GISELA LIZETH ROJAS BERNAL

Existência e propriedades de elementos k-normais em corpos finitos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2023

GISELA LIZETH ROJAS BERNAL

Existência e propriedades de elementos k-normais em corpos finitos

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

Área de Concentração: Matemática.
Linha de Pesquisa: Álgebra.

Orientador(a): Prof(a). Dr(a). Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2023

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

B517 Bernal, Gisela Lizeth Rojas, 1993-
2023 Existência e propriedades de elementos k-normais em corpos finitos [recurso eletrônico] : existência e propriedades de elementos k-normais em corpos finitos / Gisela Lizeth Rojas Bernal. - 2023.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.369
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

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

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 112, PPGMAT				
Data:	31 de julho de 2023	Hora de início:	14:00	Hora de encerramento:	15:30
Matrícula do Discente:	12122MAT003				
Nome do Discente:	Gisela Lizeth Rojas Bernal				
Título do Trabalho:	Existência e propriedades de elementos k-normais em corpos finitos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Estudo de elementos primitivos e normais em corpos finitos				

Reuniu-se na Sala Multiuso da Faculdade de Matemática (Sala 1F 119) da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Fábio Enrique Brochero Martinez - UFMG; Cícero Fernandes de Carvalho - FAMAT/UFU e Victor Gonzalo Lopez Neumann - FAMAT/UFU, orientador da candidata.

Iniciando os trabalhos o presidente da mesa, Dr. Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e a candidata, agradeceu a presença do público, e concedeu a Discente a palavra para a exposição do seu trabalho. A duração da apresentação da Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

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

Aprovada.

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

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

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

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 31/07/2023, às 16:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 31/07/2023, às 16:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez**, **Usuário Externo**, em 31/07/2023, às 18:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4681261** e o código CRC **E9AA6B2B**.

Dedicatória

A meus pais Olga Elena Bernal Diaz e Juan de Jesus Rojas Espinosa, a meu irmão Jesus Francisco Rojas Bernal e a minha avó Ana Cecilia Espinosa Bernal.

Agradecimentos

Agradeço primeiramente a Deus. Agradeço a agência CAPES pelo fornecimento da bolsa de pesquisa ao longo da Pós-Graduação. Ao meu orientador Victor Gonzalo Lopez Neumann pelos ensinamentos, ajuda e dedicação nos seminários, por ter paciência de explicar uma, duas ou três vezes quando eu não conseguia entender. Aos Professores. Drs. Fabio Enrique Brochero Martínez e Cícero Fernandes de Carvalho por terem aceitado o convite para fazerem parte da minha banca.

À minha família por me apoiar quando senti que não ia conseguir, especialmente aos meus pais por cada momento que reservam todas as manhãs para me desejar sucesso, ouvirem-me e lembrarem-me que tudo está em minha cabeça. Ao meu irmãozinho por me ensinar que os sonhos se perseguem, por ser uma cumplicidade incondicional neste sonho, por me ensinar a não ter medo de ficar sozinha. A minha avó por superar seus medos para vir e procurar sua neta, trazendo consigo suas arepas como era o costume nas tardes. Só posso dizer que isso é fruto do apoio que recebi por vocês, sem vocês não teria conseguido concluir essa etapa da minha vida, obrigada família, vocês são demais.

BERNAL,G. L. R. *Existência e propriedades de elementos k-normais em corpos finitos.* 2023. ix+81 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Este trabalho consiste em um estudo detalhado dos elementos k-normais em um determinado corpo finito e suas propriedades. Nele apresenta-se a definição de elemento k-normal dada inicialmente pelos autores S. Huczynska, G. Mullen, D. Panario, D. Thomson em [11], que generaliza a noção de elemento normal. Também exibem-se quatro teoremas de grande impacto dados em [11], que permitem caracterizar estes elementos, calcular a quantidade exata de elementos k-normais presentes em um corpo finito e calcular a densidade dos mesmos. Por último apresenta-se um resultado dado pelos autores mencionados anteriormente, que garante a existência de elementos 1-normais primitivos para determinados corpos finitos.

Palavras-chave: corpos finitos, elemento normal, elemento k-normal, elemento primitivo, densidade.

BERNAL, G. L. R. *Existence and properties of k-normal elements in finite fields.* 2023. ix+81 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

This work consists of a detailed study of the k-normal elements in a given finite field and their properties. In it is presented the definition of k-normal element given initially by the authors S. Huczynska, G. Mullen, D. Panario, D. Thomson in citeartiprinci, which generalizes the notion of normal element. It also shows four theorems of great impact given in [11], which allow characterizing these elements, calculating the exact amount of k-normal elements present in a finite field and calculating their density. Finally, it is presented a result given by the authors mentioned above, which guarantees the existence of primitive 1-normal elements for certain finite fields.

Keywords: finite fields, normal element, k-normal element, primitive element, density.

Sumário

Introdução

Este trabalho está inserido na área da Álgebra, especialmente na linha da teoria dos corpos finitos. De acordo com os autores R. Lidl e H. Niederreiter em [14], a teoria dos corpos finitos começou com os trabalhos de Carl Friedrich Gauss (1777-1855) e Evariste Galois (1811-1832). Desde então diversos autores têm trabalhado neste ramo, aportando ideias que permitiram o desenvolvimento desta teoria, entre os quais destacam-se os seguintes: Pierre de Fermat (1601-1665), Leonard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) e Andrien-Marie Legendre (1752-1833), e na atualidade autores como Cícero Carvalho, Daniel Panario, David Thomson, Sophie Huczynska, Gudmund Frandsen, entre outros.

Os corpos finitos têm uma grande transcendência ao longo da sua história, especialmente nos últimos 50 anos esta teoria alcançou um impacto relevante em outros segmentos da ciência. Alguns exemplos são a computação, a análise combinatória, a teoria dos códigos, o estudo matemático de circuitos comutativos, etc.

Para a elaboração desta dissertação estudaram-se principalmente as definições e resultados apresentados em [11] publicado em 2013, onde surgiu a definição de elemento k-normal, que é uma generalização da noção de elemento normal; nesse artigo também são estudadas várias propriedades dos elementos k-normais. Esta referência é muito importante porque os autores propõem vários problemas que na última década foram resolvidos parcialmente e cujas soluções forneceram novos problemas. Além disso, estudaram-se os artigos [6] e [7], para mostrar os resultados mais relevantes do artigo principal.

O objetivo deste trabalho é apresentar um resultado que permite estabelecer quando um elemento de uma extensão de corpos finitos é k-normal, quantos elementos k-normais existem em um corpo finito dado, e alguns resultados que permitem conhecer qual é a probabilidade (chamada de **densidade** neste trabalho) de encontrar um elemento k-normal. A noção de elemento k-normal generaliza a definição de elemento normal dada em [14, Theorem 3.73] e, portanto, diversos resultados importantes que envolvem esta definição têm sido generalizados. Destes podem ser citados, a caracterização de elementos normais dada em [14, Theorem 2.39], a quantidade de elementos normais presentes em um corpo finito determinado, dado também em [14, Theorem 3.73], entre outros.

Para o desenvolvimento do objetivo mencionado anteriormente serão apresentados quatro teoremas:

O primeiro (veja Teorema 2.11, Capítulo 2), mostrado inicialmente em [11, Theorem 2.5], os autores dão uma caracterização dos elementos k-normais em um corpo finito dado. Este teorema é provado basicamente usando as noções de elemento conjugado (veja Definição 1.17), de resultante (veja Definição 2.3) e algumas propriedades da resultante.

O segundo teorema (veja Teorema 3.8, Capítulo 3), provado em [11, Theorem 3.5], é fundamental porque indica quantos elementos k-normais existem em um determinado corpo finito. Para provar este resultado os autores usam propriedades importantes da Função ϕ de Euler, bem conhecidas na literatura, e a noção de $\mathrm{Ord}(\alpha)$ para α um elemento k-normal de uma determinada extensão de corpos finitos.

O terceiro e quarto teorema (veja Teorema 4.35 e Teorema 4.26, Capítulo 4) são resultados mostrados em [11, Lemma 4.4 and Corollary 4.8] que dão uma cota superior e inferior da

densidade. Estudar a **densidade** é tão importante como estudar a quantidade de elementos k-normais presentes em um corpo finito, pois calcula a probabilidade de, ao escolher um elemento do corpo finito, ele ser k-normal. Para demonstrar estes resultados os autores usam as mesmas técnicas utilizadas nos artigos [6] e [7] que envolvem teoria avançada dos números, programas computacionais, propriedades das funções de Euler e Möbius, entre outras.

Para finalizar, é importante ressaltar que um dos desafios atuais da teoria dos corpos finitos é mostrar a existência de elementos k-normais primitivos em um corpo dado $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Para abordar estes problema os pesquisadores têm utilizado diversas técnicas e ferramentas, como por exemplo a teoria dos números e a computação. Em [11, Theorem 5.10] os autores mostram a existência de elementos 1-normais primitivos em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ para determinados pares (q, n), veja capítulo 5 para mais detalhes.

Este trabalho foi organizado da seguinte forma: no Capítulo 1 apresentam-se a noção de corpos finitos e algumas propriedades destes corpos finitos, e por último as definições de polinômios linearizados e Função ϕ de Euler com os resultados mais relevantes que envolvem estas definições.

No Capítulo 2 apresentam-se as definições da resultante, elemento normal, elemento k-normal, as propriedades destes elementos, resultados que envolvem a noção de elemento normal e elemento k-normal e por último o Teorema 2.11.

No Capítulo 3 define-se o polinômio $\mathrm{Ord}(\alpha)$, para um elemento α do corpo finito determinado, o qual é de grande importância para o desenvolvimento do trabalho, e por último apresenta-se o Teorema 3.8.

No Capítulo 4 exibem-se todas as definições e resultados do artigo [6], e as noções e teoremas importantes que permitem mostrar o Teorema 4.17 e o Corolário 4.35 que, como mencionado anteriormente, dão um limite inferior e superior da **densidade**.

Por fim no Capítulo 5 apresentam-se as definições de caracter; soma de Gauss; elemento m-livre, com m um inteiro positivo e elemento g-livre, com g um polinômio com coeficientes em um corpo finito determinado. Além disso, exibe-se o Teorema 5.30 que mostra a existência de elementos 1-normais primitivos para uma determinada extensão de corpos finitos.

Gisela Lizeth Rojas Bernal
Uberlândia-MG, 31 de Julho de 2023.

Capítulo 1

Conceitos básicos

Como foi mencionado anteriormente, este trabalho esta inserido na linha da álgebra e teoria dos números, especificamente na teoria dos corpos finitos. Com esse enfoque, neste capítulo, apresentam-se as noções básicas e importantes para a compreensão e desenvolvimento deste trabalho, tais como: corpo finito, Matriz de Sylvester, resultante, q-polinômios (conhecidos na literatura também como polinômios linearizados), polinômio ciclotômico, q-módulo, Função ϕ de Euler e as principais propriedades destes conceitos. Além disso, exibem-se resultados importantes que abrangem os corpos finitos, os q-polinômios, a resultante e a Função ϕ de Euler, os quais são indispensáveis para as noções e demonstrações dos teoremas que envolvem os elementos k-normais dados em [11], que são os principais objetos de estudo nesta dissertação.

Todos os resultados e definições apresentados neste capítulo foram tomados de [14], especificamente nos Capítulos 1, 2 e 3 desta referência. Os conceitos, lemas e teoremas trabalhados neste capítulo são de grande impacto, já que a noção de elemento k-normal é uma generalização da definição de elemento normal. Esta abordagem foi feita pelos autores R. Lidl e H. Niederreiter em [14] nos capítulos já mencionados, assim como a existência e a quantidade de elementos normais presentes em um corpo finito dado.

1.1 Corpos finitos

O objetivo desta seção é apresentar a noção de corpo finito, já que é o ambiente geral onde estão inseridos os elementos k-normais. Além disso exibem-se algumas propriedades, definições e alguns resultados que envolvem os corpos finitos, que serão utilizados no decorrer do trabalho.

Definição 1.1. Um anel comutativo com unidade, com um número finito de elementos, no qual todo elemento não nulo possui inverso multiplicativo, é chamado **corpo finito**.

A definição anterior induz a seguinte noção:

Definição 1.2. Um corpo finito que não contém um subcorpo próprio é chamado **corpo primo**.

Se $\mathbb{K}$ é um corpo, o grupo multiplicativo dos elementos não nulos de $\mathbb{K}$ é denotado por $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$.

Definição 1.3. Dizemos que um corpo $\mathbb{K}$ tem **característica** positiva se existe um inteiro positivo n tal que $nr = 0$, para todo $r \in \mathbb{K}$. O menor inteiro positivo n, com essa propriedade, é chamado de **característica** de $\mathbb{K}$ e diz-se que $\mathbb{K}$ tem característica (positiva) n. Se não existir tal inteiro positivo n, diz-se que $\mathbb{K}$ tem característica 0.

Uma propriedade dos corpos finitos que abrange a definição anterior é a seguinte:

Teorema 1.4. *[14, Corollary 1.45] Um corpo finito tem característica prima.*

Outra propriedade fundamental dos corpos finitos é a seguinte.

Teorema 1.5. *[14, Theorem 1.46] Seja $\mathbb{K}$ um anel comutativo de característica prima p. Então*

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

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

Os seguintes resultados são de grande relevância no decorrer do trabalho, já que serão utilizados nas demonstrações de alguns teoremas importantes mencionados nos próximos capítulos.

Um corpo $\mathbb{F}$ é uma extensão de $\mathbb{K}$, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$. Se $\mathbb{F}$, considerado como espaço vetorial sobre $\mathbb{K}$, é de dimensão finita, então dita extensão é finita e, baixo estas condições, a dimensão do espaço vetorial $\mathbb{F}$ sobre $\mathbb{K}$ é chamada de indice e denotada por $[\mathbb{F} : \mathbb{K}]$.

Assim, tem-se o seguinte resultado.

Lema 1.6. *Seja $\mathbb{F}$ um corpo finito contendo um subcorpo $\mathbb{K}$ com q elementos. Então $\mathbb{F}$ tem q^n elementos, onde $n = [\mathbb{F} : \mathbb{K}]$.*

Demonstração. Como $\mathbb{F}$ é um espaço vetorial sobre $\mathbb{K}$ e $\mathbb{F}$ é finito, então $\mathbb{F}$ é um espaço vetorial de dimensão finita sobre $\mathbb{K}$. Se $[\mathbb{F} : \mathbb{K}] = n$, segue que $\mathbb{F}$ tem uma base $\beta = \{b_1, b_2, \ldots, b_n\}$ sobre $\mathbb{K}$ com exatamente n elementos. Assim para cada elemento de $\mathbb{F}$ existe uma única representação da forma $a_1b_1 + a_2b_2 + \cdots + a_nb_n$, onde $a_1, \ldots, a_n \in \mathbb{K}$. Logo, cada $a_i \in \mathbb{K}$ tem q possibilidades, portanto $\mathbb{F}$ tem exatamente q^n elementos. □

Outra propriedade importante dos corpos finitos é a seguinte:

Lema 1.7. *Se $\mathbb{F}$ é um corpo finito com q elementos, então todo $a \in \mathbb{F}$ satisfaz $a^q = a$.*

Demonstração. Para $a = 0$ tem-se que $a^q = a$.

Seja $a \neq 0$ um elemento de $\mathbb{F}$. Como $\mathbb{F}$ é corpo finito com q elementos, tem-se que $\mathbb{F}^*$ é um grupo multiplicativo de ordem $q-1$. Pelo Teorema de Lagrange, tem-se $a^{q-1} = 1$. Assim, $a^q = a$ para todo $a \in \mathbb{F}$. □

Lema 1.8. *Se $\mathbb{F}$ é um corpo finito com q elementos e $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, então o polinômio $x^q - x$ em $\mathbb{K}[x]$ se fatora em $\mathbb{F}[x]$ como*

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

e $\mathbb{F}$ é o corpo de decomposição de $x^q - x$ sobre $\mathbb{K}$.

Demonstração. Para cada $a \in \mathbb{F}$ tem-se

$$a^q - a = a - a = 0.$$

Assim, a é raiz de $x^q - x$. Como o polinômio $x^q - x$ tem no máximo q raízes diferentes em $\mathbb{F}$, obtém-se que $\mathbb{F}$ é o conjunto de raízes de $x^q - x$. Como $\prod_{a \in \mathbb{F}} (x - a)$ e $x^q - x$ têm as mesmas raízes e são mônicos, segue que são iguais. □

Teorema 1.9. *[14, Theorem 2.8] Para cada corpo finito $\mathbb{F}_q$ o grupo multiplicativo $\mathbb{F}_q^*$ de elementos distintos de zero de $\mathbb{F}_q$ é cíclico.*

A seguinte noção é importante no decorrer do trabalho, já que um dos desafios da pesquisa atual enfoca-se em demonstrar a existência de elementos normais primitivos.

Definição 1.10. Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de **elemento primitivo** de $\mathbb{F}_q$.

Os próximos resultados são propriedades dos corpos finitos e dos aneis de polinômios sobre corpos finitos que são de grande importância na álgebra.

Lema 1.11. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre o corpo finito $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão de corpo $\mathbb{F}_q$. Então para um polinômio $h \in \mathbb{F}_q[x]$ tem-se $h(\alpha) = 0$ se e somente se f divide h.*

Demonstração. $\Rightarrow$ Suponhamos que $f(x)$ não divide $h(x)$. Como $mdc(f(x), h(x))$ divide $f(x)$ e $f(x)$ é irredutível, segue que $mdc(f(x), h(x)) = 1$. Do Teorema de Bezout sabemos que existem $a(x), b(x) \in \mathbb{F}_q[x]$ tais que $a(x)f(x) + b(x)h(x) = 1$. Substituindo x por α temos que

$$1 = a(\alpha)f(\alpha) + b(\alpha)h(\alpha) = 0$$

o que é contraditório. Portanto, $f|g$.

$\Leftarrow$ Se $f|h$ então existe $g \in \mathbb{F}_q[x]$ tal que $h(x) = f(x)g(x)$. Como α é raiz de f, segue que $h(\alpha) = f(\alpha)g(\alpha) = 0$. □

O seguinte teorema é fundamental para determinar quando uma raiz de um polinômio tem multiplicidade maior que 1.

Teorema 1.12. *[14, Theorem 1.68] O elemento $b \in \mathbb{F}$ é uma raiz múltipla de $f \in \mathbb{F}[x]$ se e somente se é uma raiz de f e f', onde f' representa a derivada formal de f.*

Teorema 1.13. *[14, Theorem 2.6] Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, cada subcorpo de $\mathbb{F}_q$ têm p^m elementos, 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.*

Teorema 1.14. *[14, Theorem 2.5][Existência e unicidade de um corpo finito]*
Para cada p primo e cada inteiro positivo n existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de raízes de $x^q - x$ sobre $\mathbb{F}_p$.

O lema a seguir é vital no desenvolvimento deste trabalho, e será utilizado nas demonstrações dos teoremas do Capítulo 4.

Lema 1.15. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se e somente se m divide n.*

Demonstração. $\Rightarrow$ Suponhamos que $f(x) \mid (x^{q^n} - x)$. Seja α uma raiz de f, então $\alpha^{q^n} - \alpha = 0$. Isto é $\alpha^{q^n} = \alpha$. Logo, $\alpha \in \mathbb{F}_{q^n}$ e $\mathbb{F}_q[\alpha]$ é um subcorpo de $\mathbb{F}_{q^n}$. Assim,

$$\begin{aligned} [\mathbb{F}_{q^n} : \mathbb{F}_q] &= [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]][\mathbb{F}_q[\alpha] : \mathbb{F}_q] \\ n &= [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]] \cdot m. \end{aligned}$$

Portanto, $m \mid n$.

$\Leftarrow$ Se $m \mid n$ segue do Teorema 1.13 que $\mathbb{F}_{q^n}$ contém o subcorpo $\mathbb{F}_{q^m}$. Se α é uma raiz de f, então $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = m$ e assim $\mathbb{F}_q[\alpha] \underbrace{=}_{Teo.1.14} \mathbb{F}_{q^m}$. Como $\alpha \in \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, segue que α é raiz de $x^{q^n} - x$. Logo, $\alpha^{q^n} = \alpha$ e, pelo Lema 1.11, tem-se $f(x) \mid (x^{q^n} - x)$. □

Teorema 1.16. *Se f é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n, então f tem uma raiz α em $\mathbb{F}_{q^n}$. Além disso, todas as raízes de f são simples e são dadas pelos n elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ de $\mathbb{F}_{q^n}$.*

Demonstração. Seja α uma raiz de f. Nesse caso, $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = n$ e, portanto, $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^n}$. Assim, $\alpha \in \mathbb{F}_{q^n}$. Agora, seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ com $a_i \in \mathbb{F}_q$ para $0 \leq i \leq n$. Se β é uma raiz arbitrária de f, tem-se

$$\begin{aligned} f(\beta^q) &= a_n(\beta^q)^n + a_{n-1}(\beta^q)^{n-1} + \cdots + a_1(\beta^q) + a_0 \\ &= a_n^q \beta^{qn} + a_{n-1}^q \beta^{q(n-1)} + \cdots + a_1^q \beta^q + a_0^q \\ &= (a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0)^q \\ &= f(\beta)^q \\ &= 0, \end{aligned}$$

isto é, β^q é raiz de f. Portanto, como α é raiz, então α^q é raiz, e indutivamente $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ são raízes de f.

A seguir mostra-se que $\alpha^{q^j} \neq \alpha^{q^k}$ se $0 \leq j < k < n$. Suponhamos que $\alpha^{q^j} = \alpha^{q^k}$ para alguns inteiros j e k com $0 \leq j < k \leq n-1$, de modo que elevando essa igualdade à potência q^{n-k}, obtemos

$$\begin{aligned} (\alpha^{q^j})^{q^{n-k}} &= (\alpha^{q^k})^{q^{n-k}} \\ \alpha^{q^{j+n-k}} &= \alpha^{q^{k+n-k}} \\ \alpha^{q^{n-k+j}} &= \alpha^{q^n} = \alpha. \end{aligned}$$

Como $f(\alpha) = 0$ e α é raiz de $x^{q^n} - x$, pelo Lema 1.11, segue-se que $f \mid (x^{q^{n-k+j}} - x)$ e, pelo Lema 1.6, obtém-se que $n \mid (n-k+j)$, o que é impossível pois $j - k < 0$. Portanto, $\alpha^{q^j} \neq \alpha^{q^k}$. □

A seguinte definição é importante porque nos próximos capítulos será apresentada a noção de elemento normal e sua caracterização que tem a ver com os elementos conjugados.

Definição 1.17. Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^n}$. Os elementos $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ dados no teorema anterior são chamados de **conjugados** de α com respeito a $\mathbb{F}_q$.

Uma consequência do teorema anterior é o seguinte:

Corolário 1.18. *[14, Corollary 2.19] Se α é um elemento primitivo de $\mathbb{F}_q$, então o mesmo acontece com todos os seus conjugados em relação a qualquer subcorpo de $\mathbb{F}_q$.*

A seguir exibem-se a definição de traço de um elemento, e algumas propriedades que envolvem esta noção, pois a partir disso definem-se e caracterizam-se os elementos normais.

Definição 1.19. Para $\alpha \in \mathbb{F}_{q^n}$, o **traço** $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ de α sobre $\mathbb{F}_q$ é definido por

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

Se $\mathbb{F}_p$ é o corpo primo de $\mathbb{F}_{q^n}$, então $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha)$ é chamada de **traço absoluto** de α e é denotado simplesmente por $Tr_{\mathbb{F}_{q^n}}(\alpha)$.

Teorema 1.20. *A função traço $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ satisfaz as seguintes propriedades:*

i. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha + \beta) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$ *para todos* $\alpha, \beta \in \mathbb{F}_{q^n}$;

ii. $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *para todos* $c \in \mathbb{F}_q$ *e* $\alpha \in \mathbb{F}_{q^n}$.

Demonstração. i. Para todos $\alpha, \beta \in \mathbb{F}_{q^n}$, temos

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^q + \cdots + (\alpha + \beta)^{q^{n-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} \\ &= (\alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}) + (\beta + \beta^q + \cdots + \beta^{q^{n-1}}) \\ &= Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta). \end{aligned}$$

ii. Para todos $c \in \mathbb{F}_q$ e $\alpha \in \mathbb{F}_{q^n}$, temos

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

□

A seguinte definição será utilizada no Capítulo 2 para definir elemento normal.

Definição 1.21. Uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ da forma $\{\alpha, \alpha^q, \ldots \alpha^{q^{n-1}}\}$, consistindo de um elemento adequado $\alpha \in \mathbb{F}_{q^n}$ e seus conjugados com respeito a $\mathbb{F}_q$, é chamada de **base normal** de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

A próxima definição permite estabelecer quando um conjunto é uma base do corpo $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Definição 1.22. Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ de grau n sobre $\mathbb{F}_q$. O conjunto **discriminante** $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n)$ dos elementos $\alpha_1, \ldots, \alpha_n \in F$ é definido pelo determinante de ordem n dado por

$$\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_2) & \ldots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_n) \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_2) & \ldots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_1) & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_2) & \ldots & Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_n) \end{vmatrix}.$$

Teorema 1.23. *Seja $\mathbb{F}_q$ um corpo finito, $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ de grau n sobre $\mathbb{F}_q$, e $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^n}$. O conjunto $\{\alpha_1, \ldots, \alpha_n\}$ é base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se e somente se $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Demonstração. $\Rightarrow$ Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Será demonstrado $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n) \neq 0$, mostrando que os vetores coluna do determinante definido por $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n)$ são linearmente independentes. Suponhamos que existem $c_1, \ldots, c_n \in \mathbb{F}_q$ tais que $c_1Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_j) + \cdots + c_nTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_j) = 0$ para todo $1 \leq j \leq n$. Isto é equivalente a

$$\begin{gathered} c_1Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_1) + \cdots + c_nTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_1) = 0 \\ c_1Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_2) + \cdots + c_nTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_2) = 0 \\ \vdots \\ c_1Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_n) + \cdots + c_nTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_n) = 0. \end{gathered}$$

Se $b = c_1\alpha_1 + \cdots + c_n\alpha_n$, então $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b\alpha_j) = 0$ para $1 \leq j \leq n$. De fato para cada $1 \leq j \leq n$ tem-se

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b\alpha_j) &= Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}((c_1\alpha_1 + \cdots + c_n\alpha_n)\alpha_j) \\ &= c_1Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_j) + \cdots + c_nTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_j) \\ &= 0, \end{aligned}$$

como $(\alpha_1, \ldots, \alpha_n)$ é base para $\mathbb{F}_{q^n}$ segue-se que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b\alpha) = 0$ para todo $\alpha \in \mathbb{F}_{q^n}$.

Porém, isto é possível se $b = 0$. De fato, suponhamos que $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b\alpha) = 0$ para todo $\alpha \in \mathbb{F}_{q^n}$ e que $b \neq 0$. Considere o polinômio

$$\begin{aligned} f(x) &= bx + (bx)^q + (bx)^{q^2} + \cdots + (bx)^{q^{n-1}} \\ &= bx + b^q x^q + \cdots + b^{q^{n-1}} x^{q^{n-1}}, \end{aligned}$$

que é um polinômio não nulo de grau q^{n-1}. Como $f(\alpha) = 0$ para todo $\alpha \in \mathbb{F}_{q^n}$, temos que f possui pelo menos q^n raízes. Logo, tem mais raízes que o grau, o que é contraditório. Desta forma $b = 0$.

$\Leftarrow$ Reciprocamente, suponha que $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n) \neq 0$ e que $c_1\alpha_1 + \cdots + c_n\alpha_n \neq 0$ para todo $c_1, \ldots, c_n \in \mathbb{F}_q$, onde não todos os c_i são nulos. Logo,

$$c_1\alpha_1\alpha_j + \cdots + c_n\alpha_n\alpha_j = 0 \quad \text{para todo} \quad 1 \leq j \leq n$$

e aplicando a função $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ tem-se,

$$c_1 Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_j) + \cdots + c_n Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_j) = 0 \quad \text{para todo} \quad 1 \leq j \leq n.$$

Como os vetores coluna da matriz cujo determinante é $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n)$ são linearmente independentes, então $c_1 = \cdots = c_n = 0$. Logo, $\alpha_1, \ldots, \alpha_n$ são linearmente independentes sobre $\mathbb{F}_q$. Portanto, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

□

Corolário 1.24. *Seja $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^n}$. O conjunto $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se e somente se*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_n^q \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \ldots & \alpha_n^{q^{n-1}} \end{vmatrix} \neq 0.$$

Demonstração. Seja

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_n^q \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{q^{i-1}} & \alpha_2^{q^{i-1}} & \ldots & \alpha_n^{q^{i-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \ldots & \alpha_n^{q^{n-1}} \end{pmatrix},$$

e desse modo,

$$A^T = \begin{pmatrix} \alpha_1 & \alpha_1^q & \ldots & \alpha_1^{q^{j-1}} & \ldots & \alpha_1^{q^{n-1}} \\ \alpha_2 & \alpha_2^q & \ldots & \alpha_2^{q^{j-1}} & \ldots & \alpha_2^{q^{n-1}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_n & \alpha_n^q & \ldots & \alpha_n^{q^{j-1}} & \ldots & \alpha_n^{q^{n-1}} \end{pmatrix}.$$

Assim, $B = A^T \cdot A = (Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\alpha_j))$.
$\Rightarrow$ Se $\{\alpha_1, \ldots, \alpha_n\}$ é base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, então, pelo Teorema 1.23,

$$\begin{aligned} 0 \neq \Delta_{F/K}(\alpha_1, \ldots, \alpha_n) &= \det(A) \cdot \det(A^T) \\ &= \det(A)^2. \end{aligned}$$

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

$\Leftarrow$ Se $\det(A) \neq 0$, então $\det(A^T) = \det(A) \neq 0$. Assim,

$$\begin{aligned} \det(B) &= \Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n) \\ &= \det(A) \cdot \det(A^T) \\ &\neq 0, \end{aligned}$$

e, pelo Teorema 1.23, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. □

1.2 Polinômios linearizados

Nesta seção apresentam-se as definições de q-polinômios (conhecidos também na literatura como polinômios linearizados), q-módulos e polinômios q-associados. Além disso, exibem-se também resultados que são importantes no desenvolvimento dos próximos capítulos.

Definição 1.25. Um polinômio da forma

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$$

com coeficientes em uma extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$, é chamado de **q-polinômio** sobre $\mathbb{F}_{q^n}$, (também chamado de **polinômio linearizado** sobre $\mathbb{F}_{q^n}$).

Se $\mathbb{F}_{q^s}$ é uma extensão arbitrária de $\mathbb{F}_{q^n}$ e $L(x)$ é um polinômio linearizado (ou seja, um q-polinômio) sobre $\mathbb{F}_{q^n}$, então, $n \mid s$ e

$$L(\beta + \gamma) = L(\beta) + L(\gamma) \quad \text{para todos } \beta, \gamma \in \mathbb{F}_{q^s}, \tag{1.1}$$

$$L(c\beta) = cL(\beta) \text{ para todo } c \in \mathbb{F}_q \text{ e todo } \beta \in \mathbb{F}_{q^s}. \tag{1.2}$$

Como, $\mathbb{F}_{q^s}$ é um espaço vetorial sobre $\mathbb{F}_q$, segue que, os polinômios linearizados sobre $\mathbb{F}_q$ são operadores $\mathbb{F}_q$-lineares.

Teorema 1.26. *Seja $L(x)$ um q-polinômio não nulo sobre $\mathbb{F}_{q^n}$ e seja $\mathbb{F}_{q^s}$ a extensão de corpo de $\mathbb{F}_{q^n}$ contendo todas as raízes de $L(x)$. Então, cada raiz de $L(x)$ tem a mesma multiplicidade, que é uma potência de q, e as raízes formam um $\mathbb{F}_q$-subespaço linear de $\mathbb{F}_{q^s}$.*

Demonstração. Segue das Equações (1.1) e (1.2) que qualquer combinação linear das raízes com coeficientes em $\mathbb{F}_q$ é de novo uma raiz, logo as raízes de $L(x)$ formam um subespaço linear de $\mathbb{F}_{q^s}$. Se

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i},$$

então

$$\begin{aligned} L'(x) &= \alpha_0 + q(\alpha_1 x^{q-1}) + q(q\alpha_2 x^{q^2-1}) + \cdots + q(q^{m-1}\alpha_m x^{q^m-1}) \\ &= \alpha_0. \end{aligned}$$

Assim, $L(x)$ tem unicamente raízes simples no caso $\alpha_0 \neq 0$.

