Elementos Normais e Primitivos em Extensões de Corpos Finitos

Lucas Ribeiro Coutinho
IM-UFRJ

Fevereiro de 2018

Elementos Normais e Primitivos em Extensões de Corpos Finitos

por

Lucas Ribeiro Coutinho
IM-UFRJ

Dissertação de Mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Luciane Quoos Conte

Rio de Janeiro
Fevereiro de 2018

C871e

Coutinho, Lucas Ribeiro
Elementos Normais e Primitivos em Extensões de Corpos Finitos / Lucas Ribeiro Coutinho. – Rio de Janeiro, 2018.
86 f.
Orientadora: Luciane Quoos Conte.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-graduação em Matemática, 2018.

1. Álgebra. 2. Corpos Finitos. 3. Caráteres. I. Conte, Luciane Quoos, orient. II. Título.

Elementos Normais e Primitivos em Extensões de Corpos Finitos

por

Lucas Coutinho

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração: Matemática

Aprovada por:

Profa. Dra. Luciane Quoos Conte - IM-UFRJ
(Orientadora)

Prof. Dr. Daniel Panario - Carleton University

Prof. Dr. Ilir Snopche - IM-UFRJ

Prof. Dr. Severino Collier Coutinho - IM-UFRJ

Rio de Janeiro
Fevereiro de 2018

Resumo

Neste trabalho apresentamos uma demonstração do *Teorema da Base Normal e Primitiva* feita por Cohen e Huczynska em 2003, sobre a existência de elementos normais e primitivos em extensões de corpos finitos. Este resultado é obtido sem o uso de computadores e utiliza teoria de caráteres e somas de Gauss para criar funções que contam o número de elementos normais e primitivos em extensões de corpos finitos. Ainda mostramos que sempre é possível prescrever o traço e a norma de um elemento normal e primitivo. Finalizamos mostrando um resultado sobre a existência de elementos 1-normais e primitivos com norma prescrita.

Abstract

The aim of this work is to give a proof of the *Primitive Normal Basis Theorem*, due to Cohen and Huczynska in 2003, about the existence of primitive and normal elements in finite fields extensions. This result does not depend on a computer and uses character theory and Gaussian sums to build functions that count the number of primitive and normal elements in finite fields extensions. We also show that it is possible to prescribe the trace and norm of such an element. Finally, we show an existence result about primitive 1-normal elements with prescribed norm.

Agradecimento

Agradeço aos meus pais, pelo apoio incondicional durante todas as fases do meu aprendizado. Agradeço à minha orientadora, por acreditar em mim e por todos os conselhos e suporte dados desde o início da minha graduação. Agradeço também ao CNPq e à CAPES pelo apoio financeiro.

Sumário

1 Introdução

A Teoria dos Corpos Finitos, conhecidos também como Corpos de Galois, em homenagem ao matemático Évariste Galois (1811-1832) consagrou-se como uma área de estudo desde 1893, quando o matemático E. H. Moore (1862-1932) publicou seu artigo chamado *A doubly infinite system of simple groups*, dando início à Teoria dos Corpos Finitos de uma forma abstrata [26, p. 10]. Resultados que hoje são interpretados com a linguagem de corpos finitos datam de muito antes. Em seu livro *History of Theory of Numbers*, Leonard Dickson (1874-1954) afirma que os Chineses em torno de 500 A.C. já sabiam que, se p é um primo ímpar, $2^{p-1}-1$ é divisível por p, um caso particular do *Pequeno Teorema de Fermat*. Desde o século XV congruências módulo um inteiro n foram estudadas por matemáticos brilhantes como Fermat (1601-1665), Euler (1707-1783), Lagrange (1736-1813), Legendre (1752-1833) e Gauss (1777-1855) e todos já sabiam que quando n é primo, estas congruências possuíam propriedades especiais (ver [12, p. 295]). Dentre estes matemáticos, Gauss foi o primeiro a dar uma definição explícita das congruências módulo n em seu trabalho *Disquisitiones Arithmeticae* publicado em 1808. Ele estudou ainda a fatoração de polinômios com coeficientes módulo um primo p e mostrou que qualquer polinômio irredutível módulo p, diferente de X de grau $m \geq 1$ é um divisor de $X^{p^m-1}-1$, assim como obteve uma fórmula para o número de polinômios mônicos irredutíveis de grau fixo com coeficientes módulo p. Galois publica em 1830 um artigo intitulado *Sur la théorie des nombres*, onde constrói o corpo finito com p^n elementos, onde p é um primo e n um inteiro positivo, contudo outros matemáticos também descobriram os corpos finitos independentemente, como Schönemann, que descreveu uma teoria para os corpos finitos baseado em congruências (ver [12, p. 296]).

Atualmente, o interesse no estudo da Teoria dos Corpos Finitos se intensifica com suas diversas aplicações e conexões com outras áreas, como por exemplo a Teoria de Códigos, Geometria Finita, Polinômios de Permutação, Curvas Algébricas sobre Corpos Finitos e Criptografia.

Seja q uma potência de um primo p e $\mathbb{F}_q$ o corpo finito com q elementos. Um resultado clássico na Teoria dos Corpos Finitos é a existência de *elementos normais* para extensões de corpos $\mathbb{F}_{q^n}|\mathbb{F}_q$, ou seja, a existência de um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que o conjunto $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ seja uma base de $\mathbb{F}_{q^n}$ como espaço vetorial sobre $\mathbb{F}_q$, onde σ é o automorfismo de Frobenius sobre $\mathbb{F}_q$. Dizemos que um elemento $\alpha \in \mathbb{F}_{q^n}$ é um *elemento primitivo* se α gera o grupo multiplicativo $\mathbb{F}_{q^n}^*$.

Garantir a existência de elementos normais e primitivos é útil na prática, pois a existência de elementos geradores que possuem propriedaes conhecidas e simples de se trabalhar pode melhorar os cálculos envolvendo a aritmética em corpos finitos. Em 1952, Carlitz [3], [4] mostrou a existência de elementos normais e primitivos para q e n suficientemente grandes. Davenport [13] em 1968 mostrou a existência de um elemento normal e primitivo para extensões finitas do corpo primo $\mathbb{F}_p$. O resultado mais geral foi obtido somente em 1987 com o trabalho de Lenstra e Schoof [23], onde foi mostrada a existência de elementos normais e primitivos para qualquer extensão finita de corpos finitos, conhecido como o *Teorema da Base Normal e Primitiva*. A demonstração de Lenstra e Schoof é dependente do computador, onde uma grande parte de seu trabalho foi apresentada em formas de tabelas. Para um resultado de tamanha magnitude, é desejável uma demonstração que não dependa do computador. Motivado por este fato, Cohen e Huczynska em 2003 utilizam uma técnica de redução e mostram o Teorema sem a necessidade do uso de um computador.

Uma ferramenta central que aparece nos trabalhos de Lenstra e Schoof [23] e de Cohen e Huczynska [8] é a Teoria de Caráteres, mais especificamente as Somas de Gauss. As Somas de Gauss são uma das mais importantes somas exponenciais em corpos finitos, pois elas conectam suas estruturas aditiva e multiplicativa.

Elas também aparecem em vários outros contextos em álgebra e Teoria dos Números, bem como para determinar o número de pontos racionais em curvas algébricas sobre corpos finitos. Técnicas para calcular o número de elementos normais sobre $\mathbb{F}_q$ e primitivos em $\mathbb{F}_{q^n}$ envolvem Somas de Gauss.

Dizemos que um polinômio $f \in \mathbb{F}_q[X]$ de grau n é normal e primitivo se for o polinômio mínimo de um elemento normal e primitivo da extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$. Em 1994 Morgan e Mullen [25] conjecturaram o seguinte: sejam $n \geq 2$ e $a \in \mathbb{F}_q^*$. Então existe um polinômio normal e primitivo de grau n com traço a. Esta conjectura é uma versão mais forte do Teorema da Base Normal e Primitiva e foi provada por Cohen [6]. Cohen ainda mostrou que é possível, além do traço, prescrever a norma do elemento [5]. Sejam $\alpha \in \mathbb{F}_{q^n}$ e $f = X^m + a_1X^{m-1} + \cdots + a_m \in \mathbb{F}_q[X]$ seu polinômio mínimo, então $\mathrm{Tr}(\alpha) = -\mathrm{a}_1$ e $\mathrm{N}(\alpha) = (-1)^{\mathrm{m}}\mathrm{a}_{\mathrm{m}}$ são respectivamente o traço e a norma de α de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Ou seja, prescrever a norma e o traço de um elemento $\alpha \in \mathbb{F}_{q^n}$, normal e primitivo em $\mathbb{F}_{q^n}|\mathbb{F}_q$ é equivalente a prescrever o primeiro e o último coeficientes de um polinômio normal e primitivo. Resultados mais gerais foram obtidos nesta direção, prescrevendo ainda mais coeficientes de um polinômio normal e primitivo (ver [16], [17], [18] e [19]). Uma generalização dos elementos normais foi feita por Huczynska et al [21] em 2013, definindo o conceito de elemento k-normal $\alpha \in \mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, que pode ser caracterizado como um elemento que gera um $\mathbb{F}_q$-subespaço vetorial de codimensão k de $\mathbb{F}_{q^n}$. No mesmo artigo é provado um resultado existencial para os elementos 1-normais e primitivos quando a característica de $\mathbb{F}_q$ não divide n.

Todos os artigos [16], [17], [18], [19], assim como o resultado existencial sobre elementos 1-normais e primitivos utilizam técnicas similares às usadas para mostrar o Teorema da Base Normal e Primitiva assim como a existência de elementos normais e primitivos com normas e traço prescritos. Utiliza-se caráteres multiplicativos e aditivos em $\mathbb{F}_{q^n}$ para construir funções características para elementos com as propriedades desejadas (normal, primitivo, 1-normal, ter traço ou norma fixados, etc.) e com isso é possível contar o número N de elementos com tais propriedades, onde surgem fórmulas envolvendo Somas de Gauss. Com isso, é possível também obter cotas inferiores para N em função de q e n.

Neste trabalho, damos uma demonstração do Teorema da Base Normal e Primitiva, assim como uma demonstração da existência de elementos normais e primitivos com traço e normas prescritos.

