F}_{q^m}$ ser uma raiz de um polinômio irredutível de grau m em $\mathbb{F}_q[x]$ ou não.

Definição 1.38. *Sejam $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^m}$. Então chamamos conjugados de α em relação a $\mathbb{F}_q$ aos elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.*

Observação 1.39. *Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ em relação a $\mathbb{F}_q$ são distintos se, e somente se, o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau m. Caso contrário, o grau d deste polinômio minimal é um divisor próprio de m, e então os conjugados distintos de α em relação a $\mathbb{F}_q$ são os d elementos distintos $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, cada um repetido $\frac{m}{d}$ vezes.*

Teorema 1.40 ([10], Teorema 2.18). *Os conjugados de $\alpha \in \mathbb{F}_q^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ têm a mesma ordem no grupo $\mathbb{F}_q^*$.*

Corolário 1.41 ([10], Corolário 2.19). *Se α é um elemento primitivo de $\mathbb{F}_q$, então também são elementos primitivos, todos os conjugados de α em relação a qualquer subcorpo de $\mathbb{F}_q$.*

Exemplo 1.42. *Seja $\alpha \in \mathbb{F}_{16}$ uma raiz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Vamos encontrar os conjugados de α em relação a $\mathbb{F}_2$. Como $q^m = 16 = 2^4$, temos, $q = 2$ e $m = 4$; portanto, pela Definição 1.38, os conjugados de α são $\alpha, \alpha^2, \alpha^{2^2}$ e $\alpha^{2^{4-1}} = \alpha^{2^3}$, isto é, os conjugados são, $\alpha, \alpha^2, \alpha^4, \alpha^8$.*

Uma vez que α é uma raiz de f, temos que $\alpha^4 = \alpha + 1$ e $\alpha^8 = (\alpha^4)^2 = (\alpha+1)^2 = \alpha^2 + 1$. É fácil verificar que os conjugados de α, têm todos a mesma ordem 15 no grupo $\mathbb{F}_{16}^*$. Consequentemente, todos eles são elementos primitivos de $\mathbb{F}_{16}$.

Observação 1.43. *Existe uma relação muito forte entre elementos conjugados e certos automorfismos de um corpo finito. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$. Por um automorfismo σ de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ queremos dizer um automorfismo de $\mathbb{F}_{q^m}$ que fixa os elementos de $\mathbb{F}_q$.*

Teorema 1.44 ([10], Teorema 2.21). *Os automorfismo distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente as funções $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, definidas por $\sigma_j(\alpha) = \alpha^{q^j}$, para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leqslant j \leqslant m-1$.*

Observação 1.45. *Com base no Teorema 1.44, os conjugados de $\alpha \in \mathbb{F}_{q^m}$ em relação a $\mathbb{F}_q$ são obtidos pela aplicação de todos os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ com a operação usual de composição de funções, formam um grupo cíclico de ordem m gerado por σ_1.*

1.2.2 Polinômios e Extensões Ciclotômicas

O principal objeto algébrico de estudo neste trabalho são os corpos finitos e, sobretudo, polinômios sobre esses corpos. E se tratando de corpos finitos, temos uma classe interessante de polinômios, os *polinômios ciclotômicos*.

Um conceito que precisaremos introduzir y que será decorrente nos próximos capítulos é o de *função de Euler*.

Definição 1.46. *Para $m \in \mathbb{N}$ definimos a função de Euler, $\varphi(m)$, como o número de inteiros k tal que $1 \leqslant k \leqslant m$ e $mdc(k, m) = 1$.*

Exemplo 1.47. *Por exemplo, $\varphi(1) = 1$, $\varphi(p) = p - 1$ se p é primo e $\varphi(2^k) = 2^{k-1}$.*

Proposição 1.48. *Sejam $m, n, s \in \mathbb{N}$ e p um número primo. São válidas as seguintes propriedades sobre a função de Euler.*

(i) $\varphi(p^s) = p^s\left(1 - \frac{1}{p}\right)$,

(ii) $\varphi(mn) = \varphi(m)\varphi(n)$ *se* $mdc(m, n) = 1$,

(iii) $\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right)$, *onde* $m = p_1^{e_1}\cdots p_r^{e_r}$ *é a decomposição de m em primos.*

Vamos analisar o corpo de decomposição do polinômio $x^n - 1$ sobre um corpo arbitrário K, onde n é um inteiro positivo. Também obteremos uma generalização do conceito de raiz da unidade, já bem conhecido para os números complexos.

Definição 1.49. *Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre o corpo K é chamado o n-ésimo corpo ciclotômico sobre K e denotado por $K^{(n)}$. As raízes de $x^n - 1$ em $K^{(n)}$ são chamadas as raízes n-ésimas da unidade sobre K e o conjunto dessas raízes é denotado por $E^{(n)}$.*

O caso que mais nos interessa, é quando K é um corpo finito.

Definição 1.50. *Sejam K um corpo de característica p e n um inteiro positivo tal que $p \nmid n$. Então, um gerador do grupo cíclico $E^{(n)}$ é chamado de raiz n-ésima primitiva da unidade sobre K.*

Observação 1.51. *Notemos que sob as condições da Definição 1.50, existem exatamente $\varphi(n)$ raízes n-ésimas primitivas da unidade diferentes sobre K. Seja ζ uma delas, então todas as raízes n-ésimas primitivas da unidade são dadas por ζ^s, com $1 \leqslant s \leqslant n$ e $mdc(s, n) = 1$.*

A seguir definiremos um polinômio cujas raízes são exatamente as raízes n-ésimas primitivas da unidade. Este polinômio será fundamental para os nossos propósitos neste trabalho.

Definição 1.52. *Sejam K um corpo de característica p, n um inteiro positivo tal que $p \nmid n$, e ζ uma raiz n-ésima primitiva da unidade sobre K. O polinômio*

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

é chamado o n-ésimo polinômio ciclotômico sobre K.

Observação 1.53. *O polinômio Q_n é independente da escolha de ζ. Notemos que $\deg Q_n(x) = \varphi(n)$ e seus coeficientes são elementos do n-ésimo corpo ciclotômico sobre K.*

Para provarmos o próximo teorema precisaremos de um lema bastante conhecido, o qual enunciaremos sem demonstração.

Lema 1.54 (Lema de Gauss)**.** *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Então $f(x)$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(x)$ é irredutível em $\mathbb{Z}[x]$ (isto é, não podemos escrever $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$ não constantes).*

Teorema 1.55 ([10], Teorema 2.45)**.** *Sejam K um corpo de característica p e n um inteiro positivo tal que $p \nmid n$. Então*

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

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

Demonstração.

(i) Cada raiz n-ésima da unidade sobre K é uma raiz d-ésima da unidade sobre K para exatamente um divisor positivo d de n. En detalhe, se ζ é uma raiz n-ésima primitiva da unidade sobre K e ζ^s uma raiz n-ésima da unidade arbitrária sobre K, então $d = \frac{n}{mdc(s,n)}$; isto é, d é a ordem de ζ^s em $E^{(n)}$. Uma vez que

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

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

(ii) Este item será provado por indução em n, notemos que $Q_n(x)$ é um polinômio mônico.

(a) Para $n = 1$ temos que $Q_1(x) = x - 1$.

(b) Passo indutivo: Seja $n > 1$ e suponha a proposição válida para todo $Q_d(x)$ com $1 \leqslant d < n$. Então segue do item **(i)**,

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

onde

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

A hipótese de indução implica que $f(x)$ é um polinômio com coeficientes no subcorpo primo de K ou em $\mathbb{Z}$ no caso da característica de K ser 0. Fazendo uma longa divisão com $x^n - 1$ é o polinômio mônico $f(x)$, vemos que os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K se os coeficientes de $f(x)$ estão em K. Já se estes coeficientes estão em $\mathbb{Q}$ pelo Lema 1.54 segue que os coeficientes de $Q_n(x)$ estarão sobre $\mathbb{Z}$.

■

Exemplo 1.56. *Sejam p um número primo e $m \in \mathbb{N}$. Então*

$$Q_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = \sum_{j=0}^{p-1} x^{jp^{m-1}},$$

desde que

$$x^{p^m} - 1 = \prod_{j=0}^{m} Q_{p^j} = Q_{p^m} \prod_{j=0}^{m-1} Q_{p^j} = (x^{p^{m-1}} - 1) Q_{p^m},$$

*pelo item **(i)** do Teorema 1.55.*

Para $m = 1$ simplesmente temos

$$Q_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

As propriedades sobre polinômios ciclotômicos da próxima proposição serão de extrema importância nos capítulos subsequentes.

Proposição 1.57. *São válidas as seguintes propriedades sobre polinômios ciclotômicos.*

(i) $Q_{mp}(x) = \dfrac{Q_m(x^p)}{Q_m(x)}$ *se p é primo e $m \in \mathbb{N}$ não é divisível por p,*

(ii) $Q_{mp}(x) = Q_m(x^p)$ *para todo $m \in \mathbb{N}$ tal que $p \mid m$,*

(iii) $Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}})$ *se p é um primo e $m, k \in \mathbb{N}$ são arbitrários,*

(iv) $Q_{2n}(x) = Q_n(-x)$ *se $n \geqslant 3$ e n é ímpar,*

(v) $Q_n(0) = 1$ *se* $n \geqslant 2$,

(vi) $Q_n(x^{-1})x^{\varphi(n)} = Q_n(x)$ *se* $n \geqslant 2$,

(vii) $$Q_n(1) = \begin{cases} 0 & \text{se } n = 1, \\ p & \text{se } n \text{ é uma potência de um primo } p, \\ 1 & \text{se } m \text{ tem pelo menos dois fatores primos distintos}, \end{cases}$$

(viii) $$Q_n(-1) = \begin{cases} -2 & \text{se } n = 1, \\ 0 & \text{se } n = 2, \\ p & \text{se } n \text{ é duas vezes uma potência de um primo } p, \\ 1 & \text{em outro caso}. \end{cases}$$

Demonstração.

(i) Provaremos por indução sobre m.

(a) Para $m = 1$ temos

$$Q_p(x)Q_1(x) = x^p - 1 = Q_1(x^p).$$

(b) Passo indutivo: Seja $m \in \mathbb{N}$ tal que $m > 1$ e m não é divisível por p. A afirmação é válida para todo s tal que $1 \leqslant s < m$ e s não é divisível por p. Devemos mostrar que a afirmação é válida para $s = m$.

Se $s \mid mp$, então $mdc(s, p) = 1$ ou $mdc(s, p) = p$. Logo, $s \mid m$ ou $s = lp$ para algum $l \in \mathbb{N}$. No caso de que $s = lp$, então $l \mid m$. Por outro lado, $tp \mid mp$ para todo $t \in \mathbb{N}$ que divida a m.

Do anterior temos que

$$\prod_{s \mid mp} Q_s(x) = \prod_{s \mid m} Q_s(x) \prod_{l \mid m} Q_{lp}(x). \tag{2}$$

Como

$$\prod_{s \mid mp} Q_s(x) = x^{mp} - 1 \tag{3}$$

e

$$\prod_{s \mid m} Q_s(x) = x^m - 1. \tag{4}$$

Substituindo (3) e (4) em (2) obtemos

$$x^{mp} - 1 = (x^m - 1) \prod_{l \mid m} Q_{lp}(x). \tag{5}$$

Mas

$$\prod_{l|m} Q_{lp}(x) = \left(\prod_{\substack{l|m \\ l\neq m}} Q_{lp}(x) \right) Q_{mp}(x). \tag{6}$$

Como $mdc(m,p) = 1$ então, se $l \mid m$, $mdc(l,p) = 1$.

Pela Hipótese de Indução temos que

$$\begin{aligned} \prod_{\substack{l|m \\ l\neq m}} Q_{lp}(x) &= \prod_{\substack{l|m \\ l\neq m}} \frac{Q_l(x^p)}{Q_l(x)} \\ &= \frac{\prod_{l|m} Q_l(x^p)}{\prod_{l|m} Q_l(x)} \cdot \frac{Q_m(x)}{Q_m(x^p)} \\ &= \frac{(x^p)^m - 1}{x^m - 1} \cdot \frac{Q_m(x)}{Q_m(x^p)}. \end{aligned} \tag{7}$$

Substituindo (7) em (6) e (6) em (5), obtemos

$$x^{mp} - 1 = (x^m - 1)\frac{(x^{mp}) - 1}{x^m - 1} \cdot \frac{Q_m(x)}{Q_m(x^p)} Q_{mp}(x).$$

Assim

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

(ii) Da definição podemos escrever

$$Q_m(x^p) = \prod_{\substack{s=1 \\ mdc(s,m)=1}}^{m} (x^p - \gamma^s)$$

e

$$Q_{mp}(x) = \prod_{\substack{s=1 \\ mdc(s,mp)=1}}^{mp} (x - \zeta^s),$$

em que γ é uma raiz m-ésima primitiva da unidade e ζ é uma raiz mp-ésima primitiva da unidade.

Para provar que esses dois polinômios são iguais mostraremos que eles tem o mesmo grau e as mesmas raízes.

Como $p \mid m$ segue $\varphi(mp) = p \cdot \varphi(m)$, assim o grau de $Q_{mp}(x)$ é igual a $p \cdot \varphi(m)$ e portanto o grau de $Q_m(x^p)$ é igual ao grau de $Q_{mp}(x)$.

Seja θ raiz de $x^p - \gamma$, assim $\theta^p - \gamma = 0$, desse modo $\theta^p = \gamma$, mas γ é uma raiz m-ésima primitiva da unidade, então $(\theta^p)^m = \gamma^m = 1$ o que nos dá

$\theta^{mp} = 1$.

Por outro lado, denotemos por n a ordem de θ. Desse modo $\theta^n = 1$, assim $\gamma^n = (\theta^p)^n = (\theta^n)^p = 1$, logo $\gamma^n = 1$ donde segue que $m \mid n$. Como $\theta^{mp} = 1$ temos que $n \mid mp$ e consequentemente $m = n$ ou $n = mp$.

Suponhamos que $n = m$. Como $p \mid m$ segue que $\gamma^{m/p} = (\theta^p)^{m/p} = \theta^m = \theta^n = 1$, o que é absurdo, pois $\frac{m}{p} < m$. Então só pode ser $n = mp$ e assim a ordem de θ é mp.