Por outro lado, se $k \geq 1$ é o menor subíndice tal que se $\alpha_0 = \alpha_1 = \cdots = \alpha_{k-1} = 0$, e $\alpha_k \neq 0$ (que existe já que $L(x)$ é não nulo) tem-se

$$\begin{aligned} L(x) &= \sum_{i=k}^{m} \alpha_i x^{q^i} \\ &= \sum_{i=k}^{m} \alpha_i^{q^{nk}} x^{q^i} \\ &= \alpha_k^{q^{nk}} x^{q^k} + \alpha_{k+1}^{q^{nk}} x^{q^{k+1}} + \cdots + \alpha_m^{q^{nk}} x^{q^m} \\ &= \left(\alpha_k^{q^{(n-1)k}} x\right)^{q^k} + \left(\alpha_{k+1}^{q^{(n-1)k}} x^q\right)^{q^k} + \cdots + \left(\alpha_m^{q^{(n-1)k}} x^{q^{(m-k)}}\right)^{q^k} \\ &= \left(\alpha_k^{q^{(n-1)k}} x + \alpha_{k+1}^{q^{(n-1)k}} x^q + \cdots + \alpha_m^{q^{(n-1)k}} x^{q^{(m-k)}}\right)^{q^k} \\ &= \left(\sum_{i=k}^{m} \alpha_i^{q^{(n-1)k}} x^{q^{i-k}}\right)^{q^k}, \end{aligned}$$

este último é q^k-ésima potência de um q-polinômio com coeficiente independente não nulo, então as raízes deste q polinômio têm multiplicidade q^k. □

Teorema 1.27. *Sejam $\beta_1, \beta_2, \ldots, \beta_m$ elementos de $\mathbb{F}_{q^n}$. Então*

$$\begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{m-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{m-1}} \\ \vdots & \vdots & \vdots & \vdots & \\ \beta_m & \beta_m^q & \beta_m^{q^2} & \ldots & \beta_m^{q^{m-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{m-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k\right), \tag{1.3}$$

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

Demonstração. Seja D_m o determinante do lado esquerdo da Equação (1.3). Será demonstrado o teorema usando o método de indução sobre m.

Para $m = 1$ tem-se que $D_m = \beta_1$ e se interpreta

$$\prod_{j=1}^{0} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k\right) = 1,$$

logo a Equação (1.3) é valida.

Suponha que o resultado é valido para $r = m \geq 1$ e será demonstrado que isso é verdade para $r = m + 1$. Considere o polinômio

$$D(x) = \begin{vmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{m-1}} & \beta_1^{q^m} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{m-1}} & \beta_2^{q^m} \\ \vdots & \vdots & \vdots & \vdots & & \\ \beta_m & \beta_m^q & \beta_m^{q^2} & \ldots & \beta_m^{q^{m-1}} & \beta_m^{q^m} \\ x & x^q & x^{q^2} & \ldots & x^{q^{m-1}} & x^{q^m} \end{vmatrix},$$

isto é

$$D(x) = D_m x^{q^m} + \sum_{i=0}^{m-1} (-1)^{m-1-i} \alpha_i x^{q^i},$$

onde os α_i são os determinantes das matrizes $m \times m$ que surgem depois de eliminar a coluna i-ésima e a última linha, com $\alpha_i \in \mathbb{F}_{q^n}$ para todo $i = 0, \ldots, m-1$.

Caso 1. Suponhamos que $\beta_1, \ldots, \beta_m$ são linearmente independentes sobre $\mathbb{F}_q$, então $D(\beta_i) = 0$ para $i = 1, \ldots, m$. Como $D(x)$ é um q-polinômio, segue-se que toda combinação linear $c_1\beta_1 + \cdots + c_m\beta_m$ com $c_i \in \mathbb{F}_q$ uma raiz do polinômio $D(x)$. Como todas as raízes são diferentes, tem-se uma fatoração

$$D(x) = D_m \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(x - \sum_{k=1}^{m} c_k\beta_k \right). \tag{1.4}$$

Caso 2. Suponhamos que $\beta_1, \ldots, \beta_m$ são linearmente dependentes sobre $\mathbb{F}_q$, então $D_m = 0$ e existem $b_1, \ldots, b_m \in \mathbb{F}_q$ com pelo menos um $b_l \neq 0$ tal que $\sum_{i=1}^{m} b_i\beta_i = 0$. Assim

$$\begin{aligned} \sum_{i=1}^{m} b_i\beta_i^{q^j} &= \sum_{i=1}^{m} b_i^{q^j}\beta_i^{q^j} \\ &= \sum_{i=1}^{m} (b_i\beta_i)^{q^j} \\ &= \left(\sum_{i=1}^{m} b_i\beta_i \right)^{q^j} \\ &= 0, \end{aligned}$$

para todo $j = 0, \ldots, m$.

Por conseguinte, as primeiras m colunas do determinante que definem o polinômio $D(x)$ são linearmente dependentes sobre $\mathbb{F}_q$. Logo $D(x) = 0$, desse modo a Equação (1.4) é satisfeita sem importar a independência dos β_i. Consequentemente,

$$D_{m+1} = D(\beta_{m+1}) = D_m \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(\beta_{m+1} - \sum_{k=1}^{m} c_k\beta_k \right). \tag{1.5}$$

Por hipótese de indução,

$$D_m = \beta_1 \prod_{j=1}^{m-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k\beta_k \right),$$

de modo que,

$$\begin{aligned} D_{m+1} &= \beta_1 \prod_{j=1}^{m-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k\beta_k \right) \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(\beta_{m+1} - \sum_{k=1}^{m} c_k\beta_k \right) \\ &= \beta_1 \prod_{j=1}^{m} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k\beta_k \right). \end{aligned}$$

□

Teorema 1.28. *Seja U um subespaço linear de $\mathbb{F}_{q^n}$ considerado como um espaço vetorial sobre $\mathbb{F}_q$. Então para qualquer inteiro não negativo k, o polinômio*

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

é um q-polinômio sobre $\mathbb{F}_{q^n}$.

Demonstração. A potência q^k de um q-polinômio sobre $\mathbb{F}_{q^n}$ é de novo um q-polinômio. De fato se $G(x) = \sum_{i=0}^{m} \alpha_i x^{q^i}$ é um q-polinômio, então

$$\begin{aligned} G(x)^{q^k} &= \left(\sum_{i=0}^{m} \alpha_i x^{q^i}\right)^{q^k} \\ &= \left(\alpha_0 x + \alpha_1 x^q + \cdots + \alpha_m x^{q^m}\right)^{q^k} \\ &= \alpha_0^{q^k} x^{q^k} + \alpha_1^{q^k} x^{q^{k+1}} + \cdots + \alpha_m^{q^k} x^{q^{m+k}} \\ &= \sum_{i=0}^{m} \alpha_i^{q^k} x^{q^{i+k}}. \end{aligned}$$

Assim, $G(x)^{q^k}$ é de novo um q-polinômio para todo $k \geq 0$, então basta-se demonstrar o resultado para $k = 0$. Como U é subespaço linear de $\mathbb{F}_{q^n}$, seja $\{\beta_1, \ldots, \beta_m\}$ uma base de U sobre $\mathbb{F}_q$, logo pelo Teorema 1.27 $D_m \neq 0$.

Por outro lado, se

$$L(x) = \prod_{\beta \in U} (x - \beta),$$

como $\beta \in U$ e $\{\beta_1, \ldots, \beta_m\}$ é base de U segue-se que existem $c_1, \ldots, c_m \in \mathbb{F}_q$ tal que

$$\begin{aligned} \beta &= c_1\beta_1 + c_2\beta_2 + \cdots + c_m\beta_m \\ &= \sum_{i=1}^{m} c_i\beta_i. \end{aligned}$$

Por conseguinte,

$$(x - \beta) = \left(x - \sum_{i=1}^{m} c_i\beta_i\right),$$

desse modo

$$L(x) = \prod_{c_1,\ldots,c_m \in \mathbb{F}_q} \left(x - \sum_{i=1}^{m} c_i\beta_i\right) = D_m^{-1} D(x),$$

e como $D(x)$ é q-polinômio, então $L(x)$ é q-polinômio. □

Definição 1.29. Os polinômios

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{e} \quad L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

sobre $\mathbb{F}_{q^n}$ são chamados **q-associados** um do outro. Mais especificamente, $l(x)$ é o q-associado convencional de $L(x)$ e $L(x)$ é o q-associado linearizado de $l(x)$.

O produto ordinário de polinômios linearizados não precisa ser um polinômio linearizado. No entanto, a composição $L_1(L_2(x))$ de dois q-polinômios $L_1(x)$, $L_2(x)$ sobre $\mathbb{F}_{q^n}$ é novamente um q-polinômio. Em vez da palavra composição, usamos a expressão multiplicação simbólica. Assim, definimos a **multiplicação simbólica** por

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

Se $L_1(x)$ e $L(x)$ são q-polinômios sobre $\mathbb{F}_q$, dizemos que $L_1(x)$ **divide simbolicamente** $L(x)$ (ou que $L(x)$ é simbolicamente divisível por $L_1(x)$) se $L(x) = L_1(x) \otimes L_2(x)$ para algum q-polinômio $L_2(x)$ sobre $\mathbb{F}_q$.

Teorema 1.30. *[14, Corollary 3.60] Sejam $L_1(x)$ e $L(x)$ q-polinômios sobre $\mathbb{F}_q$ com q-associados convencionales $l_1(x)$ e $l(x)$. Então $L_1(x)$ divide simbolicamente a $L(x)$ se e somente se $l_1(x)$ divide $l(x)$.*

Definição 1.31. Um espaço vetorial de dimensão finita M sobre $\mathbb{F}_q$ que está contido em alguma extensão de corpos de $\mathbb{F}_q$ e tem a propriedade que a q-ésima potência de cada elemento de M é novamente um elemento de M é chamado de **q-módulo**.

Teorema 1.32. *O polinômio mônico $L(x)$ é um q-polinômio sobre $\mathbb{F}_q$, se e somente se, cada raiz de $L(x)$ tem a mesma multiplicidade, a qual é uma potência de q e as raízes formam um q-módulo.*

Demonstração. $\Rightarrow$ Segue do Teorema 1.26 e pelo fato que a q-ésima potência de uma raiz é uma raiz, portanto, as raízes formam um q-módulo.

$\Leftarrow$ Pela hipótese e o Teorema 1.28, tem-se que $L(x)$ é um q-polinômio sobre alguma extensão de corpos de $\mathbb{F}_q$. Isto é, se M é um q-módulo que consiste de todas as raízes de $L(x)$, então

$$L(x) = \prod_{\beta \in M} (x - \beta)^{q^k},$$

para algum inteiro positivo k. Como a funcão

$$\begin{array}{ccc} M & \to & M \\ \beta & \mapsto & \beta^q \end{array}$$

é injetora segue que $M = \{\beta^q \mid \beta \in M\}$, assim obtém-se que

$$\begin{aligned} (L(x))^q &= \left(\prod_{\beta \in M} (x - \beta)^{q^k} \right)^q \\ &= \prod_{\beta \in M} (x^q - \beta^q)^{q^k} \\ &= \prod_{\beta \in M} (x^q - \beta)^{q^k} \\ &= L(x^q). \end{aligned}$$

Desta forma se

$$L(x) = \sum_{i=0}^{m} \alpha_i x^{q^i},$$

então

$$\sum_{i=0}^{m} \alpha_i^q x^{q^{i+1}} = L(x)^q = L(x^q) = \sum_{i=0}^{m} \alpha_i x^{q^{i+1}},$$

logo, para $0 \leq i \leq m$ implica-se que $\alpha_i^q = \alpha_i$ isto é, dado $\alpha_i \in \mathbb{F}_q$ então $L(x)$ é q-polinômio sobre $\mathbb{F}_q$. □

Este conceito pode ser visto a seguir: seja $g(x)$ o polinômio minimal de ζ sobre $\mathbb{F}_{q^n}$. Então, ζ é uma q-raiz primitiva de $L(x)$ sobre $\mathbb{F}_{q^n}$ se e somente se, $g(x)$ divide a $L(x)$ e $g(x)$ não divide nenhum q-polinômio de grau menor.

1.3 Funções ϕ e Φ_q de Euler

Nesta seção apresentam-se as definições da Função de Euler para números inteiros e para polinômios, além de algumas consequências relevantes para este trabalho. Estas noções são significativas porque a quantidade e a densidade dos elementos normais e k-normais podem ser calculadas em função destas definições.

A seguir exibem-se as definições da Função de Euler para números inteiros e para polinômios.

Definição 1.33. Para $m \in \mathbb{N}$, a **função** $\phi(m)$ é definida como o número de inteiros k com $1 \leq k \leq m$ e $\text{mdc}(k, m) = 1$. Esta função é conhecida na literatura como a Função ϕ de Euler.

Definição 1.34. Para $f \in \mathbb{F}_q[x]$ não nulo, $\Phi_q(f(x)) = \Phi_q(f)$ denota o número de polinômios $g \in \mathbb{F}_q[x]$ tal que:

i. $\text{grau}(g) < \text{grau}(f)$,

ii. $\text{mdc}(f, g) = 1$.

Outra definição para a Função Φ_q de Euler para polinômios, em termos do anel de polinômios $\mathbb{F}_q[x]$ é dada a seguir.

Definição 1.35. Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico, a função Euler Φ para polinômios é dada por

$$\Phi_q(f) = \left| \left(\mathbb{F}_q[x] \Big/ f\mathbb{F}_q[x] \right)^* \right|,$$

onde $f\mathbb{F}_q[x] = (f)$ é o ideal de $\mathbb{F}_q[x]$ gerado por $f(x)$.

As definições 1.34 e 1.35 são equivalentes, isto é.

Teorema 1.36. *Seja* $\overline{g} \in \left(\mathbb{F}_q[x] \Big/ (f) \right)^*$ *se e somente se* $\text{mdc}(f, g) = 1$.

Demonstração. $\Leftarrow$ Se $\text{mdc}(f, g) = r > 1$, então existem $f_1, g_1 \in \mathbb{F}_q[x]$ tais que $f = f_1 r$ e $g = g_1 r$, logo $\overline{g_1}$, $\overline{r}$ e $\overline{f_1}$ são diferentes de $\overline{0}$. Assim

$$\overline{f_1}\overline{g} = \overline{f_1 g} = \overline{f_1 g_1 r} = \overline{f g_1} = \overline{0},$$

isto mostra que $\overline{g} \notin \left(\mathbb{F}_q[x] \Big/ (f) \right)^*$, já que $\overline{g}$ é divisor de zero, e os divisores de zero não tem inverso.

$\Rightarrow$ Seja $\text{mdc}(f, g) = 1$, então existem $a, b \in \mathbb{F}_q[x]$ tais que $af + bg = 1$, logo $\overline{af + bg} = \overline{1}$, e assim $\underbrace{\overline{af}}_{\in (f)} + \overline{bg} = \overline{1}$, desta forma $\overline{bg} = \overline{b}\overline{g} = \overline{1}$, o que implica $\overline{g} \in \left(\mathbb{F}_q[x] \Big/ (f) \right)^*$. □

Observação 1.37. A expressão $\Phi_q(f) = \left| \left(\mathbb{F}_q[x] \Big/ (f) \right)^* \right|$ conta o número de elementos invertíveis de $\mathbb{F}_q[x] \Big/ (f)$. Isto é

$$\left| \left(\mathbb{F}_q[x] \Big/ (f) \right)^* \right| = |\{g \in \mathbb{F}_q[x]; \text{grau}(g) < \text{grau}(f) \text{ e } \text{mdc}(f, g) = 1\}| = \Phi_q(f).$$

Lema 1.38. *A função* Φ_q *definida para polinômios não nulos em* $\mathbb{F}_q[x]$ *tem as seguintes propriedades:*

i. $\Phi_q(f) = 1$ *se* $\text{grau}(f) = 0$*;*

ii. $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$*, sempre que* f *e* g *sejam primos relativos;*

iii. se $\text{grau}(f) = n \geq 1$*, então*

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \dots (1 - q^{-n_l}) = q^n \prod_{i=1}^{l} \left(1 - \frac{1}{q^{n_i}}\right), \tag{1.6}$$

onde os n_l *são os graus dos polinômios mônicos irredutíveis distintos que aparecem na fatoração canônica de* f *em* $\mathbb{F}_q[x]$*.*

Demonstração. i. Como $\text{grau}(f) = 0$, então $f = m$ com $m \in \mathbb{F}_q$. Logo, não existe um polinômio mônico $g \in \mathbb{F}_q[x]$ com $\text{grau}(g(x)) \leq \text{grau}(f)$ além do 1. Portanto, $\Phi_q(f) = 1$.

ii. Seja $\Phi_q(f) = s$ e $\Phi_q(g) = t$. Sejam $f_1, \dots, f_s$ e $g_1, \dots, g_t$ os polinômios contados por $\Phi_q(f)$ e $\Phi_q(g)$. Se $h \in \mathbb{F}_q[x]$ é um polinômio com $\text{grau}(h) < \text{grau}(fg)$ e $\text{mdc}(fg, h) = 1$, então $\text{mdc}(f, h) = 1$ e $\text{mdc}(g, h) = 1$, assim $h \equiv f_i \pmod f$ e $h \equiv g_j \pmod g$ para um único par ordenado (i, j) com $1 \leq i \leq s$, $1 \leq j \leq t$.

Por outro lado, dado um par ordenado (i, j), o Teorema do Resto Chinês para o anel $\mathbb{F}_q[x]$ garante que existe um único $h \in \mathbb{F}_q[x]$ com $h \equiv f_i \pmod f$ e $h \equiv g_j \pmod g$ e $\text{grau}(h) < \text{grau}(fg)$. Este h satisfaz que $\text{mdc}(f, h) = \text{mdc}(h, g) = 1$ e assim $\text{mdc}(fg, h) = 1$. Por isso, existe uma correspondência $1 - 1$ entre os st pares ordenados (i, j) e os polinômios $h \in \mathbb{F}_q[x]$ com $\text{grau}(h) < \text{grau}(fg)$ e $\text{mdc}(fg, h) = 1$, consequentemente, $\Phi_q(fg) = st = \Phi_q(f)\Phi_q(g)$.

iii. Para um polinômio irredutível b em $\mathbb{F}_q[x]$ de grau m e um inteiro positivo s, pode-se calcular $\Phi_q(b^s)$ da seguinte forma: os polinômios $h \in \mathbb{F}_q[x]$ com $\text{grau}(h) < \text{grau}(b^s) = ms$ que não são primos relativos a b^s são precisamente os que são divisíveis por b. Isto é, os polinômios da forma $h = gb$ com $\text{grau}(g) < ms - m$, como existem q^{ms-m} possibilidades diferentes de g. Então

$$\Phi_q(b^s) = q^{ms} - q^{ms-m} = q^{ms}(1 - q^{-m}).$$

Agora, seja $f \in \mathbb{F}_q[x]$ com $\text{grau}(f) = n \geq 1$ tal que

$$f = f_1^{s_1} \cdot f_2^{s_2} \cdot \dots \cdot f_l^{s_l}$$

é uma fatoração de f, onde f_i é irredutível sobre $\mathbb{F}_q$ e $\text{grau}(f_i) = n_i$ para cada $i = 1, \dots, l$.

Pelo item *ii.* tem-se que,

$$\begin{aligned}
\Phi_q(f) &= \Phi_q(f_1^{s_1}) \cdot \Phi_q(f_2^{s_2}) \cdot \dots \cdot \Phi_q(f_l^{s_l}) \\
&= q^{s_1 n_1}(1 - q^{-n_1}) \cdot q^{s_2 n_2}(1 - q^{-n_2}) \cdot \dots \cdot q^{s_l n_l}(1 - q^{-n_l}) \\
&= q^{\sum_{i=1}^{l} s_i n_i} \left(1 - q^{-n_1}\right) \cdot \left(1 - q^{-n_2}\right) \cdot \dots \cdot \left(1 - q^{-n_l}\right) \\
&= q^n \left(1 - q^{-n_1}\right) \cdot \left(1 - q^{-n_2}\right) \cdot \dots \cdot \left(1 - q^{-n_l}\right).
\end{aligned}$$

□

Da Expressão (1.6), tem-se que $\Phi_q(f)$ somente depende do número de fatores irredutíveis distintos que f tem de cada grau.

Definição 1.39. Seja $L(x)$ um q-polinômio não nulo sobre $\mathbb{F}_{q^n}$. Uma raiz ζ de $L(x)$ é chamada uma q**- raiz primitiva** sobre $\mathbb{F}_{q^n}$, se esta não é raiz de qualquer q-polinômio não nulo sobre $\mathbb{F}_{q^n}$ de menor grau.

Os seguintes teoremas serão utilizados nos próximos capítulos para determinar a quantidade de elementos normais em um determinado corpo finito:

Teorema 1.40. *[14, Theorem 3.70] Seja $L(x)$ um q-polinômio não nulo sobre $\mathbb{F}_q$ com q-associado convencional $l(x)$. Então o número N_L de q-raízes primitivas de $L(x)$ sobre $\mathbb{F}_q$ é dado por $N_L = 0$ se $L(x)$ tiver raízes múltiplas e por $N_L = \Phi_q(l(x))$ se $L(x)$ tiver raízes simples.*

Teorema 1.41. *[14, Theorem 3.73] Seja M um q-módulo de dimensão $m \geq 1$ sobre $\mathbb{F}_q$. Então existe um elemento $\zeta \in M$ tal que $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{m-1}}\}$ é uma base de M sobre $\mathbb{F}_q$.*

1.4 Polinômios ciclotômicos

Nesta seção apresentam-se a noção de polinômio ciclotômico e algumas consequências que serão utilizadas no Capítulo 4.

Definição 1.42. Seja n um inteiro positivo. O menor corpo que contém as raízes de $x^n - 1$ sobre um corpo $\mathbb{K}$ é chamado de **n-ésimo corpo ciclotômico** sobre $\mathbb{K}$ e denotado por $\mathbb{K}^{(n)}$. As raízes de $x^n - 1$ em $\mathbb{K}^{(n)}$ são chamadas de **n-ésimas raízes da unidade** sobre $\mathbb{K}$ e o conjunto de todas essas raízes é denotado por $E^{(n)}$.

Definição 1.43. Seja $\mathbb{K}$ um corpo de característica p e n um inteiro positivo não divisível por p. Então um gerador do grupo cíclico $E^{(n)}$ é chamado de **n-ésima raiz primitiva da unidade** sobre $\mathbb{K}$.

Veremos mais na frente (Teorema 2.9) que as raízes do polinômio $x^n - 1$ são primitivas em uma determinada extensão de corpo finito. Como esse fato apresenta-se a seguinte definição.

Definição 1.44. Sejam $\mathbb{K}$ um corpo de caracteríStca p, n um inteiro positivo não divisível por p, e ζ uma n-ésima raiz primitiva da unidade sobre $\mathbb{K}$. Então o polinômio

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

é chamado de **n-ésimo polinômio ciclotômico** sobre $\mathbb{K}$.

O polinômio $Q_n(x)$ é claramente independente da escolha de ζ. O grau de $Q_n(x)$ é $\phi(n)$ e seus coeficientes pertencem ao n-ésimo corpo ciclotômico sobre $\mathbb{K}$.

Teorema 1.45. *[14, Theorem 2.45] Sejam $\mathbb{K}$ um corpo de característica p e n um inteiro positivo não divisível por p. Então:*

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

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

Proposição 1.46. *[12, Proposition 8.2] Sejam $n \in \mathbb{N}$, K um corpo de característica p, tal que p não divide n e $Q_n(x)$ é o n-ésimo polinômio ciclotômico sobre K. Então*

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

Proposição 1.47. *[12, Proposition 8.3] Seja F uma extensão ciclotômica de ordem n do corpo $\mathbb{Q}$ de números racionais e $Q_n(x)$ o n-ésimo polinômio ciclotômico sobre $\mathbb{Q}$. Então $Q_n(x)$ é irredutível em $\mathbb{Q}[x]$.*

Capítulo 2

Elementos k-normais

Neste capítulo apresentam-se as noções de elemento normal, elemento k-normal e como se relacionam estas definições. A importância de estudar os elementos normais em uma determinada extensão de corpos finitos, é essencialmente porque estes elementos geram bases normais (só os 0-normais) que são amplamente utilizadas em aplicações tais como a criptografia e o processamento de sinais devido à eficiência da exponenciação. Além disso, exibe-se um dos quatro teoremas fundamentais deste trabalho onde caracterizam-se os elementos k-normais dado inicialmente em [11, Theorem 2.5] pelos autores S. Huczynska, G. Mullen, D. Panario, D Thomson veja Teorema 2.11.

É importante ressaltar que a noção de elemento k-normal é uma generalização de elemento normal. Uma motivação para estudar estes elementos é que eles surgiram implicitamente durante o processo de construção de bases quase-normais de corpos finitos. Estas bases são uma classe de $\mathbb{F}_q$-bases de $\mathbb{F}_{q^n}$ que oferecem multiplicação eficiente em $\mathbb{F}_{q^n}$.

Este capítulo está dividido em três seções: na primeira define-se a resultante e exibem-se resultados importantes desta noção, a segunda e terceira seção apresentam-se a definição e caracterização de elemento normal e k-normal, respectivamente.

2.1 A resultante

Nesta seção apresentam-se a definição da resultante de dois polinômios quaisquer f e g e exibem-se alguns resultados importantes para o desenvolvimento deste capítulo. Com exceção do Lema 2.6 todos os lemas desta seção foram tomados de [17]. A noção de resultante é importante porque permite estabelecer, quando dois polinômios f e g com coeficientes em um corpo têm raízes em comum, ou seja permite saber se existe um polinômio h tal que $h \mid g$ e $h \mid f$. Esta definição e os resultados apresentados nesta seção são fundamentais para definir e caracterizar os elementos normais e k-normais apresentados no decorrer deste capítulo.

Com essa motivação, sejam $\mathbb{F}$ um corpo e $f,\ g \in \mathbb{F}[x]$. O seguinte lema diz que o anulamento da combinação linear $(-s)f + tg = 0$ pode ser dado por polinômios s e t de graus menores que os de g e f respectivamente se e somente se $\mathrm{mdc}(f, g) \neq 1$.

Lema 2.1. *Sejam $f, g \in \mathbb{F}[x]$ distintos de zero. Então $\mathrm{mdc}(f, g) \neq 1$ se e somente se existem $s, t \in \mathbb{F}[x] \setminus \{0\}$ tais que $sf + tg = 0$, com $\mathrm{grau}(s) < \mathrm{grau}(g)$, e $\mathrm{grau}(t) < \mathrm{grau}(f)$.*

Demonstração. $\Rightarrow$ Seja $h = \mathrm{mdc}(f, g)$, se $h \neq 1$ então $\mathrm{grau}(h) \geq 1$. Considere,

$$s = -\frac{g}{h} \text{ e } t = \frac{f}{h} \in \mathbb{F}[x] \setminus \{0\},$$

assim, tem-se que s e t satisfazem a igualdade $sf + tg = 0$, e $\mathrm{grau}(s) < \mathrm{grau}(g)$, $\mathrm{grau}(t) < \mathrm{grau}(f)$.

$\Leftarrow$ Sejam $s, t \in \mathbb{F}[x] \setminus \{0\}$ tais que $sf + tg = 0$, com grau$(s) <$ grau(g) e grau$(t) <$ grau(f). Então $sf = -tg$, assim se f e g foram coprimos, implica que $f \mid t$ o qual é impossível pois $t \neq 0$ e grau$(t) <$ grau(f), portanto, mdc$(f, g) \neq 1$. □

Agora reformulando o Lema 2.1 em uma linguagem diferente, para isso, sejam $f, g \in \mathbb{F}[x]$ de graus n e m, respectivamente. Considere a seguinte "aplicação linear"

$$\begin{aligned} \varphi = \varphi_{f,g} := \mathbb{F}[x] \times \mathbb{F}[x] &\to \mathbb{F}[x] \\ (s, t) &\mapsto sf + tg. \end{aligned}$$

Para $d \in \mathbb{N}$, considere

$$P_d = \{a \in \mathbb{F}[x] : \text{grau}(a) < d\},$$

com a condição de que $P_0 = \{0\}$. φ é uma aplicação linear entre espaços vetoriais de dimensão infinita. A restrição de φ a $\varphi_0 : P_m \times P_n \to P_{m+n}$ é uma $\mathbb{F}$ aplicação linear entre espaços da mesma dimensão.

Sejam $\mathcal{B} = \{(x^i, 0)$ para $i < m$ e $(0, x^j)$ para $j < n\}$ uma base para $P_m \times P_n$ e $\mathcal{Y} = \{x^{n+m-1}, \ldots, x^2, x, 1\}$ uma base para P_{m+n}. Como φ_0 é uma aplicação linear, φ_0 pode ser representada por uma matriz nas bases $\mathcal{B}$ e $\mathcal{Y}$. Esta matriz é chamada de matiz de Sylvester e é definida a seguir.

Definição 2.2. Seja $\mathbb{F}$ um corpo e sejam $f, g \in \mathbb{F}[x]$ com

$$f(x) = \sum_{0 \leq j \leq n} f_j x^j \text{ e } g(x) = \sum_{0 \leq j \leq m} g_j x^j$$

com todos os $f_j, g_j \in \mathbb{F}$. A **matriz de Silvester** $S_{f,g}$ é a matriz $(m+n) \times (m+n)$ dada por

$$\left.\begin{pmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_n & \cdots & \cdots & \cdots & f_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & f_n & \cdots & \cdots & \cdots & \cdots & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & g_m & \cdots & \cdots & \cdots & \cdots & g_0 \end{pmatrix}\right\} \begin{matrix} m \text{ linhas} \\ \\ \\ \\ \\ n \text{ linhas} \end{matrix}$$

O determinante da matriz de Sylvester $S_{f,g}$ é a resultante, $R(f, g)$, dos polinômios f e g.

Definição 2.3. Sejam $f(x) = \sum_{0 \leq j \leq n} f_j x^j$ e $g(x) = \sum_{0 \leq j \leq m} g_j x^j \in \mathbb{F}[x]$ dois polinômios de grau n e m respetivamente, com $n, m \in \mathbb{N}$. Então a **resultante** $R(f, g)$ dos dois polinômios é definida pelo determinante $R(f, g) = \det(S_{f,g})$, isto é

$$R(f,g) = \left.\begin{vmatrix} f_n & f_{n-1} & \cdots & f_1 & & 0 & \cdots & 0 & 0 \\ 0 & f_n & \cdots & \cdots & & f_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & f_n & \cdots & & \cdots & \cdots & \cdots & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & \cdots & \cdots & 0 & \\ 0 & g_m & g_{m-1} & \cdots & \cdots & g_0 & \cdots & & \\ \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & g_m & \cdots & & \cdots & \cdots & \cdots & g_0 \end{vmatrix}\right\} \begin{matrix} m \text{ linhas} \\ \\ \\ \\ \\ n \text{ linhas} \end{matrix}$$

A resultante de dois polinômios f e g serve para determinar se f e g têm raízes em comum. Esta afirmação é uma consequência do Lema 2.1 e apresenta-se formalmente como segue.

Lema 2.4. *Sejam $f, g \in \mathbb{F}[x]$ distintos de zero, então* $\text{mdc}(g, f) = 1$ *se, e somente se* $R(f, g) \neq 0$.

Demonstração. $\Rightarrow$ Se o $\text{grau}(\text{mdc}(f, g)) \geq 1$, pelo Lema 2.1, existem polinômios não nulos, $s \in P_m = \{a \in \mathbb{F}[x] : \text{grau}(a) < m\}$ e $t \in P_n = \{a \in \mathbb{F}[x] : \text{grau}(a) < n\}$ tal que $\varphi(s, t) = sf + gt = 0$. Logo $\ker(\varphi) \neq \{0\}$. Portanto, φ_0 não é injetivo, consequentemente φ_0 não é um isomorfismo, isto é $S_{f,g}$ não é invertível. Portanto, $R(f, g) = 0$.

$\Leftarrow$ Suponha que $R(f, g) = 0$, então $S_{f,g}$ não é invertível, logo φ_0 não é um isomorfismo, como $P_m \times P_n$ e P_{m+n} são espaços vetoriais da mesma dimensão, segue que φ_0 não é injetivo, então existe pelo menos um par (s, t), com $s, t \in \mathbb{F}[x] \setminus \{0\}$ tal que $\varphi(s, t) = 0$, isto é $sf + gt = 0$ e pelo Lema 2.1 conclui-se que $\text{mdc}(f, g) \neq 1$. □

A seguir exibe-se uma generalização do Lema 2.1 que é fundamental para caracterizar os elementos k-normais mais na frente.