Na Seção 2 definimos o conceito de módulo assim como algumas de suas propriedades, que serão usadas ao considerarmos $\mathbb{F}_{q^n}$ como um módulo sobre $\mathbb{F}_q[X]$. Fazemos uma exposição sobre os Corpos Finitos, definindo formalmente o conceito de base normal, elemento primitivo, assim como as funções traço e norma. Definimos uma operação em $\mathbb{F}_{q^n}$ que o torna um $\mathbb{F}_q[X]$-módulo, obtendo uma caracterização dos elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. A Seção 3 é dedicada ao estudo dos caráteres sobre grupos abelianos finitos, assim como os casos particulares de nosso interesse, caráteres sobre $\mathbb{F}_q$ e $\mathbb{F}_q^*$. Nesta seção construímos uma função característica para os elementos primitivos sobre um grupo abeliano finito e a função característica dos elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Também estudamos as *Somas de Gauss*, um tipo de soma de caráteres de fundamental importância para o texto. Na Seção 4 mostramos o Teorema da Base Normal e Primitiva, utilizando uma técnica de redução desenvolvida por Cohen para evitar o uso computacional. A Seção 5 é dedicada à demonstração da existência de elementos normais e primitivos com norma e traço prescritos, fazendo uso da mesma técnica de redução usada na demonstração do Teorema da Base Normal e Primitiva para lidar com alguns casos excepcionais. A Seção 6 é dedicada a uma introdução sobre os elementos k-normais e é obtido um resultado sobre a existência de elementos 1-normais e primitivos com a norma prescrita.

2 Preliminares Algébricas

2.1 Módulos

Nesta seção introduzimos a definição de módulos sobre anéis comutativos, bem como algumas de suas propriedades que usaremos durante o texto. A teoria aqui descrita pode ser encontrada em [2] e [15].

Definição 2.1. Seja R um anel comutativo. Um R-módulo é um par (M, τ), onde M é um grupo abeliano (aditivo) e τ é um mapa de $R \times M$ em M tal que, denotando por ax o valor de $\tau(a, x)$ $(a \in R, x \in M)$, as seguintes condições são satisfeitas:

i) $a(x + y) = ax + ay$,

ii) $(a + b)x = ax + bx$,

iii) $(ab)x = a(bx)$,

iv) $1x = x$,

para todo $a, b \in R$ e $x \in M$.

Exemplo 2.1. i) Se K é um corpo, então um K-módulo M é equivalente a um K-espaço vetorial.

ii) Seja G um grupo abeliano. Então G é um $\mathbb{Z}$-módulo com a operação $\tau(n, g) = ng = \underbrace{g + g + \cdots + g}_{\text{n vezes}}$, se n é positivo, $\tau(n, g) = -ng = \underbrace{-g - g - \cdots - g}_{\text{|n| vezes}}$ se n é negativo e $0g = \tau(0, g) = 0$.

Definição 2.2. Seja M um R-módulo.

1. O anulador de $x \in M$ em R, denotado por $\mathrm{Ann}_R(x)$ é o conjunto $\mathrm{Ann}_R(x) = \{a \in R \mid ax = 0\}$. Quando não houver risco de confusão, escreveremos apenas $\mathrm{Ann}(x)$ para denotar o anulador de x em R.

2. O conjunto $\mathrm{Ann}_R(M) = \{r \in R \mid rx = 0, \forall x \in M\}$ é chamado de *anulador* de M.

3. Para um elemento $a \in R$, definimos também $U_a = \{x \in M \mid ax = 0\}$, o conjunto dos elementos que são *anulados* por a.

Temos que $\mathrm{Ann}_R(M)$ e $\mathrm{Ann}_R(x)$ são ideais de R e U_a é um R-submódulo de M.

Proposição 2.3. *Seja M um R-módulo, onde R é um domínio de ideais principais. Se $Ann(x) = tR$ e $Ann(y) = sR$, onde $r, s \in R$ são tais que* $\mathrm{mdc(r, s)} = 1$*, então $Ann(x + y) = tsR$.*

Demonstração. A inclusão $tsR \subseteq \mathrm{Ann}(x + y)$ é imediata pois se $a \in tsR$, então existem $a_1, a_2 \in R$ tais que $ax + ay = tsa_1x + tsa_2y = 0$ pois $\mathrm{Ann}(x) = tR$ e $\mathrm{Ann}(y) = sR$. Reciprocamente, se $a \in \mathrm{Ann}(x + y)$, então $0 = a(x + y) = ax + ay$. Portanto, $ax = -ay$, multiplicando ambos os lados por t, temos que $0 = tax = -tay$, logo $ta \in \mathrm{Ann}(y) = sR$. Temos que s divide ta, mas como $\mathrm{mdc(t, s)} = 1$, necessariamente s divide a. Analogamente obtemos que t divide a o que implica que st divide a, ou seja, $a \in tsR$. □

Definição 2.4. Um *submódulo* N de um R-módulo M é um subgrupo de M fechado por multiplicação por elementos de R. O grupo quociente M/N tem uma estrutura de R-módulo natural, dada por $a(x + N) = ax + N$. O R-módulo M/N é chamado de *módulo quociente* de M por N.

Exemplo 2.2. 1. Se $m \in M$, então o subgrupo mM é um submódulo de M.

2. Se N e H são R-submódulos de M, então $N \cap H$ e $N + H := \{n+h \mid n \in N, h \in H\}$ são R-submódulos de M.

Definição 2.5. Sejam M, N, R-módulos. Um mapa $f : M \to N$ é um *homomorfismo de R-módulos* se

i) $f(x+y) = f(x) + f(y)$,

ii) $f(ax) = af(x)$,

para todo $a \in R$ e $x, y \in M$. Se f é uma bijeção, diremos que f é um *isomorfismo*. O *núcleo* de f é definido por $\mathrm{Ker}(f) = \{x \in M \mid f(x) = 0\}$.

O núcleo de f é um submódulo de M e a imagem de f, denotada por $\mathrm{Im}(f)$ é um submódulo de N.

Exemplo 2.3. Seja $\mathbb{Q}$ o corpo dos números racionais. Tanto $\mathbb{Q}$ quanto $\mathbb{Q}^*$ são $\mathbb{Z}$-módulos, por serem grupos abelianos. Contudo a operação τ que os torna $\mathbb{Z}$-módulos é diferente. De fato, para o grupo aditivo a operação é a soma herdada do anel $\mathbb{Q}$. Já em $\mathbb{Q}^*$ a operação é a seguinte

$$\tau(n, q) = q^n,$$

para todo $n \in \mathbb{Z}$, sendo a operação também herdada do corpo $\mathbb{Q}$. O mapa $f(x) = x^2$, para todo $x \in \mathbb{Q}$ é um homomorfismo de $\mathbb{Z}$-módulos entre $\mathbb{Q}^*$ e ele mesmo. De fato,

$$f(xy) = (xy)^2 = f(x)f(y),$$

$$f(x^n) = (x^n)^2 = x^{2n} = (x^2)^n = f(x)^n.$$

Contudo, a mesma função não define um homomorfismo de $\mathbb{Z}$-módulos entre $\mathbb{Q}$ e ele mesmo, pois $f(2+3) = 25 \neq f(2) + f(3) = 13$.

Definição 2.6. Uma sequência de R-módulos e homomorfismos

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

é dita *exata em M_i* se $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. A sequência é *exata* se ela é exata em cada M_i.

Temos, em particular

a) $0 \to N \xrightarrow{f} M$ é exata se, e somente se f é injetiva.

b) $M \xrightarrow{g} N \to 0$ é exata se, e somente se g é sobrejetiva.

A partir de agora e até o fim da seção, consideramos R um domínio de ideais principais.

Proposição 2.7. *Seja M um R-módulo. Suponha que $M = R/tR$, para algum $t \in R \setminus \{0\}$. Sejam $m \in M$ e $s \in R$ tal que $Ann_R(m) = sR$. Então*

i) Existe $h \in R$ tal que $t = sh$.

ii) Existe $n \in M$ tal que $m = hn$.

Demonstração. A afirmação i) segue do fato que, $tm = 0$ para qualquer $m \in M$, portanto $t \in \mathrm{Ann}(m)$, logo s divide t, portanto existe $h \in R$ tal que $sh = t$. Já a afirmação ii), como $s \mid t$, temos que $tR \subseteq sR \subseteq R$ e tR é um R-submódulo de sR, sendo assim sR/tR é um R-módulo. Considere a função

$$w : \ R/tR \to sR/tR \tag{2.1}$$

$$a + tR \mapsto sa + tR; \tag{2.2}$$

w está bem definida e é um homomorfismo de R-módulos. Temos que

$$sa + tR = 0 \Leftrightarrow sa \in tR \Leftrightarrow h \mid a,$$

pois $t = sh$. Logo $\mathrm{Ker}(w) = hR/tR$. Assim, temos a seguinte sequência exata

$$0 \to \frac{hR}{tR} \to \frac{R}{tR} \xrightarrow{w} \frac{sR}{tR} \to 0.$$

Portanto, se $ms = 0$, então $ms + tR = 0$ em R/tR, ou seja, $m \in \mathrm{Ker}(w)$, pela exatidão da sequência acima, $m = y + tR$, com $y = y_0 h$ ou seja, $\exists r_0 \in R$ tal que $m = y + tr_0 = h(y_0 + sr_0)$, pois $sh = t$. Definindo $n = y_0 + sr_0$ obtemos o resultado desejado: existe $n \in M$ tal que $hn = m$. □

2.2 A estrutura dos corpos finitos

Esta seção é dedicada a uma breve introdução aos corpos finitos, onde os resultados básicos que nos serão úteis durante o texto são expostos. Será assumido um conhecimento básico de teoria de grupos, assim como o estudo de extensões de corpos. Os resultados podem ser encontrados em [24] ou [1].