(iii) Aplicando p^{k-1} vezes o item **(ii)** temos

$$Q_{mp^k}(x) = Q_{mp^{k-1}}(x^p) = Q_{mp^{k-2}}(x^{p^2}) = \cdots = Q_{mp}(x^{p^{k-1}}).$$

(iv) Provaremos por indução sobre n.

(a) Para $n = 3$ temos

$$Q_{2n}(x) = Q_6(x) = x^2 - x + 1 = Q_3(-x).$$

(b) Passo indutivo: Seja $n \in \mathbb{N}$ tal que $n > 3$ e n é ímpar. A afirmação é válida para todo m ímpar com $3 \leqslant m < n$. Devemos mostrar que a afirmação é válida para $m = n$.

Como

$$x^{2n} - 1 = \prod_{d|2n} Q_d(x) = \prod_{m|n} Q_m(x) \prod_{m|n} Q_{2m}(x),$$

então

$$x^{2n} - 1 = (x^n - 1) \left(\prod_{\substack{m|n \\ 1<m<n}} Q_{2m}(x) \right) Q_2(x) Q_{2n}(x). \tag{8}$$

Mas pela hipótese de indução

$$\prod_{\substack{m|n \\ 1<m<n}} Q_{2m}(x) = \prod_{\substack{m|n \\ 1<m<n}} Q_m(-x). \tag{9}$$

Substituindo (9) em (8), obtemos

$$\begin{aligned} x^{2n}-1 &= (x^n-1)\left(\prod_{\substack{m|n\\ 1<m<n}} Q_m(-x)\right) Q_2(x)Q_{2n}(x) \\ &= (x^n-1)\left(\prod_{m|n} Q_m(-x)\right)\frac{Q_2(x)Q_{2n}(x)}{Q_1(-x)Q_n(-x)} \\ &= (x^n-1)((-x)^n-1)\frac{(x+1)Q_{2n}(x)}{(-x-1)Q_n(-x)}. \end{aligned}$$

Simplificando e lembrando que $(-1)^n = -1$ pois n é ímpar, obtemos que

$$Q_{2n}(x) = Q_n(-x).$$

(v) Vamos dividir em dois casos.

(a) $n = 2$.

$$Q_2(x) = \frac{x^2-1}{x-1} = x+1,$$

então $Q_2(0) = 1$.

(b) $n > 2$.

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

então

$$Q_n(0) = (-1)^{\varphi(n)} \prod_{\substack{s=1\\ mdc(s,n)=1}}^{n} \zeta^s = 1,$$

uma vez que $\varphi(n)$ é sempre par para todo $n > 2$.

(vi) Como

$$\begin{aligned} Q_n(x^{-1}) &= \prod_{\substack{s=1\\ mdc(s,n)=1}}^{n} (x^{-1}-\zeta^s) \\ &= \prod_{\substack{s=1\\ mdc(s,n)=1}}^{n} (x^{-1}-\zeta^{-s}) \\ &= \frac{(-1)^{\varphi(n)}}{x^{\varphi(n)}} \prod_{\substack{s=1\\ mdc(s,n)=1}}^{n} (x-\zeta) \\ &= \frac{1}{x^{\varphi(n)}} Q_n(x), \end{aligned}$$

uma vez que $\varphi(n)$ é sempre par para todo $n > 2$, então

$$Q_n(x^{-1})x^{\varphi(n)} = Q_n(x).$$

(vii) Para $n = 1$, é fácil ver que $Q_1(x) = x - 1$, logo $Q_1(1) = 0$.

Para $n = p^k$ com $k \geqslant 1$, temos

$$\begin{aligned} Q_{p^k}(x) &= \frac{x^{p^k}-1}{\prod\limits_{\substack{d|p^k \\ d\neq p^k}} Q_d(x)} = \frac{x^{p^k}-1}{Q_p(x)Q_{p^2}(x)\cdots Q_{p^{k-2}}(x)Q_{p^{k-1}}(x)} \\ &= \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = \underbrace{x^{p^{k-1}(p-1)} + \cdots + x^{p^{k-1}} + 1}_{p \text{ somandos}}, \end{aligned}$$

por conseguinte, $Q_n(1) = p$.

Para $n = mp^k$ com $mdc(m, p) = 1$, utilizando os itens **(iii)** e **(i)** na primeira e segunda igualdade, respectivamente, temos

$$Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}}) = \frac{Q_m(x^{p^{k-1}p})}{Q_m(x^{p^{k-1}})} = \frac{Q_m(x^{p^k})}{Q_m(x^{p^{k-1}})}, \tag{10}$$

assim, $Q_{mp^k}(1) = 1$.

(viii) Para $n = 1$ é simples ver que $Q_1(x) = x - 1$, logo $Q_1(-1) = -2$.

Para $n = 2$ é claro que $Q_2(x) = x + 1$, logo $Q_2(-1) = 0$.

Observemos que

$$Q_p(-1) = (-1)^{p-1} + (-1)^{p-2} + \cdots + (-1)^2 + (-1)^1 + 1 = \begin{cases} 1 & \text{se } p \neq 2, \\ 0 & \text{se } p = 2. \end{cases}$$

No caso $n = p^k$ com $k \geqslant 2$, pelo item **(iii)** temos que

$$Q_{p^k}(-1) = Q_p((-1)^{p^{k-1}}) = \begin{cases} 1 & \text{se } p \neq 2, \\ 2 & \text{se } p = 2. \end{cases}$$

Assim falta considerar o caso que n tem pelo menos dois divisores primos distintos. Suponhamos que $n = mp^k$ com $mdc(m, p) = 1$.

Se $m = 2$, pelo item **(iv)** temos que

$$Q_{2p^k}(x) = Q_{p^k}(-x),$$

então

$$Q_{2p^k}(-1) = Q_{p^k}(1) = p.$$

No caso $m \neq 2$, de (10) segue que

$$Q_{mp^k}(-1) = \frac{Q_m((-1)^{p^k})}{Q_m((-1)^{p^{k-1}})} = 1.$$

■

Visando algumas aplicações em corpos finitos, será muito útil conhecermos algumas propriedades dos corpos ciclotômicos.

Existe um resultado interessante que determina o número de fatores irredutíveis de qualquer polinômio ciclotômico $Q_n(x)$ sobre qualquer corpo finito K. Usamos novamente φ para denotar a função de Euler introduzida na Definição 1.46.

Teorema 1.58 ([10], Teorema 2.47). *O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K. Além disso*

- **(i)** *se $K = \mathbb{Q}$, então o polinômio ciclotômico Q_n é irredutível sobre K e $[K^{(n)} : K] = \varphi(n)$,*
- **(ii)** *se $K = \mathbb{F}_q$ com $mdc(q, n) = 1$, então Q_n se fatora em $\frac{\varphi(n)}{d}$ polinômios mônicos irredutíveis distintos em $K[x]$ de mesmo grau d, $K^{(n)}$ é o corpo de decomposição de qualquer um desses fatores irredutíveis sobre K, e $[K^{(n)} : K] = d$, sendo que d é o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n}$.*

Exemplo 1.59. *Sejam $K = \mathbb{F}_{11}$ e $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Vamos usar o item **(ii)** do Teorema 1.58, para mostrar que $Q_{12}(x)$ se fatora em $d = 2$ polinômios mônicos distintos de mesmo grau 2 em $\mathbb{F}_{11}[x]$.*

Primeiramente, deg $Q_{12}(x) = \varphi(12) = 4$ e como devemos ter $11^k \equiv 1 \pmod{12}$, encontramos que o menor inteiro positivo que satisfaz a congruência é $k = 2$; portanto, temos $d = 2$. Assim, $\frac{\varphi(12)}{2} = 2$ e vemos que $Q_{12}(x) = x^4 - x^2 + 1$ se fatora em 2 polinômios mônicos distintos de mesmo grau $d = 2$.

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

Teorema 1.60 ([10], Teorema 2.49). *O corpo finito $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um dos seus subcorpos.*

Demonstração.

O polinômio $x^{q-1} - 1$ é fatorado em $\mathbb{F}_q$, já que suas raízes são todos os elementos de $\mathbb{F}_q^*$. Notando que $x^{q-1} - 1$ não pode ser fatora en nenhum subcorpo

próprio de $\mathbb{F}_q$, concluímos que $\mathbb{F}_q$ é o corpo de decomposição de $x^{q-1}-1$ sobre qualquer um dos seus subcorpos. ■

Como $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q-1$ pelo Teorema 1.30, existirá, para qualquer divisor positivo n de $q-1$ um subgrupo cíclico $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de $\mathbb{F}_q^*$ de ordem n. Todos os elementos desse subgrupo são raízes n-ésimas da unidade sobre qualquer subcorpo de $\mathbb{F}_q$ e o elemento gerador α é uma raiz n-ésima primitiva da unidade sobre qualquer subcorpo de $\mathbb{F}_q$.

Lema 1.61 ([10], Lema 2.50). *Se n é um inteiro positivo tal que $Q_n(x)$ está definido e d é um divisor de n com $1 \leqslant d < n$, então $Q_n(x) \mid \frac{x^n-1}{x^d-1}$.*

Demonstração.

Pelo item **(i)** do Teorema 1.55, sabemos que $Q_n(x) \mid (x^n-1)$. Como

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

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

Mas, uma vez que d é um divisor próprio de n, os polinômios $Q_n(x)$ e x^d-1 não possuem raízes comuns, daí, $mdc(Q_n(x), x^d-1) = 1$. Assim $Q_n(x) \mid \frac{x^n-1}{x^d-1}$. ■

1.2.3 Construção de Polinômios Irredutíveis

Definição 1.62. *Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo. Se $f(0) \neq 0$, então o menor inteiro positivo α, tal que $f(x)$ divide $x^\alpha - 1$ é chamada a ordem de f, que denotamos por $ord(f) = ord(f(x))$. Se $f(0) = 0$, então $f(x) = x^h g(x)$, onde $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$ com $g(0) \neq 0$ são unicamente determinados; neste caso a $ord(f)$ é definida como sendo $ord(g)$.*

A ordem de um polinômio irredutível f pode ser caracterizada da seguinte maneira alternativa.

Teorema 1.63 ([10], Teorema 3.3). *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m e com $f(0) \neq 0$. Então a ordem de f é igual a ordem de alguma raiz de f no grupo multiplicativo $\mathbb{F}_{q^m}^*$*

O Teorema 1.64 a seguir, mostra uma fórmula para o número de polinômios mônicos irredutíveis de grau e ordem dados. A seguinte terminologia será conveniente: se n e b, inteiros positivos relativamente primos então o menor inteiro positivo k para o qual $b^k \equiv 1 \pmod{n}$ é chamado de *ordem multiplicativa* de b módulo n.

Teorema 1.64 ([10], Teorema 3.5). *O número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau m e ordem α é igual a*

(i) $\frac{\varphi(\alpha)}{m}$ *se* $\alpha \geqslant 2$ *e* m *é a ordem multiplicativa de* $q \pmod{\alpha}$,

(ii) *2 se* $m = \alpha = 1$,

(iii) *0 em todos os outros casos.*

Demonstração.

Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ com $f(0) \neq 0$. Então de acordo com o Teorema 1.63, temos que $ord(f) = \alpha$ se, e somente se todas as raízes de f são raízes α-ésimas primitivas da unidade sobre $\mathbb{F}_q$. Em outras palavras, $ord(f) = \alpha$ se, e somente se f divide o polinômio ciclotômico Q_α. Pela condição **(ii)** do Teorema 1.58 , qualquer polinômio mônico irredutível de Q_α tem o mesmo grau m, o menor inteiro positivo tal que $q^m \equiv 1 \pmod{\alpha}$, e o número desses fatores é dado por $\frac{\varphi(\alpha)}{m}$. Para $m = \alpha = 1$, também temos que considerar em nossa contagem, o polinômio mônico irredutível $f(x) = x$. ■

Agora descrevemos um principio geral para obtermos novos polinômios irredutíveis de outros já conhecidos. Isso depende de um resultado técnico auxiliar de teoria dos números. Observamos que a ordem multiplicativa divide qualquer outro inteiro positivo h para o qual $b^h \equiv 1 \pmod{n}$.

Lema 1.65 ([10], Lema 3.34)**.** *Seja* $s \geqslant 2$ *e* $\alpha \geqslant 2$ *inteiros relativamente primos, e* m *a ordem multiplicativa de* s *módulo* α*. Seja* $t \geqslant 2$ *um inteiro tal que seus fatores primos dividem* α *mas não dividem* $\frac{(s^m-1)}{\alpha}$*. Assuma também que* $s^m \equiv 1 \pmod{4}$ *se* $t \equiv 0 \pmod{4}$*. Então a ordem multiplicativa de* $s \pmod{\alpha t}$ *é igual a* mt*.*

Teorema 1.66 ([10], Teorema 3.35)**.** *Sejam* $f_1(x), f_2(x), \ldots, f_N(x)$ *todos os polinômios mônicos irredutíveis e distintos em* $\mathbb{F}_q[x]$*, de grau* m *e ordem* α*, e seja* $t \geqslant 2$ *um inteiro cujos fatores primos dividem* α *mas não dividem* $\frac{(q^m-1)}{\alpha}$*. Assuma também que* $q^m \equiv 1 \pmod{4}$ *se* $t \equiv 0 \pmod{4}$*. Então* $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ *são todos os polinômios mônicos irredutíveis distintos em* $\mathbb{F}_q[x]$ *de grau* mt *e ordem* αt*.*

Demonstração.