Lema 2.5. *[17, Exercise 6.16] Sejam $f, g \in \mathbb{F}[x]$ polinômios distintos de zero de graus n e m respectivamente, e $h = \text{mdc}(f, g) \in \mathbb{F}[x]$ de grau d. Então* $\dim(\ker(S_{f,g})) = \text{grau}(h)$.

Demonstração. Para o desenvolvimento da demostração do lema vamos seguir o seguinte roteiro:

i. Inicialmenente vamos mostrar que existe um par $(s, t) \in P_{m-i} \times P_{n-i}$ distinto de zero com $\varphi_0 = (s, t) = 0$, se e somente se $i < d$.

ii. Depois vamos demonstrar que dados d pares $(s_1, t_1), \ldots, (s_d, t_d) \in P_m \times P_n$ tais que $\varphi_0(s_i, t_i) = 0$ com s_i um polinômio mônico de grau $m - i$ para todo i.

iii. A seguir vamos supor que $(s, t) \in P_m \times P_n$ é linearmente independente para todo par do item ii. e $\varphi_0(s, t) = 0$, e provaremos posteriormente que existe um par $(s^*, t^*) \in P_{m-d-1} \times P_{n-d-1}$ distinto de zero com $\varphi_0(s^*, t^*) = 0$, contradizendo o item i.

iv. Finalmente concluiremos que $dim(\ker(S_{f,g})) = \text{grau}(\text{mdc}(f, g))$.

Desta maneira pela hipótese se $h = \text{mdc}(f, g) \in \mathbb{F}[x]$ com $\text{grau}(h) = d$, então existem $f_1, g_1 \in \mathbb{F}[x]$ tais que $f = f_1 h$ e $g = g_1 h$ com $\text{grau}(g_1) = n - d$ e $\text{grau}(g_1) = m - d$.

i. $\Rightarrow$ Suponha que existe $(s, t) \in P_{m-i} \times P_{n-i}$ tal que $sf + tg = 0$, logo

$$sf_1 h + tg_1 h = (sf_1 + tg_1)h = 0,$$

como $h \neq 0$ segue-se que,

$$sf_1 + tg_1 = 0. \tag{2.1}$$

Além disso,

$$\begin{aligned} h &= \text{mdc}(f, g) \\ &= \text{mdc}(f_1 h, g_1 h) \\ &= h(\text{mdc}(f_1, g_1)), \end{aligned}$$

assim

$$\text{mdc}(f_1, g_1) = 1. \tag{2.2}$$

Da equação (2.1) obtém-se que $sf_1 = -tg_1$, então $f_1 \mid -tg_1$ e por a equação (2.2) obtém-se que $f_1 \mid t$, portanto

$$n - d = \text{grau}(f_1) \leq \text{grau}(t) < n - i, \tag{2.3}$$

pela equação (2.3) segue-se que $i < d$.

$\Leftarrow$ Como $h = \frac{g}{g_1}$ e $h = \frac{f}{f_1}$, então $\frac{g}{g_1} = \frac{f}{f_1}$, isto é $f_1 g = g_1 f$, o que implica $f_1 g + (-g_1) f = 0$. Assim, se $t = f_1$ e $s = -g_1$ tem-se que $tg + sf = 0$, consequentemente, $\varphi_0(s,t) = 0$, como

$$\begin{aligned} \text{grau}(s) &= m - d \\ &< m - i, \text{ já que } i < d, \end{aligned}$$

e

$$\begin{aligned} \text{grau}(t) &= n - d \\ &< n - i, \text{ já que } i < d, \end{aligned}$$

logo, $t \in P_{n-i}$ e $s \in P_{m-i}$, portanto $(s,t) \in P_{m-i} \times P_{n-i}$.

ii. Seja $s_d = -g_1$ e $t_d = f_1$, considere $s_{d-1} = -g_1(x+b)$ e $t_{d-1} = f_1(x+b)$, logo s_{d-1} e t_{d-1} têm graus $m-d+1$ e $n-d+1$, respectivamente. Seja $s_{d-2} = s_{d-1}(x+b)$ e $t_{d-2} = t_{d-1}(x+b)$, consequentemente s_{d-2} e t_{d-2} têm graus $m-d+2$ e $n-d+2$, respectivamente. Desse modo, tem-se que $s_1 = s_2(x+b)$ e $t_1 = t_2(x+b)$ com $\text{grau}(s_1) = m-1$ e $\text{grau}(t_1) = n-1$. Para cada $i \in \{1, \ldots, d\}$ segue-se que s_i tem grau $m-i$, e é da forma

$$s_i = h_{m-i}x^{m-i} + \cdots + h_0 \tag{2.4}$$

com $h_j \in \mathbb{F}$, para todo $j = 1, \ldots, m-i$, e $h_{m-i} \neq 0$, então dividindo a equação (2.4) por h_{m-i} tem-se

$$\bar{s_i} = x^{m-i} + \cdots + \left(\frac{h_0}{h_{m-i}}\right)$$

é um polinômio mônico.

Por outro lado t_i é da forma $t_i = k_{n-i}x^{n-i} + \cdots + k_0$, com $k_j \in \mathbb{F}$ para todo $j = 1, \ldots, n-i$. Considere $\bar{t_i} = \frac{t_i}{h_{m-i}}$. Será demonstrado que para todo $i \in \{1, \ldots, d\}$, $\varphi_0(\bar{s_i}, \bar{t_i}) = 0$. Como

$$\begin{aligned} \varphi_0(\bar{s_i}, \bar{t_i}) &= \varphi_0\left(\frac{1}{h_{m-i}}s_i, \frac{1}{h_{m-i}}t_i\right) \\ &= \frac{1}{h_{m-i}}(s_i f + t_i g) \\ &= \frac{1}{h_{m-i}}\left(s_d(x+b)^{d-i}f + t_d(x+b)^{d-i}g\right) \\ &= \frac{(x+b)^{d-i}}{h_{m-i}}(s_d f + t_d g) \\ &= \frac{(x+b)^{d-i}}{h_{m-i}}\underbrace{(-g_1 f + f_1 g)}_{=0} \\ &= 0. \end{aligned}$$

Por último, será demonstrado que $\{(\bar{s_1}, \bar{t_1}), \ldots, (\bar{s_d}, \bar{t_d})\}$ são linearmente independentes.

Sejam $\alpha_1, \ldots, \alpha_d \in F$ tais que $\alpha_1(\bar{s_1}, \bar{t_1}) + \cdots + \alpha_d(\bar{s_d}, \bar{t_d}) = 0$, então

$$\begin{aligned} \alpha_1\bar{s_1} + \cdots + \alpha_d\bar{s_d} &= 0, \\ \alpha_1\bar{t_1} + \cdots + \alpha_d\bar{t_d} &= 0, \end{aligned}$$

como $\bar{s_i}$ e $\bar{t_i}$ têm grau maior que 0 para $1 \leq i \leq d$, então a solução do sistema é

$$\alpha_1 = \alpha_2 = \cdots = \alpha_d = 0.$$

iii. Seja $(s,t) \in P_m \times P_n$ tal que $\varphi_0(s,t) = 0$, isto é $(s,t) \in \ker(\varphi_0)$. Como $(s,t) \in P_m \times P_n$ e $(\bar{s_1}, \bar{t_1}) \in P_m \times P_n$, então existem $a_1, b_1 \in \mathbb{F}$ tais que

$$\begin{aligned} s - a_1\bar{s_1} &\in P_{m-1}, \\ t - b_1\bar{t_1} &\in P_{n-1} \end{aligned}$$

e

$$\varphi_0(s - a_1\bar{s_1}, t - b_1\bar{t_1}) = \varphi(s,t) - (a_1, b_1)\varphi_0(\bar{s_1}, \bar{t_1}) = 0.$$

Existem também $a_2, b_2 \in \mathbb{F}$ tais que

$$\begin{aligned} s - a_1\bar{s_1} - a_2\bar{s_2} &\in P_{m-2}, \\ t - b_1\bar{t_1} - b_2\bar{t_2} &\in P_{n-2} \end{aligned}$$

e $\varphi_0(s - a_1\bar{s_1} - a_2\bar{s_2}, t - b_1\bar{t_1} - b_2\bar{t_2}) = 0$.

Por conseguinte tem-se que existem a_d, b_d tais que

$$\begin{aligned} \hat{s} = s - a_1\bar{s_1} - \cdots - a_d\bar{s_d} &\in P_{m-d}, \\ \hat{t} = t - b_1\bar{t_1} - \cdots - b_d\bar{t_d} &\in P_{n-d} \end{aligned}$$

e $\varphi_0(\hat{s}, \hat{t}) = 0$. Pelo item i. tem-se que $\hat{s} = 0$ e $\hat{t} = 0$, já que $d > i$.

Por outro lado como $\bar{s_i}$ é mônico para todo i, e pelo item ii. sabe-se que $\bar{s_i}f + \bar{t_i}g = 0$, então, se

$$\begin{aligned} f = f_n x^n + \cdots + f_0, \quad & g = g_m x^m + \cdots + g_0, \\ \bar{t_i} = t_{n-i}x^{n-i} + \cdots + t_{0i} \quad & \text{e } \bar{s_i} = x^{m-i} + s_{m-i-1}x^{m-i-1} + \cdots + s_{0i}, \end{aligned}$$

segue-se que

$$f_n + t_{n-i}g_m = 0, \tag{2.5}$$

pela equação (2.5) obtém-se que

$$t_{n-i} = -\frac{f_n}{g_m}. \tag{2.6}$$

Seja $(s,t) \in P_m \times P_n$ tal que $\varphi_0(s,t) = 0$ com

$$\begin{aligned} s &= a_{m-1}x^{m-1} + \cdots + a_0, \\ t &= b_{n-1}x^{n-1} + \cdots + b_0. \end{aligned}$$

Como $sf + tg = 0$, então

$$(a_{m-1}f_n x^{n+m-1} + \cdots + f_0 a_0) + (b_{n-1}g_m x^{n+m-1} + \cdots + b_0 g_0) = 0,$$

assim

$$a_{m-1}f_n + b_{n-1}g_m = 0. \tag{2.7}$$

Já que $s - a_{m-1}\bar{s_1} \in P_{m-1}$, das equações (2.6) e (2.7) obtém-se $t - a_{m-1}\bar{t_1} \in P_{n-1}$. De fato

$$\begin{aligned} b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0 - a_{m-1}(t_{n-1}x^{n-1} + t_{n-2}x^{n-2} + \cdots + t_{0_1}) = \\ (b_{n-1} - a_{m-1}t_{n-1})x^{n-1} + (b_{n-2} - a_{m-1}t_{n-2}x^{n-2}) + \cdots + (b_0 - a_{m-1}t_{0_1}) \end{aligned}$$

e

$$\begin{aligned} b_{n-1} - a_{m-1}t_{n-1} &= b_{n-1} - a_{m-1}\frac{f_n}{g_m} \\ &= \frac{\overbrace{g_m b_{n-1} - a_{m-1}f_n}^{=0}}{g_m} \\ &= 0. \end{aligned}$$

Desse modo pode-se concluir que

$$s^* = s - a_{m-1}\bar{s_1} - a_{m-2}\bar{s_2} - \cdots - a_{m-d}\bar{s_d} \in P_{m-d}, \tag{2.8}$$

$$t^* = t - a_{m-1}\bar{t_1} - a_{m-2}\bar{t_2} - \cdots - a_{m-d}\bar{t_d} \in P_{n-d} \tag{2.9}$$

e $\varphi(s^*, t^*) = 0$. Novamente pelo item i. segue-se que $s^* = 0 = t^*$ já que $i < d$. Portanto das equações (2.8) e (2.9) obtém-se

$$\begin{aligned} s &= a_{m-1}\bar{s_1} + a_{m-2}\bar{s_2} + \cdots + a_{m-d}\bar{s_d}, \\ t &= a_{m-1}\bar{t_1} + a_{m-2}\bar{t_2} + \cdots + a_{m-d}\bar{t_d}, \end{aligned}$$

isto é, $(s,t) = a_{m-1}(\bar{s_1}, \bar{t_1}) + \cdots + a_{m-d}(\bar{s_d}, \bar{t_d})$, consequentemente (s,t) é linearmente dependente dos elementos $(\bar{s_1}, \bar{t_1}), \ldots, (\bar{s_d}, \bar{t_d})$.

iv. De iii. tem-se que uma base para $\ker(\varphi_0)$ é $\{(\bar{s_1}, \bar{t_1}), \ldots, (\bar{s_d}, \bar{t_d})\}$, então

$$\begin{aligned} \dim(\ker(\varphi_0)) &= d \\ &= \text{grau}(\text{mdc}(g, f)), \end{aligned}$$

portanto

$$\begin{aligned} \ker(S_{f,g})) &= d \\ &= \text{grau}(\text{mdc}(g, f)). \end{aligned}$$

□

Uma consequência do lema anterior é a seguinte, dada em [11, Lemma 2.4]

Lema 2.6. *Seja $\mathbb{F}$ um corpo. Para dois polinômios diferentes de zero $f, g \in \mathbb{F}[x]$,*

$$rang(S_{f,g}) = \text{grau}(f) + \text{grau}(g) - \text{grau}(\text{mdc}(f, g)).$$

Demonstração. Seja

$$\begin{aligned} \varphi_0 := P_m \times P_n &\to P_{m+n} \\ (s,t) &\mapsto sf+tg \end{aligned}$$

uma aplicação linear, com P_m e P_n definidos como antes. A matriz associada à aplicação linear φ_0 é matriz de Sylvester dada por

$$S_{f,g} = \begin{pmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & \cdots & \cdots \\ 0 & f_n & \cdots & \cdots & \cdots & f_0 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 0 & \cdots & f_n & \cdots & \cdots & \cdots & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & \cdots & \cdots \\ 0 & g_m & g_{m-1} & \cdots & \cdots & g_0 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 0 & \cdots & g_m & \cdots & \cdots & \cdots & g_0 \end{pmatrix}.$$

Pelo teorema do núcleo e da imagem tem-se que

$$\begin{aligned} \dim(Im(\varphi_0)) + \dim(\ker(\varphi_0)) &= m+n, \\ posto(S_{f,g}) + \dim(\ker(S_{f,g})) &= m+n. \end{aligned}$$

Assim

$$\begin{aligned} posto(S_{f,g}) &= m+n-\dim(\ker(S_{f,g})) \\ &\underbrace{=}_{Lema\ 2.5} m+n-\text{grau}(\text{mdc}(f,g)) \\ &= \text{grau}(g)+\text{grau}(f)-\text{grau}(\text{mdc}(f,g)). \end{aligned}$$

Portanto $posto(S_{f,g}) = \text{grau}(g)+\text{grau}(f)-\text{grau}(\text{mdc}(f,g))$. □

2.2 Elementos normais

Nesta seção apresentam-se a noção de elemento normal e exibem-se um resultado que caracteriza os elementos normais dado pelos autores R. Lidl e H. Niederreiter em [14, Theorem 2.39] e um resultado que garante a existência de elementos normais primitivos dado em [13] pelos autores H. Lenstra e R. Schoof.

A seguir apresentam-se uma das definições mais importantes deste trabalho.

Definição 2.7. Seja q uma potência de um primo e $n \in \mathbb{N}$. Um elemento $\alpha \in \mathbb{F}_{q^n}$ é chamado de **elemento normal** sobre $\mathbb{F}_q$, se o conjunto $B = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ é uma base para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ (veja Definição 1.21). Neste caso tal tipo de base é chamada de base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Um critério bem conhecido para verificar se um elemento gera uma base normal é dado pelo seguinte teorema dado em [14, Theorem 2.39].

Teorema 2.8. *Para $\alpha \in \mathbb{F}_{q^n}$, $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ é uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, se e somente se os polinômios x^n-1 e $\alpha x^{n-1}+\alpha^q x^{n-2}+\cdots+\alpha^{q^{n-2}}x+\alpha^{q^{n-1}}$ em $\mathbb{F}_{q^n}[x]$ são primos relativos, isto é, o grau do máximo comum divisor em $\mathbb{F}_{q^n}[x]$ é 0.*

Demonstração. Seja $\alpha_1 = \alpha$, $\alpha_2 = \alpha^q$, $\ldots$, $\alpha_m = \alpha^{q^{n-1}}$. Usando o fato que $\alpha^{q^n} = \alpha$ segue que o determinante exposto no Corolário 1.24 é

$$\begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \\ \alpha^{q^2} & \alpha^{q^3} & \alpha^{q^4} & \ldots & \alpha^q \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{n-2}} \end{vmatrix}. \tag{2.10}$$

O determinante (2.10) é igual ao seguinte determinante

$$D = \pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{n-2}} \\ \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \alpha & \ldots & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \end{vmatrix}, \tag{2.11}$$

obtido depois de trocar no determinante (2.10) a linha 2 com linha n, a linha 3 com linha $n-1$, a linha 4 com a linha $n-2$, e assim por diante. Considere a resultante $R(f,g)$ dos polinômios $f(x) = x^n - 1$ e $g = g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ de graus n e $n-1$, respectivamente. Esta resultante é um determinante de uma matriz de ordem $2n-1$ dado a seguir

$$R(f,g) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 & 0 & -1 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & 0 & \ldots & 0 \\ 0 & \alpha & \alpha^q & \ldots & \alpha^{q^{n-3}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & \alpha & \alpha^q & \alpha^{q^2} & \ldots & 0 \end{vmatrix}. \tag{2.12}$$

O determinante (2.12) é igual ao determinante da matriz que é formada depois de somar a $(n+1)$-ésima coluna com a coluna 1 para obter a coluna 1; somar a $(n+2)$-ésima coluna com a coluna 2 para obter a coluna 2, e assim por diante até somar a coluna $2n-1$ com a coluna $n+1$ para obter a coluna $n+1$. Isto é, o determinante (2.12) é igual ao seguinte determiante

$$R(f,g) = \begin{vmatrix} 0 & 0 & 0 & \ldots & 0 & -1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{n-1}} & 0 & 0 & 0 & \ldots & 0 \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha & \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & 0 \end{vmatrix}.$$

Assim, a resultante é o produto do determinante de uma matriz $(n-1) \times (n-1)$ com -1 na diagonal principal com o determinante de (2.10). Portanto, $R(f,g)$ é igual ao determinante de (2.10) a exceção do sinal.

Logo, f e g têm raízes em comum (ou seja, são primos relativos), se e somente se $R(f,g) \neq 0$, se e somente se $\det(D) \neq 0$, se e somente se $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ é base normal, isto é α é normal. □

Na literatura é conhecido que todo corpo finito possui uma base normal gerada por elementos primitivos, este resultado foi provado por H. Lenstra e R. Schoof em [13]. Além disso, este resultado é de grande importância para a pesquisa atual, já que um dos maiores desafios, é mostrar a existência de elementos k-normais primitivos. Essencialmente os autores já mencionados mostraram o seguinte resultado.

Teorema 2.9. *[13, Theorem] Para qualquer corpo finito $\mathbb{F}$ existe uma base normal de $\mathbb{F}$ sobre seu subcorpo primo que consiste em elementos primitivos de $\mathbb{F}$.*

2.3 Elementos k-normais

Nesta seção apresenta-se a definição mais importante deste trabalho: a noção de elemento k-normal dada inicialmente em [11, Definition 2.2] que como foi mencionado anteriormente generalizando a noção de elemento normal. Além disso, exibe-se a caracterização para os elementos k-normais dada também em [11, Theorem 2.5].

Com esta motivação, apresenta-se formalmente a definição de elemento k-normal.

Definição 2.10. [11, Definition 2.2] Seja $\alpha \in \mathbb{F}_{q^n}$. Denotemos por $g_\alpha(x)$ o polinômio $\sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i} \in \mathbb{F}_{q^n}[x]$. Se $\mathrm{mdc}(x^n-1, g_\alpha(x))$ sobre $\mathbb{F}_{q^n}$ tem grau k (onde $0 \leq k \leq n-1$), então α é chamado de **elemento k-normal** de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Usando esta terminologia, um elemento normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é 0-normal.

Será introduzida a primeira caracterização dos elementos k-normais.

Teorema 2.11. *[11, Theorem 2.5] Sejam $\alpha \in \mathbb{F}_{q^n}$ e*

$$A_\alpha = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-1}} \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \dots & \alpha^{q^{n-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha \end{pmatrix}. \tag{2.13}$$

O elemento α é k-normal sobre $\mathbb{F}_q$ se e somente se posto$(A_\alpha) = n-k$.

Demonstração. Será demonstrado que $\mathrm{mdc}(x^n-1, g_\alpha(x))$ tem grau k, se e somente se a matriz A_α tem posto $n-k$. A matriz de Sylvester S_{f,g_α} com $f(x) = x^n - 1$ e

$$g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$$

é dada por

$$S_{f,g_\alpha} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & -1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 & -1 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & -1 \\ \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & 0 & \dots & 0 \\ 0 & \alpha & \alpha^q & \dots & \alpha^{q^{n-3}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & 0 & \dots & 0 \\ 0 & 0 & \alpha & \dots & \alpha^{q^{n-4}} & \alpha^{q^{n-3}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \alpha & \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha^{q^{n-1}} \end{pmatrix},$$

trocando a coluna n pela coluna $n+1$, depois trocando a coluna $n+1$ pela coluna $n+2$ e assim por diante, até trocar a coluna $2n-2$ pela coluna $2n-1$, obtém-se,

$$S^*_{f,g_\alpha} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & -1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & -1 & 0 \\ \alpha & \alpha^q & \alpha^{q^2} & \dots & \alpha^{q^{n-2}} & 0 & 0 & \dots & 0 & \alpha^{q^{n-1}} \\ 0 & \alpha & \alpha^q & \dots & \alpha^{q^{n-3}} & \alpha^{q^{n-1}} & 0 & \dots & 0 & \alpha^{q^{n-2}} \\ 0 & 0 & \alpha & \dots & \alpha^{q^{n-4}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \dots & 0 & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \alpha & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha^{q^{n-1}} & \alpha^q \end{pmatrix}.$$

Logo, adicionando a coluna 1 à coluna n, adicionando a coluna 2 à coluna $n+1$ e assim por diante, até adicionar a coluna $n-1$ à coluna $2n-1$. Para obter a matriz

$$S^{**}_{f,g_\alpha} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ \alpha & \alpha^q & \dots & \alpha^{q^{n-2}} & \alpha & \alpha^q & \dots & \alpha^{q^{n-1}} \\ 0 & \alpha & \dots & \alpha^{q^{n-3}} & \alpha^{q^{n-1}} & \alpha & \dots & \alpha^{q^{n-2}} \\ 0 & 0 & \dots & \alpha^{q^{n-4}} & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \dots & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \alpha & \alpha^{q^2} & \alpha^{q^3} & \dots & \alpha^q \end{pmatrix},$$

finalmente escalona-se as primeiras $n-1$ colunas da matriz S^{**}_{f,g_α}. Para obter a seguinte matriz

$$S^{***}_{f,g_\alpha} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & \alpha & \alpha^q & \dots & \alpha^{q^{n-1}} \\ 0 & 0 & 0 & \dots & 0 & \alpha^{q^{n-1}} & \alpha & \dots & \alpha^{q^{n-2}} \\ 0 & 0 & 0 & \dots & 0 & \alpha^{q^{n-2}} & \alpha^{q^{n-1}} & \dots & \alpha^{q^{n-3}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \dots & 0 & \alpha^q & \alpha^{q^2} & \dots & \alpha \end{pmatrix},$$

ou seja obtém-se a matriz

$$S^{***}_{f,g_\alpha} = \begin{pmatrix} I_{n-1,n-1} & O_{n-1,n} \\ O_{n,n-1} & A_\alpha \end{pmatrix},$$

onde $I_{n-1,n-1}$ é a matriz identidade de tamanho $n-1 \times n-1$, e as matrizes $O_{n-1,n}$ e $O_{n,n-1}$ são matrizes nulas. Assim, tem-se que

$$posto(S_{f,g_\alpha}) = posto(S^{***}_{f,g_\alpha}) = \quad posto(I_{n-1,n-1}) + posto(A_\alpha) = n-1+posto(A_\alpha). \quad (2.14)$$

Pelo Lema 2.6 tem-se que

$$posto(S_{f,g_\alpha}) = n + (n-1) - \text{grau}(\text{mdc}(f, g_\alpha)), \tag{2.15}$$

logo das Equações (2.14) e (2.15), tem-se

$$n + (n-1) - \text{grau}(\text{mdc}(f, g_\alpha)) = n - 1 + posto(A_\alpha),$$

portanto, $\text{grau}(\text{mdc}(f, g_\alpha)) = n - posto(A_\alpha)$, assim se $\text{grau}(\text{mdc}(f, g_\alpha)) = k$, então

$$posto(A_\alpha) = n - k.$$

□

Foi demonstrado que se f e g têm um polinômio divisor em comum de grau k, se e somente se $posto(A_\alpha) = n - k$, se e somente se α é um elemento k- normal. Uma consequência do lema anterior é a seguinte.

Corolário 2.12. *[11, Corollary 2.6] Seja $\alpha \in \mathbb{F}_{q^n}$. Se α é k-normal sobre $\mathbb{F}_q$, então qualquer conjugado de α é k-normal sobre $\mathbb{F}_q$.*

Demonstração. Seja α^{q^i} um conjugado de α para algum $i = 1, \ldots, n-1$, então a matriz $A_{\alpha^{q^i}}$ é

$$A_{\alpha^{q^i}} = \begin{pmatrix} \alpha^{q^i} & \alpha^{q^{i+1}} & \ldots & \alpha^{q^{i+n-1}} \\ \alpha^{q^{i+n-1}} & \alpha^{q^i} & \ldots & \alpha^{q^{i+n-2}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{q^{i+1}} & \alpha^{q^{i+2}} & \ldots & \alpha^{q^i} \end{pmatrix},$$

trocando as linhas ou as colunas de $A_{\alpha^{q^i}}$ necessárias, tem-se que a matriz resultante é igual à matriz A_α, assim $posto(A_{\alpha^{q^i}}) = posto(A_\alpha) = n - k$. Portanto, o $\text{grau}(\text{mdc}(f, g_{\alpha^{q^i}})) = k$, logo α^{q^i} é um elemento k-normal, (Definição 2.10). Como i foi arbitrário segue-se que qualquer conjugado de α é k-normal. □

Capítulo 3

Número de elementos k-normais

Neste capítulo apresenta-se o segundo objetivo deste trabalho, especificamente exibem-se dois resultados que mostram expresões que permitem calcular o número de elementos normais e k-normais em um corpo dado. Estes resultados foram tomados de [14, Theorem 3.73] e [11, Theorem 3.5], respectivamente. As equações que envolvem estes teoremas estão em termos da função Φ de Euler para polinômios, cuja definição e consequências foram apresentadas no Capítulo 1.

Com essa motivação apresenta-se o seguinte resultado dado em [14, Theorem 3.73] que exibe a quantidade de elementos normais em um corpo $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Teorema 3.1. *Em $\mathbb{F}_{q^n}$ existem exatamente $\Phi_q(x^n-1)$ elementos α tais que $\{\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, onde Φ_q é a função Φ de Euler para polinômios definida no Capítulo 1.*

Demonstração. Como $\mathbb{F}_{q^n}$ pode ser visto como um q-módulo, então pelo Lema 1.8 e o Teorema 1.32 tem-se que

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^n}} (x - \beta) = x^{q^n} - x,$$

é um q-polinômio.

Pelo Teorema 1.41 toda q-raiz primitiva ζ de $L(x)$ sobre $\mathbb{F}_q$ gera uma base do tipo $\{\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}\}$. Por outro lado, se $\zeta \in \mathbb{F}_{q^n}$ não é uma q-raiz primitiva de $L(x)$ sobre $\mathbb{F}_q$, então existe $\bar{L}(x)$ q-polinômio tal que $q^s = \text{grau}(\bar{L}(x)) < \text{grau}(L(x))$ e ζ sendo raiz de $\bar{L}(x)$, isto é $\bar{L}(\zeta) = 0$ determina uma combinação linear não nula de $\zeta, \zeta^q, \ldots, \zeta^{q^s}$. Como $s + 1 \leq n$, segue que $\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}$ são linearmente dependentes sobre $\mathbb{F}_q$, e portanto, eles não formam uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Consequentemente, o número de $\zeta \in \mathbb{F}_{q^n}$ tal que $\{\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}\}$ seja base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é igual ao número das q-raízes primitivas de $L(x)$ sobre $\mathbb{F}_q$, o qual é exatamente $\Phi(x^n - 1)$ pelo Teorema 1.40. □

Uma consequência do Teorema 2.11 e do Teorema 3.1 é a seguinte:

Lema 3.2. *Seja $\alpha \in \mathbb{F}_{q^n}$ e seja A_α a matriz dada no Teorema 2.11. Denote por M o espaço vetorial gerado pelo conjunto $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ sobre $\mathbb{F}_{q^n}$. Então posto$(A_\alpha) = \dim(M)$.*

Demonstração. O espaço coluna da matriz A_α é dado por $Span\{c_0, c_1, \ldots, c_{n-1}\}$ onde cada coluna c_i está formada pelo vetor transposto $\left[\alpha^{q^i}, (\alpha^{q^i})^{q^{n-1}}, (\alpha^{q^i})^{q^{n-2}}, \ldots, (\alpha^{q^i})^q\right]$. Suponhamos que M tenha dimensão m como um espaço vetorial sobre $\mathbb{F}_q$, então uma base para o espaço coluna de A_α é dada por um conjunto de m-colunas de A_α, cujas primeiras entradas são os elementos base de M.

Reciprocamente, dado uma base do espaço coluna de A_α, uma base de M é obtida tomando a primeira entrada de cada coluna que pertence à base do espaço coluna de A_α. □

Definição 3.3. Denote por L_f o polinômio q-associado linearizado de f. O polinômio L_f define uma aplicação linear

$$\begin{aligned} L_f : \ \overline{\mathbb{F}_q} &\longrightarrow \overline{\mathbb{F}_q} \\ \alpha &\longmapsto f \circ \alpha = \sum_{i=0}^{m} a_i \alpha^{q^i}, \end{aligned}$$

onde $\overline{\mathbb{F}_q}$ denota o fecho algébrico de $\mathbb{F}_q$.

Seja $\zeta \in \mathbb{F}_{q^n}$. Denota-se por I_ζ o ideal de $\mathbb{F}_q[x]$ dado por $I_\zeta = \{g \in \mathbb{F}_q[x] \mid g \circ \zeta = 0\}$. Este ideal é o conjunto de anuladores de ζ. Como $\mathbb{F}_q[x]$ é um domínio principal, tem-se $I_\zeta = (f)$, para algum $f \in \mathbb{F}_q[x]$. A seguir, apresenta-se a noção de $\mathrm{Ord}(\zeta)$; esta definição é importante no desenvolvimento do presente capítulo e dos próximos capítulos.

Definição 3.4. O polinômio mônico de $\mathbb{F}_q[x]$ que gera I_ζ é chamado de $\mathbb{F}_q$**-ordem de** ζ e é denotado por $\mathrm{Ord}(\zeta)$.

Isto é, $\mathrm{Ord}(\zeta)$ é o associado do q-polinômio mônico sobre $\mathbb{F}_{q^n}$ de menor grau positivo tendo ζ como raiz sobre $\mathbb{F}_{q^n}$.

A seguir expõe-se um resultado dado em [15, Corolário 1.52], que envolve a definição anterior e é utilizado para mostrar o Lema 3.7, que é fundamental para desenvolvimento do objetivo deste capítulo.

Teorema 3.5. *[15, Corolário 1.52] Sejam $\alpha \in \mathbb{F}_{q^n}$ um elemento normal sobre $\mathbb{F}_q[x]$ e $g \in \mathbb{F}[x]$. Então*

$$\mathrm{Ord}(g \circ \alpha) = \frac{x^n - 1}{\mathrm{mdc}(x^n - 1, g)}.$$

Com a definição anterior apresenta-se outra caracterização para os elementos k-normais.

Teorema 3.6. *Seja $\alpha \in \mathbb{F}_{q^n}$. As seguintes três propriedades são equivalentes:*

i. *α é k-normal sobre $\mathbb{F}_q$.*

ii. *α da origem à base $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ de um q-módulo de dimensão $n-k$ sobre $\mathbb{F}_q$.*

iii. $\mathrm{grau}(\mathrm{Ord}(\alpha)) = n - k$.