Seja p um número primo. O corpo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ é o menor corpo de característica p, chamado de *corpo primo*; ele é isomorfo à interseção de todos os subcorpos de qualquer corpo de característica p. Dada uma extensão finita de corpos $E \mid \mathbb{F}_p$ de grau $n > 0$, E possui p^n elementos pois pode ser visto como um espaço vetorial de dimensão n sobre $\mathbb{F}_p$. Reciprocamente, para cada potência p^n do primo p, existe, a menos de isomorfismo, um único corpo finito E com p^n elementos, mais precisamente, $E \simeq \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^{p^n} - \alpha = 0\}$, onde $\overline{\mathbb{F}}_p$ denota o fecho algébrico de $\mathbb{F}_p$.

Seja $q = p^n$, denotamos por $\mathbb{F}_q$ o corpo finito com q elementos. O fecho algébrico $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$ pode ser caracterizado da seguinte maneira:

$$\overline{\mathbb{F}}_q = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}.$$

A seguir temos alguns resultados importantes sobre a estrutura multiplicativa dos corpos finitos.

Proposição 2.8. *O grupo multiplicativo $\mathbb{F}_q^*$ é cíclico de ordem $q - 1$.*

Tal resultado motiva a seguinte definição.

Definição 2.9. Um elemento gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de *elemento primitivo* de $\mathbb{F}_q$. A ordem (multiplicativa) de um elemento $\alpha \in \mathbb{F}_q$ será denotada por $\mathrm{ord}(\alpha)$.

A estrutura cíclica de $\mathbb{F}_q$ nos permite obter alguns resultados acerca das k-potências de um elemento $\alpha \in \mathbb{F}_q$.

Proposição 2.10. *Sejam $\mathbb{F}_q$ um corpo finito e $k \in \mathbb{N}$. Um elemento não nulo $c \in \mathbb{F}_q$ é uma k-potência se, e somente se $c^{(q-1)/d} = 1$, onde $d = mdc(q-1, k)$.*

Agora focamos nas propriedades de extensões finitas de corpos finitos.

Definição 2.11. Sejam $\mathbb{F}_{q^n}|\mathbb{F}_q$ uma extensão de corpos finitos e $\alpha \in \mathbb{F}_{q^n}$. O polinômio $f \in \mathbb{F}_q[X]$ de menor grau tal que $f(\alpha) = 0$ é chamado de *polinômio mínimo* de α sobre $\mathbb{F}_q$.

Definição 2.12. Um polinômio $f \in \mathbb{F}_q[X]$ de grau $n \geq 1$ é um *polinômio primitivo* sobre $\mathbb{F}_q$ se é o polinômio mínimo sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^n}$.

Proposição 2.13. *Se $f \in \mathbb{F}_q[x]$ é irredutível de grau n, então f possui uma raiz $\alpha \in \mathbb{F}_{q^n}$. Todas as raízes de f são da forma α^{q^i}, para $i = 0, \ldots, n-1$. Ademais, todas as raízes de f são distintas.*

O corpo $\mathbb{F}_{q^n}$ pode ser visto como o corpo de decomposição de $\mathbb{F}_q$ para qualquer polinômio irredutível (e consequentemente separável, pela proposição anterior) de grau n sobre $\mathbb{F}_q$. Portanto, a extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$ é Galoisiana e denotamos por $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ o seu grupo de Galois.

Proposição 2.14. *Seja $\mathbb{F}_{q^n}$ um corpo finito. Então $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ é cíclico de ordem n, gerado pelo automorfismo de Frobenius $\sigma(\alpha) = \alpha^q$, para todo $\alpha \in \mathbb{F}_{q^n}$.*

Definimos agora uma base normal de $\mathbb{F}_{q^n}$ como um espaço vetorial sobre $\mathbb{F}_q$.

Definição 2.15. Dados a extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ e σ o automorfismo de Frobenius, se existe $\alpha \in \mathbb{F}_{q^n}$, tal que $\{\sigma^0(\alpha), \sigma^1(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)\} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ como espaço vetorial, então esta é chamada de uma *base normal* para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Dizemos que α como acima é um elemento normal (livre) de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Definição 2.16. Um polinômio $f \in \mathbb{F}_q[X]$ de grau $n \geq 1$ é um *polinômio normal e primitivo* sobre $\mathbb{F}_q$ se f for o polinômio mínimo de um elemento normal e primitivo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Veremos que bases normais sempre existem em extensões finitas de corpos finitos. No próximo exemplo construímos uma base normal de $\mathbb{F}_9$ sobre $\mathbb{F}_3$ gerada por um elemento primitivo.

Exemplo 2.4. Seja $\mathbb{F}_3 = \{0, 1, 2\}$, considere a extensão quadrática de $\mathbb{F}_3$, $\mathbb{F}_9 \simeq \frac{\mathbb{F}_3[X]}{(X^2+2X+2)} = \{a_0 + a_1\alpha \mid \alpha^2 = \alpha + 1, a_1, a_2 \in \mathbb{F}_3\}$. O polinômio $f(X) = X^2 + X + 2$ é irredutível sobre $\mathbb{F}_3$. Note que $f(\alpha+2) = (\alpha+2)^2 + (\alpha+2) + 2 = \alpha^2 + \alpha + 1 + \alpha + 1 = 3(\alpha+1) = 0$, portanto $(\alpha+2)$ é uma raiz de f, logo $(\alpha+2)^3$ também é uma raiz, e $(\alpha+2)^3 = \alpha^3 + 2 = 2\alpha$. Temos que $\{2\alpha, \alpha+2\}$ é uma base para a extensão $\mathbb{F}_9|\mathbb{F}_3$, sendo uma base normal, por definição.

O grupo multiplicativo $\mathbb{F}_9^*$ possui 8 elementos, portanto qualquer elemento de $\mathbb{F}_9$ diferente de 0, necessariamente tem ordem dividindo $8 = 2^3$. Temos que $(2\alpha)^2 = \alpha^2 = \alpha + 1 \neq 0$, $(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = 2 \neq 0$, portanto $(2\alpha)^8 = 1$, e concluímos que 2α é um elemento primitivo de $\mathbb{F}_9$. Logo a base $\{2\alpha, \alpha+2\}$ é uma base normal de $\mathbb{F}_9$ sobre $\mathbb{F}_3$ gerada por um elemento primitivo. □

Como a extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$ é galoisiana e cíclica com $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ gerado pelo automorfismo de Frobenius σ, definimos respectivamente a norma $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ e o traço $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ de um elemento α em $\mathbb{F}_{q^n}$ da seguinte

maneira

$$\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q} = \prod_{i=0}^{n-1} \sigma^i(\alpha),$$
$$\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha).$$

As funções traço e norma quando definidas para uma extensão $\mathbb{F}_q$ sobre seu corpo primo $\mathbb{F}_p$ serão chamadas de *traço absoluto* e *norma absoluta* e denotados por $\mathrm{Tr}_{\mathbb{F}_q}$ e $\mathrm{N}_{\mathbb{F}_q}$, respectivamente. Se m divide n, então existe um único subcorpo $\mathbb{F}_{q^m}$ contido em $\mathbb{F}_{q^n}$. Escrevendo $n = mk$, para $\alpha \in \mathbb{F}_{q^n}$, temos que

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^m}}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^k}.$$

A seguir, listamos algumas propriedades das funções traço e norma.

Proposição 2.17. *A função traço definida acima é tal que* $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$ *e satisfaz as seguintes propriedades para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$ *e* $c \in \mathbb{F}_q$*:*

i) $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{F}_{\mathrm{q}^\mathrm{n}}|\mathbb{F}_\mathrm{q}}(\alpha) + Tr_{\mathbb{F}_{\mathrm{q}^\mathrm{n}}|\mathbb{F}_\mathrm{q}}(\beta)$;

ii) $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$;

iii) $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ *é uma transformação linear sobrejetiva entre* $\mathbb{F}_{q^n}$ *e* $\mathbb{F}_q$*;*

iv) $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(c) = nc$*;*

v) $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha^{q^i}) = Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$*, para todo* $i = 0, \ldots, n-1$*.*

Proposição 2.18. *A função norma é tal que* $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha^{(q^n-1)/(q-1)}$ *e satisfaz as seguintes propriedades para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$ *e* $c \in \mathbb{F}_q$*.*

i) $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha\beta) = N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\beta)$*;*

ii) $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ *é um homomorfismo sobrejetivo entre* $\mathbb{F}_{q^n}^*$ *e* $\mathbb{F}_q^*$*;*

iii) $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(c) = c^n$*;*

iv) $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha^{q^i}) = N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$*, para todo* $i = 0, \ldots, n-1$*.*

Proposição 2.19 (Transitividade do traço e da norma)**.** *Sejam* K, E *e* F *corpos finitos tais que* $E \mid F \mid K$ *são extensões finitas. Então, para todo* $\alpha \in E$*,*

$$Tr_{E|K}(\alpha) = Tr_{F|K}(Tr_{E|F}(\alpha)),$$
$$N_{E|K}(\alpha) = N_{F|K}(N_{E|F}(\alpha)).$$

2.3 $\mathbb{F}_{q^n}$ visto como um módulo sobre $\mathbb{F}_q[X]$

Nesta seção descrevemos $\mathbb{F}_{q^n}$ como um módulo sobre $\mathbb{F}_q[X]$ com a finalidade de caracterizar os elementos que geram uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ como espaço vetorial. Os resultados nesta seção podem ser encontrados em [8], [22], e [27].

O grupo aditivo $\overline{\mathbb{F}}_q$ (e consequentemente $\mathbb{F}_{q^n}$) pode ser visualizado como um módulo sobre $\mathbb{F}_q[X]$ da seguinte maneira, se $\alpha \in \overline{\mathbb{F}}_q$ e $f = \sum_{i=0}^{m} a_i X^i \in \mathbb{F}_q[X]$, definimos a operação

$$f \circ \alpha := f^{\sigma}(\alpha) := \sum_{i=0}^{m} a_i \sigma^i(\alpha) = \sum_{i=0}^{m} a_i \alpha^{q^i},$$

onde f^{σ} é obtido a partir do polinômio f substituindo X^i por X^{q^i} (observe que o termo constante $a_0 X^0$ é levado em $a_0 X^{q^0} = a_0 X$). Para $\alpha \in \overline{\mathbb{F}}_q$, o seu anulador

$$\mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha) = \{f \in \mathbb{F}_q[X] \mid f \circ \alpha = 0\} \subseteq \mathbb{F}_q[X]$$

é um ideal principal. Observe que para $\alpha \in \mathbb{F}_{q^n}$ temos

$$\alpha^{q^n} = \alpha \Leftrightarrow \sigma^n(\alpha) = \alpha \Leftrightarrow \sigma^n(\alpha) - \alpha = 0 \Leftrightarrow (X^n - 1) \circ \alpha = 0.$$

Portanto, $\mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha) \neq (0)$ e existe um único polinômio mônico $g_\alpha \in \mathbb{F}_q[X]$ tal que $(g_\alpha) = \mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha)$.