A condição sobre α implica que $\alpha \geqslant 2$. De acordo com o Teorema 1.64, polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau m e ordem $\alpha \geqslant 2$ existem, somente se m é a ordem multiplicativa de $q \pmod{\alpha}$, e então o número de tais polinômios é $N = \frac{\varphi(\alpha)}{m}$. Pelo Lema 1.65 a ordem multiplicativa de $q \pmod{\alpha t}$ é igual a mt, e desde que $\frac{\varphi(\alpha)}{m}$ pela fórmula no item **(iii)** da Proposição 1.48 e usando o fato que todo primo que divide t também divide α, segue que o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau mt e ordem αt é

$$\frac{\varphi(\alpha t)}{mt} = \frac{t\varphi(\alpha)}{mt} = \frac{\varphi(\alpha)}{m} = N.$$

Além disso, isso nos mostra que cada um dos polinômios $f_j(x^t)$, $1 \leqslant j \leqslant N$, é irredutível em $\mathbb{F}_q[x]$ e de ordem αt. Uma vez que, as raízes de cada $f_j(x)$ são raízes α-ésimas primitivas da unidade sobre $\mathbb{F}_q$ pelo Teorema 1.63, segue que $f_j(x)$ divide o polinômio ciclotômico $Q_\alpha(x)$ sobre $\mathbb{F}_q$. Então $f_j(x^t)$ divide $Q_\alpha(x^t)$, e usando repetidamente o item **(i)** da Proposição 1.57 mostramos que $Q_\alpha(xt) = Q_{\alpha t}(x)$. Desse modo $f_j(x^t)$ divide $Q_{\alpha t}(x)$. De acordo com o item **(ii)** do Teorema 1.58, o grau de cada fator irredutível de $Q_{\alpha t}(x)$ em $\mathbb{F}_q[x]$ é igual à ordem multiplicativa de $q \pmod{\alpha t}$, que pelo Lema 1.65 é mt. Portanto, $f_j(x^t)$ tem grau mt, segue que $f_j(x^t)$ é irredutível em $\mathbb{F}_q[x]$. Além disso, desde que $f_j(x^t)$ divide $Q_{\alpha t}(x)$, a ordem de $f_j(x^t)$ é αt. ■

Exemplo 1.67. *Os polinômios irredutíveis em $\mathbb{F}_2[x]$ de grau 4 e ordem 15 são $x^4 + x + 1$ e $x^4 + x^3 + 1$. Então os polinômios irredutíveis em $\mathbb{F}_2[x]$ de grau 12 e ordem multiplicativa 45 são $x^{12} + x^3 + 1$ e $x^{12} + x^9 + 1$. Os polinômios irredutíveis em $\mathbb{F}_2[x]$ de grau 60 e ordem 225 são $x^{60} + x^{15} + 1$ e $x^{60} + x^{45} + 1$. Os polinômios irredutíveis em $\mathbb{F}_2[x]$ de grau 100 e ordem 375 são $x^{100} + x^{25} + 1$ e $x^{100} + x^{75} + 1$.*

O próximo teorema nos diz a quantidade desses polinômios irredutíveis que encontramos.

Teorema 1.68 ([10], Teorema 3.37)**.** *Sejam $f_1(x), f_2(x), \ldots, f_N(x)$ todos os polinômios mônicos irredutíveis, distintos em $\mathbb{F}_q[x]$ de grau ímpar m e ordem α. Seja $q = 2^a u - 1$, $t = 2^b v$ com $a, b \geqslant 2$, onde u, v são ímpares e todos os fatores primos de t dividem α mas não $\frac{q^m-1}{\alpha}$. Se $k = min\{a, b\}$ então cada polinômio $f_j(x^t)$ se fatora como um produto de 2^{k-1} polinômios mônicos irredutíveis $g_{ij}(x)$ em $\mathbb{F}_q[x]$ de grau $mt2^{1-k}$. Os $2^{k-1}N$ polinômios $g_{ij}(x)$ são todos distintos e irredutíveis em $\mathbb{F}_q[x]$ de grau $mt2^{1-k}$ e ordem αt.*

1.2.4 Fatores Irredutíveis

No que segue, estudaremos polinômios irredutíveis com algumas característica especiais.

Um *binômio* é um polinômio com dois coeficientes diferentes de zero, onde um deles é o termo constante. Um *trinômio* é um polinômio com três coeficientes diferentes de zero, onde um deles é o termo constante. Binômios irredutíveis podem ser caracterizados explicitamente. Para esse propósito é suficiente considerarmos binômios mônicos não lineares.

O teorema a seguir trata da irredutibilidade de tais polinômios.

Teorema 1.69 ([10], Teorema 3.75)**.** *Seja $t \geqslant 2$ um inteiro e $a \in \mathbb{F}_q^*$. Então o binômio $x^t - a$ é irredutível em $\mathbb{F}_q[x]$ se, e somente se as seguintes duas condições são satisfeitas.*

(i) *cada fator primo de t divide a ordem α de $a \in \mathbb{F}_q$, mas não $\frac{q-1}{\alpha}$,*

(ii) *se t for divisível por 4 então $q \equiv 1 \pmod 4$.*

Demonstração.

Suponha que os itens **(i)** e **(ii)** são satisfeitos. Notamos que $f(x) = x - a$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de ordem α, e assim $f(x^t) = x^t - a$ é irredutível em $\mathbb{F}_q[x]$, pelo Teorema 1.66.

Suponha que o item **(i)** seja violado. Então existe um fator primo r de t que divide $\frac{q-1}{\alpha}$ ou não divide α. No primeiro caso temos que $rs = \frac{q-1}{\alpha}$ para algum $s \in \mathbb{N}$. O subgrupo de $\mathbb{F}_q^*$ consistindo de todas as r-ésimas potências, tem ordem $\frac{q-1}{\alpha} = rs$ desse modo, contém um subgrupo de $\mathbb{F}_q^*$ de ordem α gerado por a. Em particular, $a = b^r$ para algum $b \in \mathbb{F}_q^*$, e assim $x^t - a = x^{t_1 r} - b^r$ tem um fator $x^{t_1} - b$. No outro caso, r não divide $\frac{q-1}{\alpha}$ nem α e assim r não divide $q-1$. Então $r_1 r \equiv 1 \pmod{q-1}$ para algum $r_1 \in \mathbb{N}$, e assim $x^t - a = x^{t_1 r} - a^{r_1 r}$ tem um fator $x^{t_1} - a^{r_1}$.

Finalmente suponha que o item **(i)** seja satisfeito e o item **(ii)** violado. Então $t = 4t_2$ para algum $t_2 \in \mathbb{N}$ e $q \not\equiv 1 \pmod 4$. Mas o item **(i)** implica que α é par, e como α divide $q-1$ devemos ter q ímpar. Assim, $q \equiv 3 \pmod 4$. O fato de $x^t - a$ ser redutível em $\mathbb{F}_q[x]$ é então consequência do Teorema 1.68. ■

Agora vamos descrever explicitamente os fatores irredutíveis de $x^n - 1$ sobre $\mathbb{F}_q$ quando $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e q é potência de um primo tal que $mdc(n, q) = 1$. Para cada primo p e cada inteiro m, $\nu_p(m)$ denotará a máxima potência de p que divide m e $rad(m)$ denota o radical de m, i.e., se $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$ é a fatoração de m em fatores primos, então $rad(m) = p_1 p_2 \cdots p_l$. Nos baseamos parcialmente em [3]. O próximo teorema nos auxilia nessa descrição.

Teorema 1.70 ([3], Teorema 1)**.** *Seja $\mathbb{F}_q$ um corpo finito e $n \in \mathbb{N}$ com*

(i) *$q \equiv 1 \pmod 4$ ou $8 \nmid n$,*

(ii) *$rad(n)$ divide $q-1$.*

Então todo fator irredutível de $x^n - 1$ é da forma $x^t - a$ onde, t divide $\frac{n}{mdc(n,q-1)}$, $a \in \mathbb{F}_q$ e $ord_q(a)$ divide $mdc(\frac{n}{t}, q-1)$.

Demonstração.

Provaremos esse teorema por indução sobre $\Omega(n)$, o número total de fatores primos de n (i.e., $\Omega(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_k$, onde $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$). Temos dois casos a considerar.

1. $n \mid (q-1)$.

   Pelo Teorema 1.30 sabemos que existe θ elemento gerador do grupo multiplicativo $\mathbb{F}_q^*$. Como $(\theta^{(q-1)/n})^n = \theta^{q-1} = 1$ segue que, $\zeta_n = \theta^{(q-1)/n}$ é raiz

n-ésima primitiva da unidade que pertence a $\mathbb{F}_q$ e portanto temos que

$$x^n - 1 = \prod_{j=0}^{n-1} (x - \zeta_n^j)$$

é a fatoração do polinômio $x^n - 1$ no anel de polinômios $\mathbb{F}_q[x]$. Em particular, se $\Omega(n) = 1$ então $n = rad(n)$ é um primo que divide $q - 1$, portanto o primeiro passo da indução é verdadeiro.

2. $n \nmid (q-1)$ mas, $rad(n) \mid (q-1)$.

   Suponhamos que o resultado seja verdadeiro para todo n tal que $rad(n) \mid (q-1)$ e $\Omega(n) \leqslant N \in \mathbb{N}$, para algum $N \geqslant 1$.

   Consideremos n um inteiro tal que $rad(n) \mid (q-1)$ e $\Omega(n) = N + 1$. Assim

$$x^n - 1 = \prod_{d|n} Q_d(x) = Q_n(x) \cdot \prod_{\substack{d|n \\ d \neq n}} Q_d(x),$$

   mas se $d \neq n$ e $d \mid n$ então $\Omega(d) \leqslant N$. Como $Q_d(x) \mid (x^d - 1)$ segue da hipótese de indução que todo fator de $Q_d(x)$ é da forma $x^t - a$, onde t divide $\frac{d}{mdc(d,q-1)}$. Observe que, para todo primo p, $\nu_p(d) \leqslant \nu_p(n)$, assim

$$\begin{aligned} \nu_p(d) - \nu_p(mdc(d, q-1)) &= \nu_p(d) - min\{\nu_p(d), \nu_p(q-1)\} \\ &\leqslant \nu_p(n) - min\{\nu_p(n), \nu_p(q-1)\}, \end{aligned}$$

   desse modo $\frac{d}{mdc(d,q-1)}$ divide $\frac{n}{mdc(d,q-1)}$. Donde segue que t divide $\frac{n}{mdc(d,q-1)}$. Além disso

$$ord_q(a) \mid mdc(\frac{d}{t}, q-1) \mid mdc(\frac{n}{t}, q-1).$$

   Portanto é suficiente verificar o resultado para os fatores de $Q_n(x)$. Como o teorema é válido quando $n \mid (q-1)$, podemos supor sem perda de generalidade $n \nmid (q-1)$, então existe um número primo p divisor de n, tal que $\nu_p(n) > \nu_p(q-1) \geqslant \nu_p(rad(n)) = 1$. Logo, podemos assumir que $n = pm$ com $\nu_p(m) \geqslant \nu_p(q-1) \geqslant 1$.

   Neste ponto dividiremos a demostração em dois casos.

   2.1. $p \neq 2$ ou $q \equiv 1 \pmod 4$.

   Pelo item **(i)** da Proposição 1.57 segue que

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

   Como $\Omega(m) = N < N + 1 = \Omega(n)$, pela hipótese de indução, todo

fator irredutível de $Q_m(x)$ é da forma $x^t - a$. Logo $Q_m(x^p)$ é fatorado como produto de fatores da forma $x^{tp} - a$, onde t divide $\frac{m}{mdc(m,q-1)} = \frac{m}{mdc(mp,q-1)}$. Portanto, tp divide $\frac{mp}{mdc(mp,q-1)} = \frac{n}{mdc(n,q-1)}$. Assim $rad(t)$ divide $ord_q(a)$ e $mdc\left(tp, \frac{q-1}{ord_q(a)}\right) = 1$ ou p.

Se $mdc\left(tp, \frac{q-1}{ord_q(a)}\right) = 1$ então $\nu_p(ord_q(a)) = \nu_p(q-1) \geqslant 1$. Desse modo p divide $ord_q(a)$ e $rad(tp)$ divide $ord_q(a)$, assim, a condição **(i)** do Teorema 1.69 é satisfeita. Além disso, se $q \equiv 3 \pmod 4$ segue que $p \neq 2$. Como por hipótese de indução sabemos que $4 \nmid t$, segue que $4 \nmid tp$, consequentemente a condição **(ii)** do Teorema 1.69 é também satisfeita e daí temos que $x^{tp} - a$ é irredutível.

Caso contrário, $mdc\left(tp, \frac{q-1}{ord_q a}\right) = p$, temos que $\nu_p(q-1) > \nu_p(ord_q(a))$ e $p \nmid t$. Como $\mathbb{F}_q^* = \langle\theta\rangle$ temos que $a = \theta^s$ para algum $s \in \mathbb{N}$ e $ord_q(a) = \frac{q-1}{mdc(q-1,s)}$ donde $p \mid s$. Desse modo, existe $b \in \mathbb{F}_q^*$ tal que $a = b^p$ e como $\zeta_p \in \mathbb{F}_q$ é uma raiz p-ésima primitiva da unidade, segue que

$$x^{tp} - a = x^{tp} - b^t = \prod_{j=0}^{p-1}(x^t - \zeta_p^j b)$$

é uma fatoração em $\mathbb{F}_q[x]$. Note que

$$mdc\left(t, \frac{q-1}{ord_q(\zeta_p^j b)}\right) = mdc\left(t, \frac{q-1}{mmc(ord_q(\zeta_p^j), ord_q(b))}\right),$$

mas sabemos que

$$mdc\left(t, \frac{q-1}{ord_q(a)}\right) = 1$$

e

$$mdc\left(tp, \frac{q-1}{ord_q(a)}\right) = p,$$

portanto t não tem fator p e assim

$$mdc\left(t, \frac{q-1}{mmc(ord_q\zeta_p^j, ord_q b)}\right) = 1$$

e novamente pelo Teorema 1.69 segue que cada fator da forma $x^t - \zeta_p^j b$ é um fator irredutível de $x^n - 1$. Isso completa o primeiro caso.

2.2. $p = 2$, $q \equiv 3 \pmod 4$ e $\nu_{p'}(n) \leqslant \nu_{p'}(q-1)$ para todo p' fator primo ímpar de n.

Como $8 \nmid n$ temos que $n = 2m$ ou $n = 4m$ com m ímpar. Das hipóteses do teorema segue que $q - 1 \equiv 2 \pmod 4$, uma vez que $q \equiv 3 \pmod 4$.