Demonstração.

i.⇒ ii. Suponha que $\alpha \in \mathbb{F}_{q^n}$ é k-normal. Pelo Teorema 2.11 A_α tem posto $n-k$, assim pelo Lema 3.2 segue-se que o espaço vetorial M tem dimensão $n-k$ sobre $\mathbb{F}_q$. Tem-se $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ forma uma base para M sobre $\mathbb{F}_q$. De fato, para cada $i = n-k, \ldots, n-1$ o conjunto $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\} \cup \{\alpha^{q^i}\}$ (contendo $n-k+1$ elementos) deve ser linearmente dependente.

Portanto, α^{q^i} pode ser escrito como uma combinação linear de $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ e assim, estes $n-k$ elementos linearmente independentes geram o espaço M. Se $\beta \in M$, então $\beta = \sum_{i=0}^{n-k-1} a_i \alpha^{q^i}$ e $\beta^q = \sum_{i=0}^{n-k-2} a_i \alpha^{q^{i+1}} + a_{n-k-1}\alpha^{q^{n-k}} \in M$, portanto M é um q-módulo de dimensão $n-k$ sobre $\mathbb{F}_q$.

ii. ⇒ iii. Suponha que $\mathscr{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ é base de um q-módulo N de dimensão $n-k$ sobre $\mathbb{F}_q$. Seja $L(x) = \prod_{\gamma \in N}(x - \gamma)$. Pelo Teorema 1.32, L é um q-polinômio mônico de grau q^{n-k} sobre $\mathbb{F}_q$. Como $\alpha \in N$, α é uma raiz de L, e como os elementos de $\mathscr{B}$ são linearmente independentes, então α não pode ser raiz de um q-polinômio sobre $\mathbb{F}_q$ de grau menor que q^{n-k}. Portanto, $\mathrm{Ord}(\alpha) = l$, onde l é o polinômio q-associado de L de grau $n-k$.

iii. $\Rightarrow$ i. Suponha que $\mathrm{Ord}(\alpha)$ tem grau $n-k$, isto é, α é uma raiz q-primitiva de algum q-polinômio L sobre $\mathbb{F}_q$ de grau q^{n-k}. Então $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ forma uma base para M. Assim, pelo Lema 3.2, A_α tem posto $n-k$ e portanto, α é k-normal sobre $\mathbb{F}_q$.

□

O lema a seguir é uma propriedade que relaciona as noções de $\mathrm{Ord}(\alpha)$ e a Função Φ de Euler para polinômios. Este resultado é indispensável para demonstrar o Teorema 3.8 que identifica quantos elementos k-normais existem em um corpo. Este lema foi mostrado inicialmente em [16].

Lema 3.7. *Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico primo relativo com x. O número de elementos α no fecho algébrico de $\mathbb{F}_q$ com $\mathrm{Ord}(\alpha) = f$ é igual a $\Phi_q(f)$.*

Demonstração. Seja $f \in \mathbb{F}_q[x]$ tal que $\mathrm{mdc}(x, f) = 1$ ou seja $f(0) \neq 0$. Denota-se por L_f o polinômio q-associado linearizado de f como na Definição 3.3. Como,

$$\frac{d(L_f)}{dx} = \sum_{i=0}^{m} a_i q^i x^{q^i-1} = a_0 + \sum_{i=1}^{m} q^i a_i x^{q^i-1} = a_0 \neq 0,$$

temos que todas as raízes de L_f são diferentes. Dessa forma, o número de raízes de L_f é $|\ker(L_f)| = q^m$, pois $\mathrm{grau}(f) = m$. Dado que $\ker(L_f)$ é um conjunto finito, existe $n \in \mathbb{N}$ tal que $\ker(L_f) \subseteq \mathbb{F}_{q^n}$. Dessa forma, $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n} - \alpha = 0$. Logo, pelo Teorema 1.30, $f \mid x^n - 1$, já que $L_f \mid x^{q^n} - x$.

Como toda extensão $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ possui uma base normal (veja por exemplo Teorema 2.9), existe um elemento normal $\gamma \in \mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Logo,

$$\mathbb{F}_{q^n} = \{g \circ \gamma \mid g \in \mathbb{F}_q[x] \text{ e } \mathrm{grau}(g) \leq n-1\}.$$

Consideremos

$$V = \{\beta \in \overline{\mathbb{F}_q} \mid \mathrm{Ord}(\beta) = f\}.$$

Pela definição de $\mathrm{Ord}(\alpha)$ e de L_f segue-se que,

$$V = \{\beta \in \overline{\mathbb{F}_q} \mid \mathrm{Ord}(\beta) = f\} \subseteq \ker(L_f) \subseteq \mathbb{F}_{q^n}.$$

Logo, $V = \{\beta \in \mathbb{F}_{q^n} \mid \mathrm{Ord}(\beta) = f\}$. Assim,

$$V = \{g \circ \gamma \mid g \in \mathbb{F}_q[x], \mathrm{grau}(g) \leq n-1 \text{ e } \mathrm{Ord}(g \circ \gamma) = f\}.$$

Pelo Teorema 3.5, $f = \mathrm{Ord}(g \circ \gamma) = \frac{x^n-1}{\mathrm{mdc}(x^n-1, g)}$. Logo, $\mathrm{mdc}(x^n - 1, g) = \frac{x^n-1}{f}$ e, consequentemente, $\frac{x^n-1}{f} \Big| g$, isto é, $g = g_1 \cdot \frac{x^n-1}{f}$, onde $g_1 \in \mathbb{F}_q[x]$, com

$$\begin{aligned} \mathrm{grau}(g_1) + (n - \mathrm{grau}(f)) &\leq n-1, \\ \mathrm{grau}(g_1) &\leq \mathrm{grau}(f) - 1. \end{aligned}$$

Como,

$$\mathrm{mdc}\,(x^n - 1, g) = \mathrm{mdc}\left(x^n - 1, g_1 \cdot \frac{x^n-1}{f}\right) = \frac{x^n-1}{f},$$

então $\mathrm{mdc}(f, g_1) = 1$. Isto implica

$$V = \left\{ g \circ \gamma \mid g = g_1 \cdot \frac{x^n-1}{f}, g_1 \in \mathbb{F}_q[x], \mathrm{grau}(g_1) \leq \mathrm{grau}(f) - 1 \text{ e } \mathrm{mdc}(f, g_1) = 1 \right\}.$$

Como existem $\Phi_q(f)$ polinômios $g_1 \in \mathbb{F}_q[x]$ satisfazendo $\mathrm{grau}(g_1) \leq \mathrm{grau}(f)-1$ e $\mathrm{mdc}(f, g_1) = 1$, tem-se $\mid V \mid = \Phi_q(f)$. □

O resultado a seguir dado inicialmente em [11, Theorem 3.5] é o mais importante deste capítulo, já que permite identificar a quantidade exata de elementos k-normais em um determinado corpo finito.

Teorema 3.8. *O número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é dado por*

$$\sum_{\substack{h|(x^n-1)\\ \text{grau}(h)=n-k}} \Phi_q(h), \tag{3.1}$$

onde os divisores são mônicos e a divisão polinomial é sobre $\mathbb{F}_q$.

Demonstração. Seja $h \in \mathbb{F}_q[x]$ com $\text{grau}(h) = n-k$ e tal que h é primo relativo com x, isto é $h \mid (x^n-1)$. Pelo Lema 3.7 tem-se que o número de elementos α tais que $\text{Ord}(\alpha) = h$ é $\Phi_q(h)$. Como $\text{grau}(\text{Ord}(\alpha)) = n-k$, segue do Teorema 3.6 item iii. que o número de elementos α que são k-normais para o polinômio $h \in \mathbb{F}_q[x]$ é $\Phi_q(h)$. Assim, o número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é

$$\sum_{\substack{h|(x^n-1)\\ \text{grau}(h)=n-k}} \Phi_q(h),$$

□

Enfatiza-se que a fatoração de x^n-1 na Equação (3.1) é a $\mathbb{F}_q$-fatoração de x^n-1.

Observação 3.9. Quando $k=0$, o somatório do Teorema 3.8 se reduz a

$$\Phi_q(x^n-1).$$

Como demonstrou-se no Teorema 3.1.

Observação 3.10. Observe que os únicos valores de k para os quais os elementos k-normais são garantidos para todo (q,n) são $0, 1, n-1$, já que $x-1$ é sempre divisor de x^n-1, pois $x^n-1 = (x-1)(x^{n-1}+x^{n-2}+\cdots+x+1)$, isto é, sempre possui pelo menos um fator de grau 1 e um de grau $n-1$ de x^n-1.

Capítulo 4

Limites no número de elementos normais e k-normais

Neste capítulo apresentam-se a definição de densidade de elementos normais e k-normais em um determinado corpo finito. No capítulo anterior provou-se um resultado que permite saber quantos elementos normais e k-normais existem em um corpo finito (Teorema 3.8), no entanto encontrar esses elementos o saber como estão "espalhados" no corpo ainda é um trabalho difícil, por essa razão é importante o estudo da densidade desses elementos, já que esta noção permite saber a probabilidade de encontrar um elemento k-normal no corpo. Na atualidade não se conhece com exatidão a densidade dos elementos k-normais, porém existem diversos trabalhos onde se estabelecem limites superiores e inferiores para a densidade, entre os quais destacam-se os artigos [11], [7] e [6].

Neste capítulo, apresentam-se o terceiro e quarto objetivo do trabalho, onde exibem-se os limites inferiores e superiores da densidade dos elementos k-normais dados em [11, Lemma 4.4] e [11, Theorem 4.6]. Para o desenvolvimento desses objetivos estudaram-se os resultados de [6] cujos enunciados e demonstrações são expostos neste capítulo.

4.1 Definições e resultados importantes

Nesta seção exibem-se as definições e resultados importantes para a compreensão das demonstrações dos lemas e teoremas expostos neste capítulo.

Com essa motivação exibe-se a seguinte noção que será usada no decorrer do capítulo.

Definição 4.1. Seja d um inteiro positivo. $I_q(d)$ denota o número de polinômios mônicos irredutíveis $g \in \mathbb{F}_q[x]$, tal que g tem grau d.

- $I_q^*(d)$ denota o número de polinômios mônicos irredutíveis $g \in \mathbb{F}_q[x]$, tal que: g tem grau d, e $g(0) \neq 0$.
- $I_q(d; f)$ denota o número de polinômios mônicos irredutíveis $g \in \mathbb{F}_q[x]$, tal que: g tem grau d, e g divide f.
- $I_q^*(d; f)$ denota o número de polinômios mônicos irredutíveis $g \in \mathbb{F}_q[x]$, tal que: g tem grau d, $g(0) \neq 0$, e g divide f.

Observe que o único polinômio irredutível g para o qual $g(0) = 0$ é o polinômio $g(x) = x$, e portanto $I_q(d) = I_q^*(d)$ exceto para $d = 1$. Daqui para frente, considere apenas f para o qual $f(0) \neq 0$. Para tais f, tem-se $I_q^*(d; f) = I_q(d; f)$ para todo d, e isso permite provar um limite inferior ligeiramente mais forte em $\Phi_q(f)$.

Na notação da Definição 4.1, a Equação (1.6) pode ser reescrita como

$$\Phi_q(f) = q^n \prod_{d=1}^{n} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d;f)}. \tag{4.1}$$

Além disso sabemos que

$$\text{grau}(f) \geq \sum_{d=1}^{n} d \cdot I_q^*(d; f), \tag{4.2}$$

onde a igualdade vale precisamente quando f é livre de quadrados.

Com base nesses argumentos, tem-se o seguinte teorema.

Teorema 4.2. *[6, Theorem 2] Para qualquer corpo finito $\mathbb{F}_q$ e para qualquer polinômio $f \in \mathbb{F}_q[x]$ de grau $n \geq 2$ tal que $f(0) \neq 0$, tem-se*

$$\Phi_q(f) \geq \frac{q^n}{e\lceil \log_q(n) \rceil}.$$

Demonstração. Seja $\prod_{i=1}^{t} f_i^{e_i}$ uma fatoração de polinômios irredutíveis de f pelo Lema 1.38, sabemos que $\Phi_q(f) = \prod_{i=1}^{t} q^n \left(1 - \frac{1}{q^{n_i}}\right)$ onde n_i é o grau da f_i.

Logo $\Phi_q(f) = q^n \prod_{d=1}^{n} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d;f)}$. Assim de [14, Corollary 3.21] segue que

$$\text{grau}(f) = \sum_{d=1}^{n} d I_q^*(d; f),$$

então, se l é um inteiro tal que $\text{grau}(f) \leq 1 + \sum_{d=1}^{l} d I_q^*(d)$ tem-se

$$\Phi_q(f) \geq q^n \prod_{d=1}^{l} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d)}. \tag{4.3}$$

Novamente por [14, Corollary 3.21] obtém-se

$$q^l = \sum_{d|l} d I_q(d) = 1 + \sum_{d|l} d I_q^*(d). \tag{4.4}$$

para $l = \lceil \log_q(n) \rceil$, então da Equação (4.4), tem-se $q^{\log_q(n)} \leq q^l = 1 + \sum_{d|l} d I_q^*(d; f)$, desse modo

$n \leq 1 + \sum_{d|l} dI_q^*(d;f)$ e $I_q^*(d) \leq \frac{q^d-1}{d}$. Pela Equação (4.3), segue que

$$\begin{aligned}
\Phi_q(f) &\geq q^n \prod_{d=1}^{\lceil \log_q(n) \rceil} \left(1 - \frac{1}{q^d}\right)^{\frac{q^d-1}{d}} \\
&= q^n \prod_{d=1}^{\lceil \log_q(n) \rceil} \left(\left(1 - \frac{1}{q^d}\right)^{q^d-1}\right)^{\frac{1}{d}} \\
&\geq q^n \prod_{d=1}^{\lceil \log_q(n) \rceil} e^{-\frac{1}{d}} \\
&= q^n e^{\sum_{d=2}^{\lceil \log_q(n) \rceil} \frac{1}{d}} e^{-1} \\
&\geq q^n e^{-\ln(l)} e^{-1} \\
&= q^n l^{-1} e^{-1} \\
&= \frac{q^n}{e\lceil \log_q(n) \rceil}
\end{aligned}$$

□

Desse modo com base nesse teorema vai-se trabalhar no presente trabalho com a desigualdade,

$$\Phi_q(f) \geq \frac{q^n}{e\sqrt{\log_q(n)}}.$$

A seguir apresentam-se as notações de o-pequena e O-grande, com as suas propriedades. Estas notações serão utilizadas ao longo deste capítulo.

Definição 4.3. Sejam f e g funções cujos domínios de definição contêm um subconjunto dos números reais da forma $(a, +\infty)$, para algum $a \in \mathbb{R}$.

Escrevemos $f(x) = O(g(x))$ se existem um número real positivo M e um número real x_0 tais que $\mid f(x) \mid \leq Mg(x)$, para todo $x > x_0$.

Escrevemos $f(x) = o(g(x))$ se $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Lema 4.4. *As notações o-pequena e O-grande satisfazem as seguintes propriedades.*

i. $no(n) = o(n^2)$.

ii. $\pm o(n^2) \pm o(n^2) = \pm o(n^2)$.

iii. $o(n)^2 = o(n^2)$.

iv. *Para* $i < n$ *tem-se* $\sum o(i) = o(n^2)$.

v. *Seja* A *um conjunto finito, então* $o(\mid A \mid^2) = O(1)$.

vi. *Seja* A *um conjunto finito, então* $o(\mid A \mid^2) = 2(\mid A \mid \log_2(\mid A \mid))$.

vii. *Sejam* $k_1, k_2 \in \mathbb{R}$, *então* $O(k_1) + O(k_2) = O(k_1) = O(k_2)$.

viii. $\sum_{d=1}^{k} \mu(d) O\left(\frac{k}{d}\right) = O\left(k \sum_{d=1}^{k} \frac{1}{d}\right)$.

ix. $O\left(k^2 \sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2}\right) = O(k)$.

x. $\sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2} = O\left(\sum_{d=k+1}^{\infty} \frac{1}{d^2}\right)$.

xi. $O(log(k)) = O\left(\sum_{d=1}^{k} \frac{1}{d}\right)$.

Demonstração. i. Suponhamos que $f(n) = o(n)$ logo, $\lim_{n\to\infty} \frac{f(n)}{n} = 0$ então, $\lim_{n\to\infty} \frac{nf(n)}{n^2} = 0$, portanto $nf(n) = o(n^2)$, consequentemente $no(n) = o(n^2)$.

ii. Sera monstrado que $o(n^2) + o(n^2) = o(n^2)$ as outras combinações são análogas. Suponha que $f(n) = o(n^2)$, então $\lim_{n\to\infty} \frac{f(n)}{n^2} = 0$. Como $o(n^2) + o(n^2) = 2f(n)$ e $\lim_{n\to\infty} \frac{2f(n)}{n^2} = \lim_{n\to\infty} \frac{f(n)}{n^2} = 0$, segue-se que $o(n^2) + o(n^2) = f(n) = o(n^2)$.

iii. Suponha que $f(n) = o(n)$, logo $\lim_{n\to\infty} \frac{f(n)}{n} = 0$, assim $\lim_{n\to\infty} \frac{f(n)^2}{n^2} = 0$ e $f(n)^2 = o(n)^2$, portanto $o(n)^2 = o(n^2)$.

iv. Seja $f = o(i)$, assim $\lim_{i\to\infty} \frac{f}{i} = 0$, desse modo $\lim_{n\to\infty} \frac{f}{n} = \lim_{n\to\infty} \frac{f}{i}\frac{i}{n} = \left(\lim_{i\to\infty} \frac{f}{i}\right)\left(\lim_{i,n\to\infty} \frac{i}{n}\right) = 0$, portanto $f = o(n)$, logo

$$\sum_{i=1}^{n} o(i) = \sum_{i=1}^{n} o(n) = (n)o(n) = o(n^2).$$

v. Seja $P =\mid A \mid$. Suponha que $f(n) = o(P^2)$, logo $\lim_{n\to\infty} \frac{f(n)}{P^2} = 0$, então para $n \gg 0$ tem-se que $\frac{f(n)}{P^2} \leq 1$, isto implica que $f(n) \leq 1 \cdot k$, portanto $f(n) = O(1)$.

vi. Seja $P =\mid A \mid$. Como $o(P^2) = O(1) = 2P\log(P)$. Portanto $o(P^2) = 2(P\log_2(P))$.

vii. Se $k_1 = k_2 = 0$ o resultado segue. Suponha $k_i \neq 0$ para $i = 1, 2$. Seja $\mid f_i(x) \mid \leq k_i c_i$, então

$$\mid f_1(x) + f_2(x) \mid \leq c_1k_1 + c_2k_2 = k_1\left(c_1 + \frac{c_2k_2}{k_1}\right) = O(k_1).$$

De maneira semelhante tem-se que $O(k_1) + O(k_2) = O(k_2)$.

viii. Como

$$\sum_{d=1}^{k} \mu(d) \underbrace{O\left(\frac{k}{d}\right)}_{=\frac{k}{d}} \leq k\sum_{d=1}^{k} \frac{1}{d},$$

assim

$$\sum_{d=1}^{k} \mu(d)O\left(\frac{k}{d}\right) = O\left(k\sum_{d=1}^{k} \frac{1}{d}\right).$$

ix. Se $f(x) = O\left(k^2 \sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2}\right)$, então

$$\begin{aligned} f(x) &\leq c\left(k^2 \sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2}\right) \text{ onde } c > 0 \\ &= \underbrace{k\left(ck \sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2}\right)}_{c'} \text{ onde } c' > 0. \end{aligned}$$

Assim $f(x) = O(k)$, portanto $O\left(k^2 \sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2}\right) = O(k)$.

x. Como

$$\sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2} \leq \sum_{d=k+1}^{\infty} \frac{1}{d^2},$$

segue-se que, $\sum_{d=k+1}^{\infty} \frac{\mu(d)}{d^2} = O\left(\sum_{d=k+1}^{\infty} \frac{1}{d^2}\right)$.

xi. Para cada $k > 0$, tem-se que $\log(k) \leq \sum_{d=1}^{k} \frac{1}{d}$ ou $\sum_{d=1}^{k} \frac{1}{d} \leq \log(k)$.

Suponha que $\log(k) \leq \sum_{d=1}^{k} \frac{1}{d}$. Se $f(x) = O(\log(k))$, então

$$\begin{aligned} f(x) &\leq c(\log(k)), \text{ com } c > 0 \\ &\leq c\left(\sum_{d=1}^{k} \frac{1}{d}\right). \end{aligned}$$

Assim $f(x) = O\left(\sum_{d=1}^{k} \frac{1}{d}\right)$, portanto $O(\log(k)) = O\left(\sum_{d=1}^{k} \frac{1}{d}\right)$.

De maneira análoga se suponha-se que $\sum_{d=1}^{k} \frac{1}{d} \leq \log(k)$.

□

Definição 4.5. Define-se a **função de Möbius** $\mu : \mathbb{Z}_+ \to \mathbb{Z}$ por

$$\mu(m) = \begin{cases} 1 & \text{se } m = 1, \\ 0 & \text{se existe } a > 1 \text{ tal que } a^2 \mid m, \\ (-1)^n & \text{se } m \text{ é o produto de } n \text{ primos distintos.} \end{cases}$$

A versão para polinômios é dada como segue.

Definição 4.6. Define-se a **função de Möbius** $\mu_q : \mathbb{F}_q[x] \setminus \{0\} \to \mathbb{Z}$ por

$$\mu_q(f) = \begin{cases} 1 & \text{se } f \in \mathbb{F}_q \setminus \{0\}, \\ 0 & \text{se existe } h \in \mathbb{F}_q[x] \text{ de grau maior ou igual a 1 tal que } h^2 \mid f, \\ (-1)^n & \text{se } f \text{ é o produto de } n \text{ polinômios irredutíveis em } \mathbb{F}_q[x] \text{ não associados} \\ & \text{entre eles.} \end{cases}$$

Definição 4.7. A **função Zeta de Riemann** $\zeta(s)$ está definida, para valores complexos com parte real maior que 1, pela serie de Dirichlet:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Um resultado que relaciona a definição anterior com a função de Möbius é o seguinte.

Teorema 4.8. *[10, Theorem 287]*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \quad (s > 1).$$

4.2 Limite inferior da densidade para os elementos normais.

A seguir apresenta-se uma das definições mais importante deste capítulo, isto é a noção de densidade dos elementos normais.

Definição 4.9. Suponha que $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau n e seja $\mathbb{F}_{q^n}$ a extensão de $\mathbb{F}_q$ que contém todas as raízes de f. A **densidade** relativa do polinômio f sobre $\mathbb{F}_q$ é dada por $\kappa(f) = q^{-n}\Phi_q(f)$.

Definição 4.10. A **densidade** dos elementos normais sobre $\mathbb{F}_q$ é dada pela medida $\kappa(x^n - 1) = q^{-n}\Phi_q(x^n - 1)$.

A seguir usamos a forma multiplicativa de $\Phi_q(f)$ para descrever a densidade.

Teorema 4.11. *Seja $f \in \mathbb{F}_q[x]$ e suponhamos que f tenha fatoração completa $f = \prod_{i=1}^{t} f_i^{e_i}$ sobre $\mathbb{F}_q[x]$ (isto é, os fatores irredutíveis f_i, f_j são distintos quando $i \neq j$). Então*

$$\kappa(f) = \prod_{i=1}^{t} \left(1 - \frac{1}{q^{n_i}}\right),$$

onde n_i é o grau de f_i, e $n \geq 1$ é o grau de f.

No Lema 1.38 no item *iii*, mostrou-se que $\Phi_q(f) = q^n \prod_{i=1}^{t} \left(1 - \frac{1}{q^{n_i}}\right)$ e como $\kappa(f) = \frac{\Phi_q(f)}{q^n}$ tem-se a demonstração deste Teorema é a mesma prova apresentada no Lema 1.38 no item *iii*.

O seguinte lema é necessário para mostrar o Teorema 4.13 que dá um limite inferior da densidade para qualquer polinômio.

Lema 4.12. *Se $0 < x < 1$, então $(1-x)^n \leq 1 - x^n$, para todo $n \in \mathbb{N}$.*

Demonstração. Para $n = 1$ tem-se a igualdade. Suponha que isto é valido para $n = s$ ou seja $(1-x)^s \leq 1 - x^s$.

Será demonstrado que vale o resultado para $n = s+1$. Observe primeiro que como $0 < x < 1$, então $x^{s+1} < x^s$ e $x^{s+1} < x$. Logo,

$$\begin{aligned} (1-x)^{s+1} &= (1-x)^s(1-x) \leq (1-x^s)(1-x) = 1 - x - x^s + x^{s+1} \\ &< 1 - x^{s+1} - x^{s+1} + x^{s+1} = 1 - x^{s+1}. \end{aligned}$$

□

O seguinte teorema é importante já que dá um limite inferior da densidade para qualquer polinômio f, este resultado foi dado inicialmente em [7, Theorem 2.1].

Teorema 4.13. *Para qualquer $f \in \mathbb{F}_q[x]$ de grau n com $f(0) \neq 0$. Então*

$$\kappa(f) \geq \begin{cases} \frac{1}{e^{0,83}(1+\log_q(n))}, & \text{se } n \geq q \\ \frac{1}{e} & \text{se } n < q. \end{cases}$$

Demonstração. Para qualquer inteiro positivo m tem-se pelo Lema 4.12

$$1 - \frac{1}{q^m} \geq \left(1 - \frac{1}{q}\right)^m \text{ para } q \geq 2. \tag{4.5}$$

Por outro lado,

$$\begin{aligned} \kappa(f) &= q^{-n}\Phi(f) \\ &= q^{-n} \underbrace{\prod_{i=1}^{l} \left(1 - \frac{1}{q^{n_i}}\right) q^n}_{\text{Lema 1.38 item iii.}} \\ &= \prod_{i=1}^{l} \left(1 - \frac{1}{q^{n_i}}\right). \end{aligned} \tag{4.6}$$

Assim

$$\begin{aligned} \kappa(f) &\underbrace{\geq}_{Eq\ (4.5)} \prod_{i=1}^{l} \left(1 - \frac{1}{q}\right)^{n_i} \\ &= \left(1 - \frac{1}{q}\right)^{\sum_{i=1}^{l} n_i} \\ &\geq \left(1 - \frac{1}{q}\right)^{n}. \end{aligned}$$

Se $n < q$, então $n \leq q - 1$ e

$$\begin{aligned} \left(1 - \frac{1}{q}\right)^n &\geq \left(1 - \frac{1}{q}\right)^{q-1} \\ &= \left(\frac{q-1}{q}\right)^{q-1} \\ &= \left(\left(\frac{q}{q-1}\right)^{q-1}\right)^{-1} \\ &= \left(\left(\frac{q-1+1}{q-1}\right)^{q-1}\right)^{-1} \\ &= \left(\left(1 + \frac{1}{q-1}\right)^{q-1}\right)^{-1} \\ &> \frac{1}{e}. \end{aligned}$$

A última desigualdade decorre do fato que a função $\left(1+\frac{1}{x}\right)^x$ é crescente para $x>0$ e converge para e, quando x tende ao infinito.

Se $n \geq q$, para $s \in \{1,\ldots,n\}$ consideremos

$$\tau_s = \left|\{i; n_i = s, 1 \leq i \leq r\}\right|,$$

logo

$$\sum_{s=1}^{n} s\tau_s \leq n \quad \text{e} \quad \kappa(f) = \prod_{s=1}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s}. \tag{4.7}$$

Das Equações (4.6) e (4.7) segue-se que

$$\kappa(f) = \prod_{i=1}^{l}\left(1-\frac{1}{q^{n_i}}\right) = \prod_{s=1}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s}, \tag{4.8}$$

pela definição de τ_s, para $s \geq 1$ tem-se que $\tau_s \leq I_s$, onde I_s é o número de polinômios mônicos irredutíveis de grau s em $\mathbb{F}_q[x]$ que são diferentes de x. Além disso $I_s \leq \frac{q^s-1}{s}$. De fato, $I_s = \frac{1}{s}\sum_{d|s}\mu(d)q^{\frac{s}{d}}$. Logo

$$\begin{aligned} sI_s &\leq \sum_{d|s}\mu(d)q^{\frac{s}{d}} \\ &= q^s + \underbrace{\sum_{\substack{d|s \\ d\neq 1}}\mu(d)q^{\frac{s}{d}}}_{<-1} \\ &\leq q^s - 1, \end{aligned}$$

desse modo, $I_s \leq \frac{q^s-1}{s}$, para $s \geq 1$, portanto

$$\tau_s \leq I_s \leq \frac{q^s-1}{s}. \tag{4.9}$$

Se definimos $U = \lfloor log_q(n) \rfloor$, como $n < q^n$ para $q \geq 2$, então $\log_q n < n$, assim $U+1 \leq n$. Da Equação (4.9), e do fato de que os fatores irredutíveis de $x^{q^{U+1}} - x = x\left(x^{q^{U+1}-1}-1\right)$ que são diferentes de x, são todos distintos e de grau menor ou igual que $U+1$, segue-se que

$$\sum_{s=1}^{U+1} sI_s \geq q^{U+1} - 1.$$

Como $U < \log_q(n) < U+1$, então $q^{U+1} > n$, assim $q^{U+1} - 1 \geq n$, portanto

$$\sum_{s=1}^{U+1} sI_s \geq q^{U+1} - 1 \geq n \geq \sum_{s=1}^{n} s\tau_s. \tag{4.10}$$

Afirmamos que,

$$\prod_{s=1}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s} \geq \prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{I_s}. \tag{4.11}$$

De fato, como $\tau_s \leq I_s \leq \frac{q^s-1}{s}$ para $s \geq 1$, segue-se que $q^s - 1 \geq s(I_s - \tau_s)$. Pela equação (4.10) tem-se que $\sum_{s=1}^{U+1} sI_s - \sum_{s=1}^{n} s\tau_s \geq 0$, portanto

$$\begin{aligned}(U+1)\sum_{s=1}^{U+1}(I_s-\tau_s) &\geq \sum_{s=1}^{U+1} s(I_s-\tau_s)\\ &\underbrace{\geq}_{Eq\ (4.10)} \sum_{s=U+2}^{n} s\tau_s\\ &\geq (U+1)\sum_{s=U+2}^{n}\tau_s\end{aligned}$$

de modo que,

$$\sum_{s=1}^{U+1}(I_s-\tau_s) \geq \sum_{s=U+2}^{n}\tau_s. \tag{4.12}$$

Por outro lado,

$$\begin{aligned}\left(\prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{I_s}\right)\left(\prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{\tau_s}\right)^{-1} &= \prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{I_s-\tau_s}\\ &\leq \prod_{s=1}^{U+1}\left(1-\frac{1}{q^{U+1}}\right)^{I_s-\tau_s}\\ &= \left(1-\frac{1}{q^{U+1}}\right)^{\sum_{s=1}^{U+1}(I_s-\tau_s)}\\ &\underbrace{\leq}_{Eq\ (4.12)} \left(1-\frac{1}{q^{U+1}}\right)^{\sum_{s=U+2}^{n}\tau_s}\\ &= \prod_{s=U+2}^{n}\left(1-\frac{1}{q^{U+1}}\right)^{\tau_s}\\ &\leq \prod_{s=U+2}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s}.\end{aligned}$$

Por conseguinte,

$$\begin{aligned}\prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{I_s} &\leq \left(\prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{\tau_s}\right)\left(\prod_{s=U+2}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s}\right)\\ &= \prod_{s=1}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s},\end{aligned}$$

o que mostra a afirmação.