Definição 2.20. A $\mathbb{F}_q$-ordem de $\alpha \in \overline{\mathbb{F}}_q$ é definida por $\mathrm{Ord}(\alpha) = g_\alpha$, onde g_α é o polinômio mônico que gera o anulador de α sobre $\mathbb{F}_q[X]$.

Como $\mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha) = (\mathrm{Ord}(\alpha))$, temos que que $\mathrm{Ord}(\alpha)$ divide $X^n - 1$, onde n é o grau da menor extensão de $\mathbb{F}_q$ que contém α. Ademais, se $h \in \mathbb{F}_q[X]$ é tal que $h \circ \alpha = 0$, então $\mathrm{Ord}(\alpha)$ divide h. A ordem do elemento $\alpha \in \mathbb{F}_{q^n}$ referente ao grupo multiplicativo é mencionada como a ordem *multiplicativa* de α, enquanto a $\mathbb{F}_q$-ordem é mencionada como a $\mathbb{F}_q$-ordem (ou apenas ordem, quando o corpo $\mathbb{F}_q$ estiver fixo) *aditiva* de α.

Usamos a noção de $\mathbb{F}_q$-ordem para caracterizar os elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Observe a analogia entre o próximo teorema e a caracterização dos elementos primitivos no grupo multiplicativo: um elemento $\alpha \in \mathbb{F}_q^*$ é primitivo se, e somente se $\mathrm{ord}(\alpha) = q^n - 1$.

Teorema 2.21. *Um elemento $\alpha \in \overline{\mathbb{F}}_q$ define uma base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ se, e somente se, Ord$(\alpha) = X^n - 1$.*

Demonstração. Suponha inicialmente que α seja um elemento normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Isso implica que o conjunto $\{\alpha, \ldots, \alpha^{q^{n-1}}\}$ é linearmente independente sobre $\mathbb{F}_q$, logo o grau do polinômio $\mathrm{Ord}(\alpha)$ é maior ou igual a n. Como $\mathrm{Ord}(\alpha)$ divide $X^n - 1$, segue que $\mathrm{Ord}(\alpha) = X^n - 1$.

Reciprocamente, se $\mathrm{Ord}(\alpha) = X^n - 1$, então o conjunto $\{\alpha, \ldots, \alpha^{q^{n-1}}\}$ é linearmente independente sobre $\mathbb{F}_q$. De fato, se existissem $a_i \in \mathbb{F}_q$, $i = 1, \ldots, n-1$, tais que $a_0\alpha + \cdots + a_{n-1}\alpha^{q^{n-1}} = 0$, teríamos necessariamente $\mathrm{grau}(\mathrm{Ord}(\alpha)) < n$, contrariando a hipótese. Portanto, o subespaço vetorial gerado por $\{\alpha, \ldots, \alpha^{q^{n-1}}\} \subseteq \mathbb{F}_{q^n}$ tem exatamente q^n elementos sendo igual a $\mathbb{F}_{q^n}$. Logo, o conjunto $\{\alpha, \ldots, \alpha^{q^{n-1}}\}$ é uma base (normal) para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. □

Exemplo 2.5. Retornando ao Exemplo 2.4, já vimos que o conjunto $\{2\alpha, \alpha + 2\}$ é uma base normal para a extensão quadrática $\mathbb{F}_9|\mathbb{F}_3$, então devemos necessariamente ter $\mathrm{Ord}(2\alpha) = X^2 - 1 = X^2 + 2$. Verifiquemos o fato. Como $X^2 + 2 = (X + 2)(X + 1)$ e $\mathrm{Ord}(2\alpha)$ divide $X^2 + 2$, segue que as possibilidades para $\mathrm{Ord}(2\alpha)$ são $X + 2, X + 1$ ou $X^2 + 2$. Observe que $(X + 2) \circ (2\alpha) = (2\alpha)^3 + 2(2\alpha) = 2(2\alpha + 1) + \alpha = 2\alpha + 2 \neq 0$, assim como $(X + 1) \circ (2\alpha) = 2 \neq 0$, portanto $\mathrm{Ord}(2\alpha) = X^2 + 2$, como esperado.

O elemento $\alpha+1$ é tal que $(X+1)\circ(\alpha+1) = (\alpha+1)^3+\alpha+1 = \alpha^3+1+\alpha+1 = 2\alpha+1+1+\alpha+1 = 0$, logo $\alpha+1$ não gera uma base normal para a extensão $\mathbb{F}_9 \mid \mathbb{F}_3$. De fato, o conjunto $\{\alpha+1, (\alpha+1)^3\} = \{\alpha+1, 2\alpha+2\}$ não é linearmente independente sobre $\mathbb{F}_3$. □

Definição 2.22. Seja n um número inteiro. A função $\varphi : \mathbb{Z} \to \mathbb{N}$ definida por

$$\varphi(n) = \#\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*,$$

é chamada de *função de Euler*.

Do mesmo modo que a função φ de Euler desempenha um papel importante no estudo dos números inteiros, definiremos uma função análoga para polinômios em uma variável sobre $\mathbb{F}_q$, que nos auxiliará no estudo do $\mathbb{F}_q[X]$-módulo $\mathbb{F}_{q^n}$.

Definição 2.23 (Função de Euler para polinômios)**.** Sejam $f \in \mathbb{F}_q[X]$ mônico de grau m, (f) o ideal gerado por f em $\mathbb{F}_q[X]$ e $\frac{\mathbb{F}_q[X]}{(f)}$ o anel quociente de $\mathbb{F}_q[X]$ por (f). Definimos as funções $N, \Phi : \mathbb{F}_q[X] \to \mathbb{N}$ por

$$N(f) = \#\left(\frac{\mathbb{F}_q[X]}{(f)}\right) = q^m,$$

o número de elementos no anel $\frac{\mathbb{F}_q[X]}{(f)}$, e

$$\Phi(f) = \#\left(\frac{\mathbb{F}_q[X]}{(f)}\right)^*,$$

o número de elementos invertíveis no anel $\frac{\mathbb{F}_q[X]}{(f)}$.

Identificando o anel quociente $\frac{\mathbb{F}_q[X]}{(f)}$ com o seguinte conjunto

$$\frac{\mathbb{F}_q[X]}{(f)} = \{a_0 + a_1X + \cdots + a_{m-1}X^{m-1} | a_i \in \mathbb{F}_q, f(X) = 0\}, \tag{2.3}$$

os elementos de $\frac{\mathbb{F}_q[X]}{(f)}$ podem ser vistos como polinômios em $\mathbb{F}_q[X]$ de grau estritamente menor que o grau de f. Ao nos restringirmos ao conjunto $(\mathbb{F}_q[X]/(f))^*$, estamos considerando apenas as unidades do anel quociente, em outras palavras, apenas os polinômios de grau estritamente menor que o grau de f e primos com f. Portanto a função Φ conta o número de polinômios $g \in \mathbb{F}_q[X]$ tais que $\text{grau}(g) < \text{grau}(f)$ e $\text{mdc}(f, g) = 1$.

A seguinte proposição reflete a semelhança entre a função φ e a função Φ. Para todo $n \in \mathbb{N}$, a função φ de Euler satisfaz

$$\sum_{d|n} \varphi(n) = n \text{ e } \varphi(n) = n \prod_{p|n,\ p \text{ primo}} \left(1 - \frac{1}{p}\right).$$

Proposição 2.24. *Seja $f \in \mathbb{F}_q[X]$. As seguintes propriedades são válidas para a função Φ:*

i) $\sum_{g|f} \Phi(g) = N(f)$, *e*

ii) $\Phi(f) = N(f) \prod_{g|f,\ g\ irred.} \left(1 - \frac{1}{N(g)}\right)$.

Demonstração. Para um divisor mônico $d \in \mathbb{F}_q[X]$ de f, defina

$$A_d = \{g \in \mathbb{F}_q[X]/(f) \mid \text{mdc}(g, f) = d\}.$$

Para qualquer g pertencente ao anel quociente, obtemos

$$g \in A_d \Leftrightarrow \text{mdc}(f, g) = d \Leftrightarrow \text{mdc}\left(\frac{f}{d}, \frac{g}{d}\right) = 1 \Leftrightarrow \frac{g}{d} \in \left(\frac{\mathbb{F}_q[X]}{(f/d)}\right)^*.$$

Logo, $\#A_d = \Phi(f/d)$. Observe também que para um elemento qualquer $h \in \mathbb{F}_q[X]/(f)$, temos que $\text{grau}(h) < \text{grau}(f)$ (por (2.3)). Portanto $h \in A_d$ para um, e somente um, (pela unicidade do mdc) d divisor de f. Concluímos então que

$$\frac{\mathbb{F}_q[X]}{(f)} = \bigcup_{d|f} A_d;$$

sendo a união disjunta, levando-nos às seguinte igualdades

$$N(f) = \#\frac{\mathbb{F}_q[X]}{(f)} = \sum_{d|f} \#A_d = \sum_{d|f} \Phi\left(\frac{f}{d}\right) = \sum_{d|f} \Phi(d).$$