Observe que $n \neq 2m$, desde que $n \nmid (q-1)$ e $m \mid (q-1)$. Assim, $n = 4m$. Pelos itens **(i)** e **(iv)** da Proposição 1.57 temos que

$$Q_n(x) = Q_{4m}(x) = Q_{2m}(x^2) = Q_m(-x^2).$$

Como $m \mid (q-1)$ podemos escrever

$$Q_m(x) = \prod_{\substack{mdc(m,j)=1 \\ 1 \leqslant j \leqslant m}} (x - \zeta_m^j).$$

Desse modo

$$\begin{aligned} Q_n(x) &= Q_m(-x^2) \\ &= \prod_{mdc(m,j)=1} (-x^2 - \zeta_m^j) \\ &= (-1)^{\varphi(m)} \prod_{mdc(m,j)=1} (-x^2 - (-\zeta_m^j)) \\ &= \prod_{mdc(m,j)=1} (-x^2 - (-\zeta_m^j)). \end{aligned}$$

Sabemos que

$$ord_q(-\zeta_m^j) = mmc(ord_q(-1), ord_q(\zeta_m^j)) = mmc(2, ord_q(\zeta_m^j)) = 2m.$$

Portanto, $t = 2$ divide $ord_q(-\zeta_m^j)$ e assim $rad(t) \mid ord_q(-\zeta_m^j)$. Por outro lado, $\frac{q-1}{ord_q(-\zeta_m^j)}$ é ímpar uma vez que, $2 \mid (q-1)$ e $ord_q(-\zeta_m^j) = 2m$. Então pelo Teorema 1.69 temos que $x^2 + \zeta_m^j$ é irredutível sobre $\mathbb{F}_q[x]$.

■

No próximo corolário, analisamos a fatoração de $x^n - 1$ no caso que $8 \mid n$ e $q \equiv 3 \pmod 4$.

Teorema 1.71 ([3], Teorema 2)**.** *Se $q \equiv 3 \pmod 4$, $8 \mid n$ e $rad(n) \mid (q-1)$, então os fatores irredutíveis de $x^n - 1$ em $\mathbb{F}_q[x]$ são dos seguintes tipos*

(i) *$x^t - a$, se $a \in \mathbb{F}_q \subset \mathbb{F}_{q^2}$ e $ord_{q^2} a$ divide $mdc(\frac{n}{t}, q-1)$,*

(ii) *$x^{2t} - (b + b^q)x^t + b^{q+1}$, se $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ e $ord_{q^2} b$ divide $mdc(\frac{n}{t}, q^2 - 1)$.*

Demonstração.

Seja $f(x)$ um fator irredutível de $x^n - 1$ sobre $\mathbb{F}_q[x]$. Então temos dois casos.

1. $f(x)$ é um binômio.

   O Teorema 1.70 garante o resultado.

2. $f(x)$ não é um binômio.

   Primeiramente observemos que se $q \equiv 3 \pmod 4$ então $q^2 \equiv 1 \pmod 4$, assim pelo Teorema 1.70 segue que os fatores irredutíveis de $x^n - 1$ sobre $\mathbb{F}_{q^2}[x]$ são da forma $x^t - a$, onde

   (a) t divide $\dfrac{n}{mdc(n, q^2-1)}$,

   (b) $a \in \mathbb{F}_{q^2}$,

   (c) $ord_{q^2}(a)$ divide $mdc(\frac{n}{t}, q^2 - 1)$.

   Desse modo, $f(x)$ é redutível sobre $\mathbb{F}_{q^2}$. Assim existe $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ tal que o binômio $x^t - b$ divide $f(x)$.

   Considerando a transformação de Frobenius

$$\begin{aligned} \tau_q : \mathbb{F}_{q^2} &\to \mathbb{F}_{q^2} \\ b &\mapsto b^q. \end{aligned}$$

   Observamos que, τ_q restrita a $\mathbb{F}_q$ é o homomorfismo identidade. Como, por hipótese, $x^t - b$ divide $f(x)$ segue que $\tau_q(x^t - b)$ divide $\tau_q(f(x))$ e desse modo $x^t - \tau_q(b)$ divide $f(x)$. Assim, $x^t - b^q$ também divide $f(x)$, mas $b \neq b^q$, e portanto, $(x^t - b)(x^t - b^q)$ divide $f(x)$. Logo, $x^{2t} - (b + b^q)x^t + b^{q+1}$ divide $f(x)$.

   Mas note que, $\tau_q(x^{2t} - (b + b^q)x^t + b^{q+1}) = x^{2t} - (b + b^q)x^t + b^{q+1}$ então $x^{2t} - (b + b^q)x^t + b^{q+1} \in \mathbb{F}_q[x]$, como $f(x)$ é irredutível sobre $\mathbb{F}_q[x]$, segue que $f(x) = x^{2t} - (b + b^q)x^t + b^{q+1}$.

■

Capítulo 2

Polinômios de Dickson

Apresentamos agora uma classe especial de polinômios chamados polinômios de Dickson. Esses polinômios são úteis em aspectos tanto teóricos como aplicados, e têm sido amplamente estudados, pois geram polinômios de permutação, isto é, sob algumas condições, os polinômios de Dickson podem ser vistas como funções bijetivas $\mathbb{F}_q$ em $\mathbb{F}_q$ que possuem inverso de mesmo tipo. Uma excelente referência para os polinômios de Dickson é [9]. Desta referência se baseiam os resultados das seções 2.1 e 2.2 deste capítulo.

2.1 Polinômios de Dickson do primeiro tipo

2.1.1 Definição dos polinômios de Dickson do primeiro tipo

Para cada $n \geqslant 1$, seja $S_n = x_1^n + x_2^n$ a soma de n-potências em duas variáveis. Temos que S_n é um polinômio simétrico, e pelo teorema fundamental dos polinômios simétricos elementares (Teorema 1.21), pode ser escrito como um polinômio em termos dos polinômios simétricos elementares $e_1 = x_1 + x_2$ e $e_2 = x_1 x_2$. Essa representação pode ser obtida pela Fórmula de Waring (Teorema 1.22) da seguinte forma

$$S_n = x_1^n + x_2^n = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-e_2)^i (e_1)^{n-2i}.$$

Do anterior temos que $S_1 = e_1$ e $S_2 = e_1^2 - 2e_2$. Logo, em $\mathbb{Z}[x_1, x_2]$ a equação quadrática

$$z^2 - e_1 z + e_2 = 0 \tag{1}$$

tem raízes x_1 e x_2.

Multiplicando (1) por z^{n-2}, encontramos, substituindo z por x_1 e x_2, que

$$x_1^n = e_1 x_1^{n-1} - e_2 x_1^{n-2} \tag{2}$$

e

$$x_2^n = e_1 x_2^{n-1} - e_2 x_2^{n-2}, \tag{3}$$

logo, somando as equações (2) e (3), temos que S_n satisfaz a relação de recorrência

$$S_n = e_1 S_{n-1} - e_2 S_{n-2},$$

para todo $n \geqslant 3$, com condições iniciais $S_1 = e_1$ e $S_2 = e_1^2 - 2e_2$. Segue que S_n é um polinômio em e_1 e e_2 com coeficientes inteiros.

Definição 2.1. *Seja $n \geqslant 1$ um inteiro. Os polinômios $D_n(x, w)$ sobre $\mathbb{Z}[x, w]$ são definidos como*

$$D_n(x, w) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-w)^i x^{n-2i}. \tag{4}$$

Onde $\lfloor c \rfloor$ denota o maior inteiro $\leq c$.

A abordagem original para definir os polinômios $D_n(x, w)$ era fazer uso de uma relação entre somas de n potencias e funções simétricas elementares

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1 x_2).$$

Agora, podemos definir os polinômios $D_n(x, a)$ sobre $\mathbb{F}_q$ com $a \in \mathbb{F}_q$.

Definição 2.2. *Seja $n \geqslant 1$ um inteiro e $a \in \mathbb{F}_q$. Os polinômios $D_n(x, a) \in \mathbb{F}_q[x]$ definidos como*

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i} \tag{5}$$

*são chamados **polinômios de Dickson do primeiro tipo de grau n na indeterminada x e com parâmetro a.***

Observação 2.3.

1. *Os polinômios de Dickson $D_n(x, a)$ são mônicos.*
2. *Notemos que se $a = 0$, $D_n(x, 0) = x^n$. Logo os polinômios de Dickson $D_n(x, a)$ podem se olhar como uma generalização dos polinômios de potências x^n.*

Exemplo 2.4. *Seja $\mathbb{F}_7$ o corpo finito com 7 elementos. Abaixo apresentamos os polinô-*

mios de Dickson de grau n, com $0 \leqslant n \leqslant 10$.

$$\begin{aligned}
D_0(x,a) &= 2\\
D_1(x,a) &= x\\
D_2(x,a) &= x^2+5\\
D_3(x,a) &= x^3+4x\\
D_4(x,a) &= x^4+3x^2+2\\
D_5(x,a) &= x^5+2x^3+5x\\
D_6(x,a) &= x^6+x^4+2x^2+5\\
D_7(x,a) &= x^7\\
D_8(x,a) &= x^8+6x^6+6x^4+5x^2+2\\
D_9(x,a) &= x^9+5x^7+6x^5+5x^3+9\\
D_{10}(x,a) &= x^{10}+4x^8+6x^4+4x^2+5.
\end{aligned}$$

2.1.2 Propriedades dos polinômios de Dickson do primeiro tipo

Agora, para descrever algumas propriedades dos polinômios de Dickson, primeiro provamos o seguinte teorema.

Teorema 2.5. *Os polinômios de Dickson do primeiro tipo satisfazem a equação funcional*

$$D_n\left(y+\frac{a}{y},a\right)=y^n+\left(\frac{a}{y}\right)^n, \tag{6}$$

onde $a \in \mathbb{F}_q$ *e* $y \neq 0$ *é uma indeterminada.*

Demonstração.

Seja $y \neq 0$ uma indeterminada tal que $x = y + \frac{a}{y}$. Então temos a equação quadrática $P(y) = y^2 - xy + a = 0$, logo $\mathbb{F}_q[y]$ é uma extensão algébrica de $\mathbb{F}_q[x]$ de grau 2. Formalmente

$$y_1=\frac{x+\sqrt{x^2-4a}}{2} \qquad \text{e} \qquad y_2=\frac{x-\sqrt{x^2-4a}}{2}$$

são raízes da equação $P(y) = 0$. A regra de Vieta implica que x é a soma das raízes dessa equação quadrática e o termo constante a é produto das raízes.

Sejam x_1 e x_2 indeterminadas. Lembremos que os polinômios de Dickson do primeiro tipo surgem da Fórmula de Waring (Teorema 1.22) que garante:

$$x_1^n+x_2^n=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\binom{n-i}{i}(-x_1x_2)^i(x_1+x_2)^{n-2i}$$

e assim, se $x_1 = y$, $x_2 = \frac{a}{y}$ e $x = y + \frac{a}{y}$, obtemos

$$\begin{aligned} y^n + \left(\frac{a}{y}\right)^n &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}\left(-y\left(\frac{a}{y}\right)\right)^i \left(y + \left(\frac{a}{y}\right)\right)^{n-2i} \\ &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i \left(y + \frac{a}{y}\right)^{n-2i}. \end{aligned}$$

Portanto,

$$D_n(x,a) = D_n\left(y + \frac{a}{y}, a\right) = y^n + \left(\frac{a}{y}\right)^n.$$

■

Observação 2.6. *Temos a representação alternativa formal dos polinômios de Dickson do primeiro tipo como*

$$D_n(x,a) = \left(\frac{x + \sqrt{x^2 - 4a}}{2}\right)^n + \left(\frac{x - \sqrt{x^2 - 4a}}{2}\right)^n.$$

A equação funcional do Teorema 2.5 é a propriedade mais importante dos polinômios de Dickson do primeiro tipo e é frequentemente usada para obter propriedades de $D_n(x,a)$. Uma forma fácil de gerar polinômios de Dickson é através de relações de recorrência.

Lema 2.7 ([9], Lema 2.3)**.** *$D_n(x,a)$ satisfaz a relação de recorrência de segunda ordem*

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a), \tag{7}$$

para $n \geq 2$ com valores iniciais $D_0(x,a) = 2$ e $D_1(x,a) = x$.

Demonstração.

Segue imediatamente da representação em (6) para $D_n(x,a)$ e para $x = y + \frac{a}{y}$.

$$\begin{aligned} xD_{n-1}(x,a) - aD_{n-2}(x,a) &= \left(y + \frac{a}{y}\right) D_{n-1}\left(y + \frac{a}{y}, a\right) - aD_{n-2}\left(y + \frac{a}{y}, a\right) \\ &= \left(y + \frac{a}{y}\right)\left[y^{n-1} + \left(\frac{a}{y}\right)^{n-1}\right] - a\left[y^{n-2} + \left(\frac{a}{y}\right)^{n-2}\right] \\ &= y^n + ay^{n-2} + \frac{a^{n-1}}{y^{n-2}} + \left(\frac{a}{y}\right)^n - ay^{n-2} - \frac{a^{n-1}}{y^{n-2}} \\ &= y^n + \left(\frac{a}{y}\right)^n = D_n\left(y + \frac{a}{y}, a\right) = D_n(x,a). \end{aligned}$$

■

Temos algumas outras propriedades.

Lema 2.8 ([9], Lema 2.6)**.** *Os polinômios de Dickson $D_n(x,a)$ satisfazem o seguinte*

(i) $D_{mn}(x,a) = D_m(D_n(x,a),a^n)$ *para* $m \geqslant 0$ *e* $n \geqslant 0$,

(ii) $D_{np^r}(x,a) = [D_n(x,a)]^{p^r}$ *para* $n \geqslant 0$, $r \geqslant 0$ *e onde* p *é a característica de* $\mathbb{F}_q$,

(iii) $b^n D_n(x,a) = D_n(bx, b^2a)$ *para* $n \geqslant 0$,

(iv) $b^n D_n(b^{-1}x,a) = D_n(x,b^2a)$ *para* $n \geqslant 0$ *e* $b \neq 0$.

Demonstração.