Assim,

$$
\begin{aligned}
\kappa(f) &\underbrace{=}_{Eq\ (4.8)} \prod_{s=1}^{n}\left(1-\frac{1}{q^s}\right)^{\tau_s} \\
&\underbrace{\geq}_{Eq\ (4.9)} \prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{I_s} \\
&\geq \prod_{s=1}^{U+1}\left(1-\frac{1}{q^s}\right)^{\frac{q^s-1}{s}} \\
&= \prod_{s=1}^{U+1}\left(\left(\frac{q^s-1}{q^s}\right)^{q^s-1}\right)^{\frac{1}{s}} \\
&= \prod_{s=1}^{U+1}\left(\left(\left(\frac{q^s}{q^s-1}\right)^{q^s-1}\right)^{-1}\right)^{\frac{1}{s}} \\
&= \prod_{s=1}^{U+1}\left(\left(\left(\frac{q^s-1+1}{q^s-1}\right)^{q^s-1}\right)^{-1}\right)^{\frac{1}{s}} \\
&= \prod_{s=1}^{U+1}\left(\left(\left(1+\frac{1}{q^s-1}\right)^{q^s-1}\right)^{-1}\right)^{\frac{1}{s}} \\
&\underbrace{\geq}_{q\to\infty} \prod_{s=1}^{U+1}\left(\frac{1}{e}\right)^{\frac{1}{s}} \\
&= \left(\frac{1}{e}\right)^{\sum_{s=1}^{U+1}\frac{1}{s}}.
\end{aligned}
$$

Uma aproximação dada em [8, pag 452] para $H_m = \sum_{s=1}^{m}\frac{1}{s}$ é

$$H_m = \ln(m) + \gamma + \frac{1}{2m} - \frac{1}{12m^2} + O(m^{-4})$$

onde $\gamma = 0,577216\ldots$ é a constante de Euler-Mascheroni. Por isso

$$H_{U+1} = \sum_{s=1}^{U+1}\frac{1}{s} \approx \ln(U+1) + \gamma + \frac{1}{2(U+1)} - \frac{1}{12(U+1)^2} + O((U+1)^{-4}).$$

Consequentemente,

$$\begin{aligned}\kappa(f) &\geq \left(\frac{1}{e}\right)^{\sum_{s=1}^{U+1}\frac{1}{s}} \\ &\geq \left(\frac{1}{e}\right)^{\ln(U+1)+\gamma+\frac{1}{2(U+1)}} \\ &= \frac{1}{e^{\ln(U+1)+\gamma+\frac{1}{2(U+1)}}} \\ &= \frac{1}{(U+1)e^{\gamma+\frac{1}{2(U+1)}}} \\ &\geq \frac{1}{(\log_q(n)+1)e^{\gamma+\frac{1}{2(\log_q(n)+1)}}},\end{aligned}$$

quando $n > q$, tem-se $\gamma + \frac{1}{2(\log_q(n)+1)} < \gamma + \frac{1}{4} \approx 0,83$. De fato, $\log_q(n) > 1$ para todo $n \geq q$, se não for assim, existiria $0 < x \leq 1$ tal que $\log_q(n) = x$. Logo $q^x = n$, isto implica que $q^x \leq q$ que é uma contradição, assim $\log_q(n) \neq 1$ para todo $n > q$ e $q \geq 1$, portanto $1 + \log_q(n) > 2$ quando $q < n$. Por isso $\gamma + \frac{1}{2(\log_q(n)+1)} < \gamma + \frac{1}{4} \approx 0,83$. Finalmente conclui-se que

$$\kappa(f) \geq \frac{1}{e^{0,83}(1+\log_q(n))}.$$

□

Observação 4.14. Se $n < q$ o resultado do Teorema 4.13 pode ser melhorado para $\kappa(f) \geq e^{\frac{-n}{(q-1)}}$ seguindo os mesmos passos, de fato

$$\begin{aligned}\left(1-\frac{1}{q}\right)^n &= \left[\left(1-\frac{1}{q}\right)^{q-1}\right]^{\frac{n}{(q-1)}} \\ &\geq \left[\left(1+\frac{1}{q-1}\right)^{q-1}\right]^{-\frac{n}{(q-1)}} \\ &\geq e^{-\frac{n}{(q-1)}}.\end{aligned}$$

Portanto, para qualquer h de grau $n-k$, $\kappa(h) \geq \frac{1}{e^{0,83}(1+\log_q(n-k))}$. No entanto, o limite inferior da densidade de elementos normais foi melhorada em [6, Theorem 3] considerando o caso particular $f(x) = x^n - 1$. Este resultado é o Teorema 4.26 deste trabalho.

4.3 Limite inferior da densidade para os elementos k-normais

Nesta seção apresenta-se um limite inferior da densidade dos elementos k-normais, todos os resultados apresentados nesta subseção são dados em [6] e [11].

Com essa motivação exibe-se a seguinte definição que será utilizada ao longo desta subseção.

Definição 4.15. Seja $f \in \mathbb{F}[x]$ um polinômio de grau $n-k$ tal que $f \mid (x^n - 1)$. Denota-se por $A_{q,n,k}^{(f)}$ como o conjunto dos graus $d \in \{1, \ldots, n-k\}$ para o qual

$$I_q^*(d; f) > \frac{q^d - 1}{2d^2}.$$

Seja $B_{q,n,k}^{(f)}$ o conjunto dos graus $d \in \{1, \ldots, n\}$ para o qual

$$I_q^*(d; f) \leq \frac{q^d - 1}{2d^2}.$$

O seguinte lema é necessario para mostrar o Lema 4.17 que dá um limite inferior da densidade em termos dos conjuntos $A_{q,n,k}^{(f)}$ e $B_{q,n,k}^{(f)}$ definidos acima.

Lema 4.16. *Têm-se as seguintes desigualdades*

i.

$$\sum_{i=1}^{s} \frac{1}{i} \leq \ln(s) + \gamma + \frac{1}{2\gamma}.$$

ii.

$$\sum_{i=s+1}^{\infty} \frac{1}{i^3} \leq \frac{1}{2s^2}.$$

iii.

$$\sum_{i=s+1}^{\infty} \frac{1}{2i^2} \leq \frac{1}{2s}.$$

Demonstração. i. Pelo critério da integral,

$$\begin{aligned} \sum_{i=1}^{s} \frac{1}{i} &\leq \int_1^{s+1} \frac{1}{x} dx \\ &= \ln(s+1) \\ &\leq \ln(s) + \gamma + \frac{1}{2\gamma}. \end{aligned}$$

ii. Pelo critério da integral,

$$\begin{aligned} \sum_{i=s+1}^{\infty} \frac{1}{i^3} &\leq \int_s^{\infty} \frac{1}{x^3} dx \\ &= \frac{1}{2s^2}. \end{aligned}$$

iii. Pelo critério da integral,

$$\begin{aligned} \sum_{i=s+1}^{\infty} \frac{1}{2i^2} &\leq \frac{1}{2} \int_s^{\infty} \frac{1}{x^2} dx \\ &= \frac{1}{2s}. \end{aligned}$$

□

O lema a seguir é dado em [11, Lemma 4.4] e é demonstrado em [6, Lemma 8], como já foi mencionado anteriormente, este resultado dá um limite inferior da densidade em função dos conjuntos $A_{q,n,k}^{(f)}$ e $B_{q,n,k}^{(f)}$ definidos acima.

Lema 4.17. *Sejam f, $A_{q,n,k}^{(f)}$ e $B_{q,n,k}^{(f)}$ como na Definição 4.15. Então*

$$\kappa(f) \geq \begin{cases} e^{-\frac{\zeta(2)}{2}} \approx 0,43935 & \text{se } A_{q,n,k}^{(f)} = \emptyset, \\ e^{-\gamma}\left(\frac{e^{-\left(\left|A_{q,n,k}^{(f)}\right|^{-1}\right)}}{\left|A_{q,n,k}^{(f)}\right|}\right) & \text{em outro caso.} \end{cases}$$

onde γ é a constante de Euler-Mascheroni e ζ é a função zeta de Riemann.

Demonstração. Como $\kappa(f) = q^{-n}\Phi_q(f)$. Segue que

$$\begin{aligned}
\kappa(f) &\geq q^{-n}q^n \prod_{d=1}^{n}\left(1-\frac{1}{q^d}\right)^{I_q^*(d;f)} \\
&\geq \prod_{d\in A_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{I_q^*(d;f)} \prod_{d\in B_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{I_q^*(d;f)} \\
&\underbrace{\geq}_{Eq\ (4.9)} \prod_{d\in A_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{\frac{q^d-1}{d}} \prod_{d\in B_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{I_q^*(d;f)} \\
&\geq \prod_{d\in A_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{\frac{q^d-1}{d}} \prod_{d\in B_{q,n,k}^{(f)}}\left(1-\frac{1}{q^d}\right)^{\frac{q^d-1}{2d^2}} \\
&\geq \prod_{d\in A_{q,n,k}^{(f)}}\left(\left(1-\frac{1}{q^d}\right)^{q^d-1}\right)^{\frac{1}{d}} \prod_{d\in B_{q,n,k}^{(f)}}\left(\left(1-\frac{1}{q^d}\right)^{q^d-1}\right)^{\frac{1}{2d^2}} \\
&\geq \prod_{d\in A_{q,n,k}^{(f)}}\left(\frac{1}{e}\right)^{\frac{1}{d}} \prod_{d\in B_{q,n,k}^{(f)}}\left(\frac{1}{e}\right)^{\frac{1}{2d^2}} \\
&= \left(\frac{1}{e}\right)^{\sum_{d\in A_{q,n,k}^{(f)}}\frac{1}{d}}\left(\frac{1}{e}\right)^{\sum_{d\in B_{q,n,k}^{(f)}}\frac{1}{2d^2}} \\
&= \left(\frac{1}{e}\right)^{\sum_{d=1}^{\left|A_{q,n,k}^{(f)}\right|}\frac{1}{d}}\left(\frac{1}{e}\right)^{\sum_{d=\left|A_{q,n,k}^{(f)}+1\right|}^{n-k}\frac{1}{2d^2}},
\end{aligned}$$

no caso que $A_{q,n,k}^{(f)} = \emptyset$ então $\left(\frac{1}{e}\right)^{\sum_{d\in A_{q,n,k}^{(f)}}\frac{1}{d}} = 1$. Logo

$$\kappa(f) \geq \left(\frac{1}{e}\right)^{\sum_{d=\left|A_{q,n,k}^{(f)}\right|+1}^{n-k}\frac{1}{2d^2}} \geq \left(\frac{1}{e}\right)^{\sum_{d=1}^{\infty}\frac{1}{2d^2}} \underbrace{=}_{Teo\ 4.8} \left(\frac{1}{e}\right)^{\frac{\zeta(2)}{2}},$$

portanto, $\kappa(f) \geq \left(\frac{1}{e}\right)^{\frac{\zeta(2)}{2}} \approx 0,43935$.

Agora, se $A_{q,n,k}^{(f)} \neq \emptyset$ então usando o Lema 4.16 tem-se,

$$\begin{aligned}
\kappa(f) &\geq \left(\frac{1}{e}\right)^{\sum_{d=1}^{\left|A_{q,n,k}^{(f)}\right|}\frac{1}{d}} \left(\frac{1}{e}\right)^{\sum_{d=\left|A_{q,n,k}^{(f)}+1\right|}^{n-k}\frac{1}{2d^2}} \\
&\geq \left(\frac{1}{e}\right)^{\ln\left(\left|A_{q,n,k}^{(f)}\right|\right)+\gamma+\frac{1}{2\left|A_{q,n,k}^{(f)}\right|}} \left(\frac{1}{e}\right)^{\frac{1}{2\left|A_{q,n,k}^{(f)}\right|}} \\
&= \frac{1}{\left|A_{q,n,k}^{(f)}\right| e^{\left(\gamma+\frac{1}{2\left|A_{q,n,k}^{(f)}\right|}\right)}} \frac{1}{e^{\left(\frac{1}{2\left|A_{q,n,k}^{(f)}\right|}\right)}} \\
&= \frac{1}{\left|A_{q,n,k}^{(f)}\right| e^{\left(\gamma+\frac{1}{\left|A_{q,n,k}^{(f)}\right|}\right)}} \\
&= e^{-\gamma}\left(\frac{e^{-\left(\left|A_{q,n,k}^{(f)}\right|^{-1}\right)}}{\left|A_{q,n,k}^{(f)}\right|}\right).
\end{aligned}$$

□

4.3.1 Limites superiores para $|A_{q,n,k}^{(f)}|$

Anteriormente foi exibido um limite inferior para a densidade dos elementos k-normais, porém esta densidade ainda não é a mais eficiente porque está em função do conjunto $|A_{q,n,k}^{(f)}|$. Nesta subseção apresentam-se limites superiores para o conjunto $|A_{q,n,k}^{(f)}|$ (Lema 4.25), para encontrar posteriormente um limite inferior numérico da densidade que não dependa de outras variáveis.

A seguir exibem-se alguns lemas, teoremas e proposições necessárias para demonstrar o Lema 4.25 que expõe os limites superiores para o conjunto $|A_{q,n,k}^{(f)}|$.

Lema 4.18. *Seja M um subconjunto finito já seja de $\mathbb{Z}$ ou de $\mathbb{Q}[x]$. Então*

$$\operatorname*{mmc}_{m\in M}(m) = \frac{\displaystyle\prod_{\substack{I\subset M \\ |I| \text{ímpar}}} \operatorname*{mdc}_{m\in I}(m)}{\displaystyle\prod_{\substack{I\subset M \\ |I| par}} \operatorname*{mdc}_{m\in I}(m)}.$$

Este lema afirma que para calcular o mmc de um conjunto finito de inteiros ou polinômios basta calcular o mdc de todos os subconjuntos de M.

Demonstração. Seja p um número primo que aparece na fatoração de $\operatorname*{mmc}_{m\in M}(m)$. Suponha que α seja o maior inteiro positivo tal que p^α divide $\operatorname*{mmc}_{m\in M}(m)$. Nesse caso existe $m_1 \in M$ tal que $p^\alpha \mid m_1$ e $p^{\alpha+1} \nmid m_1$. Defina $M_1 = M - \{m_1\}$, ou seja $M = M_1 \cup \{m_1\}$. Será demonstrado que p^α divide

$$A = \frac{\displaystyle\prod_{\substack{I\subset M \\ |I| \text{ímpar}}} \operatorname*{mdc}_{m\in I}(m)}{\displaystyle\prod_{\substack{I\subset M \\ |I| par}} \operatorname*{mdc}_{m\in I}(m)}.$$

Para $I \subseteq M_1$ com $I \neq \emptyset$, tem-se p não divide $\frac{\underset{m\in I}{\operatorname{mdc}}(m,m_1)}{\underset{m\in I}{\operatorname{mdc}}(m)}$. Como

$$\frac{\prod\limits_{\substack{I\subseteq M\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m)}{\prod\limits_{\substack{I\subseteq M\\ |I|par}} \underset{m\in I}{\operatorname{mdc}}(m)} = \frac{\prod\limits_{\substack{I\subseteq M_1\\ |I|par\\ I\neq\emptyset}} \underset{m\in I}{\operatorname{mdc}}(m,m_1)}{\prod\limits_{\substack{I\subseteq M_1\\ |I|par\\ I\neq\emptyset}} \underset{m\in I}{\operatorname{mdc}}(m)} \cdot \operatorname{mdc}(m_1) \cdot \frac{\prod\limits_{\substack{I\subseteq M_1\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m)}{\prod\limits_{\substack{I\subseteq M_1\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m,m_1)}$$

e p não divide $\dfrac{\prod\limits_{\substack{I\subseteq M\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m)}{\prod\limits_{\substack{I\subseteq M_1\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m,m_1)}$.

Então a máxima potência de p que divide A é igual à máxima potência de p que divide a $\frac{\operatorname{mdc}(m_1)}{1} = m_1$. Portanto p divide $\dfrac{\prod\limits_{\substack{I\subseteq M\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m)}{\prod\limits_{\substack{I\subseteq M\\ |I|par}} \underset{m\in I}{\operatorname{mdc}}(m)}$ e $p^{\alpha+1} \nmid A$.

Por outro lado, se algum primo p que aparece na fatoração de $\prod\limits_{\substack{I\subseteq M\\ |I|\text{ímpar}}} \underset{m\in I}{\operatorname{mdc}}(m)$ ou $\prod\limits_{\substack{I\subseteq M\\ |I|par}} \underset{m\in I}{\operatorname{mdc}}(m)$, é divisor de algum $m \in M$ e portanto $p \mid \underset{m\in M}{\operatorname{mmc}}(m)$, aplicando o que acaba-se de mostrar, obtém-se que p aparece no numerador de A e $p^\alpha \mid A$, assim $p^\alpha \mid \underset{m\in A}{\operatorname{mmc}}(m)$. □

Lema 4.19. *Seja A um conjunto finito de números e $q \in \mathbb{N}$. Então*

$$\underset{d\in A}{\operatorname{mdc}}(q^d - 1) = q^{\underset{d\in A}{\operatorname{mdc}}(d)} - 1.$$

Demonstração. Seja $p^k \in \mathbb{Z}$ tal que $p^k \mid q^d - 1$, logo $q^d \equiv 1 \pmod{p^k}$. Considere o conjunto $\operatorname{Ord}_{p^k} q = min\{n \mid q^n \equiv 1 \pmod{p^k}$, então $\operatorname{Ord}_{p^k} q \mid d$. De fato, se $\operatorname{Ord}_{p^k} q \nmid d$ implica que $d = \operatorname{Ord}_{p^k} qh + t$ com $h, t \in \mathbb{Z}$ com $0 < t < \operatorname{Ord}_{p^k} q$ por conseguinte,

$$\begin{aligned} 1 \equiv q^d \pmod{p^k} \Leftrightarrow 1 &\equiv q^{\operatorname{Ord}_{p^k} qh+t} \pmod{p^k} \\ &\equiv \left(q^{\operatorname{Ord}_{p^k} q}\right)^h q^t \pmod{p^k} \\ &\equiv q^t \pmod{p^k}, \end{aligned}$$

que contradiz a minimalidade do $\operatorname{Ord}_{p^k} q$.

Assim,

$$\underset{d\in A}{\operatorname{mdc}}(q^d - 1) = \prod_{\substack{p^k \mid (q^d-1)\\ \forall d\in A}} p^k,$$

mas $p^k \mid q^d - 1$ para todo $d \in A$ se, e somente se, $\operatorname{Ord}_{p^k} q \mid d$ para todo $d \in A$ se, e somente se, $\operatorname{Ord}_{p^k} q \mid \underset{d\in A}{\operatorname{mdc}} d$, se e somente se, $p^k \mid q^{\underset{d\in A}{\operatorname{mdc}}(d)} - 1$. Portanto

$$\underset{d\in A}{\operatorname{mdc}}(q^d - 1) = q^{\underset{d\in A}{\operatorname{mdc}}(d)} - 1.$$

□

Lema 4.20. *Sejam A um conjunto finito de números naturais, q um número natural e seja $Q_n(z)$ que denota o n-ésimo polinômio ciclotômico. Então*

$$\operatorname*{mdc}_{d\in A}(q^d-1)=\prod_{\{e|\exists d\in A;e|d\}}Q_e(q).$$

Demonstração. Pelas Proposições 1.46 e 1.47 segue-se que $Q_n(z)$ é irredutível sobre $\mathbb{Q}$ e que

$$z^d-1=\prod_{e|d}Q_e(z).$$

Logo,

$$\begin{aligned}\operatorname*{mdc}_{d\in A}(z^d-1) &= \operatorname*{mdc}_{d\in A}\left(\prod_{e|d}Q_e(z)\right)\\ &= \prod_{\{e\,:\,e\mid d \text{ para todo } d\in A\}}Q_e(z)\\ &= \prod_{e|\operatorname*{mdc}_{d\in A}(d)}Q_e(z)\\ &= z^{\operatorname*{mdc}_{d\in A}(d)}-1.\end{aligned}$$

Assim,

$$\operatorname*{mdc}_{d\in A}(z^d-1)=z^{\operatorname*{mmc}_{d\in A}(d)}-1 \tag{4.13}$$

e

$$\operatorname*{mmc}_{d\in A}(z^d-1)=\operatorname*{mmc}_{d\in A}\left(\prod_{e|d}Q_e(z)\right)=\prod_{\{e|\exists d\in A;e|d\}}Q_e(z). \tag{4.14}$$

Pelo Lema 4.18 tem-se que se a substituição de z por q na Equação (4.13) é valida, então a substituição de z por q na Equação (4.14) é valida também, e pelo Lema 4.19 pode-se substituir a variável z por q na Equação (4.13). Portanto tem-se que,

$$\operatorname*{mmc}_{d\in A}(q^d-1)=\prod_{\{e|\exists d\in A;e|d\}}Q_e(q).$$

□

Lema 4.21. *Para $0\leq s\leq\frac{1}{2}$ tem-se que:*

i. $\ln(1-s)\geq s\ \ln\left(\frac{1}{4}\right)$.

ii. $\ln(1-s)^{-1}\leq s\ \ln(4)$.

Demonstração. i. Como $-\ln(x)$ é uma função convexa, tem-se que para todo $0\leq t\leq 1$ e para todos $x_1,x_2\in\mathbb{R}^+$, cumple-se que

$$-\ln(tx_1+(1-t)x_2)\leq -t\ \ln(x_1)-(1-t)\ln(x_2),$$

isto é

$$\ln(tx_1+(1-t)x_2)\geq t\ \ln(x_1)+(1-t)\ln(x_2). \tag{4.15}$$

Dado que $0\leq t\leq 1$ e $0\leq s\leq\frac{1}{2}$, então $t=2s$. Se $x_2=1$ segue-se da Equação 4.15 que $x_1=\frac{1}{2}$, assim $\ln\left(2s\left(\frac{1}{2}\right)+1-2s\right)\geq 2s\ln\left(\frac{1}{2}\right)$, isto é $\ln(1-s)\geq s\ \ln\left(\frac{1}{4}\right)$ para $0\leq s\leq\frac{1}{2}$.

ii. Do item i. tem-se que $-\ln(1-s) \leq s\left(-\ln\left(\frac{1}{4}\right)\right)$, isto é $\ln(1-s)^{-1} \leq s \ \ln(4)$.

□

Lema 4.22. *Seja $n \in \mathbb{N}$ e q uma potência de um número primo, e seja $Q_n(z)$ o n-ésimo polinômio ciclotômico. Então*

$$\frac{1}{4}q^{\phi(n)} \leq Q_n(q) \leq 4q^{\phi(n)}$$

onde ϕ é a função de Euler.

Demonstração. O n-ésimo polinômio ciclotômico é mônico e tem grau $\phi(n)$. Para mostrar os limites do lema, será utilizada a seguinte caracterização multiplicativa

$$Q_n(z) = \prod_{d|n}\left(z^{\frac{n}{d}} - 1\right)^{\mu(d)} \tag{4.16}$$

onde μ denota a função de Möbius. Uma caracterização da Função ϕ de Euler para inteiros dada em [10, Theorem 2.62] é a seguinte

$$\phi(n) = \sum_{d|n}\mu(d)\frac{n}{d}, \tag{4.17}$$

exponenciado a Expressão (4.17) com base q em ambos lados tem-se

$$q^{\phi(n)} = q^{\sum_{d|n}\mu(d)\frac{n}{d}}, \tag{4.18}$$

substituindo q por z na Equação (4.16).

Obtém-se,

$$\begin{aligned} Q_n(q) &= \prod_{d|n}\left(q^{\frac{n}{d}} - 1\right)^{\mu(d)} \\ &= \prod_{d|n}\left(q^{\frac{n}{d}}\right)^{\mu(d)}\left(1 - \frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)} \\ &= \prod_{d|n} q^{\sum_{d|n}\mu(d)\frac{n}{d}}\left(1 - \frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)}. \end{aligned}$$

Logo, usando a Expressão (4.18) segue que

$$Q_n(q) = q^{\phi(n)}\prod_{d|n}\left(1 - \frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)}, \tag{4.19}$$

para limitar o fator do lado direito da Equação (4.19), use o fato que $\mu(d) = \{-1, 0, 1\}$. Portanto

$$\prod_{d|n}\left(1 - \frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)} \geq \prod_{d|n}\left(1 - \frac{1}{q^{\frac{n}{d}}}\right) \geq \prod_{i=1}^{\infty}\left(1 - \frac{1}{q^i}\right), \tag{4.20}$$

tomando ln na Equação (4.20), usando o Lema 4.21 item i. tem-se,

$$\begin{aligned}\ln\left(\prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)}\right) &\geq \ln\left(\prod_{i=1}^{\infty}\left(1-\frac{1}{q^i}\right)\right)\\ &= \sum_{i=1}^{\infty}\ln\left(1-\frac{1}{q^i}\right)\\ &\geq \sum_{i=1}^{\infty}\frac{1}{q^i}\left(\ln\left(\frac{1}{4}\right)\right)\\ &\geq \ln\left(\frac{1}{4}\right).\end{aligned}$$

Desse modo $\prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)} \geq \frac{1}{4}$, portanto $Q_n(q) \geq \frac{1}{4}q^{\phi(n)}$.

Para o limite superior usa-se o fato que $\mu(d)$ pode tomar o valor -1 como segue,

$$\prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)} \leq \prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{-1} \leq \prod_{i=1}^{\infty}\left(1-\frac{1}{q^i}\right)^{-1}, \tag{4.21}$$

tomando ln na Equação (4.21), usando o Lema 4.21 item ii. tem-se,

$$\begin{aligned}\ln\left(\prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)}\right) &\leq \ln\left(\prod_{i=1}^{\infty}\left(1-\frac{1}{q^i}\right)^{-1}\right)\\ &= \sum_{i=1}^{\infty}\ln\left(1-\frac{1}{q^i}\right)^{-1}\\ &\leq \sum_{i=1}^{\infty}\frac{1}{q^i}(\ln(4))\\ &\leq \ln(4).\end{aligned}$$

Por isso, $\prod_{d|n}\left(1-\frac{1}{q^{\frac{n}{d}}}\right)^{\mu(d)} \leq 4$, de modo que $Q_n(q) \leq (4)q^{\phi(n)}$. Assim,

$$\frac{1}{4}q^{\phi(n)} \leq Q_n(q) \leq 4q^{\phi(n)}.$$

□

Lema 4.23. *Sejam A um conjunto finito de números naturais, $K = \mid A \mid$ e seja ϕ que denota a Função de Euler. Então*

$$\sum_{d\in A}\phi(d) \geq cK^2 - o(K^2)$$

onde $c = \frac{\zeta(6)}{(2\zeta(2)\zeta(3))} \approx 0,25726$.

Demonstração. Considere o conjunto $M_n = \{x \in \mathbb{N}; \phi(x) \leq n\}$, Dressler em [4], Erdos em [5] e Bateman em [2] mostraram que

$$\mid M_n \mid = c'n + o(n) \tag{4.22}$$

com $c' = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \approx 1,9436$.

Se existe $n \in \mathbb{N}$ tal que $A = M_n$, então

$$\sum_{d \in A} \phi(d) = \sum_{d \in M_n} \phi(d).$$

Tem-se $M_{n+1} = M_n \cup \{z \in \mathbb{N}; \phi(z) = n+1\}$ como M_n é uma sequência de inteiros positivos, então existe $l \in \mathbb{N}$ tal que $\mid M_l \mid \leq \mid A \mid$.

Se $A = \{a_1, \ldots, a_k\}$ e $M_l = \{b_1, \ldots, b_s\}$ com $s \leq k$. Ordenando os elementos da forma

$$\begin{gathered} \phi(a_1) \leq \phi(a_2) \leq \cdots \leq \phi(a_k), \\ \phi(b_1) \leq \phi(b_2) \leq \cdots \leq \phi(b_s) \leq n. \end{gathered}$$

Obtém-se $\phi(b_i) \leq \phi(a_1)$ para todo $i = 1, \ldots, s$, já que $\phi(b_i) \leq l \leq n$, desse modo

$$\sum_{d \in A} \phi(d) \geq \sum_{d \in M_l} \phi(d). \tag{4.23}$$

Por outro lado, da Equação (4.22) segue-se que $\mid M_l \mid = c'l + o(l) \leq \mid A \mid$, assim

$$l \leq \frac{\mid A \mid}{c'} - \frac{o(l)}{c'}. \tag{4.24}$$

Além disso, da Equação (4.22), que $|M_l| = c'l + f(l) \leq |A|$ com $\lim_{l\to\infty} \frac{f(l)}{l} = 0$ e $|M_{l+1}| = c'(l+1) + g(l+1) \geq |A|$ com $\lim_{l\to\infty} \frac{g(l+1)}{l+1} = 0$, consequentemente $f(l) \leq |A| - c'l \leq c' + g(l+1) = h(l)$ com $\lim_{l\to\infty} \frac{h(l)}{l} = 0$. Portanto $l \geq \frac{|A|}{c'} - \frac{h(l)}{c'}$ isto é

$$l \geq \frac{|A| - o(l)}{c'}. \tag{4.25}$$

Desse modo, das Expressões (4.24) e (4.25) segue-se que

$$l = \frac{\mid A \mid}{c'} - \frac{o(l)}{c'} = \frac{\mid A \mid}{c'} - o(l). \tag{4.26}$$

Por outro lado, se $M_i = \{x \in \mathbb{N}; \phi(x) \leq i\}$ e $M_{i-1} = \{x \in \mathbb{N}; \phi(x) \leq i-1\}$, por isso

$$\tilde{M}_i = M_i - M_{i-1} = \{x \in \mathbb{N}; \phi(x) = i\},$$

por conseguinte $M_n = \bigcup_{i=1}^{n} \tilde{M}_i$. Logo,

$$\begin{aligned}
\sum_{d\in M_n} \phi(d) &= \sum_{i=1}^{n} \sum_{d\in \tilde{M}_i} \phi(d) \\
&= \sum_{i=1}^{n} \sum_{d\in \tilde{M}_i} i \\
&= \sum_{i=1}^{n} i \mid \tilde{M}_i \mid \\
&= \sum_{i=1}^{n} i \left(\mid M_i \mid - \mid M_{i-1} \mid\right) \\
&= \sum_{i=1}^{n} i \mid M_i \mid - \sum_{i=1}^{n} i \mid M_{i-1} \mid \\
&= n \mid M_n \mid + \sum_{i=1}^{n-1} i \mid M_i \mid - \sum_{i=2}^{n} i \mid M_{i-1} \mid \\
&= n \mid M_n \mid + \sum_{i=1}^{n-1} i \mid M_i \mid - \sum_{j=1}^{n-1} (j+1)\cdot \mid M_j \mid \\
&= n \mid M_n \mid + \sum_{i=1}^{n-1} i \mid M_i \mid - \sum_{i=1}^{n-1} (i+1)\cdot \mid M_i \mid \\
&= n \mid M_n \mid - \sum_{i=1}^{n-1} \mid M_i \mid . \qquad (4.27)
\end{aligned}$$

Pela Equação, (4.22) segue-se que,

$$\begin{aligned}
\sum_{d\in M_n} \phi(d) &= n(c'n + o(n)) + \sum_{i=1}^{n-1} (c'i + o(i)) \\
&= c'n^2 - o(n^2) - \sum_{i=1}^{n-1} (c'i - o(n^2)) \\
&= c'n^2 - c'\frac{n(n-1)}{2} - o(n^2) \\
&= \frac{c'}{2}n^2 + c'\frac{n}{2} - o(n^2) \\
&= \frac{c'}{2}n^2 + o(n^2). \qquad (4.28)
\end{aligned}$$

A última igualdade segue do seguinte fato, $\lim_{n\to\infty} \frac{\frac{c'n}{2}}{n^2} = 0$ implica que, $\frac{c'n}{2} - o(n^2) = o(n^2)$.

Das Equações (4.23), (4.26), (4.27) e (4.28) segue-se finalmente,

$$\begin{aligned}\sum_{d\in A}\phi(d) &\geq \frac{c'}{2}\left(\frac{|A|}{c'}+o(\mid A\mid)\right)^2 - o\left(\frac{\mid A\mid}{c'}+o(\mid A\mid)\right)^2\\ &= \frac{\mid A\mid^2}{2c'}+\underbrace{\mid A\mid o(\mid A\mid)}_{o(|A|^2)}+\frac{o(\mid A\mid)^2c'}{2}-o(\mid A\mid^2)\\ &= \frac{\mid A\mid^2}{2c'}-o(\mid A\mid^2).\end{aligned}$$

□

Lema 4.24. *Seja A um conjunto finito de números naturais, seja $K =\mid A\mid$, e seja ϕ que denota a função Euler. Então*

$$\sum_{d\in A}(\phi(d)-log_2(d))\geq cK^2-o(K^2)$$

onde $c=\frac{\zeta(6)}{(2\zeta(2)\zeta(3))}\approx 0,25726$.