Quanto ao segundo item, observe primeiramente que se $g, h \in \mathbb{F}_q[X]$ são primos entre si, então $g\mathbb{F}_q[X] + h\mathbb{F}_q[X] = \mathbb{F}_q[X]$, portanto temos que

$$\Phi(gh) = \#\left(\frac{\mathbb{F}_q[X]}{(gh)}\right)^* = \#\left(\frac{\mathbb{F}_q[X]}{(g)}\right)^* \cdot \#\left(\frac{\mathbb{F}_q[X]}{(h)}\right)^* = \Phi(g)\Phi(h),$$

pelo Teorema Chinês dos Restos. Sejam $g \in \mathbb{F}_q[X]$ um polinômio irredutível de grau m e $e \in \mathbb{N}$, $e \geq 1$. Seja $h \in \mathbb{F}_q[X]/(g^e)$, h não é invertível se, e somente se, $\text{mdc}(h, g^e) \neq 1$ e $\text{grau}(h) < me$ (h pertence ao anel quociente). Como $\text{mdc}(h, g^e)$ divide g^e e h, temos que $h = tg$ para algum $t \in \mathbb{F}_q[X]$ e $\text{grau}(t) + m = \text{grau}(h) < me$. Logo $\text{grau}(t) < me - m$ e temos q^{em-m} escolhas para o polinômio t. Daí conclui-se que temos q^{em-m} polinômios que não são unidades em $\frac{\mathbb{F}_q[X]}{(g^e)}$. Assim $\Phi(g^e) = q^{me} - q^{me-m} = q^{me}(1 - q^{-m})$. Agora, dado um polinômio qualquer $f \in \mathbb{F}_q[X]$

$$\Phi(f) = \Phi(g_1^{e_1} \dots g_s^{e_s}) = \prod_{i=1}^{s} q^{\text{grau}(g_i)e_i} \left(1 - \frac{1}{q^{\text{grau}(g_i)}}\right).$$

O resultado segue observando que $N(g_i) = q^{\text{grau}(g_i)}$ e que $N(f) = q^{\text{grau}(f)} = \prod q^{\text{grau}(g_i^{e_i})} = \prod q^{\text{grau}(g_i)e_i}$. □

Proposição 2.25. *Seja $f = X^n + \dots + a_1X + a_0 \in \mathbb{F}_q[X]$ tal que $a_0 \neq 0$. Então*

$$\sum_{g|f} \#\{\alpha \in \overline{\mathbb{F}}_q : Ord(\alpha) = g\} = N(f).$$

Demonstração. Primeiramente, observe que

$$\bigcup_{g|f}\{\alpha \in \overline{\mathbb{F}}_q \mid \mathrm{Ord}(\alpha) = g\} = \{\alpha \in \overline{\mathbb{F}}_q \mid f^\sigma(\alpha) = 0\},$$

pois se $\alpha \in \overline{\mathbb{F}}_q$ é tal que $g^\sigma(\alpha) = g\circ\alpha = 0$, então, como g divide f, $f^\sigma(\alpha) = f\circ\alpha = gh\circ\alpha = h(g\circ\alpha) = h\circ 0 = 0$. Temos também que qualquer raiz de f^σ é tal que $f \circ \alpha = 0$, logo $\mathrm{Ord}(\alpha)$ divide f. Observe também que a inclusão acima é disjunta, pois a $\mathbb{F}_q$-ordem de um elemento é única. Como $\frac{\partial f^\sigma}{\partial X} = a_0 \neq 0$, o polinômio f^σ possui apenas zeros simples, totalizando $\mathrm{grau}(f^\sigma) = q^{\mathrm{grau}(f)} = N(f)$. □

Estamos aptos a demonstrar o seguinte resultado, devido a Ore [27].

Teorema 2.26. *Seja $f \in \mathbb{F}_q[X]$ mônico e relativamente primo com X. Então o número de elementos $\alpha \in \overline{\mathbb{F}}_q$ com $Ord(\alpha) = f$ é igual a $\Phi(f)$.*

Demonstração. O resultado é válido se $\mathrm{grau}(f) = 1$. De fato, se $f = X + a$, temos que $\Phi(f) = q - 1$ e, aplicando a proposição anterior, observando que os divisores de f são apenas 1 e f e notando que $\mathrm{Ord}(\alpha) = 1$ se, e somente se, $\alpha = 0$, temos o resultado.

Suponha agora o teorema válido para todo o polinômio mônico de grau menor ou igual a $n-1$ e primo com X. Seja f mônico de grau n e primo com X. Pela Proposição 2.25, temos que

$$\sum_{g|f} \#\{\alpha \in \overline{\mathbb{F}}_q : \mathrm{Ord}(\alpha) = g\} = N(f) = \sum_{g|f} \Phi(g).$$

Para cada divisor próprio de f, aplicamos a hipótese de indução, visto que um divisor próprio tem grau estritamente menor que $\mathrm{grau}(f) = n$. Obtemos então:

$$\sum_{g|f, g\neq f} \Phi(g) + \#\{\alpha \in \overline{\mathbb{F}}_q : \mathrm{Ord}(\alpha) = f\} = \sum_{g|f, g\neq f} \Phi(g) + \Phi(f).$$

Cancelando os termos iguais, obtemos o resultado. □

Em particular, existem $\Phi(X^n - 1)$ elementos livres (normais) em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, o que nos mostra que bases normais sempre existem. Para completar a analogia entre o grupo multiplicativo $\mathbb{F}_{q^n}^*$ e o grupo aditivo $\mathbb{F}_{q^n}$ (visto como um $\mathbb{F}_q[X]$-módulo), seja $\alpha \in \mathbb{F}_{q^n}$ normal e considere o mapa $\psi : \mathbb{F}_q[X] \to \mathbb{F}_{q^n}$

$$\psi(f) = f^\sigma(\alpha) = f \circ \alpha.$$

Temos que ψ é um homomorfismo de $\mathbb{F}_q[X]$-módulos (observando que, ao considerar $\mathbb{F}_{q^n}$ como um módulo sobre $\mathbb{F}_q[X]$, estamos nos restringindo apenas à sua estrutura como grupo aditivo) tal que $\mathrm{Ker}(\psi) = \mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha)$. Já que α foi escolhido como sendo um elemento normal sobre $\mathbb{F}_q$, segue que $\mathrm{Ann}_{\mathbb{F}_q[X]}(\alpha) = (X^n - 1)\mathbb{F}_q[X]$ e temos, portanto,

$$\mathbb{F}_{q^n} \simeq \frac{\mathbb{F}_q[X]}{(X^n - 1)\mathbb{F}_q[X]}, \text{ vistos como } \mathbb{F}_q[X] - \text{módulos.}$$

Tal resultado é análogo a

$$\mathbb{F}_{q^n}^* \simeq \frac{\mathbb{Z}}{(q^n-1)\mathbb{Z}}, \text{ vistos como } \mathbb{Z}-\text{módulos},$$

pois, fixando $\alpha \in \mathbb{F}_{q^n}^*$ primitivo e definindo $z_\alpha : \mathbb{Z} \longrightarrow \mathbb{F}_{q^n}^*$ como $z_\alpha(\ell) = \alpha^\ell$, obtemos um homomorfismo sobrejetivo de $\mathbb{Z}$-módulos com núcleo $\mathrm{Ker}(z_\alpha) = (q^n-1)\mathbb{Z}$.

Em particular, se $\alpha \in \mathbb{F}_{q^n}$ tem $\mathbb{F}_q$-ordem g, então $\alpha = h \circ \beta$, para algum $\beta \in \mathbb{F}_q$, onde $h = \frac{X^n-1}{g}$ (Proposição 2.7).

3 Caráteres

Em um corpo finito $\mathbb{F}_{q^n}$ os elementos primitivos estão naturalmente relacionados à estrutura do seu grupo multiplicativo. Já os elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ estão relacionados à estrutura aditiva de $\mathbb{F}_{q^n}$. Nossa finalidade é contar a quantidade de elementos em $\mathbb{F}_{q^n}$ com propriedades fixadas. Como $\mathbb{F}_{q^n}^*$ e $\mathbb{F}_{q^n}$ são ambos grupos abelianos finitos, na teoria de caráteres, suporemos G um grupo abeliano finito (usaremos a notação multiplicativa). Quando necessário, nos restringiremos aos grupos $\mathbb{F}_{q^n}^*$ ou $\mathbb{F}_{q^n}$. Os resultados dessa sessão podem ser encontrados em [24] ou [1] para uma abordagem mais geral sobre a teoria de caráteres.

3.1 Definição e propriedades básicas

Definição 3.1. Seja G um grupo abeliano de ordem n. Um *caráter* χ de G é um homomorfismo entre G e o grupo multiplicativo $U = \{x \in \mathbb{C} \mid |x| = 1\}$ dos números complexos com valor absoluto 1.

Proposição 3.2 (Propriedades básicas dos caráteres)**.** *Seja χ um caráter de G, um grupo abeliano de ordem n. Então:*

i) $\chi(1) = 1$;

ii) $\chi(g)$ *é uma n-ésima raiz da unidade;*

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

Denotamos por $\widehat{G}$ o conjunto dos caráteres de um grupo G, $\widehat{G}$ é chamado de *dual* de G. Para $\chi, \psi \in \widehat{G}$, definimos o produto $\chi\psi$ como $\chi\psi(g) := \chi(g)\psi(g)$, para todo $g \in G$. É fácil verificar que esta operação torna o conjunto $\widehat{G}$ um grupo abeliano. Denotamos o *caráter trivial* por χ_0 que é definido por $\chi_0(g) = 1$, para todo $g \in G$. Como os valores de um caráter de G são raízes da unidade de ordem n, o grupo $\widehat{G}$ é finito.

Proposição 3.3. *Sejam G um grupo cíclico de ordem n e g um gerador de G. Para um inteiro fixado j, $0 \leq j \leq n-1$, a função*

$$\chi_j(g^k) = e^{(2\pi ijk)/n}, \quad k = 0, \ldots, n-1,$$

onde $i \in \mathbb{C}$, define um caráter de G. Reciprocamente, se χ é um caráter de G, então $\chi(g) = e^{2\pi ij/n}$, para algum j, $0 \leq j \leq n-1$, logo $\chi = \chi_j$. Portanto $\widehat{G}$ possui exatamente n elementos.