(i)
$$\begin{aligned} D_{mn}(x,a) &= D_{mn}\left(y+\frac{a}{y},a\right) = y^{mn} + \left(\frac{a}{y}\right)^{mn} = D_m\left(y^n + \left(\frac{a}{y}\right)^n, a^n\right) \\ &= D_m\left(D_n\left(y+\frac{a}{y},a\right),a^n\right) = D_m(D_n(x,a),a^n). \end{aligned}$$

(ii)
$$\begin{aligned} D_{np^r}(x,a) &= D_{np^r}\left(y+\frac{a}{y},a\right) = y^{np^r} + \left(\frac{a}{y}\right)^{np^r} = \left[y^n + \left(\frac{a}{y}\right)^n\right]^{p^r} \\ &= \left[D_n\left(y+\frac{a}{y},a\right)\right]^{p^r} = [D_n(x,a)]^{p^r}. \end{aligned}$$

(iii)
$$\begin{aligned} b^n D_n(x,a) &= b^n D_n\left(y+\frac{a}{y},a\right) = b^n\left[y^n + \left(\frac{a}{y}\right)^n\right] = (by)^n + \left(\frac{ba}{y}\right)^n \\ &= (by)^n + \left(\frac{b^2a}{by}\right)^n = D_n\left(by+\frac{b^2a}{by}, b^2a\right) = D_n\left(by+\frac{ba}{y}, b^2a\right) \\ &= D_n\left(b\left(y+\frac{a}{y}\right), b^2a\right) = D_n(bx, b^2a). \end{aligned}$$

(iv) Do item **(iii)**

$$b^n D_n(b^{-1}x,a) = D_n(bb^{-1}x, b^2a) = D_n(x,b^2a).$$

■

Observação 2.9.

1. *Em particular, quando* $a = 0$ *ou* 1*, da condição* ***(i)*** *do lema anterior temos que o polinômio de Dickson* $D_n(x,a)$ *do primeiro tipo satisfaz*

$$D_{mn}(x,a) = D_m(D_n(x,a),a) = D_m(x,a) \circ D_n(x,a),$$

onde $\circ$ *denota a composição de polinômios, logo a comutatividade dos inteiros* m*,* n *implica a propriedade comutativa baixo a composição*

$$D_m(x,a) \circ D_n(x,a) = D_{mn}(x,a) = D_{nm}(x,a) = D_n(x,a) \circ D_m(x,a).$$

2. *Se q é par, então podemos expressar cada polinômio de Dickson $D_n(x,a)$, $a \in \mathbb{F}_q^*$, em termos de $D_n(x,1)$, pois como a característica de $\mathbb{F}_q$ é 2, para todo $a \in \mathbb{F}_q^*$ existe $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, então pela condição **(iv)** do lema anterior, temos*

$$D_n(x,a) = D_n(x,b^2) = b^n D_n(b^{-1}x,1).$$

Se q é ímpar, então podemos expressar cada polinômio de Dickson $D_n(x,a)$, $a \in \mathbb{F}_q^*$, em termos de $D_n(x,1)$ ou $D_n(x,c)$ onde c é fixo e não é um quadrado em $\mathbb{F}_q$. Para isso temos 2 casos:

   (a) *Se existir $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, então pela condição **(iv)** do lema anterior temos*
   $$D_n(x,a) = D_n(x,b^2) = b^n D_n(b^{-1}x,1).$$

   (b) *Quando não existir $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, então existem $b, c \in \mathbb{F}_q^*$ tais que $a = b^2 c$, onde c não é um quadrado em $\mathbb{F}_q$ (Notemos que se θ é um gerador de $\mathbb{F}_q^*$ e não existir $b \in \mathbb{F}_q^*$ tal que $b^2 = a$, então $a = \theta^n$ com n ímpar. Isto é, $a = (\theta^t)^2\theta$ onde $t \in \mathbb{N}$). Portanto*
   $$D_n(x,a) = D_n(x,b^2c) = b^n D_n(b^{-1}x,c).$$

Apenas como curiosidade apresentamos o seguinte lema.

Lema 2.10 ([9], Teorema 2.15)**.** *$D_n(x,a)$ satisfaz a equação diferencial*

$$(x^2 - 4a)D_n''(x,a) + xD_n'(x,a) - n^2 D_n(x,a) = 0.$$

Demonstração.

Começamos derivando

$$D_n\left(y + \frac{a}{y}, a\right) = y^n + \left(\frac{a}{y}\right)^n$$

e multiplicando o resultado por y temos

$$\left(y - \frac{a}{y}\right) D_n'(x,a) = n\left[y^n - \left(\frac{a}{y}\right)^n\right].$$

Fazendo o mesmo processo de novo temos

$$\left(y - \frac{a}{y}\right)^2 D_n''(x,a) + \left(y + \frac{a}{y}\right) D_n'(x,a) = n^2\left[y^n + \left(\frac{a}{y}\right)^n\right].$$

Como $x = y + \frac{a}{y}$ então $y^2 - 2a + \frac{a^2}{y^2} = x^2 - 4a$. ■

2.2 Polinômios de Dickson do segundo tipo

2.2.1 Definição dos polinômios de Dickson do segundo tipo

Seja $n \geqslant 1$ um inteiro, pela regra de Pascal temos que o coeficiente binomial $\binom{n-i}{i}$ é um inteiro no caso que $0 \leqslant i \leqslant \lfloor \frac{n}{2} \rfloor$ e $t \in \mathbb{Z}$.

Definição 2.11. *Seja $n \geqslant 1$ um inteiro. Os polinômios $E_n(x, w)$ sobre $\mathbb{Z}[x, w]$ são definidos como*

$$E_n(x, w) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-w)^i x^{n-2i}. \tag{8}$$

Portanto, isso justifica definir os polinômios $E_n(x, a)$ sobre $\mathbb{F}_q$ com $a \in \mathbb{F}_q$.

Definição 2.12. *Seja $n \geqslant 1$ um inteiro e $a \in \mathbb{F}_q$. Os polinômios $E_n(x, a) \in \mathbb{F}_q[x]$ definidos como*

$$E_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i} \tag{9}$$

*são chamados **polinômios de Dickson do segundo tipo de grau n na indeterminada x e com parâmetro** a.*

Observação 2.13.

1. *Os polinômios de Dickson $E_n(x, a)$ são mônicos.*
2. *Notemos que se $a = 0$, $E_n(x, 0) = x^n$. Logo os polinômios de Dickson $E_n(x, a)$ podem se olhar como uma generalização dos polinômios de potências x^n.*

2.2.2 Propriedades dos polinômios de Dickson do segundo tipo

Os polinômios de Dickson do segundo tipo $E_n(x, a)$ de grau n não tem sido estudados tanto quanto aqueles do primeiro tipo. Para descrever algumas propriedades dos polinômios de Dickson do segundo tipo, primeiro provamos os seguintes dois resultados.

Lema 2.14. *Os polinômios de Dickson do primeiro e segundo tipo satisfazem a relação de recorrência mutua*

$$E_n(x, a) = aE_{n-2}(x, a) + D_n(x, a), \tag{10}$$

para $n \geqslant 2$.

Demonstração.

Pela definição do polinômio de Dickson do segundo tipo

$$\begin{aligned} & E_n(x,a) - aE_{n-2}(x,a) \\ &= \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i} - a \sum_{j=0}^{\lfloor \frac{n-2}{2} \rfloor} \binom{n-2-j}{j} (-a)^j x^{n-2-2j}. \end{aligned} \tag{11}$$

Fazemos a mudança de variável $j = i - 1$, então

$$-a \sum_{j=0}^{\lfloor \frac{n-2}{2} \rfloor} \binom{n-2-j}{j} (-a)^j x^{n-2-2j} = \sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n-i-1}{i-1} (-a)^i x^{n-2i}. \tag{12}$$

Substituindo (12) em (11), obtemos

$$\begin{aligned} & E_n(x,a) - aE_{n-2}(x,a) \\ &= x^n + \sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i} + \sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n-i-1}{i-1} (-a)^i x^{n-2i} \\ &= x^n + \sum_{i=1}^{\lfloor n/2 \rfloor} \left[\binom{n-i}{i} + \binom{n-i-1}{i-1} \right] (-a)^i x^{n-2i} \\ &= x^n + \sum_{i=1}^{\lfloor n/2 \rfloor} \left[\frac{n-i}{i} \binom{n-i-1}{i-1} + \binom{n-i-1}{i-1} \right] (-a)^i x^{n-2i} \\ &= x^n + \sum_{i=1}^{\lfloor n/2 \rfloor} \left(\frac{n-i}{i} + 1 \right) \binom{n-i-1}{i-1} (-a)^i x^{n-2i} \\ &= x^n + \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{n}{i} \binom{n-i-1}{i-1} (-a)^i x^{n-2i} \\ &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i} \\ &= D_n(x,a). \end{aligned}$$

■

Teorema 2.15. *Os polinômios de Dickson do segundo tipo satisfazem a equação funcional*

$$E_n\left(y + \frac{a}{y}, a\right) = \frac{y^{n+1} - \left(\frac{a}{y}\right)^{n+1}}{y - \frac{a}{y}}, \tag{13}$$

onde $a \in \mathbb{F}_q$ e $y \notin \{0, \pm\sqrt{a}\}$ é uma indeterminada. Para $y = \sqrt{a}$ e $y = -\sqrt{a}$, temos $E_n(2\sqrt{a}, a) = (n+1)(\sqrt{a})^n$ e $E_n(-2\sqrt{a}, a) = (n+1)(-\sqrt{a})^n$, respectivamente.

Demonstração.

Seja $y \neq 0$ uma indeterminada tal que $y - \frac{a}{y} \neq 0$, i.e. $y \neq \pm\sqrt{a}$. Vamos fazer

uma prova por indução sobre n o grau de $E_n(x,a)$.

(a) Para $n = 0$ temos

$$E_0(x,a) = E_0\left(y + \frac{a}{y}, a\right) = 1 = \frac{y - \frac{a}{y}}{y - \frac{a}{y}}.$$

Para $n = 1$ temos

$$E_1(x,a) = E_1\left(y + \frac{a}{y}, a\right) = y + \frac{a}{y} = \frac{\left(y + \frac{a}{y}\right)\left(y - \frac{a}{y}\right)}{y - \frac{a}{y}} = \frac{y^2 - \left(\frac{a}{y}\right)^2}{y - \frac{a}{y}}.$$

(b) Passo indutivo: Seja $n \in \mathbb{N}$ tal que $n > 0$. A afirmação é válida para todo m tal que $0 \leqslant m < n$. Devemos mostrar que a afirmação é válida para $m = n$.

Da relação de recorrência (10) temos que

$$\begin{aligned} E_n(x,a) = E_n\left(y + \frac{a}{y}, a\right) &= aE_{n-2}\left(y + \frac{a}{y}, a\right) + D_n\left(y + \frac{a}{y}, a\right) \\ &= aE_{n-2}\left(y + \frac{a}{y}, a\right) + y^n + \left(\frac{a}{y}\right)^n. \end{aligned} \tag{14}$$

Mas pela hipótese de indução

$$E_{n-2}\left(y + \frac{a}{y}, a\right) = \frac{y^{n-1} - \left(\frac{a}{y}\right)^{n-1}}{y - \frac{a}{y}}. \tag{15}$$

Substituindo (15) em (14), obtemos

$$\begin{aligned} E_n(x,a) &= E_n\left(y + \frac{a}{y}, a\right) = a\left[\frac{y^{n-1} - \left(\frac{a}{y}\right)^{n-1}}{y - \frac{a}{y}}\right] + y^n + \left(\frac{a}{y}\right)^n \\ &= \frac{ay^{n-1} - \frac{a^n}{y^{n-1}}}{y - \frac{a}{y}} + \frac{\left(y - \frac{a}{y}\right)\left[y^n + \left(\frac{a}{y}\right)^n\right]}{y - \frac{a}{y}} \\ &= \frac{ay^{n-1} - \frac{a^n}{y^{n-1}} + y^{n+1} + \frac{a^n}{y^{n-1}} - ay^{n-1} - \left(\frac{a}{y}\right)^{n+1}}{y - \frac{a}{y}} \\ &= \frac{y^{n+1} - \left(\frac{a}{y}\right)^{n+1}}{y - \frac{a}{y}}. \end{aligned}$$

Agora falta considerar o caso em que $y = \sqrt{a}$, daí que $x = y + \frac{a}{y} = 2\sqrt{a}$. Vamos fazer uma prova por indução sobre n o grau de $E_n(x,a)$ para mostrar que

$E_n(2\sqrt{a}, a) = (n+1)(\sqrt{a})^n$.

(a) Para $n = 0$ temos

$$E_0(2\sqrt{a}, a) = 1 = (0+1)(\sqrt{a})^0.$$

Para $n = 1$ temos

$$E_1(2\sqrt{a}, a) = 2\sqrt{a} = (1+1)(\sqrt{a})^1.$$

(b) Passo indutivo: Seja $n \in \mathbb{N}$ tal que $n > 0$. A afirmação é válida para todo m tal que $0 \leqslant m < n$. Devemos mostrar que a afirmação é válida para $m = n$.

Da relação de recorrência (10) temos que

$$\begin{aligned} E_n(2\sqrt{a}, a) &= aE_{n-2}\left(2\sqrt{a}, a\right) + D_n\left(2\sqrt{a}, a\right) \\ &= aE_{n-2}\left(2\sqrt{a}, a\right) + (\sqrt{a})^n + \left(\frac{a}{\sqrt{a}}\right)^n. \end{aligned} \tag{16}$$

Mas pela hipótese de indução

$$E_{n-2}\left(2\sqrt{a}, a\right) = (n-1)(\sqrt{a})^n. \tag{17}$$

Substituindo (17) em (16), obtemos

$$\begin{aligned} E_n(2\sqrt{a}, a) &= a(n-1)(\sqrt{a})^{n-2} + (\sqrt{a})^n + (\sqrt{a})^n \\ &= (n-1)(\sqrt{a})^n + 2(\sqrt{a})^n \\ &= (n+1)(\sqrt{a})^n. \end{aligned}$$

Procedemos de forma similar para mostrar que $E_n(-2\sqrt{a}, a) = (n+1)(-\sqrt{a})^n$. ■

Temos um resultado similar àquele apresentado no Lema 2.7.

Lema 2.16 ([9], Lema 2.3). *$E_n(x, a)$ satisfaz a relação de recorrência de segunda ordem*

$$E_n(x, a) = xE_{n-1}(x, a) - aE_{n-2}(x, a),$$

para $n \geq 2$ com valores iniciais $E_0(x, a) = 1$ e $E_1(x, a) = x$.

Demonstração.