Demonstração. Uma propriedade da Função ϕ de Euler dada em [10, Theorem 3.28] é a seguinte

$$\liminf \phi(n)\frac{\log(\log(n))}{n}=e^{-\gamma}\approx 0,56, \tag{4.29}$$

reescrevendo a Expressão (4.29), tem-se

$$\liminf \frac{\phi(n)}{\frac{n}{\log(\log(n))}}=e^{-\gamma}.$$

Assim para $n >> 0$ segue-se

$$\frac{\phi(n)}{\frac{n}{\log(\log(n))}}\geq\frac{1}{2},$$

logo $\phi(n)\geq\frac{n}{2\log(\log(n))}$.
Como $\sqrt{n}\leq\frac{n}{2\log(\log(n))}$ para todo $n\in\mathbb{N}$ segue que para $d\in A$ grande suficiente,

$$\sqrt{d}\leq\frac{1}{2}\frac{d}{\log(\log(d))}\leq\phi(d),$$

daí $\log_2\sqrt{d}\leq log_2\phi(d)$, portanto $\frac{1}{2}\log_2(d)\leq log_2\phi(d)$, isto é

$$\log_2(d)\leq 2\log_2\phi(d).$$

Por isso,

$$\begin{aligned}\sum_{d\in A}(\phi(d)-\log_2(d)) &= \sum_{\substack{d\in A\\ \log_2 d\leq 2log_2\phi(d)}}(\phi(d)-\log_2(d))+\sum_{\substack{d\in A\\ \log_2 d>2log_2\phi(d)}}(\phi(d)-\log_2(d))\\ &\geq \sum_{\substack{d\in A\\ \log_2 d\leq 2\log_2\phi(d)}}(\phi(d)-2\log_2(d))+\sum_{\substack{d\in A\\ \log_2 d>2\log_2\phi(d)}}(\phi(d)-2log_2\phi(d)\\ &\quad -(\log_2 d-2\log_2\phi(d))\\ &= \sum_{d\in A}(\phi(d)-2\log_2(d))-\underbrace{\sum_{\substack{d\in A\\ \log_2 d>2\log_2\phi(d)}}\underbrace{(\log_2 d-2\log_2\phi(d))}_{<0}}_{=O(1)}\\ &= \sum_{d\in A}(\phi(d)-2\log_2(d))+O(1).\end{aligned}$$

Desse modo,

$$\sum_{d\in A}(\phi(d)-\log_2(d)\geq\sum_{d\in A}(\phi(d)-2\log_2(d))+O(1), \tag{4.30}$$

pelo argumento do Lema 4.23, tem-se existe $l\in\mathbb{N}$ maximal tal que $\mid M_l\mid\leq|A|$, e como $\phi(n)\leq n$ segue-se que,

$$\sum_{d\in M_l}\log_2(\phi(d))\leq\sum_{d\in M_l}\log_2(l)\leq\mid A\mid\cdot\log_2(l)\leq\mid A\mid\log_2(\mid A\mid). \tag{4.31}$$

Como a função $f:\mathbb{R}\to\mathbb{R}$ definida por $f(x)=x-\log_2(x)$ é crescente então,

$$\sum_{d\in M_l}(\phi(d)-2\log_2(\phi(d)))\leq\sum_{d\in A}(\phi(d)-2\log_2\phi(d)), \tag{4.32}$$

das Equações (4.31) e (4.32) tem-se,

$$\sum_{d\in A}(\phi(d)-2\log_2(\phi(d)))\geq\sum_{d\in A}\phi(d)-2\mid A\mid\log_2(\mid A\mid)-O(1).$$

Pelos Lemas 4.4 e 4.23 segue-se,

$$\begin{aligned}\sum_{d\in A}(\phi(d)-2\log_2(\phi(d))) &\geq \frac{1}{2c'}|A|^2-o(|A|^2)-2|A|\log_2(|A|)+O(1)\\ &= \frac{1}{2c'}|A|^2-o(|A|^2)-o(|A|^2)+o(|A|^2)\\ &= \frac{1}{2c'}|A|^2-o(|A|^2)\end{aligned}$$

Portanto,

$$\sum_{d\in A}(\phi(d)-\log_2(d))\geq\frac{1}{2c'}|A|^2-o(|A|^2).$$

□

O lema a seguir é dado em [11, Lemma 4.5]

Lema 4.25. *Para qualquer conjunto finito de números naturais A, denote por $\underset{d\in A}{\text{mmc}}$ o mínimo múltiplo comum dos elementos de A. Tem-se as seguintes três afirmações:*

i. $I_q^*(d;f) \leq \frac{\text{mdc}(q^d-1,n)}{d}$.

ii. $n \geq \dfrac{\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}(q^d-1)}{\prod\limits_{d\in A_{q,n,k}^{(f)}}(2d)}$.

iii. Se A é um conjunto finito de números naturais. Então

$$\frac{\underset{d\in A}{\text{mmc}}(q^d-1)}{\prod\limits_{d\in A}(2d)} \geq q^{c|A|^2-o(|A|^2)},$$

onde $c = \frac{\zeta(6)}{(2\zeta(2)\zeta(3))} \approx 0,25726$.

Demonstração. i Seja $g \in \mathbb{F}_q[x]$ um polinômio mônico irredutível de grau d, tal que $g \mid f$ e $g \mid x^n-1$, seja α uma raiz de g. Como g divide x^n-1, então $\alpha^n-1=0$, e dado que g é irredutível de grau d, pelos Lemas 1.6 e 1.7 tem-se $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n-1}=1$.

Seja $\hat{d} = \text{mdc}(q^n-1,n)$, assim existem $\gamma,\beta \in \mathbb{Z}$ tal que $\hat{d} = \gamma(q^n-1)+\beta(n)$, logo

$$\alpha^{\hat{d}} = \alpha^{\gamma(q^n-1)+\beta(n)} = \alpha^{(q^n-1)\gamma}\alpha^{\beta(n)} = \left(\alpha^{q^n-1}\right)^{\gamma}(\alpha^n)^{\beta} = 1.$$

Isto implica que $\alpha^{\text{mdc}(q^n-1,n)}=1$. Como em um corpo qualquer o polinômio x^t-1 têm no máximo t raízes diferentes, então $x^{\text{mdc}(q^n-1,n)}-1$ tem no máximo $\text{mdc}(q^n-1,n)$ raízes, desse modo, existem no máximo $\text{mdc}(q^n-1,n)$ possíveis α´s.

Por outro lado, tem-se que g possuí d raízes diferentes. De fato, suponha que existe uma raiz α com multiplicidade $t<d$ de modo que,

$$\theta x^{n-t} = \frac{d^t(x^{n-1})}{dx^t} = g(x)h_1(x)+\cdots+q^t(x)h_t(x)$$

com $\theta = n(n-1)\ldots(n-t)$.

Logo,

$$\theta x^{n-t} - g(x)h_1(x) - \cdots - g^{(t-1)}(x)h_{t-1}(x) = g^t(x)h_t(x),$$

assim pelo Teorema 1.12 tem-se $\theta\alpha^{n-t}=0$, portanto $\alpha=0$ o que é uma contradição.

Tem-se também que os g´s não tem raízes em comum, já que se α é raiz de g_1 e g_2 segue-se $\alpha^q,\ldots,\alpha^{q^d-1}$ são raízes de g_1 e g_2, portanto, $g_1=g_2$ que é uma contradição, porque os g´s são diferentes. Como os g´s tem exatamente d raízes diferentes e os g´s não têm raízes em comum, segue-se que

$$dI_q^*(d;f) \leq \text{mdc}(q^d-1,n).$$

Desse modo,

$$I_q^*(d;f) \leq \frac{\text{mdc}(q^d-1,n)}{d}.$$

ii. Da Definição 4.15 e do item i. tem-se,

$$\frac{\text{mdc}(q^d-1,n)}{d} > \frac{q^d-1}{2d^2}.$$

Logo,

$$\text{mdc}(q^d-1,n) > \frac{q^d-1}{2d}, \tag{4.33}$$

o $\text{mdc}(q^d-1,n)$ é um divisor de q^d-1, assim existe $a_d \mid q^d-1$ tal que,

$$\text{mdc}(q^d-1,n) = \frac{q^{d-1}}{a_d}. \tag{4.34}$$

Das Equações (4.33) e (4.34) obtém-se,

$$\frac{q^d-1}{2d} < \frac{q^d-1}{a_d},$$

assim, $2d > a_d$.

Como $\frac{q^d-1}{a_d}$ divide a n para todo $d \in A_{q,n,k}^{(f)}$, por isso $\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\left(\frac{q^d-1}{a_d}\right)$ divide a n.

Por outro lado,

$$\begin{aligned}\prod_{d\in A_{q,n,k}^{(f)}} a_d\left(\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\left(\frac{q^d-1}{a_d}\right)\right) &= \underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\left(\frac{\prod a_d(q^d-1)}{a_d}\right)\\ &\geq \underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\ (q^d-1),\end{aligned}$$

portanto

$$\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\left(\frac{q^d-1}{a_d}\right) \geq \frac{\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\ (q^d-1)}{\prod\limits_{d\in A_{q,n,k}^{(f)}} a_d}. \tag{4.35}$$

Como $a_d < 2d$ então $\prod\limits_{d\in A_{q,n,k}^{(f)}} a_d < \prod\limits_{d\in A_{q,n,k}^{(f)}} 2d$.

Da Equação (4.35) segue-se,

$$n \geq \underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\left(\frac{q^d-1}{a_d}\right) \geq \frac{\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\ (q^d-1)}{\prod\limits_{d\in A_{q,n,k}^{(f)}} a_d} \geq \frac{\underset{d\in A_{q,n,k}^{(f)}}{\text{mmc}}\ (q^d-1)}{\prod\limits_{d\in A_{q,n,k}^{(f)}} 2d}.$$

iii. Seja $Q_n \in \mathbb{Q}[z]$ o n-ésimo polinômio ciclotômico pelo Lema 4.20, tem-se

$$\underset{d\in A}{\text{mmc}}(q^d-1) = \prod_{\{e\mid \exists d\in A; e\mid d\}} Q_e(q) \geq \prod_{d\in A} Q_d(q). \tag{4.36}$$

Como $q \geq 2$ e $Q_d(q) \geq \frac{1}{4}q^{\phi(d)}$ pelo Lema 4.22, segue

$$\prod_{d\in A} Q_d(q) \geq \prod_{d\in A} \frac{q^{\phi(d)}}{4} \geq \prod_{d\in A} q^{\phi(d)-2}, \tag{4.37}$$

pelas Equações (4.36) e (4.37) obtém-se,

$$\operatorname*{mmc}_{d\in A}(q^d-1) \geq \prod_{d\in A} q^{\phi(d)-2}.$$

Logo,

$$\begin{aligned}
\frac{\operatorname*{mmc}_{d\in A}(q^d-1)}{\prod_{d\in A} 2d} &\geq \frac{\prod_{d\in A} q^{\phi(d)-2}}{\prod_{d\in A} 2d} \\
&\geq \frac{\prod_{d\in A} q^{\phi(d)-2}}{\prod_{d\in A} qd} \\
&\geq \frac{\prod_{d\in A} q^{\phi(d)-3}}{\prod_{d\in A} q^{log_2(d)}} \\
&= \prod_{d\in A} q^{\phi(d)-log_2(d)-3} \\
&= q^{\sum_{d\in A}(\phi(d)-log_2(d)-3)} \\
&= q^{\sum_{d\in A}(\phi(d)-log_2(d))} q^{\sum_{d\in A}-3} \\
&\underbrace{\geq}_{Lema\ 4.24} q^{c|A|^2-o(|A|^2)+\sum_{d\in A}-3} \\
&= q^{c|A|^2-o(|A|^2)},
\end{aligned}$$

a última igualdade segue do seguinte fato $\sum_{d\in A} -3 = -3 \mid A \mid$, e como $\lim_{|A|\to\infty} \frac{3 \mid A \mid}{\mid A \mid^2} = 0$, segue que $3 \mid A \mid = o(\mid A \mid^2)$, assim pelo Lema 4.4 tem-se $\sum_{d\in A} -3 = -o(\mid A \mid^2)$.

□

4.3.2 Densidade dos elementos normais e k-normais

Nesta subseção apresenta-se finalmente o terceiro objetivo deste trabalho, que consiste em apresentar um limite inferior númerico da densidade tanto de elementos normais, como de elementos k-normais (Teoremas 4.26 e 4.28), respectivamente.

Teorema 4.26. *Existe uma constante $d > 0$ tal que, para toda potência de primo q e todo inteiro positivo $n \geq 2$. Tem-se*

$$\kappa(x^n-1) \geq \frac{d}{\sqrt{\lceil \log_q(n) \rceil}},$$

onde $\lceil x \rceil$ é a função teto de x (o menor inteiro maior ou igual a x).

Demonstração. Dados q, n, e tomando $f = x^n - 1$ e $k = 0$, tem-se duas possibilidades: ou $A^{(f)}_{q,n,k} = \emptyset$ ou $A^{(f)}_{q,n,k} \neq \emptyset$.
Caso 1. Se $A^{(f)}_{q,n,k} = \emptyset$ pelo Lema 4.17, e considerando $e^{-\frac{\zeta(2)}{2}} \approx 0,43935$, tem-se

$$\kappa(x^n - 1) \geq e^{-\frac{\zeta(2)}{2}} > 0,28477 > \frac{0,28477}{\sqrt{\lceil log_q(n) \rceil}},$$

já que $\sqrt{log_q(n)} \geq 1$.
Caso 2. Se $A^{(f)}_{q,n,k} \neq \emptyset$ pelo Lema 4.25, tem-se

$$n \geq \frac{\underset{d \in A^{(f)}_{q,n,k}}{\text{mmc}} (q^d - 1)}{\prod\limits_{d \in A^{(f)}_{q,n,k}} 2d}, \tag{4.38}$$

e

$$\frac{\underset{d \in A^{(f)}_{q,n,k}}{\text{mmc}} (q^d - 1)}{\prod\limits_{d \in A^{(f)}_{q,n,k}} 2d} \geq q^{c|A^{(f)}_{q,n,k}|^2 - o(|A^{(f)}_{q,n,k}|^2)}, \tag{4.39}$$

onde $c = \frac{\zeta(6)}{2\zeta(2)\zeta(3)} > 0,257255$.

Pelas Equações (4.38) e (4.39) segue que,

$$n \geq q^{c|A^{(f)}_{q,n,k}|^2 - o(|A^{(f)}_{q,n,k}|^2)},$$

logo $\log_q(n) \geq c \mid A^{(f)}_{q,n,k} \mid^2 - o(\mid A^{(f)}_{q,n,k} \mid^2)$. Dessa forma,

$$o(\mid A^{(f)}_{q,n,k} \mid^2) \geq c \mid A^{(f)}_{q,n,k} \mid^2 - \log_q(n),$$
$$\frac{o(\mid A^{(f)}_{q,n,k} \mid^2)}{\mid A^{(f)}_{q,n,k} \mid^2} \geq c - \frac{\log_q(n)}{\mid A^{(f)}_{q,n,k} \mid^2}.$$

Pela definição de o-pequena o lado direito da última desigualdade tende a 0 quando $\mid A^{(f)}_{q,n,k} \mid$ tende ao infinito. Portanto, dado $c' < c$ e tomando $\varepsilon = c - c'$, existe $C_1 > 0$ tal que se $\mid A^{(f)}_{q,n,k} \mid > C_1$, então $c - \frac{\log_q(n)}{|A^{(f)}_{q,n,k}|^2} < \varepsilon = c - c'$. Dessa desigualdade, obtém-se imediatamente, $\log_q(n) > c' \mid A^{(f)}_{q,n,k} \mid^2$ e daí, $\mid A^{(f)}_{q,n,k} \mid < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}}$.

Se $\mid A^{(f)}_{q,n,k} \mid \leq C_1$, então escolhendo n suficientemente grande de forma que $C_1 < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}}$ e assim, também tem-se $\mid A^{(f)}_{q,n,k} \mid < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}}$. Como

$$C_1 < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}} \iff c' C_1^2 < \log_q(n) \iff n > q^{c' C_1^2},$$

logo se $n > q^{c' C_1^2}$ e $\mid A^{(f)}_{q,n,k} \mid \leq C_1$, então $\mid A^{(f)}_{q,n,k} \mid < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}}$. Em outras palavras em todos os casos se $n > q^{c' C_1^2}$, então $\mid A^{(f)}_{q,n,k} \mid < \frac{\sqrt{\log_q(n)}}{\sqrt{c'}}$.

Considere agora $c'' > 0$ tal que $c' < c'' < c$. Pelo que acaba-se de provar existe $C_2 > 0$ tal que se $n > q^{c''C_2^2}$, então $\frac{\sqrt{\log_q(n)}}{\sqrt{c''}} > \mid A_{q,n,k}^{(f)} \mid$.

Por outro lado, como $\lim_{x\to\infty} e^{-\frac{1}{x}} = 1$ e $e^{-\frac{1}{x}} < 1$, tem-se que existe $C_3 > 0$ tal que, se $\mid A_{q,n,k}^{(f)} \mid > C_3$, então

$$\frac{\sqrt{c'}}{\sqrt{c''}} < e^{-\frac{1}{|A_{q,n,k}^{(f)}|}} < 1.$$

Assim, se $n > q^{c'C_1^2}$, $n > q^{c''C_2^2}$ e $\mid A_{q,n,k}^{(f)} \mid > C_3$ pelo Lema 4.17, então

$$\kappa(x^n - 1) \geq e^{-\gamma} \cdot e^{-\frac{1}{|A_{q,n,k}^{(f)}|}} \cdot \frac{1}{\mid A_{q,n,k}^{(f)} \mid} > e^{-\gamma} \cdot \frac{\sqrt{c'}}{\sqrt{c''}} \cdot \frac{\sqrt{c''}}{\sqrt{\log_q(n)}} = \frac{e^{-\gamma}\sqrt{c'}}{\sqrt{\log_q(n)}}.$$

Vejamos o que acontece se $\mid A_{q,n,k}^{(f)} \mid \leq C_3$. Como a função $\frac{1}{x}e^{-1/x}$ é decrescente para $x > 0$, então

$$\frac{e^{-\frac{1}{|A_{q,n,k}^{(f)}|}}}{\mid A_{q,n,k}^{(f)} \mid} > \frac{e^{-\frac{1}{C_3}}}{C_3}.$$

Observe que

$$\frac{e^{-\frac{1}{C_3}}}{C_3} > \frac{\sqrt{c'}}{\sqrt{\log_q(n)}} \iff \log_q(n) > c' \cdot C_3^2 \cdot e^{\frac{2}{C_3}} \iff n > q^{c' \cdot C_3^2 \cdot e^{\frac{2}{C_3}}}.$$

Assim, se $n > q^{C_1^2 \cdot c'}$, $n > q^{c'' \cdot C_2^2}$ e $n > q^{c' \cdot C_3^2 e^{\frac{2}{C_3}}}$, tem-se $\kappa(x^n - 1) \geq \frac{e^{-\gamma}\sqrt{c'}}{\sqrt{\log_q(n)}}$. Consequentemente, existe um inteiro positivo C_4 tal que se $n > q^{C_4}$, então

$$\kappa(x^n - 1) \geq \frac{e^{-\gamma}\sqrt{c'}}{\sqrt{\log_q(n)}} \geq \frac{e^{-\gamma}\sqrt{c'}}{\sqrt{\lceil \log_q(n) \rceil}}.$$

Para finalmente demonstrar o teorema, usamos o Teorema 4.2. Define-se

$$d = \min\left\{ \frac{1}{e\sqrt{C_4}}, e^{-\gamma}\sqrt{c'} \right\}.$$

já foi provado que para $n > q^{C_4}$, tem-se

$$\kappa(x^n - 1) \geq \frac{d}{\sqrt{\lceil \log_q(n) \rceil}}.$$

Para $n \leq q^{C_4}$ tem-se $\lceil \log_q(n) \rceil \leq C_4$. Dessa forma pelo Teorema 4.2, obtém-se

$$\frac{d}{\sqrt{\lceil \log_q(n) \rceil}} \leq \frac{1}{e\sqrt{C_4}\sqrt{\lceil \log_q(n) \rceil}} \leq \frac{1}{e\lceil \log_q(n) \rceil} \leq \kappa(x^n - 1).$$

Isso prova o Teorema. □

Como corolário podemos deduzir um limitante inferior explícito da densidade para n suficientemente grande.

Corolário 4.27. *Seja q uma potência de primo. Então,*

$$\liminf_{n\to\infty} \kappa(x^n-1) \geq \frac{0,28477}{\sqrt{\log_q(n)}}.$$

Demonstração. Da prova do teorema anterior tem-se que se $A_{q,n,k}^{(f)} = \emptyset$, então

$$\kappa(x^n-1) > 0,28477 > \frac{0,28477}{\sqrt{\log_q(n)}},$$

para $n > q$. Já para $A_{q,n,k}^{(f)} \neq \emptyset$ e $n > q^{C_4}$, tem-se

$$\kappa(x^n-1) \geq \frac{e^{-\gamma}\sqrt{c'}}{\sqrt{\log_q(n)}},$$

onde c' é próximo de c e C_4 depende do c' escolhido. Como $c = \frac{\zeta(6)}{2\zeta(2)\zeta(3)} > 0,257255$ pode-se escolher $c' = 0,257255$ e nesse caso,

$$e^{-\gamma}\sqrt{c'} > 0,28477.$$

Conclui-se que para $n > q^{C_4}$, tem-se

$$\kappa(x^n-1) \geq \frac{0,28477}{\sqrt{\log_q(n)}}.$$

Isso prova o corolário. □

O seguinte teorema, dado em [11, Theorem 4.6], é uma consequência do Teorema 4.26. Este resultado exibe um limite inferior da densidade para elementos k-normais. A prova deste resultado é essencialmente a mesma demonstração do Teorema 4.26.

Teorema 4.28. *Existe uma constante C tal que para todo $q \geq 2$ e $n > q^C$, o número de elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é pelo menos*

$$0,28477q^{n-k}\frac{c_{n-k}}{\sqrt{\log_q(n)}},$$

onde c_{n-k} é o número de fatores mônicos de x^n-1 de grau $n-k$ definidos em $\mathbb{F}_q[x]$.

Demonstração. Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau $n-k$ que divide x^n-1. A densidade do polinômio f é

$$\kappa(f) = \Phi_q(f)q^{-(n-k)}. \tag{4.40}$$

A demonstração do Teorema 4.26 e do Corolário 4.27 foi feita tomando $f = x^n-1$, mas pode-se seguir o mesmo raciocínio para qualquer polinômio f que divida x^n-1. Dessa forma, existe uma constante $C > 0$ tal que para todo $n > q^C$, tem-se

$$\kappa(f) \geq \frac{0,28477}{\sqrt{\log_q(n)}}.$$

Assim, pela Equação (4.40) tem-se que o número de elementos k normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é no mínimo,

$$0,28477q^{n-k}\frac{c_{n-k}}{\sqrt{\log_q(n)}}.$$

□

4.4 Limite superior para a densidade dos elementos k-normais.

Nesta seção apresenta-se o quarto objetivo deste trabalho onde exibe-se um limite superior da densidade para os elementos normais e k-normais, estes resultados são dados [11, Theorem 4.7 and Corollary 4.8] e provados em [6, Theorem 5]

Com essa motivação apresenta-se a seguinte definição.

Definição 4.29. Para uma potência prima q dada, defina a **sequência infinita** $\{n_t\}_{t=1}^{\infty}$ por

$$n_t = \operatorname{mmc}_{d=1}^{t}(q^d - 1).$$

Os seguintes lemas são uma consequência da definição anterior e são necessários para provar os teoremas que dão um limite superior da densidade para os elementos normais e k-normais (Teorema 4.34 e Corolário 4.35).

Lema 4.30. *Para n_t definido acima,*

$$I_q^*(d; x^{n_t} - 1) = I_q^*(d) \quad \textit{para todo } d \leq t.$$

Demonstração. Pelo Lema 1.15, tem-se que todo polinômio de grau d irredutível divide o polinômio $x^{q^d-1}-1$. Como x^a-1 divide $x^{ab}-1$ para todos $a, b \in \mathbb{Z}$. Logo, $x^{q^d-1}-1$ divide $x^{n_k}-1$. Assim, todo polinômio de grau d irredutível divide $x^{n_k}-1$. Portanto, $I_q^*(d; x^{n_t}-1) = I_q^*(d)$. □

Lema 4.31. *Seja ϕ que denota a função de Euler. Então,*

$$\sum_{d=1}^{t} \phi(d) = ct^2 + O((t)\log(t)),$$

onde $c = \frac{1}{2\zeta(2)} \approx 0,30396$.

Demonstração. Pelas propriedades da $\phi(n)$ tem-se,

$$\begin{aligned}
\phi(n) &= n\sum_{d|n} \frac{\mu(d)}{d} \\
&= \sum_{d|n} \frac{n}{d}\mu(d) \\
&= \sum_{d|n} d\mu\left(\frac{n}{d}\right) \\
&= \sum_{dd'\leq n} d'\mu(d).
\end{aligned}$$

Veja [10, página 235] para mais detalhes.

Assim,

$$\begin{aligned}
\sum_{d=1}^{t} &= \sum_{dd' \leq t} d'\mu(d) \\
&= \sum_{d=1}^{t} \mu(d) \sum_{d'=1}^{\frac{t}{d}} d' \\
&= \frac{1}{2} \sum_{d=1}^{t} \mu(d) \left(\left(\frac{t}{d} \right)^2 + \frac{t}{d} \right) \\
&= \frac{1}{2} \sum_{d=1}^{t} \mu(d) \left(\frac{t^2}{d^2} + O\left(\frac{t}{d} \right) \right) \quad \text{porque } \frac{t}{d} \leq 1 \cdot \frac{t}{d} \\
&= \frac{1}{2} t^2 \sum_{d=1}^{t} \frac{\mu(d)}{d^2} + \underbrace{O\left(\frac{t}{2} \sum_{d=1}^{t} \frac{1}{d} \right)}_{\textit{Lema } 4.4} \\
&= \frac{t^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \frac{t^2}{2} \sum_{d=t+1}^{\infty} \frac{\mu(d)}{d^2} + O\left(\frac{t}{2} \sum_{d=1}^{t} \frac{1}{d} \right) \\
&= \frac{1}{2} t^2 \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + \underbrace{O\left(t^2 \sum_{d=t+1}^{\infty} \frac{1}{d^2} \right)}_{\textit{Lema } 4.4} + \underbrace{O(t(\log(t)))}_{\textit{Lema } 4.4} \\
&= \underbrace{\frac{t^2}{2\epsilon(2)}}_{\text{Teo } 4.8} + \underbrace{\underbrace{O(t)}_{\textit{Lema } 4.4} + O(t(\log(t)))}_{\textit{Lema } 4.4} \\
&= ct^2 + O(t(\log(t))).
\end{aligned}$$

□

Lema 4.32. *Para toda potência de primo q, para todo inteiro $t > 0$ e n_t como na Definição 4.29, segue que*

$$\log_q(n_t) = ct^2 + O((t)\log(t)),$$

onde $c = \frac{1}{2\zeta(2)} = \frac{3}{\pi^2} \approx 0,30396$.

Demonstração. Pela Definição 4.29 e pelo Lema 4.20, pode-se expressar n_t em termos de polinômios ciclotômicos como segue,

$$n_t = \prod_{d=1}^{t} Q_d(q).$$

Pelo Lema 4.22 tem-se,

$$\prod_{d=1}^{t} Q_d(q) \leq \prod_{d=1}^{t} 4q^{\phi(d)}.$$

Assim

$$\begin{aligned}
\log_q(n_t) &\leq \log_q \prod_{d=1}^{t} 4q^{\phi(d)} \\
&= \log_q \left(4^t q^{\sum_{d=1}^{t}\phi(d)}\right) \\
&= \log_q(4^t) + \log_q \left(q^{\sum_{d=1}^{t}\phi(d)}\right) \\
&= \sum_{d=1}^{t}\phi(d) + \log_q(4^t) \\
&\underbrace{=}_{Def\ 4.3} \sum_{d=1}^{t}\phi(d) + O(t) \\
&\underbrace{=}_{Lema\ 4.31} ct^2 + O(t\log(t)) + O(t) \\
&\underbrace{=}_{Lema\ 4.4} ct^2 + O(t\log(t)). \qquad (4.41)
\end{aligned}$$

Por outro lado, pelo Lema 4.22, tem-se

$$\prod_{d=1}^{t} Q_d(q) \geq \prod_{d=1}^{t} \frac{1}{4} q^{\phi(d)}.$$

Logo,

$$\begin{aligned}
\log_q(n_t) &\geq \log_q \prod_{d=1}^{t} \frac{1}{4} q^{\phi(d)} \\
&= \log_q \left(\frac{1}{4^t} q^{\sum_{d=1}^{t}\phi(d)}\right) \\
&= \log_q \left(\frac{1}{4^t}\right) + \log_q \left(q^{\sum_{d=1}^{t}\phi(d)}\right) \\
&= \sum_{d=1}^{t}\phi(d) + \log_q \left(\frac{1}{4}\right)^t \\
&\underbrace{=}_{Def\ 4.3} \sum_{d=1}^{t}\phi(d) + O(t) \\
&\underbrace{=}_{Lema\ 4.31} ct^2 + O(t\log(t)) + O(t) \\
&\underbrace{=}_{Lema\ 4.4} ct^2 + O(t\log(t)). \qquad (4.42)
\end{aligned}$$

Portanto, das Expressões (4.41) e (4.42), tem-se

$$\log_q(n_t) = ct^2 + O(t\log(t)).$$

□

Lema 4.33. *Seja* $f \in \mathbb{F}_q[x]$ *tal que* $\text{grau}(f) = n_t$. *Então,*

$$\kappa(f) \leq \frac{1,12292}{t}.$$

Demonstração. Usando a caracterização de Φ tem-se que

$$\kappa(n_t) = \prod_{d=1}^{n_t} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d;x^{n_t}-1)}.$$

Pelo Lema 4.30, segue que $I_q^*(d; x^{n_t} - 1) = I_q^*(d)$. Logo,

$$\kappa(n_t) = \prod_{d=1}^{n_t} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d)}. \tag{4.43}$$

Considere inicialmente o caso $q = 2$. Usando SageMath e o Algoritmo 3, temos

$$\kappa(\ell) = \prod_{d=1}^{l} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d)} \leq \frac{1,1215168}{l} \text{para } l \leq 400,\ q = 2.$$

Algoritmo 1: Cálculo de $I_q^*(d)$

Entrada: Um primo q e um inteiro positivo $d \geq 1$
Saída: $I_q^*(d)$

```
se d > 1 então
    A = Σ_{r|d} μ(r) · q^{d/r}
senão
    A = q − 1
fim
retorna A
```

Algoritmo 2: Produto $\ell \cdot \kappa(\ell)$ (ver equação (4.43))

Entrada: Um primo q e um inteiro positivo L
Saída: $prod(q, L)$

```
d = 1
S = I_q^*(d) · log(1 − 1/q^d)
para d ∈ {2, ..., L + 1} faça
    S = S + I_q^*(d) · log(1 − 1/q^d)
    Pr = e^S · L
fim
retorna Pr
```

Algoritmo 3: Valor máximo do produto $\ell \cdot \kappa(\ell)$ (ver equação (4.43))

Entrada: Um primo q e um inteiro positivo $N \geq 2$
Saída: Valor máximo de $prod(q, L)$ para $2 \leq L \leq N$

```
M = (1 − 1/q)^{I_q^*(1)}
para L ∈ {2, ... N} faça
    M = max{M, prod(q, L)}
fim
retorna M
```

Agora será provado que,

$$\prod_{d=l}^{t} \left(1 - \frac{1}{q^d}\right)^{I_q^*(d)} \leq \frac{1,0012508}{t} \text{para } l \geq 400,\ q = 2, \tag{4.44}$$

para mostrar a Equação (4.44) veja que

$$\begin{aligned}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} &= \left(\left(1-\frac{1}{q^d}\right)^{q^d}\right)^{\frac{I_q^*(d)}{q^d}} \\ &\leq e^{-\frac{I_q^*(d)}{q^d}}.\end{aligned}$$

Em [1, Theorem 6.51] Bach e Shallit mostraram que,

$$\frac{I_q^*(d)}{q^d} \leq \frac{1}{d} - \frac{2}{d}(\sqrt{q})^{-d},$$

portanto

$$\begin{aligned}\prod_{d=l+1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} &\leq e^{-\sum_{d=l+1}^{t}\frac{I_q^*(d)}{q^d}} \\ &\leq e^{-\sum_{d=l+1}^{t}\frac{1}{d}-\frac{2}{d}(\sqrt{q})^{-d}}.\end{aligned}$$

Assim,

$$\prod_{d=l+1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} \leq e^{-\sum_{d=l+1}^{t}\frac{1}{d}-\frac{2}{d}(\sqrt{q})^{-d}}, \tag{4.45}$$

como

$$\begin{aligned}\left(\frac{1}{d+1}\right)+\frac{1}{2}\left(\frac{1}{d}-\frac{1}{d+1}\right) &= \frac{1}{2}\left(\frac{1}{d}+\frac{1}{d+1}\right) \\ &\geq \int_d^{d+1}\frac{1}{x}dx.\end{aligned}$$

Portanto,

$$\begin{aligned}\sum_{d=l}^{t-1}\frac{1}{2}\left(\frac{1}{d}+\frac{1}{d+1}\right) &= \frac{1}{l}+\sum_{d=l+1}^{t}\left(\frac{1}{d}\right)-\frac{1}{2t} \\ &\geq \int_l^t\frac{1}{x}dx,\end{aligned}$$

desse modo

$$\begin{aligned}\sum_{d=l+1}^{t}\frac{1}{d} &\geq \ln\left(\frac{t}{l}\right)-\frac{1}{2l}+\frac{1}{2t} \\ &> \ln\left(\frac{t}{l}\right)-\frac{1}{2l}.\end{aligned}$$

Tem-se também,

$$\begin{aligned}
\sum_{d=l+1}^{t} \frac{2(\sqrt{q})^{-d}}{d} &< \frac{2}{l+1}\sum_{d=l+1}^{t}(\sqrt{q})^{-d} \\
&< \frac{2}{l+1}\sum_{d=l+1}^{\infty}(\sqrt{q})^{-d} \\
&< \frac{2}{l+1}(\sqrt{q})^{-(l+1)}\sum_{d=0}^{\infty}(\sqrt{q})^{-d} \\
&= \frac{2}{l+1}\frac{(\sqrt{q})^{-l}}{\sqrt{q}}\frac{1}{1-\frac{1}{\sqrt{q}}} \\
&= \frac{2}{l+1}\frac{(\sqrt{q})^{-l}}{(\sqrt{q}-1)} \\
&< \frac{2}{l+1}\frac{(\sqrt{q})^{-1}}{(\sqrt{q}-1)},
\end{aligned}$$

assim da Equação (4.45) tem-se

$$\begin{aligned}
e^{-\sum_{d=l+1}^{t}\frac{1}{d}-\frac{2}{d}(\sqrt{q})^{-d}} &< e^{-\ln\left(\frac{t}{l}\right)+\frac{1}{2l}+\frac{2}{l+1}\frac{(\sqrt{q})^{-1}}{\sqrt{q}-1}} \\
&= \frac{l}{t}e^{\frac{1}{2l}+\frac{2}{l+1}\frac{(\sqrt{q})^{-1}}{\sqrt{q}-1}} \\
&\leq \frac{l}{t}1,0012508 \text{ para } l \geq 400,\ q \geq 2.
\end{aligned}$$

Combinando as Equações (4.43) e (4.44) tem-se

$$\begin{aligned}
\prod_{d=1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} &\leq \frac{(1,1215168)(1,0012508)}{t} \\
&\leq \frac{1,12292}{t}.
\end{aligned}$$

Usando o programa algébrico SageMath pode-se mostrar que

$$\prod_{d=1}^{l}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} \leq 0,63\frac{1}{l}, \text{ para } l \leq 2 \text{ e } q \geq 3. \tag{4.46}$$

De acordo com o Algoritmo 2 e usando SageMath, exibem-se os seguintes gráficos. O gráfico da Figura 4.1 mostra que para $l = 1$ e $3 \leq q \leq 100$ (abcissas), o produto do lado esquerdo da Equação (4.46) é menor que $0,5$.