Proposição 3.4. *Sejam H um subgrupo de um grupo abeliano finito G e χ um caráter definido em H. Então χ pode ser estendido a um caráter definido em G, ou seja, existe um caráter λ definido em G tal que $\lambda(h) = \chi(h)$, $\forall h \in H$.*

Demonstração. Seja H um subgrupo próprio de G e seja $a \in G \setminus H$. Sejam $H_1 = \langle H, a\rangle$ o subgrupo de G gerado por H e a, e $m \in \mathbb{Z}$ o menor inteiro positivo tal que $a^m \in H$. Portanto, qualquer elemento $g \in H_1$ pode ser representado unicamente da forma $g = a^j h$ aonde $h \in H$ e $0 \leq j < m$. Seja χ um caráter de H e escolha $\omega \in \mathbb{C}$ tal que $\omega^m = \chi(a^m)$. Vamos mostrar que a função $\chi_1(g) = \omega^j \chi(h)$ é um caráter em H_1. De fato, seja $g_1 \in H_1$, então $g_1 = a^k h_1$, onde $0 \leq k < m$ e $h_1 \in H$. Se $j + k < m$, então $\chi_1(gg_1) = \omega^{j+k}\chi(hh_1) = \chi_1(h)\chi_1(h_1)$. Se $j + k \geq m$, escreva $gg_1 = a^{j+k-m}(a^m hh_1)$ então $\chi_1(gg_1) = \omega^{j+k-m}\chi(a^m hh_1) = \omega^{j+k}\chi(hh_1) = \chi_1(h)\chi_1(h_1)$. Temos também que $\chi(h) = \chi_1(h)$ se $h \in H$. Agora, se $H_1 = G$, a proposição é válida, caso contrário, repita o processo acima, ou seja, considere $b \in G \setminus H_1$ e defina o grupo H_2 gerado por H_1 e b e prossiga analogamente. Como G é finito, em um número finito de passos obteremos um caráter χ_1 em G tal que $\chi_1(h) = \chi(h)$, para todo $h \in H$. □

Proposição 3.5. *Dados $g, h \in G$ e $g \neq h$, existe um caráter χ de G tal que $\chi(g) \neq \chi(h)$.*

Demonstração. É suficiente mostrar que se $w := gh^{-1} \neq 1$ então existe um caráter χ de G tal que $\chi(w) \neq 1$. De fato, seja H o subgrupo cíclico gerado por w. Então pela Proposição 3.3, podemos escolher um caráter em H tal que $\chi(w) \neq 1$ e pela Proposição 3.4, podemos estendê-lo a um caráter de G. □

Desse fato, seguem duas identidades envolvendo caráteres que serão de notável importância ao longo o texto.

Proposição 3.6. *Se χ é um caráter não trivial de um grupo abeliano finito G, então*

$$\sum_{g \in G} \chi(g) = 0. \tag{3.1}$$

Se $g \in G$ e $g \neq 1$, então

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0. \tag{3.2}$$

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

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

Portanto, temos

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

o que implica a primeira identidade. Para a segunda identidade, observe que a função $\hat{g} : \widehat{G} \to U$ definida por $\hat{g}(\chi) = \chi(g)$, para $\chi \in \widehat{G}$ é um caráter do grupo abeliano finito $\widehat{G}$. Note que $\hat{g}$ é não trivial, pois pela Proposição 3.5, sempre existe um caráter $\chi \in \widehat{G}$ tal que $\chi(g) \neq \chi(1) = 1$. Portanto, podemos aplicar a identidade 3.1 ao grupo $\widehat{G}$,

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

□

Como corolário dessa proposição, temos o seguinte resultado.

Corolário 3.6.1. *O número de caráteres de um grupo abeliano finito G é igual a $|G|$.*

Demonstração. Pela identidade (3.2) da Proposição 3.6, temos que

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

pois o único $g \in G$ que não anula o somatório é $g = 1$. Como as somas são finitas, podemos inverter os somatórios

$$\sum_{g \in G} \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g).$$

Agora, pela identidade (3.1) da Proposição 3.6, para todo caráter não trivial de $\widehat{G}$ o somatório $\sum_{g\in G}\chi(g)$ se anula. Quando $\chi=\chi_0$, obtemos que

$$\sum_{g\in G}\chi_0(g)=|G|.$$

O resultado segue. □

Pode-se dizer mais ainda sobre a relação entre G e $\widehat{G}$.

Teorema 3.7. *Seja G um grupo abeliano finito. Então G é isomorfo a $\widehat{G}$.*

O Teorema acima é uma consequência dos seguintes lemas.

Lema 3.8. *Se G é um grupo cíclico de ordem n, então $G\simeq\widehat{G}$.*

Demonstração. Pela Proposição 3.3, se g gera G, então $\chi(g)=e^{(2\pi i)/n}$, assim, se $\psi\in\widehat{G}$, então existe um k tal que $\psi(g)=e^{(2\pi ik)/n}=\chi(g)^k$. Logo $\psi(g^j)=\psi(g)^j=\chi(g)^{jk}=\chi(g^j)^k$, $\forall j=0,\ldots,n-1$. Temos então que $\psi=\chi^k$. Portanto, χ gera $\widehat{G}$. Como $\widehat{G}$ e G possuem o mesmo número de elementos, o resultado segue. □

Lema 3.9. *Se G e H são grupos abelianos finitos, então $\widehat{G\times H}\simeq\widehat{G}\times\widehat{H}$.*

Demonstração. Seja χ um caráter de $G\times H$. Sejam $\chi_G(g)=\chi(g,1)$ e $\chi_H(h)=\chi(1,h)$, para todo $g\in G$ e $h\in H$. Temos que χ_G e χ_H são caráteres de G e H respectivamente e $\chi(g,h)=\chi((g,1)(1,h))=\chi(g,1)\chi(1,h)=\chi_G(g)\chi_H(h)$. Assim, o mapa ϕ que leva χ em (χ_G,χ_H) é um homomorfismo de grupos. Se χ é tal que $(\chi_G,\chi_H)=(\chi_0,\psi_0)$, então $\chi(g,h)=\chi_G(g)\chi_H(h)=1$, para qualquer $(g,h)\in G\times H$. Logo, χ é o caráter trivial em $G\times H$. Portanto ϕ é injetiva. Pelo Corolário 3.6.1, temos que $\widehat{G\times H}$ tem o mesmo número de elementos que $\widehat{G}\times\widehat{H}$, logo ϕ é um isomorfismo de grupos. □

Corolário 3.9.1. *Se $G_1,G_2,\ldots,G_n$ são grupos abelianos finitos, então o dual de $G_1\times G_2\times\ldots\times G_n$ é isomorfo a $\widehat{G_1}\times\ldots\times\widehat{G_n}$.*

A prova do Teorema 3.7 segue diretamente dos Lemas 3.8 e 3.9 e do fato de que todo grupo abeliano finito é isomorfo a um produto direto de grupos cíclicos.

Definição 3.10. O anulador de $H<G$ em $\widehat{G}$ é o conjunto

$$\mathrm{Ann}_G(H)=\{\chi\in\widehat{G}\mid\chi(h)=1,\forall h\in H\}.$$

$\mathrm{Ann}_G(H)$ é um subgrupo de $\widehat{G}$.

Proposição 3.11. *Se G é um grupo abeliano finito, H um subgrupo próprio de G e $g\in G\setminus H$, então existe um caráter χ de G que anula H, mas $\chi(g)\neq 1$.*

Demonstração. Seja $gH\in G/H$ tal que $gH\neq 1$. Pela Proposição 3.5, temos que existe um caráter χ de G/H tal que $\chi(gH)\neq 1$. Denotando por ϕ o homomorfismo quociente entre G e G/H, obtemos que $\psi=\chi\circ\phi$ é um caráter de G que anula H e $\psi(g)=\chi(\phi(h))=\chi(gH)\neq 1$. □

Proposição 3.12. *Seja H um subgrupo de G. O anulador de H em $\widehat{G}$ é isomorfo a $\widehat{G/H}$.*

Demonstração. Seja $\text{Ann}(H) = \{\chi \in \widehat{G} \mid \chi(h) = 1, \forall h \in H\}$ o anulador de H em $\widehat{G}$. Seja $\phi : G \longrightarrow G/H$ o homomorfismo quociente e defina a seguinte função $\rho : \widehat{G/H} \longrightarrow \widehat{G}$

$$\rho(\chi) = \chi \circ \phi.$$

Temos que ρ é um homomorfismo de grupos e sua imagem está contida em $\text{Ann}(H)$, pois dado $\chi \in \widehat{G/H}$, se $h \in H$, então $\rho(\chi(h)) = \chi(\phi(h)) = 1$. Temos também que ρ é injetiva, pois se $\rho(\chi) = \chi_0$ (o caráter trivial em $\widehat{G}$), então $\chi(\phi(g)) = \chi(gH) = 1$, para todo $g \in G$, logo χ é o caráter trivial em $\widehat{G/H}$. Finalmente, ρ é também sobrejetiva, pois para um caráter $\chi \in \text{Ann}(H)$, definimos $\beta(gH) = \chi(g)$. Este é um caráter bem definido em G/H e $\chi = \beta \circ \phi$, o que conclui a prova. □

Corolário 3.12.1. *O anulador de H em $\widehat{G}$ é isomorfo a G/H.*

3.2 A função característica dos elementos k-livres

Seja G um grupo cíclico de ordem n e k um divisor positivo de n. Nesta seção, definimos o conceito de elemento k-livre sobre um grupo cíclico finito G e construímos uma função característica para o subconjunto formado por tais elementos.

Um elemento $g \in G$ gera G se, e somente se, sempre que escrevermos $g = g_1^d$, para algum $g_1 \in G$, então $\text{mdc}(d, n) = 1$. Uma generalização desse fato pode ser obtida da seguinte maneira.

Definição 3.13. Seja G um grupo cíclico de ordem n. Para um divisor k da ordem de G, um elemento $g \in G$ é dito *k-livre* se, sempre que $g = g_1^d$, onde $g_1 \in G$ e $d|k$, implicar $d = 1$.

Note que, com essa nova definição, os elementos que geram G são elementos n-livres. Fixado k um divisor de n, vamos construir a função característica para os elementos k-livres em um grupo cíclico.