Segue imediatamente da representação em (13) e para $x = y + \frac{a}{y}$.

$$\begin{aligned} xE_{n-1}(x,a) - aE_{n-2}(x,a) &= \left(y+\frac{a}{y}\right)E_{n-1}\left(y+\frac{a}{y},a\right) - aE_{n-2}\left(y+\frac{a}{y},a\right) \\ &= \left(y+\frac{a}{y}\right)\left[\frac{y^n - \left(\frac{a}{y}\right)^n}{y-\frac{a}{y}}\right] - a\left[\frac{y^{n-1}-\left(\frac{a}{y}\right)^{n-1}}{y-\frac{a}{y}}\right] \\ &= \frac{y^{n+1} + ay^{n-1} - \frac{a^n}{y^{n-1}} - \left(\frac{a}{y}\right)^{n+1} - ay^{n-1} + \frac{a^n}{y^{n-1}}}{y-\frac{a}{y}} \\ &= \frac{y^{n+1} - \left(\frac{a}{y}\right)^{n+1}}{y-\frac{a}{y}} = E_n\left(y+\frac{a}{y},a\right) = E_n(x,a). \end{aligned}$$

■

Temos algumas outras propriedades.

Lema 2.17. *Os polinômios de Dickson $E_n(x,a)$ satisfazem o seguinte*

(i) $E_n(x,a) = [E_m(x,a)]^{p^r}(x^2-4a)^{\frac{p^r-1}{2}}$ *para* $n \geqslant 0$ *e* $r \geqslant 0$, *onde* p *é a característica de* $\mathbb{F}_q$ *e* $n+1 = (m+1)p^r$,

(ii) $b^n E_n(x,a) = E_n(bx, b^2a)$ *para* $n \geqslant 0$,

(iii) $b^n E_n(b^{-1}x,a) = E_n(x,b^2a)$ *para* $n \geqslant 0$ *e* $b \neq 0$.

Demonstração.

(i)
$$\begin{aligned} E_n(x,a) = E_n\left(y+\frac{a}{y},a\right) &= \frac{y^{n+1}-\left(\frac{a}{y}\right)^{n+1}}{y-\frac{a}{y}} = \frac{y^{(m+1)p^r}-\left(\frac{a}{y}\right)^{(m+1)p^r}}{y-\frac{a}{y}} \\ &= \left[\frac{y^{m+1}-\left(\frac{a}{y}\right)^{m+1}}{y-\frac{a}{y}}\right]^{p^r}\left(y-\frac{a}{y}\right)^{p^r-1} = \left[E_m\left(y+\frac{a}{y},a\right)\right]^{p^r}\left(y-\frac{a}{y}\right)^{p^r-1} \\ &= [E_m(x,a)]^{p^r}(x^2-4a)^{\frac{p^r-1}{2}}. \end{aligned}$$

(ii)
$$\begin{aligned} b^nE_n(x,a) = b^nE_n\left(y+\frac{a}{y},a\right) &= b^n\left[\frac{y^{n+1}-\left(\frac{a}{y}\right)^{n+1}}{y-\frac{a}{y}}\right] = \frac{b^nby^{n+1}-\left(\frac{b^nba^{n+1}}{y^{n+1}}\right)}{by-\frac{ba}{y}} \\ &= \frac{(by)^{n+1}-\left(\frac{b^2a}{by}\right)^{n+1}}{by-\frac{b^2a}{by}} = E_n\left(by+\frac{b^2a}{by},b^2a\right) = E_n\left(by+\frac{ba}{y},b^2a\right) \\ &= E_n\left(b\left(y+\frac{a}{y}\right),b^2a\right) = E_n(bx,b^2a). \end{aligned}$$

(iii) Do item **(ii)**

$$b^n E_n(b^{-1}x, a) = E_n(bb^{-1}x, b^2a) = E_n(x, b^2a).$$

■

Assim como no caso dos polinômios de Dickson do primeiro tipo, apenas como curiosidade apresentamos o seguinte lema.

Lema 2.18 ([9], Teorema 2.15). *$E_n(x, a)$ satisfaz a equação diferencial*

$$(x^2 - 4a)E_n''(x, a) + 3xE_n'(x, a) - n(n+2)E_n(x, a) = 0.$$

Demonstração.

Procedemos de forma similar à prova do Lema 2.10 começando com a derivada da equação funcional (13). ■

2.3 a-recíprocos de Polinômios

Esta seção e a próxima se baseiam nos resultados de [8].

Definição 2.19. *Seja $a \in \mathbb{F}_q^*$. Para todo polinômio mônico f sobre $\mathbb{F}_q$ de grau n, com $f(0) \neq 0$, definimos o a-recíproco de f como sendo o polinômio*

$$f_a^*(x) = \frac{x^n}{f(0)} f\left(\frac{a}{x}\right).$$

Isto é, se $f(x) = \sum_{i=0}^n b_i x^i$ então $f_a^*(x) = \frac{1}{b_0}\sum_{i=0}^n b_i a^i x^{n-i}$.
Dizemos que o polinômio f é a-autorrecíproco se $f(x) = f_a^*(x)$.

Observação 2.20. *Notemos que a noção de polinômio 1-autorrecíproco é a noção usual de polinômio autorrecíproco.*

Lema 2.21.

(i) *f_a^* é mônico e se α é uma raiz de f então $\frac{a}{\alpha}$ é uma raiz de f_a^*,*

(ii) *o a-recíproco do produto de dois polinômios é o produto dos a-recíprocos dos polinômios dados,*

(iii) *o polinômio $f(x)$ é irredutível sobre $\mathbb{F}_q$ se, e somente se f_a^* é irredutível sobre $\mathbb{F}_q$.*

Demonstração.

(i) $f_a^*\left(\frac{a}{\alpha}\right) = \frac{\left(\frac{a}{\alpha}\right)^n}{f(0)} f\left(\frac{a}{\left(\frac{a}{\alpha}\right)}\right) = \frac{\left(\frac{a}{\alpha}\right)^n}{f(0)} f(\alpha) = 0.$

(ii) Sejam $r(x)$ e $t(x)$ dois polinômios mônicos de graus n e m respectivamente e tais que $r(0) \neq 0$ e $t(0) \neq 0$. Então

$$(rt)_a^*(x) = \frac{x^{n+m}}{rt(0)}(rt)\left(\frac{a}{x}\right) = \frac{x^n}{r(0)}r\left(\frac{a}{x}\right)\cdot\frac{x^m}{t(0)}t\left(\frac{a}{x}\right) = r_a^*(x)t_a^*(x).$$

(iii) Vamos provar que se $f(x)$ é redutível, então $f_a^*(x)$ é redutível. Suponhamos que $f(x) = r(x)t(x)$ com $\deg r(x)$, $\deg t(x) \geqslant 1$, usando o item **(ii)** temos que $f_a^*(x) = r_a^*(x)t_a^*(x)$ com $\deg r_a^*(x) = \deg r(x) \geqslant 1$ e $\deg t_a^*(x) = \deg t(x) \geqslant 1$, portanto $f_a^*(x)$ é redutível.

Seja $h(x) = f_a^*(x)$. Notemos que $h(0) = f_a^*(0) = \frac{a^n}{f(0)}$, então

$$h_a^*(x) = \frac{x^n}{h(0)}h\left(\frac{a}{x}\right) = \frac{x^n}{\frac{a^n}{f(0)}}f_a^*\left(\frac{a}{x}\right) = \frac{f(0)}{a^n}x^n\frac{\left(\frac{a}{x}\right)^n}{f(0)}f\left(\frac{a}{\frac{a}{x}}\right) = f(x),$$

assim o a-recíproco de $f_a^*(x)$ é $f(x)$. Consequentemente, $f_a^*(x)$ é irredutível sobre $\mathbb{F}_q$ se, e somente se $f(x)$ é irredutível sobre $\mathbb{F}_q$.

■

Observação 2.22. *Pode acontecer $f_a^*(x) = f_{a'}^*(x)$ para elementos distintos $a, a' \in \mathbb{F}_q^*(x)$. Por exemplo, se $f(x) = x^2 + c \in \mathbb{F}_5[x]$, $c \neq 0$, então $f_2^*(x) = f_3^*(x)$.*

Lema 2.23. *Seja g é um polinômio a-autorrecíproco de grau par $n = 2m$ sobre $\mathbb{F}_q$. Então g tem a forma*

$$g(x) = b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i),$$

onde $b_j \in \mathbb{F}_q$ para todo $j = 0, 1, \ldots, m$.

Demonstração.

Note que $g(x) = \sum_{i=0}^{n} b_i x^i$ é a-auto-recíproco se, e somente se, $b_{n-i}b_0 = b_i a^i$.

■

2.4 As aplicações Φ_a e Ψ_a

Definição 2.24. *Seja P_m a coleção de todos os polinômios mônicos sobre $\mathbb{F}_q$ de grau m e seja $S_{2m,a}$ a família de todos os polinômios mônicos a-auto-recíprocos sobre $\mathbb{F}_q$ de grau $2m$.*

Para cada inteiro positivo m, definimos as aplicações

$$\Phi_a : P_m \to S_{2m,a}$$

por

$$\Phi_a(f(x)) = x^m f\left(x + \frac{a}{x}\right)$$

e

$$\Psi_a : S_{2m,a} \to P_m$$

por

$$\begin{aligned}\Psi_a(g(x)) &= \Psi_a\left(b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i)\right)\\ &= b_m + \sum_{i=0}^{m-1} b_{2m-i} D_{m-i}(x,a).\end{aligned}$$

Teorema 2.25 ([8], Teorema 3.1)**.** *As aplicações Φ_a e Ψ_a estão bem definidas e satisfazem as relações*

(i) $\Phi_a \circ \Psi_a = id_{S_{2m,a}}$ *e* $\Psi_a \circ \Phi_a = id_{P_m}$,

(ii) Φ_a *e* Ψ_a *são multiplicativas,*

(iii) *se* $deg\, f_1(x) = d_1$ *e* $deg\, f_2(x) = d_2$ *com* $d_1 > d_2$ *então*

$$\Phi_a(f_1 + f_2) = \Phi_a(f_1) + x^{d_1 - d_2}\Phi_a(f_2),$$

(iv)
- *se $g(x)$ é um polinômio a-autorrecíproco irredutível de grau $2m$ então $\Psi_a(g(x))$ é irredutível,*
- *se $h(x)$ é um polinômio irredutível de grau m e não a-autorrecíproco então $\Psi_a(h(x)h_a^*(x))$ é irredutível.*

Demonstração.

Primeiro vamos provar que os contradomínios são corretos.

Para $f(x) = x^m + a_{m-1}x^{m-1} + \cdots$, temos

$$\Phi_a(f(x)) = x^m\left[\left(x + \frac{a}{x}\right)^m + a_{m-1}\left(x + \frac{a}{x}\right)^{m-1} + \cdots\right],$$

que é mônico de grau $2m$. Como o termo constante de $\Phi_a(f(x))$ é a^m, temos que o a-recíproco de $\Phi_a(f(x))$ é

$$\frac{x^{2m}}{a^m} \cdot \left(\frac{a}{x}\right)^m f\left(\frac{a}{x} + x\right) = x^m f\left(x + \frac{a}{x}\right) = \Phi_a(f(x)).$$

Assim $\Phi_a(P_m) \subset S_{2m,a}$. E

$$\begin{aligned}\Psi_a(g(x)) &= \Psi_a\left(b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i)\right)\\ &= b_{2m}D_m(x,a) + b_{2m-1}D_{m-1}(x,a) + \cdots\end{aligned}$$

é mônico de grau m pois $b_{2m} = 1$ e $D_j(x,a)$ é mônico de grau j. Logo $\Psi_a(S_{2m,a}) \subset P_m$.

(i) Escrevamos $g(x) = b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i)$.

$$\begin{aligned}\Phi_a \circ \Psi_a(g(x)) &= \Phi_a\left(b_m + \sum_{i=0}^{m-1} b_{2m-i}D_{m-i}(x,a)\right)\\ &= x^m\left[b_m + \sum_{i=0}^{m-1} b_{2m-i}D_{m-i}\left(x + \frac{a}{x}, a\right)\right]\\ &= x^m\left[b_m + \sum_{i=0}^{m-1} b_{2m-i}\left(x^{m-i} + \left(\frac{a}{x}\right)^{m-i}\right)\right]\\ &= b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i) = g(x),\end{aligned}$$

onde temos usado a identidade de Waring na terceira linha. Assim $\Phi_a \circ \Psi_a$ é a identidade.

Agora, em P_m o coeficiente de x^m é 1 e os outros são arbitrários, logo $|P_m| = q^m$. E para $g(x) \in S_{2m,a}$, $b_{2m-1}, \ldots, b_m$ são arbitrários, segue $|S_{2m,a}| = q^m$. Assim $\Psi_a \circ \Phi_a$ também é a identidade.

(ii) Sejam $f_1(x)$ e $f_2(x)$ dois polinômios mônicos de graus r e s respectivamente. Então

$$\begin{aligned}\Phi_a((f_1f_2)(x)) &= x^{r+s}(f_1f_2)\left(x + \frac{a}{x}\right)\\ &= x^r f_1\left(x + \frac{a}{x}\right) \cdot x^s f_2\left(x + \frac{a}{x}\right)\\ &= \Phi_a((f_1(x))\Phi_a((f_2)(x)).\end{aligned}$$

Agora suponha que $g_1(x)$ e $g_2(x)$ são polinômios mônicos a-autorrecíprocos de grau par. De **(i)** temos

$$\begin{aligned}\Phi_a(\Psi_a(g_1(x)g_2(x))) &= g_1(x)g_2(x)\\ &= (\Phi_a \circ \Psi_a)(g_1(x)) \cdot (\Phi_a \circ \Psi_a)(g_2(x))\\ &= \Phi_a(\Psi_a(g_1(x))\Psi_a(g_2(x))),\end{aligned}$$

pois já mostramos que Φ_a é multiplicativa.

Consequentemente

$$\Psi_a(g_1(x)g_2(x)) = \Psi_a(g_1(x))\Psi_a(g_2(x)),$$

pois Φ_a é injetiva pelo item **(i)**.

(iii) Notemos que

$$\begin{aligned}\Phi_a((f_1+f_2)(x)) &= x^{d_1}(f_1+f_2)\left(x+\frac{a}{x}\right)\\ &= x^{d_1}f_1\left(x+\frac{a}{x}\right)+x^{d_1-d_2}x^{d_2}f_2\left(x+\frac{a}{x}\right)\\ &= \Phi_a(f_1(x))+x^{d_1-d_2}\Phi_a(f_2(x)).\end{aligned}$$

(iv) Vamos fazer uma prova usando as transformações Φ_a e Ψ_a.