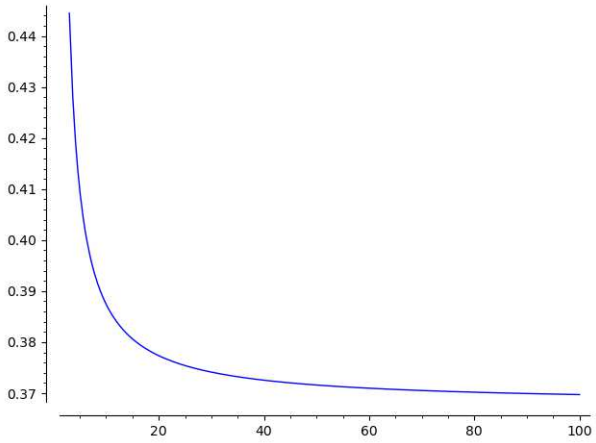

Figura 4.1: $l = 1$ e $3 \leq q \leq 100$

O gráfico da Figura 4.2 mostra que para $l = 2$ e $3 \leq q \leq 100$ (abcissas), o produto do lado esquerdo da Equação (4.46) é menor que $0,31$.

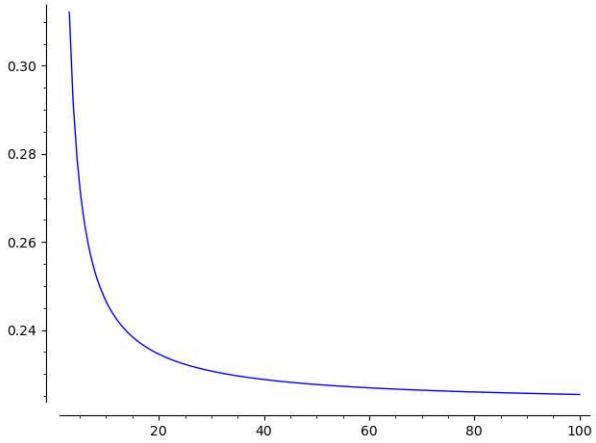

Figura 4.2: $l = 2$ e $3 \leq q \leq 100$,

Por outro lado, tem-se que

$$\begin{aligned}\prod_{d=l+1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} &= \prod_{d=l+1}^{t}\left(\left(1-\frac{1}{q^d}\right)^{q^d}\right)^{\frac{I_q^*(d)}{q^d}} \\ &\leq e^{-\sum_{d=l+1}^{t}\frac{I_q^*(d)}{q^d}} \\ &\leq e^{-\sum_{d=l+1}^{t}\frac{1}{d}-\frac{2}{d}(\sqrt{q})^{-d}},\end{aligned}$$

como

$$\begin{aligned}\left(\frac{1}{d+1}\right)+\frac{1}{2}\left(\frac{1}{d}-\frac{1}{d+1}\right) &= \frac{1}{2}\left(\frac{1}{d}+\frac{1}{d+1}\right) \\ &\geq \int_d^{d+1}\frac{1}{x}dx.\end{aligned}$$

Assim,

$$\sum_{d=l+1}^{t}\frac{1}{d} > \ln\left(\frac{t}{l}\right)-\frac{1}{2}l$$

e

$$\begin{aligned}\sum_{d=l+1}^{t}\frac{2(\sqrt{q})^{-d}}{d} &< \frac{2}{l+1}(\sqrt{q})^{-(l+1)}\\ &= \frac{2(\sqrt{q})^{-l}}{(l+1)(\sqrt{q}-1)}\\ &< \frac{2(\sqrt{q})^{-1}}{(l+1)(\sqrt{q}-1)}.\end{aligned}$$

Portanto,

$$\begin{aligned}e^{-\sum_{d=l+1}^{t}\frac{1}{d}-\frac{2}{d}(\sqrt{q})^{-d}} &< \frac{l}{t}e^{\frac{1}{2l}+\frac{2(\sqrt{q})^{-1}}{(l+1)(\sqrt{q}-1)}}\\ &\leq \frac{l}{t}(1,75),\end{aligned}$$

isto é

$$\prod_{d=l+1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} \leq \frac{l}{t}(1,75) \quad l\geq 3 \text{ e } q\geq 3. \tag{4.47}$$

Então, das Expressões (4.46) e (4.47) tem-se

$$\begin{aligned}\prod_{d=l+1}^{t}\left(1-\frac{1}{q^d}\right)^{I_q^*(d)} &\leq \frac{(1,75)(0,63)}{t}\\ &= \frac{1,1025}{t}\\ &< \frac{1,12292}{t}.\end{aligned}$$

□

A seguir apresentam-se os resultados que dão um limite superior da densidade para os elementos normais e k-normais que completam o quarto objetivo do trabalho.

Teorema 4.34. *Se n_t é como na Definição 4.29, então para toda potência de primo q e para todo inteiro t,*

$$\kappa(x^{n_t}-1) < \frac{0,61910}{\sqrt{\log_q(n_t)}}.$$

Demonstração. Do Lema 4.32, tem-se que

$$\log_q(n_t) = \underbrace{c't^2}_{>0} + \underbrace{O(t\log(t))}_{<0},$$

onde $c' = \frac{1}{2\zeta(2)} \approx 0,30396$. Logo, $\log_q(n_t) \leq c't^2$, então $\frac{1}{t^2} \leq \frac{c'}{\log_q(n_t)}$. Assim,

$$\frac{1}{t} \leq \sqrt{\frac{c'}{\log_q(n_t)}} = \frac{1}{\sqrt{2\zeta(2)}\sqrt{\log_q(n_t)}} \leq \frac{c}{\sqrt{\log_q(n_t)}}$$

para $c > 0,55133 > \frac{1}{\sqrt{2\zeta(2)}}$ e pelo Lema 4.33 sabe-se

$$\kappa(x^{n_t} - 1) \leq \frac{1,12292}{t} \leq \frac{1,12292c}{\sqrt{\log_q(n_t)}}.$$

Assim,

$$\kappa(x^{n_t-1})\sqrt{\log_q(n_t)} \leq (1,12292)(0,55133) = 0,61910$$

portanto,

$$\kappa(x^{n_t} - 1) \leq \frac{0,61910}{\sqrt{\log_q(n_t)}}.$$

□

Corolário 4.35. *Para qualquer inteiro t, seja n_t como na Definição 4.29. Então, o número de elementos k-normais de $\mathbb{F}_{q^{n_t}}$ é no máximo*

$$\frac{0,61910\left(q^{n_t-k}\right)(c_{n_t-k})}{\sqrt{\log_q(n_t)}}.$$

Demonstração. Seja $f \in \mathbb{F}_q[x]$ tal que $f \mid x^{n_t} - 1$, grau$(f) = n_t - k$. Como $\kappa(f) = \frac{\Phi(f)}{q^{n_t-k}}$, então pelos Teoremas 3.8 e 4.34 tem-se que o número de elementos k-normais de $\mathbb{F}_{q^{n_t}}$ é no máximo

$$\frac{0,61910\left(q^{n_t-k}\right)(c_{n_t-k})}{\sqrt{\log_q(n_t)}},$$

onde c_{n_t-k} é o número de polinômios de grau $n_t - k$. □

Capítulo 5

Questões de existência para elementos 1-normais primitivos

Uma extensão importante do teorema da base normal é o Teorema da base normal primitiva (veja Teorema 2.9) o qual estabelece que para todos os pares (q, n), existe um elemento primitivo α que gera uma base normal $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Que pode-se dizer acerca dos elementos k-normais para valores não nulos de k? Em particular, quando $k = 1$, existe um elemento 1-normal primitivo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$?.

Neste capítulo apresenta-se um resultado de existência para elementos 1-normais primitivos para todo $q \geq 3$ e $n \geq 6$ no caso que q e n sejam coprimos. Este resultado é dado em [11, Theorem 5.10], e generaliza o Teorema 5.29 dado em [3, Theorem 4.5] usando SageMath. Na atualidade um problema em aberto é justamente exibir uma prova sem uso do computador. Neste capítulo exibe-se este resultado, sem a demonstração. O objetivo deste capítulo é expor estes resultados que serão abordados com maior profundidade em futuras pesquisas.

5.1 Aplicabilidade do método Lenstra-Schoof

Nesta seção apresenta-se como o método tradicionalmente usado pelos autores Lenstra e Schoof e desenvolvidos por Cohen e coautores aplicando à existencia de elementos 1-normais. Este método tradicional usa a noção de ser d-livre (para divisores de q^n-1 ou x^n-1) para caracterizar e contar elementos primitivos normais.

Definição 5.1. *i.* Para $m \mid (q^n - 1)$, $\alpha \in \mathbb{F}_{q^n}$ é dito m-**livre** se sempre que $\alpha = \beta^d$, para algum divisor d de m, implica $d = 1$.

ii. Para $M \mid (x^n - 1)$, $\alpha \in \mathbb{F}_{q^n}$ é M-**livre** se $\alpha = H(\beta)$, onde H é o q-associado de um divisor h de M, então $h = 1$.

É conhecido que um elemento $\alpha \in \mathbb{F}_{q^n}^*$ é primitivo se e somente se α é $(q^n - 1)$-livre (isto é, se e somente se, sua ordem multiplicativa $\text{ord}(\alpha)$ é $q^n - 1$), e que $\alpha \in \mathbb{F}_{q^n}$ é normal se, e somente se, α é $(x^n - 1)$-livre (isto é, se e somente se sua $\mathbb{F}_q$-ordem $\text{Ord}(\alpha)$ é $x^n - 1$). É possível caracterizar elementos 1-normais via g-livres para algum $g \mid x^n - 1$?. A resposta é afirmativa e apresenta-se formalmente na próxima seção.

A partir da definição, as seguintes propriedades podem ser derivadas.

Proposição 5.2. *Seja $m \mid (q^n - 1)$ e denotamos por m_0 a parte quadrada livre de m (m_0 é o produto dos fatores primos distintos de m). Para $\alpha \in \mathbb{F}_{q^n}$, se tem*

i. Se $r \mid m$, e α é m-livre, então α é r-livre.

ii. Para qualquer divisor r de m tal que $m_0 \mid r$, α é r-livre se, e somente se, α é m-livre.

iii. α é m-livre se, e somente se, $\operatorname{mdc}\left(m, \frac{q^n-1}{\operatorname{ord}(\alpha)}\right) = 1$.

Demonstração. i. Seja d um divisor de r e $\alpha = \beta^d$. Como $r \mid m$, então $d \mid m$ e como α é m-livre, tem-se, $d = 1$, portanto, α é r-livre.

ii. Sabemos que m-livre implica r-livre para todo $r|m$. Reciprocamente se α é r-livre com $m_0|r$ e suponhamos, por contradição, que α não é m-livre. Logo existe $d|m$, $d \neq 1$ e β tal que $\alpha = \beta^d$. Como $l = \operatorname{mdc}(d, m_0) \neq 1$ temos que $\alpha = \beta^d = \left(\beta^{\frac{d}{l}}\right)^l$, desta forma existe um $l \neq 1$ com $l|m_0|r$ e desta forma α não é r-livre.

iii. Suponhamos que $\alpha \in \mathbb{F}_{q^n}$ e seja $\operatorname{ord}(\alpha) = \frac{q^n-1}{s}$, onde $s \mid (q^n - 1)$. Seja η um elemento primitivo de $\mathbb{F}_{q^n}$, sem perda de generalidade suponha que $\alpha = \eta^s$.

$\Rightarrow$ Suponhamos que $(m, s) = s_0 > 1$, logo $s = s_0 s_1$ para algum $s_1 \in \mathbb{Z}$, como $\alpha = \eta^s = (\eta^{s_1 s_0}) = (\eta^{s_1})^{s_0}$ e $s_0 > 1$, então α não é m-livre.

$\Leftarrow$ Seja $\operatorname{mdc}(m, s) = 1$, suponhamos que $\alpha = \beta^d$, onde $\beta \in \mathbb{F}_{q^n}$ e $d \mid m$, tem-se que $\beta = \eta^i$ para algum i com $1 \leq i \leq q^n - 1$, assim $\alpha = \eta^s = (\eta^i)^d = \eta^{id}$ implica que $s \equiv id \pmod{q^n - 1}$, isto é $s = di + a(q^n - 1)$ para algum inteiro a. Agora como $d \mid m$ e $m \mid q^n - 1$ por hipotesis, então $d \mid q^n - 1$, logo $d \mid di + a(q^n - 1)$, portanto $d \mid s$, como $\operatorname{mdc}(m, s) = 1$ e $d \mid m$ tem-se $\operatorname{mdc}(d, s) = 1$, desse modo $d = 1$, por isso, α é m-livre.

□

Tem-se resultados análogos aditivos do teorema anterior.

Proposição 5.3. *Seja $g \mid (x^n - 1)$ e denotamos por g_0 a parte quadrada livre de g (g_0 é o produto dos distintos fatores irredutíveis de g). Para $\alpha \in \mathbb{F}_{q^n}$,*

i. Se $f \mid g$, e α é g-livre então α é f-livre.

ii. Para qualquer divisor f de g tal que $g_0 \mid f$, $\alpha \in \mathbb{F}_{q^n}$ é f-livre se, e somente se, α é g-livre.

Demonstração. i. Seja $\alpha \in \mathbb{F}_{q^n}$ tal que $\alpha = H(\beta)$ com $\beta \in \mathbb{F}_{q^n}$, onde H é um q-associado de um divisor h de f, como $h \mid f$ e $f \mid g$, então $h \mid g$ e $f \mid x^n - 1$, como α é g-livre, logo $h = 1$, portanto α é f-livre.

ii. Sabemos pelo item i. que ser g-livre implica ser f-livre para todo $f|g$.

Reciprocamente, se α é f-livre com $g_0|f$ e suponhamos, por contradição, que α não é g-livre. Logo existe $h|g$ com $h \neq 1$ cujo q-polinômio associado linearizado é H e β tal que $\alpha = H(\beta)$. Como $\tilde{h} = \operatorname{mdc}(h, g_0) \neq 1$, temos que existe $\tilde{s} \in \mathbb{F}_q[x]$ tal que $h = \tilde{h}\tilde{s}$ e $\alpha = H(\beta) = \tilde{H}(\beta) \otimes \tilde{S}(\beta) = \tilde{H}\left(\tilde{S}(\beta)\right)$, onde $\tilde{H}, \tilde{S}$ são os polinômios q-associados linearizados de $\tilde{h}$ e $\tilde{s}$ respectivamente. Desta maneira existe $\tilde{h} \neq 1$ tal que $\tilde{h}|g_0$ e $\tilde{h}|f$ então α não é f-livre.

□

O seguinte lema e definição são necessários para mostrar o Teorema 5.7.

Definição 5.4. Dado um polinômio não nulo $f \in \mathbb{F}_q[x]$, denotamos por **rad**(f) o maior divisor mônico livre de quadrado de f. Em outras palavras, $\operatorname{rad}(f)$ é o produto dos fatores mônicos irredutíveis distintos de f.

Lema 5.5. *Se* $\operatorname{Ord}(\alpha) = f$, *então existe um elemento normal β tal que $\alpha = \frac{x^n-1}{f} \circ \beta$.*

Demonstração. Seja $\gamma \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$. Por definição, existe $g \in \mathbb{F}_q[x]$ tal que $\alpha = g \circ \gamma$. Seja $f = \frac{x^n-1}{\text{mdc}(x^n-1,g)}$, logo $\text{mdc}(x^n-1, g) = \frac{x^n-1}{f}$ e, portanto, $\frac{x^n-1}{f} | g$, Assim, existe $g_1 \in \mathbb{F}_q[x]$ tal que $g = \frac{x^n-1}{f} g_1$.

Como $\text{mdc}\left(x^n - 1, \frac{x^n-1}{f} \cdot g_1\right) = \frac{x^n-1}{f}$, segue que $\text{mdc}(f, g_1) = 1$. Definindo o seguinte polinômio livre de quadrados:

$$\overline{f} = \frac{rad\left(\frac{x^n-1}{f}\right)}{\text{mdc}\left(rad\left(\frac{x^n-1}{f}\right), rad(f)\right)}.$$

Em particular, $\text{mdc}(\overline{f}, f) = 1$. Vejamos que se $h_1(x), h_2(x) \in \mathbb{F}_q[x]$ são polinômios de grau menor que $\overline{f}$ tais que $g_1 + h_1 f \equiv g_1 + h_2 f \pmod{\overline{f}}$, então $h_1 f \equiv h_2 f \pmod{\overline{f}}$. Como f e $\overline{f}$ são primos entre si, tem-se $h_1 \equiv h_2 \pmod{\overline{f}}$, o que implica $h_1 = h_2$. Assim, $g_1 + hf$ percorre todos os elementos módulo $\overline{f}$. Isso significa que existe $h_3 \in \mathbb{F}_q[x]$ tal que $g_1 + h_3 f = 1 \pmod{\overline{f}}$. Seja $h_4 \in \mathbb{F}_q[x]$ tal que $g_1 + h_3 f = 1 + h_4 \overline{f}$.

Vejamos que $g_1 + h_3 f$ é primo com $x^n - 1$. Seja t_1 um fator irredutível de $x^n - 1$ e $g_1 + h_3 f$. Se t_1 divide f, então t_1 divide g_1. Mas isso é impossível, pois f e g_1 são primos entre si. Dessa forma, t_1 divide $\frac{x^n-1}{f}$ e não divide f. Isso implica que t_1 divide $\overline{f}$. Mas t_1 divide $g_1 + h_3 f = 1 + h_4 \overline{f}$, o que significa que t_1 divide 1. Isso é uma contradição. Portanto, $g_1 + h_3 f$ é primo com $x^n - 1$.

Denotemos por $g_2 = g_1 + h_3 f$. Observemos que $g_2 \circ \gamma$ é um elemento normal, pois

$$\text{Ord}(g_2 \circ \gamma) = \frac{x^n - 1}{\text{mdc}(x^n - 1, g_2)} = x^n - 1.$$

Por outro lado,

$$\begin{aligned} \frac{x^n - 1}{f} \circ (g_2 \circ \gamma) &= \frac{x^n - 1}{f} \circ ((g_1 + h_3 f) \circ \gamma) \\ &= \frac{x^n - 1}{f} g_1 \circ \gamma = g \circ \gamma = \alpha. \end{aligned}$$

□

Definição 5.6. Sejam A um domínio de fatoração única, α um elemento irredutível de A, $\beta \in A$ e c um inteiro positivo. Diz-se que α^c **divide exatamente** β se $\alpha^c \mid \beta$ e $\alpha^{c+1} \nmid \beta$, e denota-se por $\alpha^c \parallel \beta$.

A definição anterior pode ser aplicada aos domínios de fatoração única $\mathbb{Z}$ e $\mathbb{F}_q[x]$.

Teorema 5.7. *Seja $x^n - 1$ com fatoração em irredutíveis de $\mathbb{F}_q[x]$ dada por $f_0^{a_0} \dots f_l^{a_l}$ e para $\alpha \in \mathbb{F}_{q^n}$ seja $\text{Ord}(\alpha) = f_0^{b_0} \dots f_l^{b_l}$. Para qualquer divisor g de $x^n - 1$ as seguintes afirmações são equivalentes:*

i. α é g-livre.

ii. g e $\frac{x^n-1}{\text{Ord}(\alpha)}$ são coprimos.

iii. Se $f_i \mid g$ para algum $0 \leq i \leq l$, então $f_i^{a_i} \mid \text{Ord}(\alpha)$.

Demonstração. *i.* $\Rightarrow$ *ii.* Pelo Lema 5.5, tem-se que $\alpha = \frac{x^n-1}{\text{Ord}(\alpha)} \circ \eta$ onde $\eta \in \mathbb{F}_{q^n}$ é um elemento normal adecuado. Seja $h_0 \in \mathbb{F}_q[x]$ com $h_0 \neq 1$ tal que $h_0 = \text{mdc}\left(\frac{x^n-1}{\text{Ord}(\alpha)}, g\right)$, então, $h_0 \mid g$ e $\frac{x^n-1}{\text{Ord}(\alpha)} = h_0 h_1$ com $h_1 \in \mathbb{F}_q[x]$, logo, $\alpha = h_0 \circ (h_1 \circ \eta)$, assim, α não é g-livre.

ii. $\Rightarrow$ *iii.* Como $\mathrm{Ord}(\alpha) = f_0^{b_0} f_1^{b_1} \dots f_i^{b_i} \dots f_l^{b_l}$ e $x^n - 1 = f_0^{a_0} \dots f_l^{a_l}$, logo $\frac{x^n-1}{\mathrm{Ord}(\alpha)} = f_0^{a_0-b_0} \dots f_l{}^{a_l-b_l}$.

Se $f_i \mid g$ para algum i, então $f_i^{a_i-b_i} \nmid \frac{x^n-1}{\mathrm{Ord}(\alpha)}$ já que pela hipótese $\mathrm{mdc}\left(g, \frac{x^n-1}{\mathrm{Ord}(\alpha)}\right) = 1$, desse modo $a_i - b_i = 0$, consequentemente, $a_i = b_i$, portanto, $f_i^{a_i} \mid \mathrm{Ord}(\alpha)$.

iii. $\Rightarrow$ *i.* Suponhamos que α não é g-livre, então existem $h \in \mathbb{F}_q[x]$, tal que $h \mid g$, $h \neq 1$, e $\beta \in \mathbb{F}_{q^n}$ tais que $\alpha = h \circ \beta$. Como $h \neq 1$, o polinômio h é divisível por um fator irredutível f_i. Assim, $\alpha = h \circ \beta = \frac{f_i}{f_i} \circ (h \circ \beta) = f_i \circ \left(\frac{h}{f_i} \circ \beta\right)$. Pode-se supor que $h = f_i$ e $\alpha = f_i \circ \beta$ para algum i, com $f_i \mid g$, logo pelo Teorema 3.5, segue

$$\mathrm{Ord}(\alpha) = \frac{\mathrm{Ord}(\beta)}{\mathrm{mdc}(\mathrm{Ord}(\beta), f_i)}. \tag{5.1}$$

Pela hipótese tem-se que $f_i^{a_i} \mid \mathrm{Ord}(\alpha)$. Mas como $\mathrm{Ord}(\beta) \mid (x^n - 1)$ segue que a potência de f_i que aparece em $\mathrm{Ord}(\beta)$ é menor ou igual a $f_i^{a_i}$ e logo a potência máxima de f_i que aparece em $\mathrm{Ord}(\alpha)$ é $f^{a_i} - 1$ que é uma contradição.

□

Corolário 5.8. *i.* $\mathrm{Ord}(\alpha) = x^n - 1$ *se, e somente, se* α *é* $(x^n - 1)$*-livre (portanto,* g *é livre para qualquer* $g \mid (x^n - 1)$*.*

ii. Suponhamos que $x^n - 1$ *tem fatoração de irredutíveis em* $\mathbb{F}_q[x]$ *dada por* $f_0^{a_0} \dots f_l^{a_l}$*. Então* $\mathrm{Ord}(\alpha) = \frac{x^n-1}{f_i^a}$ *para algum* $0 \leq i \leq l$ *e* $1 \leq a \leq a_i$ *se, e somente se,* α *é* g*-livre para* g *que divide* $f_0^{a_0} \dots f_{i-1}^{a_{i-1}} f_{i+1}^{a_{i+1}} \dots f_l^{a_l}$ *e* α *não é* g*-livre para qualquer* g *que divisível por* f_i*.*

Demonstração. *i.* $\Rightarrow$ Se $\mathrm{Ord}(\alpha) = x^n - 1$, então $\mathrm{mdc}\left(x^n - 1, \frac{x^n-1}{\mathrm{Ord}(\alpha)}\right) = 1$, assim $x^n - 1$ e $\frac{x^n-1}{\mathrm{Ord}(\alpha)}$ são coprimos, logo pelo Teorema 5.7 tem-se α é $(x^n - 1)$-livre.

$\Leftarrow$ Se α é $(x^n - 1)$-livre, então, pelo Teorema 5.7 tem-se que $x^n - 1$ e $\frac{x^n-1}{\mathrm{Ord}(\alpha)}$ são coprimos, isto é, $\mathrm{mdc}\left(x^n - 1, \frac{x^n-1}{\mathrm{Ord}(\alpha)}\right) = 1$, assim $\mathrm{Ord}(\alpha) = x^n - 1$.

ii. $\Rightarrow$ Como $x^n - 1 = f_0^{a_0} \dots f_i^{a_i} \dots f_l^{a_l}$, e $\mathrm{Ord}(\alpha) = \frac{x^n-1}{f_i^a}$ para algum $0 \leq i \leq l$ e $1 \leq a \leq a_i$, então $\mathrm{Ord}(\alpha) = f_0^{a_0} \dots f_i^{a_i-a} \dots f_l^{a_l}$, seja $g \in \mathbb{F}_q[x]$ tal que $g \mid f_0^{a_0} \dots f_{i-1}^{a_{i-1}} f_{i+1}^{a_{i+1}} \dots f_l^{a_l}$, logo existe $j = \{0, \dots, l\} - \{i\}$ tal que $f_j \mid g$, e como $\mathrm{Ord}(\alpha) = f_0^{a_0} \dots f_{i-1}^{a_{i-1}} f_i^{a_i-a} f_{i+1}^{a_{i+1}} \dots f_l^{a_l}$, tem-se que $f_j^{a_j} \mid \mathrm{Ord}(\alpha)$, assim pelo Teorema 5.7, α é g-livre.

Por outro lado, suponha que $f_i \mid g$ para $g \mid x^n - 1$, como $\mathrm{Ord}(\alpha) = f_0^{a_0} \dots f_i^{a_i-a} \dots f_l^{a_l}$, tem-se $f_i^{a_i} \nmid \mathrm{Ord}(\alpha)$, logo pelo Teorema 5.7, segue que α não é g-livre.

$\Leftarrow$ Pela hipótese tem-se que se $f_i \mid g$ para $g \mid x^n - 1$, então α não é g-livre, logo pelo Teorema 5.7, segue $f_i^{a_i} \nmid \mathrm{Ord}(\alpha)$. Pela hipótese também tem-se, para todo $g \mid f_0^{a_0} \dots f_{i-1}^{a_{i-1}} f_{i+1}^{a_{i+1}} \dots f_l^{a_l}$, α é g-livre. Em particular para $g = f_j$ com $j \neq i$, segue α é f_j-livre, e novamente pelo Teorema 5.7, obtém-se $f_j^{a_j} \mid \mathrm{Ord}(\alpha)$ para todo $j \neq i$. Como $x^n - 1 = f_0^{a_0} \dots f_l^{a_l}$, $f_j^{a_j} \mid \mathrm{Ord}(\alpha)$ para todo $j \neq i$ e $f_i^{a_i} \nmid \mathrm{Ord}(\alpha)$, segue-se $\mathrm{Ord}(\alpha) = f_0^{a_0} \dots f_{i-1}^{a_{i-1}} f_i^{a_i-a} f_{i+1}^{a_{i+1}} \dots f_l^{a_l}$ para $1 \leq a \leq a_i$,

$$\mathrm{Ord}(\alpha) = \frac{f_0^{a_0} \dots f_i^{a_i} \dots f_l^{a_l}}{f_i^a} = \frac{f_0^{a_0} \dots f_l^{a_l}}{f_i^a} = \frac{x^n - 1}{f_i^a}.$$

□

Proposição 5.9. *Suponhamos que $x^n - 1$ tem um fator linear não repetido $x - \zeta$ com $\zeta \in \mathbb{F}_q$. Então,* $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-\zeta}$ *se, e somente se, α é um elemento $\left(\frac{x^n-1}{x-\zeta}\right)$-livre não normal.*

Em particular, isto se aplica quando a característica do corpo não divide n; neste caso, $x-1$ é um fator não repetido de $x^n - 1$.

Demonstração. $\Rightarrow$ Como $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-\zeta}$, então $\mathrm{grau}(\mathrm{Ord}(\alpha)) = n - 1$, logo pelo Teorema 3.6, α não é normal, como $x - \zeta$ é um fator linear não repetido de $x^n - 1$, desse modo

$$\mathrm{mdc}\left(\frac{x^n-1}{x-\zeta}, \frac{x^n-1}{\mathrm{Ord}(\alpha)}\right) = \mathrm{mdc}\left(\frac{x^n-1}{x-\zeta}, x-\zeta\right) = 1,$$

de modo que, $\frac{x^n-1}{x-\zeta}$ e $\frac{x^n-1}{\mathrm{Ord}(\alpha)}$ são coprimos, por conseguinte pelo Teorema 5.7, α é $\left(\frac{x^n-1}{x-\zeta}\right)$-livre.

$\Rightarrow$ Como α não é normal, então $\mathrm{grau}(\mathrm{Ord}(\alpha)) < n$ (Teorema 3.6), como α é $\left(\frac{x^n-1}{x-\zeta}\right)$-livre segue que $\frac{x^n-1}{x-\zeta}$ e $\frac{x^n-1}{\mathrm{Ord}(\alpha)}$ são coprimos pelo Teorema 5.7.