Definição 3.14 (Função de Mobius)**.** Seja D um domínio de ideais principais. Para um elemento não nulo $t \in D$, a função de Mobius é definida da seguinte maneira:

$$\mu(t) = \begin{cases} 1, & \text{se } t \text{ é uma unidade,} \\ (-1)^s, & \text{se } t \text{ é o produto de } s \text{ elementos irredutíveis distintos,} \\ 0, & \text{se } t \text{ é divisível pelo quadrado de um elemento irredutível.} \end{cases}$$

A função de Mobius é uma função multiplicativa, ou seja, se t, r são elementos de D tais que $\text{mdc}(t, r) = 1$, então $\mu(tr) = \mu(t)\mu(r)$. Construiremos agora a função característica para os elementos k-livres de um grupo cíclico finito G. Tal função é uma generalização da função característica para os elementos primitivos de $\mathbb{F}_q$, conhecida como a fórmula de Vinogradov .

Teorema 3.15. *Seja G um grupo cíclico de ordem n. Para k um divisor de n, defina a seguinte função*

$$V_k(g) = \sum_{d|k} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \widehat{G}, ord(\chi) = d} \chi(g), \text{ para todo } g \in G.$$

Então

$$V_k(g) = \begin{cases} 0, & \text{se } g \text{ não é } k\text{-livre}, \\ \dfrac{k}{\varphi(k)}, & \text{se } g \text{ é } k\text{-livre}. \end{cases}$$

Em particular, se $k = |G|$, então $V_{|G|}(g) \neq 0$ se, e somente se, g gera G.

Vamos primeiro mostrar o seguinte lema.

Lema 3.16. *Sejam G um grupo cíclico de ordem n e $\widehat{G}$ seu dual. Valem as seguintes afirmações:*

a) Se $\ell \in \mathbb{N}$ é um primo divisor de n, então existem $\varphi(\ell) = \ell - 1$ caráteres de ordem ℓ em $\widehat{G}$.

b) Se $\ell_1, \ell_2 \in \mathbb{N}$ são primos distintos que dividem n, então todo caráter de ordem $\ell_1\ell_2$ pode ser escrito como o produto de um caráter de ordem ℓ_1 com um caráter de ordem ℓ_2.

c) Para $g \in G$ e $\ell_1, \ell_2 \in \mathbb{N}$, primos distintos divisores de n, temos que

$$\left(\sum_{ord(\chi)=\ell_1} \chi(g)\right)\left(\sum_{ord(\chi)=\ell_2} \chi(g)\right) = \left(\sum_{ord(\chi)=\ell_1\ell_2} \chi(g)\right),$$

onde os somatórios percorrem todos os caráteres de G com dada ordem.

d) Se ℓ é um número primo divisor de n e $g \in G$, então

$$\left(\sum_{ord(\chi)=\ell} \chi(g)\right) + 1 = \sum_{\chi^\ell = \chi_0} \chi(g),$$

onde χ_0 denota o caráter trivial de G e o último somatório percorre todos os caráteres χ de G tais que $\chi^\ell = \chi_0$, i.e., $\chi(g)^\ell = 1, \forall g \in G$.

Demonstração. Os itens *a*) e *b*), são simples consequências de $\widehat{G}$ ser também um grupo cíclico e finito de ordem n. O item *c*), por sua vez segue diretamente do item *b*). Quanto ao item *d*), basta observar que como ℓ é primo, os caráteres tais que $\chi^\ell = \chi_0$ são exatamente aqueles que possuem ordem um divisor de ℓ, logo são os $\varphi(\ell) = \ell - 1$ de ordem ℓ e o caráter trivial, portanto o resultado segue. □

Vamos agora à demonstração do Teorema 3.15.

Demonstração. Seja d um divisor de k. Observe que a função de Mobius apenas retorna um valor diferente de zero se d é livre de quadrados, portanto podemos escrever $V_k(g)$ da seguinte maneira: sejam, $p_1, \ldots, p_s$ os primos distintos que aparecem na fatoração de k. Então

$$\begin{aligned} V_k(g) = \; 1 + \sum_{i=1}^{s} \frac{\mu(p_i)}{\varphi(p_i)} \sum_{\mathrm{ord}(\chi)=p_i} \chi(g) + \sum_{1\leq i<j\leq s} \frac{\mu(p_ip_j)}{\varphi(p_ip_j)} \sum_{\mathrm{ord}(\chi)=p_ip_j} \chi(g) + \\ \ldots + \frac{\mu(p_1\ldots p_s)}{\varphi(p_1\ldots p_s)} \sum_{\mathrm{ord}(\chi)=p_1\ldots p_s} \chi(g). \end{aligned} \tag{3.3}$$

Como as funções φ e μ são multiplicativas, $\mu(p_i) = -1$, $\varphi(p_i) = p_i - 1$ e pelo item c) do Lema 3.16, podemos reescrever a Equação (3.3) na seguinte forma:

$$V_k(g) = \prod_{i=1}^{s} \left(1 - \frac{1}{p_i - 1} \sum_{\mathrm{ord}(\chi)=p_i} \chi(g) \right).$$

Somando e subtraindo $\dfrac{-1}{p_i - 1}$ no produtório, obtemos

$$V_k(g) = \prod_{i=1}^{s} \left(\frac{p_i}{p_i - 1} - \frac{1}{p_i - 1} \left(\sum_{\mathrm{ord}(\chi)=p_i} \chi(g) + 1 \right) \right).$$

Pelo item d) do Lema 3.16, podemos reescrever tal produtório na forma

$$V_k(g) = \prod_{i=1}^{s} \left(\frac{p_i}{p_i - 1} - \frac{1}{p_i - 1} \sum_{\chi^{p_i}=\chi_0} \chi(g) \right).$$

Observe que, se g não é k-livre, então $g = g_1^{p_j}$ para algum $1 \leq j \leq s$. Logo

$$\sum_{\chi^{p_j}=\chi_0} \chi(g) = \sum_{\chi^{p_j}=\chi_0} \chi(g_1)^{p_j} = p_j,$$

fazendo com que $V_k(g) = 0$. Para $\ell \in \mathbb{N}$, considere o conjunto $\{\chi \in \widehat{\mathbb{F}_{q^n}^*} \mid \chi^\ell(g) = 1, \forall g \in G\} = \{\chi \in \widehat{\mathbb{F}_{q^n}^*} \mid \chi(g^\ell) = 1, \forall g \in G\} = \{\chi \in \widehat{\mathbb{F}_{q^n}^*} \mid \chi(h) = 1, \forall h \in G^\ell\}$ onde $G^\ell = \{g^\ell \mid g \in G\}$. Temos então que $\{\chi \in \widehat{\mathbb{F}_{q^n}^*} \mid \chi^\ell(g) = 1, \forall g \in G\} = \mathrm{Ann}(G^\ell)$. Logo, pela Proposição 3.12, $\mathrm{Ann}(G^\ell) \simeq \widehat{G/G^\ell}$. Se g é k-livre, ele não pode ser potência de nenhum primo dividindo k, assim, $\bar{g} \neq 1$ em G/G^{p_i} para todo $1 \leq i \leq s$. Portanto

$$\sum_{\chi^{p_i}=\chi_0} \chi(g) = \sum_{\chi \in \widehat{G/G^{p_i}}} \chi(g).$$

Pela Proposição 3.6, temos que o somatório se anula para todo $1 \leq i \leq s$ e temos o resultado. □

Definição 3.17. Se G é um grupo abeliano de ordem n e k é um divisor de n, definindo $\theta(k) := \dfrac{\varphi(k)}{k}$, temos que $\theta(k)V_k$ é a função característica para os elementos k-livres de G.

Observação 3.17.1. No caso de um corpo finito $\mathbb{F}_{q^n}$, ser k-livre é uma noção referente ao grupo multiplicativo $\mathbb{F}_{q^n}^*$, mas podemos estender a noção para $\mathbb{F}_{q^n}$ observando que 0 não é k-livre, para nenhum k, divisor de $q^n - 1$ diferente de 1, visto que $0 = 0^d$ para qualquer $d \in \mathbb{N}$. Já no caso $k = 1$, temos que 0 é 1-livre, assim como todo elemento de $\mathbb{F}_{q^n}^*$.

Proposição 3.18. *Seja $\mathbb{F}_{q^n}$ um corpo finito e seja k um divisor de $q^n - 1$ diferente de 1. Existem $\theta(k)(q^n - 1)$ elementos k-livres em $\mathbb{F}_{q^n}$.*

Demonstração. Seja n_k o número de elementos k-livres em $\mathbb{F}_{q^n}^*$. Então

$$n_k = \sum_{\alpha \in \mathbb{F}_{q^n}^*} \theta(k) V_k(\alpha) = \theta(k) \sum_{\alpha \in \mathbb{F}_{q^n}^*} V_k(\alpha).$$

Pela definição da função V_k, temos que

$$\sum_{\alpha\in\mathbb{F}_{q^n}^*} V_k(\alpha) = \sum_{\alpha\in\mathbb{F}_{q^n}^*}\sum_{d|k}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(\alpha) = \sum_{d|k}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\sum_{\alpha\in\mathbb{F}_{q^n}^*}\chi(\alpha). \tag{3.4}$$

Onde o somatório

$$\sum_{\alpha\in\mathbb{F}_{q^n}^*}\chi(\alpha),$$

só não se anula no caso em que χ é o caráter trivial, ou seja, quando $d = 1$ em (3.4). Portanto

$$\sum_{\alpha\in\mathbb{F}_{q^n}^*} V_k(\alpha) = \sum_{\alpha\in\mathbb{F}_{q^n}^*}\chi_0(\alpha) = q^n - 1.$$

O resultado segue. □

3.3 Os caráteres aditivos e multiplicativos de $\mathbb{F}_q$

Nesta seção exibiremos os dois tipos de caráteres definidos no corpo $\mathbb{F}_q$. Os caráteres definidos sobre o grupo multiplicativo de $\mathbb{F}_q$ serão chamados de *caráteres multiplicativos* enquanto os caráteres definidos sobre o grupo aditivo serão chamados de *caráteres aditivos*. Os resultados dessa seção podem ser encontrados em [24].

Os caráteres multiplicativos são facilmente determinados, pois o grupo $\mathbb{F}_q^*$ é cíclico. O próximo teorema é uma reformulação da Proposição 3.3 para o caso $G = \mathbb{F}_q^*$.