Seja $g(x) \in S_{2m,a}$ irredutível. Suponha $\Psi_a(g(x)) = r(x)s(x)$, com deg $r(x)$, deg $s(x) \geq 1$. Então usando os itens **(i)** e **(ii)**

$$g(x) = (\Phi_a \circ \Psi_a)(g(x)) = \Phi_a(r(x))\Phi_a(s(x)),$$

o que é contraditório.

Em seguida, suponhamos que $h(x)$ é um polinômio irredutível de grau m e não a-autorrecíproco tal que $\Psi_a(h(x)h_a^*(x)) = u(x)v(x)$, com deg $u(x)$, deg $v(x) \geq 1$. Então, aplicando a transformação Φ_a, temos $h(x)h_a^*(x) = \Phi_a(u(x))\Phi_a(v(x))$.

Dado que $h(x)$ é irredutível, $h(x)$ divide $\Phi_a(u(x))$ ou $\Phi_a(v(x))$. Assim podemos supor sem perda de generalidade que $h(x)$ divide $\Phi_a(u(x))$, como $\Phi_a(u(x))$ é a-autorrecíproco, $h_a^*(x)$ também divide $\Phi_a(u(x))$.

Além disso, já que $h_a^*(x)$ é irredutível e $h(x) \neq h_a^*(x)$ temos que $h(x)h_a^*(x)$ divide $\Phi_a(u(x))$. Mas então deg $\Phi_a(v(x))$ é menor do que 1, o que é contraditório.

■

Capítulo 3

Fatoração dos Polinômios de Dickson

O problema de fatoração dos polinômios de Dickson tem sido estudado por vários autores (ver [5], [7], [12]). O nosso objetivo é exibir uma abordagem mais simples. Ao longo deste capítulo estamos seguindo as mesmas técnicas usadas no artigo [3], onde são encontrados explicitamente os fatores irredutíveis de $x^n - 1$ sobre $\mathbb{F}_q[x]$, para isso assumimos que cada divisor primo de n é um divisor de $q-1$, isto é, $rad(n) \mid (q-1)$. De interesse, é como essas fatorações demonstram que os polinômios de Dickson do primeiro tipo aparecem na fatoração dos polinômios do primeiro tipo quanto aqueles do segundo tipo.

3.1 Fatoração dos polinômios de Dickson do primeiro tipo

Para $a = 0$, a fatoração de $D_n(x,a) = x^n$ é trivial; assim vamos considerar somente polinômios de Dickson $D_n(x,a)$ onde $a \neq 0$.

Lema 3.1. *Seja Φ_a a função definida em 2.4. Então*

$$\Phi_a(D_n(x,a)) = x^{2n} + a^n.$$

Demonstração.

$$\Phi_a(D_n(x,a)) = x^n D_n\left(x + \frac{a}{x}, a\right) = x^n\left[x^n + \left(\frac{a}{x}\right)^n\right] = x^{2n} + a^n,$$

onde temos usado a identidade de Waring. ■

Do lema anterior é possível mostrar que para fatorar $D_n(x,a)$ é suficiente fatorar $x^{2n} + a^n$.

3.1.1 Característica ímpar

Aqui assumamos p ímpar. Pelo item **(ii)** do Lema 2.8 temos que se $n = mp^r$ com $r \geqslant 0$, então $D_n(x,a) = [D_m(x,a)]^{p^r}$, logo, para fatorar $D_n(x,a)$, só precisamos fatorar $D_m(x,a)$ com $mdc(m,p) = 1$. Consequentemente, assumamos que $mdc(n,p) = 1$ no decorrer dessa seção.

Teorema 3.2. *Seja $a \in \mathbb{F}_q$ um quadrado em $\mathbb{F}_q$ com $q \equiv 1 \pmod 4$ ou n ímpar. Então todo fator irredutível de $D_n(x,a)$ sobre $\mathbb{F}_q$ é da forma $D_t(x,a) - b^t(\alpha + \alpha^{-1})$, onde $b^2 = a$, $\alpha \in \mathbb{F}_q^*$ e t é um divisor de $2n$ satisfazendo as seguintes condições*

(i) $\alpha^{\frac{2n}{t}} = -1$,

(ii) $rad(t) \mid ord_q(\alpha)$,

(iii) $mdc\left(t, \frac{q-1}{ord_q(\alpha)}\right) = 1$.

Demonstração.

Pelo item **(iv)** do Lema 2.8 sabemos que $D_n(x,a) = b^n D_n(b^{-1}x, 1)$ para $n \geqslant 0$ e $b \neq 0$. Assim a fatoração de $D_n(x,a)$ se obtém direitamente da fatoração de $D_n(y,1)$ onde $y = b^{-1}x$.

Dado que $y^{4n} - 1 = (y^{2n} - 1)(y^{2n} + 1)$, temos $(y^{2n} + 1) \mid (y^{4n} - 1)$. Então conhecendo os fatores irredutíveis de $y^{4n} - 1$, é possível determinar os fatores irredutíveis de $y^{2n} + 1$.

Pelo Teorema 1.70 sabemos que todo fator irredutível de $y^{4n} - 1$ é da forma $y^t - \alpha$. Destes fatores para $y^t - \alpha$ ser fator de $y^{2n} + 1$ devemos ter que $y^{2n} \equiv -1 \pmod{y^t - \alpha}$ mas $t \mid \frac{4n}{mdc(4n, q-1)}$ implica $t \mid 2n$. Logo $y^{2n} \equiv \left(y^t\right)^{\frac{2n}{t}} \equiv -1 \pmod{y^t - \alpha}$ e portanto $\alpha^{\frac{2n}{t}} = -1$.

Seja $f(y)$ fator irredutível de $D_n(y,1)$ e $h(y)$ a imagem de $f(y)$ pela aplicação Φ_1. Logo $h(y)$ é um fator de $y^{2n} + 1$. Observemos que $h(y)$ não é necessariamente um fator irredutível de $y^{2n} + 1$ em $\mathbb{F}_q[y]$.

Como estamos nas condições do Teorema 1.70 sabemos que existe um fator irredutível de $y^{2n} + 1$ da forma $y^t - \alpha$ que divide $h(y)$. Tirando recíprocos temos que $(y^t - \alpha^{-1}) \mid h^*(y)$, isto é, $(y^t - \alpha^{-1}) \mid h(y)$, pois $h(y)$ é autorrecíproco por ser imagem de Φ_1.

Neste ponto apresentamos dois casos:

(a) Suponhamos que $\alpha \neq \alpha^{-1}$:

Então $\left(y^t - \alpha\right)\left(y^t - \alpha^{-1}\right) \mid h(y)$ e por isso $\left(y^{2t} - \left(\alpha + \alpha^{-1}\right) y^t + 1\right) \mid h(y)$. Isto é, $y^t\left(y^t + \frac{1}{y^t} - \left(\alpha + \alpha^{-1}\right)\right) \mid h(y)$, assim, $y^t\left(D_t\left(y + \frac{1}{y}, 1\right) - \left(\alpha + \alpha^{-1}\right)\right) \mid h(y)$. Logo, pela aplicação Ψ_1 obtemos $\left(D_t\left(y,1\right) - \left(\alpha + \alpha^{-1}\right)\right) \mid f(y)$.

Como $f(y)$ é mônico irredutível, então $f(y) = D_t(y,1) - \left(\alpha + \alpha^{-1}\right)$. Agora voltando à variável original, obtemos $f(b^{-1}x) = D_t\left(b^{-1}x, 1\right) - \left(\alpha + \alpha^{-1}\right) = b^{-t}D_t(x,a) - \left(\alpha + \alpha^{-1}\right)$.

Daí que, $b^t f(b^{-1}x) = D_t(x,a) - b^t\left(\alpha + \alpha^{-1}\right)$ é fator irredutível de $D_n(x,a)$ sobre $\mathbb{F}_q$.

(b) Suponhamos que $\alpha = \alpha^{-1}$:

Então $\alpha^2 = 1$ e $\alpha = \pm 1$. Logo $y^t - \alpha = y^t \pm 1$. Mas $y^t - 1$ é irredutível somente no caso $t = 1$. De igual forma $y^t + 1$ é irredutível no caso $t = 1$, pois $y^2 + 1$ é redutível no caso que $q \equiv 1 \pmod 4$, isto é, -1 é um quadrado em $\mathbb{F}_q$.

Segue que se $y \pm 1$ divide $y^{2n} + 1$ temos $y^{2n} + 1 \equiv (\mp 1)^{2n} + 1 \equiv 2 \equiv 0 \pmod{y \pm 1}$ o que implica que $char(\mathbb{F}_q) = 2$, mas estamos considerando característica ímpar, o que é contraditório.

■

No teorema anterior consideramos o caso em que $a \in \mathbb{F}_q$ é um quadrado em $\mathbb{F}_q$ e $q \equiv 1 \pmod 4$ ou n é ímpar. Nos seguintes teoremas, usaremos o teorema anterior para resolver os casos complementares a estas condições.

Teorema 3.3. *Seja $a \in \mathbb{F}_q$ um quadrado em $\mathbb{F}_q$ com $q \equiv 3 \pmod 4$ e n par. Sejam $b^2 = a$, $\alpha \in \mathbb{F}_{q^2}^*$ e t um divisor de $2n$, como satisfazendo as condições **(i)**, **(ii)** e **(iii)** do teorema anterior sobre $\mathbb{F}_q^2$. Então todo fator irredutível de $D_n(x,a)$ sobre $\mathbb{F}_q$ é de uma das seguintes formas*

(a) $D_t(x,a) - b^t(\alpha + \alpha^{-1})$ *no caso que $\alpha \in \mathbb{F}_q^*$ ou $\alpha^{q+1} = 1$,*

(b) $\left(D_t(x,a) - b^t(\alpha + \alpha^{-1})\right)\left(D_t(x,a) - b^t(\alpha^q + \alpha^{-q})\right)$ *caso α não satisfazer nenhuma das condições do item anterior.*

Demonstração.

Consideremos $D_n(x,a)$ como um polinômio em $\mathbb{F}_{q^2}[x]$. Como $q \equiv 3 \pmod 4$ então $q^2 \equiv 1 \pmod 4$, e segue pelo teorema anterior que todo fator irredutível em $\mathbb{F}_{q^2}[x]$ de $D_n(x,a)$ é da forma $D_t(x,a) - b^t\left(\alpha + \alpha^{-1}\right) \in \mathbb{F}_{q^2}[x]$.

Precisamos verificar quais destes fatores estão em $\mathbb{F}_q[x]$, como $D_t(x,a) \in \mathbb{F}_q[x]$, isso acontece no caso que $\alpha + \alpha^{-1} \in \mathbb{F}_q$. Temos que $\alpha + \alpha^{-1} \in \mathbb{F}_q$ se, e somente se $\alpha + \alpha^{-1} = \left(\alpha + \alpha^{-1}\right)^q$. Fazendo algumas manipulações algébricas temos que a anterior equação é equivalente a $(\alpha^{q+1} - 1)(\alpha^{q-1} - 1) = 0$. Logo $\alpha \in \mathbb{F}_q^*$ ou $\alpha^{q+1} = 1$.

Caso não se tenha nenhuma destas condições temos que $D_t\left(x,a\right)-b^t\left(\alpha+\alpha^{-1}\right)\in \mathbb{F}_{q^2}[x]\setminus\mathbb{F}_q[x]$ é um fator de $D_n(x,a)$. Usando a aplicação de Frobenius

$$\begin{aligned}\tau:\mathbb{F}_{q^2} &\to \mathbb{F}_{q^2}\\ \beta &\mapsto \beta^q,\end{aligned}$$

como $D_n(x,a)$ é deixado fixo por esta aplicação, temos que $D_t\left(x,a\right)-b^t\left(\alpha^q+\alpha^{-q}\right)$ também é um fator de $D_n(x,a)$. Mas $\alpha+\alpha^{-1}\neq\alpha^q+\alpha^{-q}$, portanto segue que $\left(D_t(x,a)-b^t(\alpha+\alpha^{-1})\right)\left(D_t(x,a)-b^t(\alpha^q+\alpha^{-q})\right)$ é um fator de $D_n(x,a)$.

Por fim, notemos que $\left(D_t(x,a)-b^t(\alpha+\alpha^{-1})\right)\left(D_t(x,a)-b^t(\alpha^q+\alpha^{-q})\right)$ é invariante por τ, daí que $\left(D_t(x,a)-b^t(\alpha+\alpha^{-1})\right)\left(D_t(x,a)-b^t(\alpha^q+\alpha^{-q})\right)$ é um fator de $D_n(x,a)$ que está em $\mathbb{F}_q[x]$ e é irredutível neste anel. ■

Teorema 3.4. *Seja $a\in\mathbb{F}_q$ que não é um quadrado em $\mathbb{F}_q$. Sejam $b^2=a$, $b\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$, $\alpha\in\mathbb{F}_{q^2}^*$ e t um divisor de $2n$, como satisfazendo as condições **(i)**, **(ii)** e **(iii)** do Teorema 3.2 sobre $\mathbb{F}_{q^2}$. Então todo fator irredutível de $D_n(x,a)$ sobre $\mathbb{F}_q$ é de uma das seguintes formas*

- **(a)** *$D_t(x,a)-b^t(\alpha+\alpha^{-1})$ nos casos que t par e $\alpha\in\mathbb{F}_q^*$ ou $\alpha^{q+1}=1$, ou t ímpar e $\alpha^{q-1}=-1$ ou $\alpha^{q+1}=-1$,*
- **(b)** *$\left(D_t(x,a)-b^t(\alpha+\alpha^{-1})\right)\left(D_t(x,a)-b^{qt}(\alpha^q+\alpha^{-q})\right)$ caso α e t não satisfazer nenhuma das condições do item anterior.*

Demonstração.

Igual que no teorema anterior consideramos $D_n(x,a)$ como um polinômio em $\mathbb{F}_{q^2}[x]$. Neste caso $q^2\equiv 1 \pmod 4$ e a é um quadrado em $\mathbb{F}_{q^2}$ tal que $a=b^2$, onde $b\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Pelo Teorema 3.2 todo fator irredutível em $\mathbb{F}_{q^2}[x]$ de $D_n(x,a)$ é da forma $D_t\left(x,a\right)-b^t\left(\alpha+\alpha^{-1}\right)\in\mathbb{F}_{q^2}[x]$.