Note que $g = \frac{x^n-1}{\mathrm{Ord}(\alpha)}$ é um divisor de $x^n - 1$, de grau maior ou igual a 1, $g \mid x^n - 1$ e g é coprimo com $\frac{x^n-1}{x-\zeta}$, logo $g \mid x - \zeta$, pois $x^n - 1 = (x - \zeta)\frac{x^n-1}{x-\zeta}$, como $\mathrm{grau}(g) \geq 1$ e g é mônico, então $g = x - \zeta$, ou seja $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-\zeta}$. □

5.2 A existência de elementos primitivos 1-normais

Nesta seção estabelece-se a existência de elementos 1-normais para todo par (q, n) tal que q e n são coprimos e $n \geq 6$. (De fato o resultado vale para $n \geq 3$, quando $3 \leq q \leq 9$) (Teorema 5.30). Para isto inicialmente deriva-se uma função característica para uma certa classe de elementos primitivos 1-normais, e usa-se a soma de caracteres para estabelecer uma condição suficiente para a existência.

5.2.1 Caracteres e soma de Gauss

Antes de exibir o teorema que garante a existência dos elementos 1-normais, apresentam-se as noções de caracter e soma de Gauss com alguns resultados relevantes.

Definição 5.10. Seja G um grupo abeliano finito de ordem $\mid G \mid$ com elemento identidade 1_G. Um **caracter** χ de G é um homomorfismo de G no grupo multiplicativo U dos números complexos de módulo 1, isto é, $\chi : G \to U \subset \mathbb{C}^*$.

Definição 5.11. χ_0 definido por $\chi_0(g) = 1$para todo $g \in G$ é o **caracter trivial**.

Observação 5.12. Os elementos da imagem de χ são as $\mid G \mid$-ésimas raízes da unidade. Cada caracter χ de G tem um caracter associado seu conjugado $\overline{\chi}$ definido por $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$.

Teorema 5.13. *O carater χ satisfaz*

i. $\chi(g_1 \cdot g_2) = \chi(g_1)\chi(g_2)$, *para todo* $g_1, g_2 \in G$.

ii. $\chi(1_G) = \chi(1_G)\chi(1_G) = 1$.

iii. $\chi(1_G) = 1$.

iv. $(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$, *para todo* $g \in G$.

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

vi. $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$, *para todo* $g \in G$.

vii. Para todos $g_1, g_2 \in G$ *com* $g_1 \neq g_2$, *existe* χ *tal que* $\chi(g_1) \neq \chi(g_2)$.

Demonstração. As demonstrações dos itens *i*, *ii*, *iii*, *v* e *vii* seguem da definição.

iv. Para todo $g \in G$ tem-se que

$$\begin{aligned}(\chi(g))^{|G|} &= \underbrace{\chi(g)\chi(g)\cdots\chi(g)}_{|G|-vezes} \\ &= \chi(g^{|G|}) \\ &= \chi(1_G) \\ &= 1.\end{aligned}$$

vi. Sabe-se que $\chi(g)(\chi(g))^{-1} = 1$ e $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$, pela unicidade do inverso segue $\chi(g)^{-1} = \chi(g^{-1})$ e por propriedade do inverso multiplicativo dos complexos com módulo 1, $\chi(g)^{-1} = \overline{\chi(g)}$, para todo $g \in G$.

□

Teorema 5.14. *[14, Theorem 5.5] O número de caracteres de um grupo abeliano* G *é igual a* $|\ G\ |$.

Teorema 5.15. *[14, Theorem 5.2] Seja* H *um subgrupo do grupo abeliano finito* G *e seja* ψ *o caracter de* H. *Então* ψ *pode-se extender ao caracter de* G, *isto é, existe um caracter* χ *de* G *com* $\chi(h) = \psi(h)$ *para todo* $h \in H$.

Definição 5.16. Um caracter $\chi : \mathbb{F}_q \to \mathbb{C}^*$ do grupo aditivo $\mathbb{F}_q$ no grupo multiplicativo $\mathbb{C}^*$ é chamado de **caracter aditivo** de $\mathbb{F}_q$. O grupo de caracteres aditivos de $\mathbb{F}_q$ é denotado $\widehat{\mathbb{F}}_q$.

A estrutura de grupo abeliano de $\hat{G}$ é dada por $(\chi_1 + \chi_2)(c) := \chi_1(c) \cdot \chi_2(c)$, para todos $\chi_1, \chi_2 \in \hat{G}$ e $c \in \mathbb{F}_q$.

Se p é a característica de $\mathbb{F}_q$, a função $\chi_0 : \mathbb{F}_q \to \mathbb{C}^*$ definida por $\chi_0(c) = e^{\frac{2\pi i Tr_q(c)}{p}}$, para todo $c \in \mathbb{F}_q$, é um caracter aditivo chamado de caracter aditivo canônico, onde Tr_q denota o traço absoluto de $\mathbb{F}_q$ sobre $\mathbb{F}_p$.

Teorema 5.17. *Se* χ *é um caracter não trivial de um grupo abeliano finito* G. *Então*

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

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

$$\begin{aligned}\chi(h)\sum_{g \in G}\chi(g) &= \sum_{g \in G}\chi(gh) \\ &= \sum_{g \in G}\chi(g),\end{aligned}$$

porque g percorre G, então $(\chi(h) - 1)\sum_{g \in G}\chi(g) = 0$, implica que $\sum_{g \in G}\chi(g) = 0$. □

Definição 5.18. Um caracter $\psi : \mathbb{F}_q^* \to \mathbb{C}^*$ do grupo multiplicativo $\mathbb{F}_q^*$ no grupo multiplicativo $\mathbb{C}^*$ é chamado de **caracter multiplicativo** de $\mathbb{F}_q$. O grupo de caracteres multiplicativos de $\mathbb{F}_q$ é denotado $\widehat{\mathbb{F}}_q^*$.

Todo caracter multiplicativo definido em $\mathbb{F}_{q^n}^*$ pode ser extendido a $\mathbb{F}_{q^n}$. Está extensão é definida como segue

Definição 5.19. Para um caracter multiplicativo $\psi : \mathbb{F}_{q^n}^* \to \mathbb{C}^*$ define-se

$$\psi(\mathbf{0}) = \begin{cases} 1 & \text{se } \psi \text{ é o caracter trivial,} \\ \\ 0 & \text{caso contrário.} \end{cases}.$$

A definição de soma de Gauss será dada sobre $\mathbb{F}_{q^n}$ já que é nesse corpo que trabalharemos na última seção.

Definição 5.20. Sejam ψ, χ caracteres multiplicativo e aditivo de $\mathbb{F}_{q^n}$, respectivamente. Então, a **soma Gaussiana** $G_n(\psi, \chi)$ é definida por

$$G_n(\psi, \chi) = \sum_{w \in \mathbb{F}_{q^n}} \psi(w)\chi(w).$$

Uma consequência da definição anterior é o resultado a seguir.

Teorema 5.21. *Sejam ψ e χ caracteres multiplicativo e aditivo de $\mathbb{F}_{q^n}$, respectivamente. Então a soma Gaussiana $G_n(\psi, \chi)$ satisfaz:*

i. $G_n(\psi, \chi) = q^n$, *se* $\psi = \psi_0$, $\chi = \chi_0$.

ii. $G_n(\psi, \chi) = 0$, *se ou* $\psi = \psi_0$ *ou* $\chi = \chi_0$.

iii. $\mid G_n(\psi, \chi) \mid = q^{\frac{n}{2}}$, *se* $\psi \neq \psi_0$ *e* $\chi \neq \chi_0$.

Demonstração.

i. Como

$$\begin{aligned} Gn(\psi_0, \chi_0) &= \sum_{w \in \mathbb{F}_{q^n}} \psi_0(w)\chi_0(w) \\ &= \sum_{w \in \mathbb{F}_{q^n}} 1 \\ &= q^n. \end{aligned}$$

ii. Se $\psi \neq \psi_0$ e $\chi = \chi_0$, então

$$\begin{aligned} G_n(\psi, \chi_0) &= \sum_{w \in \mathbb{F}_{q^n}} \psi(w)\chi_0(w) \\ &= \sum_{w \in \mathbb{F}_{q^n}} \psi(w) \\ &= \psi(0) + \sum_{w \in \mathbb{F}_q^*} \psi(w) \\ &= 0, \end{aligned}$$

ou, se $\psi = \psi_0$ e $\chi \neq \chi_0$, então

$$\begin{aligned} G_n(\psi, \chi) &= \sum_{w \in \mathbb{F}_{q^n}} \psi(w)\chi(w) \\ &= \sum_{w \in \mathbb{F}_{q^n}} \psi_0(w)\chi(w) \\ &= \sum_{w \in \mathbb{F}_{q^n}} \chi(w) \\ &= 0. \end{aligned}$$

iii. Se $\psi \neq \psi_0$ e $\chi \neq \chi_0$, tem-se

$$\begin{aligned} \mid G_n(\psi,\chi) \mid^2 &= \overline{G_n(\psi,\chi)}G_n(\psi,\chi) \\ &= \sum_{w\in\mathbb{F}_{q^n}} \sum_{w_1\in\mathbb{F}_{q^n}} \overline{\psi(w)\chi(w)}\psi(w_1)\chi(w_1) \\ &= \sum_{w\in\mathbb{F}_{q^n}} \sum_{w_1\in\mathbb{F}_{q^n}} \psi(w^{-1}w_1)\chi(w_1-w). \end{aligned}$$

Fazendo $d = w^{-1}w_1$, assim $\mid G_n(\psi,\chi) \mid^2 = \sum_{w\in\mathbb{F}_{q^n}} \sum_{d\in\mathbb{F}_{q^n}} \psi(d)\chi(w(d-1))$. Se $d = 1$, então $\sum_{w\in\mathbb{F}_{q^n}} \chi(w(d-1)) = \sum_{w\in\mathbb{F}_{q^n}} \chi(0) = q^n$ e no caso $d \neq 1$ temos $\sum_{w\in\mathbb{F}_{q^n}} \chi(w(d-1)) = 0$ pelo Teorema 5.17. Desse modo $\mid G_n(\psi,\chi) \mid^2 = \psi(1)q^n = q^n$, portanto $\mid G_n(\psi,\chi) \mid = q^{\frac{n}{2}}$. □

5.2.2 Elementos primitivos 1-normais

O conjunto de elementos 1-normais é igual ao conjunto de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que, existe $\xi \in \mathbb{F}_q$ satisfazendo $(x-\xi) \mid (x^n-1)$ e $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-\xi}$. Pela Proposição 5.9, quando n não é divisível pela característica p, o conjunto de elementos $\alpha \in \mathbb{F}_{q^n}$ que são 1-normais, tais que $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-1}$, é dado pelo conjunto de elementos não normais $\left(\frac{x^n-1}{x-1}\right)$-livres, o qual pode também ser caracterizado como o conjunto de elementos $\left(\frac{x^n-1}{x-1}\right)$-livres com traço 0. Será provada essa afirmação.

Lema 5.22. *Suponhamos que n não é divisível pela característica p. Então o conjunto de elementos não normais $\left(\frac{x^n-1}{x-1}\right)$-livres é igual ao conjunto de elementos $\left(\frac{x^n-1}{x-1}\right)$-livres com traço 0.*

Demonstração. Se α é $\left(\frac{x^n-1}{x-1}\right)$-livre com traço 0, então $\left(\frac{x^n-1}{x-1}\right) \circ \alpha = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$. Logo, α é não normal.

Suponha agora que α é não normal e $\left(\frac{x^n-1}{x-1}\right)$-livre. Pela Proposição 5.9, $\mathrm{Ord}(\alpha) = \frac{x^n-1}{x-1}$. Logo, $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \left(\frac{x^n-1}{x-1}\right) \circ \alpha = 0$. □

Seja S o conjunto de pares (q,n) com q e n coprimos tais que o conjunto de elementos primitivos de $\mathbb{F}_q$-ordem $\left(\frac{x^n-1}{x-1}\right)$ é não vazio. Em outras palavras, pelo Lema 5.22, S é o conjunto de pares (q,n) com q e n coprimos, tais que o conjunto de elementos primitivos $\left(\frac{x^n-1}{x-1}\right)$-livres de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ com traço zero é não vazio.

Será mostrada a existência de elementos primitivos 1-normais segundo o método de Lenstra e Schoof utilizado em [13]. Suponha que $m \mid (q^n-1)$ e $g \mid (x^n-1)$. Considere as funções características para o conjunto de elementos m-livres e g-livres como a seguir.

Usa-se $\int_{d\mid m} \psi_d$ para representar a função de $\mathbb{F}_{q^n} \longrightarrow \mathbb{C}$ definida por $\sum_{d\mid m} \frac{\mu(d)}{\phi(d)} \sum_{d} \psi_d$, onde ψ_d é um caracter multiplicativo de $\mathbb{F}_{q^n}$ de ordem d, e a soma interna percorre todos os caracteres multiplicativos de ordem d.

Teorema 5.23. *[9, Theorem 13.4.4.] Para o conjunto de elementos m-livres, tem-se a função característica*

$$\theta(m) \int_{d\mid m} \psi_d(w) = \begin{cases} 1 & \text{se } w \text{ é } m\text{-livre,} \\ 0 & \text{se } w \text{ não é } m\text{-livre,} \end{cases} \tag{5.2}$$

onde $w \in \mathbb{F}_{q^n}^*$ e $\theta(m) = \frac{\phi(m)}{m}$.

Para a parte aditiva, denote por χ o caracter aditivo canônico em $\mathbb{F}_{q^n}$. Seja $\triangle_D$ o conjunto de elementos $\delta \in \mathbb{F}_{q^n}$ tais que χ_δ tem $\mathbb{F}_q$-ordem D, onde χ_δ está definido por $\chi_\delta(w) = \chi(\delta w)$, para todo $w \in \mathbb{F}_{q^n}$. Usa-se a notação $\int_{D|g} \chi_{\delta_D}$ para representar a função de $\mathbb{F}_q[x] \longrightarrow \mathbb{C}$ definida por $\sum_{D|g} \frac{\mu_q(D)}{\Phi_q(D)} \sum_{\delta_D} \chi_{\delta_D}$ onde μ_q é a função polinomial de Möbius, e a soma interna percorre todos os caracteres aditivos χ_{δ_D} de $\mathbb{F}_q$-ordem D (isto é $\mathrm{Ord}(\chi_{\delta_D}) = D$).

Teorema 5.24. *[9, Theorem 13.4.4.] A função característica do conjunto de elementos g-livres é*

$$\Theta(g) \int_{D|g} \chi_{\delta_D}(w) = \begin{cases} 1 & \text{se } w \text{ é } g\text{-livre,} \\ 0 & \text{se } w \text{ não é } g\text{-livre,} \end{cases} \tag{5.3}$$

onde $w \in \mathbb{F}_{q^n}$ *e* $\Theta(g) = \frac{\Phi_q(g)}{q^{\mathrm{grau}(g)}}$.

Finalmente a função característica para os elementos de traço zero é dada por.

Teorema 5.25.

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \chi_c(w) = \begin{cases} 1 & \text{se } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w) = 0, \\ 0 & \text{se } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w) \neq 0, \end{cases} \tag{5.4}$$

onde $w \in \mathbb{F}_{q^n}$.

Demonstração. Seja $\tilde{\chi}$ o caracter aditivo canônico de $\mathbb{F}_q$ e χ o caracter canônico aditivo de $\mathbb{F}_{q^n}$.

Como $\chi(w) = e^{\frac{2\pi i \mathrm{Tr}_{q^n}(w)}{p}}$, $\tilde{\chi}(\alpha) = e^{\frac{2\pi i \mathrm{Tr}_q(\alpha)}{p}}$ e $\mathrm{Tr}_{q^n}(w) = \mathrm{Tr}_q\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w)\right)$, para todos $w \in \mathbb{F}_{q^n}$ e $\alpha \in \mathbb{F}_q$, então $\chi(w) = \tilde{\chi}\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w)\right)$, para todo $w \in \mathbb{F}_{q^n}$.

Dessa forma para $w \in \mathbb{F}_{q^n}$ e denotando $\alpha = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w)$, tem-se

$$\begin{aligned} \frac{1}{q} \sum_{c \in \mathbb{F}_q} \chi_c(w) &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \chi(cw) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \tilde{\chi}\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(cw)\right) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \tilde{\chi}\left(c\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w)\right) \\ &= \frac{1}{q} \sum_{c \in \mathbb{F}_q} \tilde{\chi}(c\alpha). \end{aligned}$$

Definindo $\tilde{\chi}_c(\alpha) := \tilde{\chi}(c\alpha)$, tem-se que $\tilde{\chi}_c$ percorre todo n caracter aditivo de $\mathbb{F}_q$ quando c percorre todos n elementos de $\mathbb{F}_q$. Por [14, Equation 5.8] temos que

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \tilde{\chi}_c(\alpha) = \begin{cases} 1 & \text{se } \alpha = 0, \\ 0 & \text{se } \alpha \neq 0. \end{cases}$$

Isso prova o teorema. □

Teorema 5.26. *Seja* $T := \frac{x^n-1}{x-1}$ *e* N *o número de elementos primitivos* T*-livres com traço zero. Então*

$$\frac{N}{\theta(q^n-1)\Theta(T)} = \frac{1}{q}\left(q^n + \int_{\substack{d|q^n-1 \\ d\neq 1}} \int_{\substack{D|T \\ D\neq 1}} \sum_{c \in \mathbb{F}_q} G_n(\psi_d, \chi_{\delta_D + c}) + \int_{\substack{d|q^n-1 \\ d\neq 1}} \sum_{c \in \mathbb{F}_q^*} G_n(\psi_d, \chi_c)\right),$$

onde $\int\limits_{\substack{d|q^n-1\\ d\neq 1}}\int\limits_{\substack{D|T\\ D\neq 1}} G_n(\psi,\chi)=\sum_{d|m}\sum_{D|g}\frac{\mu(d)}{\phi(d)}\frac{\mu_q(D)}{\Phi_q(D)}\sum_{d}\psi_d\sum_{\delta_D}\chi_{\delta_D}.$

Demonstração. Combinando as funções características (5.2), (5.3) e (5.4) tem-se,

$$N = \sum_{w\in\mathbb{F}_{q^n}}\left(\theta(q^n-1)\int\limits_{d|q^n-1}\psi_d(w)\right)\left(\tilde{\theta}(T)\int\limits_{D|T}\chi_{\delta_D}(w)\right)\left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\chi_c(w)\right).$$

Assim,

$$\begin{aligned}\frac{N}{\theta(q^n-1)\tilde{\theta}(T)} &= \frac{1}{q}\int\limits_{d|q^n-1}\int\limits_{D|T}\sum_{c\in\mathbb{F}_q}\sum_{w\in\mathbb{F}_{q^n}}\psi_d(w)\chi_{\delta_D+c}(w)\\ &= \frac{1}{q}\int\limits_{d|q^n-1}\int\limits_{D|T}\sum_{c\in\mathbb{F}_q}G_n(\psi_d,\chi_{\delta_D+c}).\end{aligned}\tag{5.5}$$

Como n não é divisível pela característica do corpo $\mathbb{F}_q$, pela Proposição 5.9, tem-se que $x-1$ não é um fator repetido do polinômio x^n-1. Assim, se $D\mid T$, então D é coprimo com $x-1$. Em particular, $D\neq x-1$ e, portanto, $\delta_D\notin\mathbb{F}_q$ a menos que $D=1$. Assim, $\delta_D+c=0$ se, e somente se, $\delta_D=c=0$, que equivale a $D=1$ e $c=0$. Portanto, a soma de Gauss toma os seguintes valores:

i. Se $d=1$ e $D=1$ e $c=0$, então

$$\begin{aligned}G_n(\psi_d,\chi_{\delta_D+c}) &= G_n(\psi_1,\chi_0)\\ &= G(1,1)\\ &= q^n.\end{aligned}$$

ii. Se $d=1$ (mas $D\neq 1$ ou $c\neq 0$), então

$$\begin{aligned}G_n(\psi_d,\chi_{\delta_D+c}) &= G_n(1,\chi_{\delta_D+c})\\ &= 0.\end{aligned}$$

iii. Se $d\neq 1$, $D=1$ e $c=0$, então

$$\begin{aligned}G_n(\psi_d,\chi_{\delta_D+c}) &= G_n(\psi_d,\chi_0)\\ &= 0.\end{aligned}$$

iv. Se $d\neq 1$ (mas $D\neq 1$ ou $c\neq 0$), então $\mid G_n(\psi_d,\chi_{\delta_D+c})\mid = q^{\frac{n}{2}}$.

Dos itens i., ii. e iii., tem-se

$$\frac{N}{\theta(q^n-1)\Theta(T)}=\frac{1}{q}\left(q^n+\int\limits_{\substack{d|q^n-1\\ d\neq 1}}\int\limits_{\substack{D|T\\ D\neq 1}}\sum_{c\in\mathbb{F}_q}G_n(\psi_d,\chi_{\delta_D+c})+\int\limits_{\substack{d|q^n-1\\ d\neq 1}}\sum_{c\in\mathbb{F}_q^*}G_n(\psi_d,\chi_c)\right),$$

onde as duas últimas somas do lado direito serão acotadas usando o item iv. □

Definição 5.27. Seja A um domínio de fatoração única. A função $\omega : A \to \mathbb{Z}$ conta o número de divisores primos de um elemento de A e a função $W : \mathbb{Z}_+ \to \mathbb{Z}$ conta o número de divisores livres de quadrados de um elemento de ω. Isto é,

$$\omega(t) = \begin{cases} 0 & \text{se } t \in \omega(A), \\ k & \text{se } t = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \text{ é a fatoração de } t \text{ como produto de primos distintos} \end{cases}$$

e

$$W(t) = \begin{cases} 1 & \text{se } t \in \omega(A), \\ 2^k & \text{se } t = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \text{ é a fatoração de } t \text{ como produto de primos distintos} \end{cases},$$

onde $\omega(A)$ é o grupo de unidades de A.

Para um inteiro ou polinômio t denotamos por $W(t)$ o número de divisores livres de quadrados de t, isto é $W(t) = 2^{\omega(t)}$ onde $\omega(t)$ é o número de fatores primos ou irredutíveis de t. No que segue A denotara um dos anéis $\mathbb{Z}$ ou $\mathbb{F}_q[x]$.

Corolário 5.28. *Suponha que q e n são coprimos. Se*

$$q^{\frac{n}{2}-1} \geq W(q^n - 1) W\left(\frac{x^n - 1}{x - 1}\right), \tag{5.6}$$

então $(q, n) \in S$.

Demonstração. Do Teorema 5.26, e do item iv. da demonstração do Teorema 5.26, tem-se

$$\begin{aligned}
\left| \frac{N}{\theta(q^n - 1)\Theta(T)} - q^{n-1} \right| &\leq \frac{1}{q} \left| \int_{\substack{d | q^n - 1 \\ d \neq 1}} \int_{\substack{D | T \\ D \neq 1}} \sum_{c \in \mathbb{F}_q} G_n(\psi_d, \chi_{\delta_D + c}) \right| + \frac{1}{q} \left| \int_{\substack{d | q^n - 1 \\ d \neq 1}} \sum_{c \in \mathbb{F}_q^*} G_n(\psi_d, \chi_c) \right| \\
&= \frac{1}{q} \left| \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \sum_{\substack{D | T \\ D \neq 1}} \frac{\mu(d)}{\phi(d)} \frac{\mu_q(D)}{\Phi_q(D)} \sum_d \sum_{\delta_D} \sum_{c \in \mathbb{F}_q} G_n(\psi_d, \chi_{\delta_D + c}) \right| \\
&+ \frac{1}{q} \left| \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \frac{\mu(d)}{\phi(d)} \sum_d \sum_{c \in \mathbb{F}_q^*} G_n(\psi_d, \chi_{\delta_D + c}) \right| \\
&\leq \frac{1}{q} \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \sum_{\substack{D | T \\ D \neq 1}} \frac{|\mu(d)| \, |\mu_q(D)|}{\phi(d)\Phi_q(D)} \sum_d \sum_{\delta_D} \sum_{c \in \mathbb{F}_q} q^{\frac{n}{2}} \\
&+ \frac{1}{q} \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \frac{|\mu(d)|}{\psi(d)} \sum_{\psi_d} \sum_{c \in \mathbb{F}_q^*} q^{\frac{n}{2}}.
\end{aligned}$$

Como existem $\phi(d)$ caracteres multiplicativos de ordem d, existem $\Phi_q(D)$ caracteres aditivos de $\mathbb{F}_q$-ordem D, $\mathbb{F}_q$ tem q elementos e $\mathbb{F}_q^*$ tem $q - 1$ elementos, então

$$\frac{1}{q} \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \sum_{\substack{D | T \\ D \neq 1}} \frac{|\mu(d)| \, |\mu_q(D)|}{\phi(d)\Phi_q(D)} \sum_d \sum_{\delta_D} \sum_{c \in \mathbb{F}_q} q^{\frac{n}{2}} = \frac{1}{q} \sum_{\substack{d | q^n - 1 \\ d \neq 1}} \sum_{\substack{D | T \\ D \neq 1}} |\mu(d)| \, |\mu_q(D)| \, q^{\frac{n}{2}+1}$$

e

$$\frac{1}{q}\sum_{\substack{d|q^n-1\\ d\neq 1}}\frac{|\mu(d)|}{\psi(d)}\sum_{\psi_d}\sum_{c\in\mathbb{F}_q^*}q^{\frac{n}{2}}=\frac{1}{q}\sum_{\substack{d|q^n-1\\ d\neq 1}}|\mu(d)|\,(q-1)q^{\frac{n}{2}}.$$

Observemos,

$$\sum_{\substack{d|q^n-1\\ d\neq 1}}|\mu(d)|=W(q^n-1)-1 \quad \text{e} \quad \sum_{\substack{D|T\\ D\neq 1}}|\mu_q(D)|=W(T)-1.$$

Logo,

$$\begin{aligned}\left|\frac{N}{\theta(q^n-1)\Theta(T)}-q^{n-1}\right| &\leq \frac{1}{q}\left((W(q^n-1)-1)(W(T)-1)q^{\frac{n}{2}+1}+(W(q^n-1)-1)(q-1)q^{\frac{n}{2}}\right)\\ &= (W(q^n-1)-1)\left((W(T)-1)q^{\frac{n}{2}}+\frac{q-1}{q}q^{\frac{n}{2}}\right)\\ &\leq (W(q^n-1)-1)\left((W(T)-1)q^{\frac{n}{2}}+q^{\frac{n}{2}}\right)=(W(q^n-1)-1)W(T)q^{\frac{n}{2}}.\end{aligned}$$

Desta forma, se $q^{n-1}>(W(q^n-1)-1)W(T)q^{\frac{n}{2}}$, então $N>0$. Da última expressão e usando o argumento dado em [3, Proposition 4.1] segue que

$$q^{n/2-1}\geq W(q^n-1)W(T),$$

implica $(q,n)\in S$. □

Em [3, Theorem 4.5] os autores S. Cohen e D. Hachenberger obtiveram 34 pares (q,n) que não satisfazem a Equação (5.6), e garantiram a existência de elementos primitivos 1-normais para todos os outros pares. Essencialmente, os autores provaram .

Teorema 5.29. *[3, Theorem 4.5] Sejam q e n primos entre si, e assuma que $n\geq 6$ se $q\geq 11$, e que $n\geq 3$ se $3\leq q\leq 9$. Se (q,n) não satisfaz a Equação (5.6), então necessariamente (q,n) é um dos 34 pares a seguir:*
(4, 15), (13, 12), (7, 12), (5, 12), (11, 10), (4, 9), (9, 8), (5, 8), (3, 8), (8, 7), (121, 6), (61, 6), (49, 6), (43, 6), (37, 6), (31, 6), (29, 6), (25, 6), (19, 6), (13, 6), (11, 6), (7, 6), (5, 6), (9, 5), (4, 5), (3, 5), (9, 4), (7, 4), (5, 4), (3, 4), (8, 3), (7, 3), (5, 3), (4, 3).

Por fim em [11, Theorem 5.10] mostra-se um resultado mais geral que o Teorema 5.29. Embora este resultado garante mais pares satisfazendo a Equação (5.6), isto é mais pares onde se garante a existência dos elementos 1-normais, a prova dada pelos autores foi computacional. Na atualidade a prova deste resultado sem uso da computadora é um problema em aberto.

Teorema 5.30. *Seja $q=p^e$ uma potência prima e $n\in\mathbb{N}$ com $p\nmid n$. Assuma que $n\geq 6$ se $q\geq 11$, e que $n\geq 3$ se $3\leq q\leq 9$. Então existe um elemento 1-normal primitivo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

A seguir exibe-se uma tabela dada em [11] que mostra a existência de elementos k-normais e k-normais primitivos sobre alguns corpos finitos pequenos.

$q=2, n=6$		
k	$\#k$-norm.	$\#\mathrm{pr}.k$-norm.
0	24	18
1	12	12
2	18	6
3	3	0
4	5	0
5	1	0

$q=5, n=6$		
k	$\#k$-norm.	$\#\mathrm{pr}.k$-norm.
0	9216	2568
1	4608	1320
2	1344	360
3	384	72
4	64	0
5	8	0

$q=5, n=7$		
k	$\#k$-norm.	$\#\mathrm{pr}.k$-norm.
0	62496	31248
1	15624	7812
2	0	0
3	0	0
4	0	0
5	0	0
6	4	0

Referências Bibliográficas

[1] Bach, E., Shallit, J. O. Algorithmic number theory: Efficient algorithms (Vol. 1). MIT press. (1996).

[2] Bateman, P. The distribution of values of the Euler function. Acta Arithmetica, 21, (1972), 329-345. https://doi.org/10.4064/aa-21-1-329-345

[3] Cohen, S. D., Hachenberger, D. Primitive normal bases with prescribed trace. Applicable Algebra in Engineering, Communication and Computing, 9, (1999), 383-403. https://doi.org/10.1007/s002000050112

[4] Dressler, R. A density which counts multiplicity. Pacific Journal of Mathematics, 34(2), (1970), 371-378. https://doi.org/10.2140/pjm.1970.34.371

[5] Erdös, P. Some remarks on Euler's ϕ function and some related problems. Bulletin of the American Mathematical Society, 51, (1945), 540-544. https://doi.org/10.1090/S0002-9904-1945-08390-6

[6] Frandsen, G. S. On the density of normal bases in finite fields. Finite Fields and Their Applications, 6(1), (2000), 23-38. https://doi.org/10.1006/ffta.1999.0263

[7] Gao, S., Panario, D. Density of normal elements. Finite Fields and Their Applications, 3(2), (1997),141-150. https://doi.org/10.1006/ffta.1996.0177

[8] Graham, R. L., Knuth, D. E., Patashnik, O., & Liu, S. Concrete mathematics: a foundation for computer science. Computers in Physics, 3(5), (1989), 106-107. https://doi.org/10.1063/1.4822863

[9] Hachenberger, Dirk, and Dieter Jungnickel. Topics in Galois fields (Vol. 4. No. 5). Cham: Springer, 2020. https://doi.org/10.1007/978-3-030-60806-4

[10] Hardy, G. H., Wright, E. M. An introduction to the theory of numbers. Oxford University Press, (1979).

[11] Huczynska, S., Mullen, G. L., Panario, D. & Thomson, D. Existence and properties of k-normal elements over finite fields. Finite Fields and Their Applications, 24, (2013), 170-183. https://doi.org/10.1016/j.ffa.2013.07.004

[12] Hungerford, T. W. Algebra (Vol. 73). Springer Science & Business Media. (2012).

[13] Lenstra, H. W., Schoof, R. J. Primitive normal bases for finite fields. Mathematics of Computation, 48(177), (1987), 217-231. https://doi.org/10.1090/S0025-5718-1987-0866111-3

[14] Lidl, R., Niederreiter, H. Finite fields (No. 20). Cambridge University Press.(1997). https://doi.org/10.1017/CBO9780511525926

[15] Neumann, V. G. L. Sobre elementos distinguidos em corpos finitos. Universidade Federal de Uberlândia. 2022

[16] Ore, O. Contributions to the theory of finite fields. Transactions of the American Mathematical Society, 36(2), (1934), 243-274. https://doi.org/10.1090/S0002-9947-1934-1501740-7

[17] Von Zur Gathen, J., Gerhard, J. (2013). Modern computer algebra. Cambridge University Press. https://doi.org/10.1017/CBO9781139856065