Precisamos verificar quais destes fatores estão em $\mathbb{F}_q[x]$, como $D_t(x,a)\in\mathbb{F}_q[x]$, isso acontece no caso que $b^t\left(\alpha+\alpha^{-1}\right)\in\mathbb{F}_q$. Temos que $b^t\left(\alpha+\alpha^{-1}\right)\in\mathbb{F}_q$ se, e somente se $b^t\left(\alpha+\alpha^{-1}\right)=b^{qt}\left(\alpha+\alpha^{-1}\right)^q$ se, e somente se $b^{t(q-1)}\left(\alpha^q+\alpha^{-q}\right)=\alpha+\alpha^{-1}$.

Como a não é quadrado, $b^{q-1}=\left(b^2\right)^{\frac{q-1}{2}}=a^{\frac{q-1}{2}}=-1$. Vamos separar em dois casos.

1. No caso que t é par, segue que $b^{t(q-1)}\left(\alpha^q+\alpha^{-q}\right)=\alpha+\alpha^{-1}$ se, e somente se $\alpha^q+\alpha^{-q}=\alpha+\alpha^{-1}$, e logo $\alpha\in\mathbb{F}_q^*$ ou $\alpha^{q+1}=1$.
2. No caso que t é ímpar, segue que $b^{t(q-1)}\left(\alpha^q+\alpha^{-q}\right)=\alpha+\alpha^{-1}$ se, e somente se $-\alpha^q-\alpha^{-q}=\alpha+\alpha^{-1}$ se, e somente se $(\alpha^{q-1}+1)(\alpha^{q+1}+1)=0$.

Caso não se tenha nenhuma destas condições temos que $D_t(x,a) - b^t\left(\alpha + \alpha^{-1}\right) \in \mathbb{F}_{q^2}[x] \setminus \mathbb{F}_q[x]$ é um fator de $D_n(x,a)$. De maneira análoga ao teorema anterior, usando a aplicação de Frobenius, temos que $D_t(x,a) - b^{qt}\left(\alpha^q + \alpha^{-q}\right)$ é um fator de $D_n(x,a)$ e por conseguinte $\left(D_t(x,a) - b^t(\alpha + \alpha^{-1})\right)\left(D_t(x,a) - b^{qt}(\alpha^q + \alpha^{-q})\right)$ é um fator de $D_n(x,a)$ que está em $\mathbb{F}_q[x]$ e é irredutível neste anel. ■

3.1.2 Característica 2

Aqui assumamos $p = 2$. Se $n = 2^r m$ com $r \geqslant 0$, então $D_n(x,1) = [D_m(x,1)]^{2^r}$, logo, para fatorar $D_n(x,1)$, só precisamos fatorar $D_m(x,1)$ com m ímpar. Consequentemente, assumamos n ímpar no decorrer dessa seção.

Lema 3.5. *Seja $n = 2m+1$.*

(i) *$D_n(x,1) = xF_n(x)^2$, para algum polinômio $F_n(x)$ de grau m tal que $F_n(0) \neq 0$,*

(ii) $(x+1)\Phi_1(F_n(x)) = x^n + 1$.

Demonstração.

(i) Seja

$$F_n(x) = \sum_{i=0}^{m} \frac{n}{n-i}\binom{n-i}{i}x^{m-i}.$$

Então

$$\begin{aligned} xF_n(x)^2 &= x\left[\sum_{i=0}^{m} \frac{n}{n-i}\binom{n-i}{i}x^{m-i}\right]^2 = x\sum_{i=0}^{m} \frac{n}{n-i}\binom{n-i}{i}x^{2m-2i} \\ &= \sum_{i=0}^{m} \frac{n}{n-i}\binom{n-i}{i}x^{2m+1-2i} = \sum_{i=0}^{m} \frac{n}{n-i}\binom{n-i}{i}(-1)^i x^{n-2i} \\ &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-1)^i x^{n-2i} = D_n(x,1). \end{aligned}$$

(ii) Usamos o item **(i)**, o Lema 3.1 e o Teorema 2.25:

$$x^{2n} + 1 = \Phi_1(D_n(x,1)) = \Phi_1(x)\Phi_1(F_n(x)^2) = (x^2+1)\Phi_1(F_n(x))^2.$$

Logo $(x^n+1)^2 = [(x+1)\Phi_1(F_n(x))]^2$, obtemos **(ii)**.

■

Assim, neste ponto é suficiente determinar a fatoração de $F_n(x)$. Pelo item **(ii)** do lema anterior basta encontrar a fatoração de $x^n - 1$ e como estamos nas condições do Teorema 1.70 obtemos um resultado com prova essencialmente igual à prova do Teorema 3.2, a qual omitiremos.

Teorema 3.6. *Seja $a \in \mathbb{F}_q$ com $char(\mathbb{F}_q) = 2$ e n ímpar. Então todo fator irredutível de $F_n(x)$ sobre $\mathbb{F}_q$ é da forma $D_t(x,a) - b^t(\alpha + \alpha^{-1})$ onde $b^2 = a$, $\alpha \in \mathbb{F}_q^*$ e t é um divisor de n satisfazendo as seguintes condições*

(i) $\alpha^{\frac{n}{t}} = 1$,

(ii) $rad(t) \mid ord_q(\alpha)$,

(iii) $mdc\left(t, \frac{q-1}{ord_q(\alpha)}\right) = 1$,

(iv) $(\alpha, t) \neq (1,1)$.

3.2 Fatoração dos polinômios de Dickson do segundo tipo

Para $a = 0$, a fatoração de $E_n(x,a) = x^n$ é trivial; assim vamos considerar somente polinômios de Dickson $E_n(x,a)$ onde $a \neq 0$.

Lema 3.7. *Seja Φ_a a função definida em 2.4. Então*

$$\Phi_a(E_n(x,a)) = \frac{x^{2(n+1)} - a^{n+1}}{x^2 - a}.$$

Demonstração.

$$\Phi_a(E_n(x,a)) = x^n E_n\left(x + \frac{a}{x}, a\right) = x^n \left(\frac{x^{n+1} - \frac{a^{n+1}}{x^{n+1}}}{x - \frac{a}{x}} \right) = \frac{x^{2(n+1)} - a^{n+1}}{x^2 - a},$$

onde temos usado a identidade de Waring. ■

3.2.1 Característica ímpar

Aqui assumamos p ímpar. Pelo item **(i)** do Lema 2.17 temos que se $n+1 = (m+1)p^r$ com $r \geqslant 0$, então $E_n(x,a) = [E_m(x,a)]^{p^r}(x^2 - 4a)^{\frac{p^r-1}{2}}$, logo, para fatorar $E_n(x,a)$, só precisamos fatorar $E_m(x,a)$ com $mdc(m+1,p) = 1$. Consequentemente, assumamos que $mdc(n+1,p) = 1$ no decorrer dessa seção.

Teorema 3.8. *Seja $a \in \mathbb{F}_q$ um quadrado em $\mathbb{F}_q$ com $q \equiv 1 \pmod 4$ ou n par. Então todo fator irredutível de $E_n(x,a)$ sobre $\mathbb{F}_q$ é da forma $D_t(x,a) - b^t(\alpha + \alpha^{-1})$, onde $b^2 = a$, $\alpha \in \mathbb{F}_q^*$ e t é um divisor de $2(n+1)$ satisfazendo as seguintes condições*

(i) $\alpha^{\frac{2(n+1)}{t}} = 1$,

(ii) $rad(t) \mid ord_q(\alpha)$,

(iii) $mdc\left(t, \frac{q-1}{ord_q(\alpha)}\right) = 1$,

(iv) $(\alpha, t) \notin \{(1,1),(1,-1)\}$.

Usando o lema anterior, esse resultado tem prova essencialmente igual à prova do Teorema 3.2, a qual omitiremos.

Teorema 3.9. *Seja $a \in \mathbb{F}_q$ um quadrado em $\mathbb{F}_q$ com $q \equiv 3 \pmod 4$ e n ímpar. Sejam $b^2 = a$, $\alpha \in \mathbb{F}_{q^2}^*$ e t um divisor de $2(n+1)$, como satisfazendo as condições **(i)**, **(ii)**, **(iii)** e **(iv)** do teorema anterior sobre $\mathbb{F}_q^2$. Então todo fator irredutível de $E_n(x,a)$ sobre $\mathbb{F}_q$ é de uma das seguintes formas*

(a) $D_t(x,a) - b^t(\alpha + \alpha^{-1})$ *no caso que $\alpha \in \mathbb{F}_q^*$ ou $\alpha^{q+1} = 1$,*

(b) $\left(D_t(x,a) - b^t(\alpha + \alpha^{-1})\right)\left(D_t(x,a) - b^t(\alpha^q + \alpha^{-q})\right)$ *caso α não satisfazer nenhuma das condições do item anterior.*

Usando o Lema 3.7, esse resultado tem prova essencialmente igual à prova do Teorema 3.3, a qual omitiremos.

Teorema 3.10. *Seja $a \in \mathbb{F}_q$ que não é um quadrado em $\mathbb{F}_q$. Sejam $b^2 = a$, $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2}^*$ e t um divisor de $2(n+1)$, como satisfazendo as condições **(i)**, **(ii)**, **(iii)** e **(iv)** do Teorema 3.8 sobre $\mathbb{F}_{q^2}$. Então todo fator irredutível de $E_n(x,a)$ sobre $\mathbb{F}_q$ é de uma das seguintes formas*

(a) $D_t(x,a) - b^t(\alpha + \alpha^{-1})$ *nos casos que t par e $\alpha \in \mathbb{F}_q^*$ ou $\alpha^{q+1} = 1$, ou t ímpar e $\alpha^{q-1} = -1$ ou $\alpha^{q+1} = -1$.*

(b) $\left(D_t(x,a) - b^t(\alpha + \alpha^{-1})\right)\left(D_t(x,a) - b^{qt}(\alpha^q + \alpha^{-q})\right)$ *caso α e t não satisfazer nenhuma das condições do item anterior.*

Usando o Lema 3.7, esse resultado tem prova essencialmente igual à prova do Teorema 3.4, a qual omitiremos.

3.2.2 Característica 2

Aqui assumamos $p = 2$. Se $n+1 = 2^r(m+1)$ com $r \geqslant 0$, então $E_n(x,1) = [E_m(x,1)]^{2^r} x^{2^r-1}$, logo, para fatorar $E_n(x,1)$, só precisamos fatorar $E_m(x,1)$ com $m+1$ ímpar. Consequentemente, assumamos $n+1$ ímpar, isto é, n par.

Observemos que quando a característica é 2

$$E_n(x,1) = E_n\left(y + \frac{1}{y}, 1\right) = \frac{y^{n+1} - \left(\frac{1}{y}\right)^{n+1}}{y - \frac{1}{y}} = \frac{D_{n+1}\left(y + \frac{1}{y}, 1\right)}{y + \frac{1}{y}} = \frac{D_{n+1}(x,1)}{x}.$$

Então usando o item **(1)** do Lema 3.5 chegamos em $E_n(x,1) = F_{n+1}(x)^2$, logo a fatoração segue do Teorema 3.6.

Consideraçoes Finais

Nesse trabalho caracterizamos explicitamente os fatores irredutíveis de $D_n(x,a)$ e $E_n(x,a)$ sobre $\mathbb{F}_q[x]$ seguindo as mesmas técnicas usadas no artigo [3], onde são encontrados explicitamente os fatores irredutíveis de x^n-1 sobre $\mathbb{F}_q[x]$ no caso que todo fator primo de n divide $q-1$, isto é, $rad(n)|(q-1)$.

Uma perspectiva de continuidade natural do tema estudado e seguindo a mesma linha desta dissertação seria considerarmos estudar a fatoração em fatores irredutíveis de $D_n(x,a)$ e $E_n(x,a)$ sobre $\mathbb{F}_q[x]$ quando $rad(n) \nmid (q-1)$.

Uma boa opção seria tentar trabalhar com os resultados obtidos em [13], onde é fatorado explicitamente x^n-1 em fatores irredutíveis sobre $\mathbb{F}_q[x]$ e são contados o número dos seus fatores irredutíveis supondo que $rad(n) \nmid (q-1)$ e $rad(n)|(q^w-1)$, com w é primo. Além disso, outro caminho a seguir seria substituir w por um número composto, isto pode ser feito num trabalho futuro.

Bibliografia

[1] Alaca, S., *Congruences for Brewer sums*. Finite Fields Appl. **13** (2007) 1-19.

[2] Bhargava, M. and Zieve, M., *Factoring Dickson polynomials over finite fields*. Finite Fields Appl. **5** (1999) 103-111.

[3] Brochero Martínez, F.E., Giraldo Vergara, C.R. and Batista de Oliveira, L., *Explicit Factorization of* $x^n - 1 \in \mathbb{F}_q[x]$, Des. Codes Cryptogr. **77** (1) (2015) 277-286.

[4] Brochero Martínez, F.E., Moreira, C.G., et al., *Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro*, Rio de Janeiro, IMPA, 2011.

[5] Chou, W.S., *The Factorization of Dickson Polynomials over finite fields*. Finite Fields Appl. **3** (1997) 84-96.

[6] Dickson, L.E., *The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group*. Annals of Mathematics **11** (1897) 65–143.

[7] Fitzgerald, R.W. and Yucas, J.L., *Explicit factorization of cyclotomic and Dickson Polynomials over finite fields*. Arithmetic of Finite Fields. Lecture Notes in Computer Science. **4547** (2007) 1-10.

[8] Fitzgerald, R.W. and Yucas, J.L., *Generalized Reciprocals, Factors of Dickson Polynomials and Generalized Cyclotomic Polynomials over Finite Fields*. Finite Fields Appl. **13** (2007) 492-515.

[9] Lidl, R., Mullen, G.L. and Turnwald, G., *Dickson Polynomials*. Pitman Monographs and Surveys in Pure and Applied Math. Essex (1993).

[10] Lidl, R. and Niederreiter, H., *Finite Fields*. Encyclopedia of Mathematics and its Applications. **20**, Massachusetts (1983).

[11] Schur, I., *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*. S. B. Preuss. Akad. Wiss. (1923), 123–134.

[12] Tosun, S., *Explicit factorizations of generalized Dickson Polynomials of order* 2^m *via generalized cyclotomic polynomials over finite fields*. Finite Fields Appl. **38** (2016) 40-56.

[13] Wu Y., Yue Q. and Fan S., "Further factorization of $x^n - 1$ over a finite field". Submitted, October 22th, 2017.