Teorema 3.19. *Seja g um elemento primitivo de $\mathbb{F}_q$. Para cada $j = 0, 1, \ldots, q-2$, a função ν_j definida da seguinte maneira*

$$\nu_j(g^k) = e^{2\pi ijk/(q-1)} \text{ para } k = 0, \ldots, q-2,$$

onde i é a unidade imaginária, define um caráter multiplicativo de $\mathbb{F}_q$ e todo caráter multiplicativo de $\mathbb{F}_q$ pode ser obtido dessa maneira.

Observação 3.19.1. Um caráter multiplicativo de $\mathbb{F}_q$ está definido apenas para os elementos do grupo multiplicativo $\mathbb{F}_q^*$. Com a finalidade de estendermos um caráter multiplicativo para todo $\mathbb{F}_q$, faremos a seguinte convenção: se ν é um caráter multiplicativo de $\mathbb{F}_q$, diferente do trivial, então $\nu(0) = 0$. Definimos também $\nu_0(0) = 1$, onde ν_0 denota o caráter multiplicativo trivial de $\mathbb{F}_q$.

Definição 3.20. Seja d um divisor de $q-1$. Denotamos por ν_d um caráter de ordem d em $\widehat{\mathbb{F}_q^*}$.

Com essa nova definição, $\nu_0 = \nu_1$.

Proposição 3.21. *A função de $\mathbb{F}_q$ para os números complexos de módulo 1, definida por*

$$\lambda(a) = e^{2\pi i\, Tr(a)/p},$$

onde Tr denota o traço absoluto de $\mathbb{F}_q$, é um caráter do grupo aditivo $\mathbb{F}_q$, chamado de caráter aditivo canônico.

Tal caráter é chamado de caráter aditivo canônico pelo fato de que qualquer outro caráter aditivo de $\mathbb{F}_q$ poder ser obtido através dele.

Teorema 3.22. *Para $a \in \mathbb{F}_q$, a função λ_a definida por $\lambda_a(b) = \lambda(ab)$, para todo $b \in \mathbb{F}_q$ define um caráter aditivo de $\mathbb{F}_q$. Reciprocamente, qualquer caráter aditivo de $\mathbb{F}_q$ pode ser obtido dessa maneira.*

Demonstração. Ver [24], p. 190, Theorem 5.7. □

Fazendo $a = 0$ no Teorema 3.22, obtemos o caráter aditivo trivial λ_0. Para estendermos os caráteres definidos em $\mathbb{F}_q$ para qualquer $1 < n \in \mathbb{N}$, seja χ o caráter aditivo canônico de $\mathbb{F}_{q^n}$, definido de maneira análoga à definida na Proposição 3.21. Então, pela transitividade do traço, temos que, se λ é o caráter aditivo canônico de $\mathbb{F}_q$, então

$$\lambda(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)) = \chi(\beta) \text{ para todo } \beta \in \mathbb{F}_{q^n}. \tag{3.5}$$

A seguinte proposição é um caso particular da Proposição 3.6.

Proposição 3.23.

i) Seja λ o caráter aditivo canônico de $\mathbb{F}_q$ e $a \in \mathbb{F}_q$. Então:

$$\sum_{b \in \mathbb{F}_q} \lambda(b \cdot a) = \begin{cases} 0, & \text{se } a \neq 0 \\ q, & \text{se } a = 0. \end{cases}$$

ii) Se $\widehat{\mathbb{F}_q^*}$ é o dual de $\mathbb{F}_q^*$ e $a \in \mathbb{F}_q^*$, temos que:

$$\sum_{\nu \in (\mathbb{F}_q^*)^\wedge} \nu(a) = \begin{cases} 0, & \text{se } a \neq 1 \\ q-1, & \text{se } a = 1. \end{cases}$$

3.4 Somas de Gauss

Esta seção é dedicada às Somas de Gauss, que são umas das mais importantes *somas exponenciais*, ou seja, somas onde estão presentes um ou mais caráteres de $\mathbb{F}_q$. A importância das Somas de Gauss reside no fato delas conectarem a estrutura *aditiva* com a estrutura *multiplicativa* de $\mathbb{F}_q$. Os resultados nesta seção podem ser encontrados em [24].

Definição 3.24. Sejam ν um caráter multiplicativo de $\mathbb{F}_q$ e λ_a, onde $a \in \mathbb{F}_q$, um caráter aditivo de $\mathbb{F}_q$. A *Soma de Gauss* $G_1(\nu, \lambda_a)$ é definida da seguinte maneira

$$G_1(\nu, \lambda_a) = \sum_{c \in \mathbb{F}_q} \nu(c)\lambda_a(c).$$

Veremos que o número de elementos que são simultaneamente *primitivos* em $\mathbb{F}_{q^n}$ e *normais* em $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ pode ser expresso em função de Somas de Gauss, sendo assim, é natural indagar-se acerca de seu valor absoluto. É claro que $|G(\nu, \lambda_a)| \leq q$, contudo, tal valor em geral é bem menor. Relembramos que ν_0 e λ_0 denotam, respectivamente, os caráteres multiplicativo e aditivo triviais de $\mathbb{F}_q$.

Teorema 3.25. *Sejam ν um caráter multiplicativo e λ_a, para $a \in \mathbb{F}_q$ um caráter aditivo de $\mathbb{F}_q$. A Soma de Gauss $G_1(\nu, \lambda_a)$ satisfaz*

$$G_1(\nu, \lambda_a) = \begin{cases} q, & se\ \nu = \nu_0, \lambda_a = \lambda_0, \\ 0, & se\ \nu = \psi_0, \lambda_a \neq \lambda_0, \\ 0, & se\ \nu \neq \nu_0, \lambda_a = \lambda_0. \end{cases} \tag{3.6}$$

Se $\nu \neq \nu_0$ e $\lambda_a \neq \lambda_0$, então

$$|G_1(\nu, \lambda_a)| = q^{1/2}. \tag{3.7}$$

Demonstração. O primeiro caso em (3.6) é trivial. Os segundo e terceiro casos seguem diretamente da Proposição 3.23 e pela convenção do valor de ν em $0 \in \mathbb{F}_q$, mencionada na Observação 3.19.1. Agora, quando $\nu \neq \nu_0$ e $\lambda_a \neq \lambda_0$, temos que $\nu(0) = 0$ e

$$\begin{aligned} |G_1(\nu, \lambda_a)|^2 &= \overline{G(\nu, \lambda_a)}\, G(\nu, \lambda_a) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \overline{\nu(c)\lambda_a(c)} \nu(c_1)\lambda_a(c_1) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \nu(c^{-1}c_1)\lambda_a(c_1 - c). \end{aligned}$$

Onde na última igualdade usamos a Proposição 3.2. Substituindo $c^{-1}c_1 = d$, temos que

$$\begin{aligned} |G_1(\nu, \lambda_a)|^2 &= \sum_{c \in \mathbb{F}_q^*} \sum_{d \in \mathbb{F}_q^*} \nu(d)\lambda_a(c(d-1)) \\ &= \sum_{d \in \mathbb{F}_q^*} \nu(d) \left(\sum_{c \in \mathbb{F}_q} \lambda_a(c(d-1)) - \lambda_a(0) \right) \\ &= \sum_{d \in \mathbb{F}_q^*} \nu(d) \sum_{c \in \mathbb{F}_q} \lambda_a(c(d-1)), \end{aligned}$$

onde na segunda igualdade usamos o fato de que $\sum_{d \in \mathbb{F}_q^*} \nu(d) = 0$, se $\nu \neq \nu_0$. Agora, a soma

$$\sum_{c \in \mathbb{F}_q} \lambda_a(c(d-1))$$

tem valor q se $d = 1$ e valor 0 se $d \neq 1$, de novo pela Proposição 3.23. Portanto, $|G_1(\nu, \lambda_a)|^2 = \nu(1)q = q$ e temos o resultado. □

Observação 3.25.1. Trocando $\mathbb{F}_q$ por $\mathbb{F}_{q^n}$ obtemos que, se η e χ_α, onde $\alpha \in \mathbb{F}_{q^n}$ são, respectivamente, caráteres multiplicativo e aditivo de $\mathbb{F}_{q^n}$, a Soma de Gauss é denotada por $G_n(\eta, \chi_\alpha)$. Temos que $|G_n(\eta, \chi_\alpha)| = q^{\frac{n}{2}}$. Se χ é o caráter aditivo canônico em $\mathbb{F}_{q^n}$ escrevemos $G_n(\eta)$ para representar $G_n(\eta, \chi)$.

3.5 O dual de $\mathbb{F}_{q^n}$ visto como um módulo sobre $\mathbb{F}_q[X]$

Ao longo desta seção, definimos o necessário para construir a função característica dos elementos *normais* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

O grupo dos caráteres aditivos de $\mathbb{F}_{q^n}$ pode ser visto como um módulo sobre $\mathbb{F}_q[X]$. De fato, seja

$\widehat{\mathbb{F}_{q^n}} = \{\chi : \mathbb{F}_{q^n} \to \mathbb{C} \mid \chi \text{ é um caráter em } \mathbb{F}_{q^n}\}$, o dual de $\mathbb{F}_{q^n}$. Sejam $\chi \in \widehat{\mathbb{F}_{q^n}}$ e $f \in \mathbb{F}_q[X]$. A seguinte operação torna $\widehat{\mathbb{F}_{q^n}}$ em um módulo sobre $\mathbb{F}_q[X]$.

$$(\chi^f)(\alpha) := \chi(f^\sigma(\alpha)) = \chi(f \circ \alpha), \quad \forall \alpha \in \mathbb{F}_{q^n}.$$

Note que $\chi^{X^n-1}(\alpha) = \chi((X^n-1)\circ\alpha) = \chi(\alpha^{q^n} - \alpha) = \chi(0) = 1$, para todo $\alpha \in \mathbb{F}_{q^n}$. Em particular, $\mathrm{Ann}_{\mathbb{F}_q[X]}(\chi) \neq (0)$. Definimos a ordem $\mathrm{Ord}(\chi)$ do caráter χ como sendo o polinômio mônico que gera $\mathrm{Ann}_{\mathbb{F}_q[X]}(\chi)$. Em particular, $\mathrm{Ord}(\chi) = f_\chi$ é o polinômio mônico de menor grau tal que $\chi^{f_\chi}(\alpha) = 1$, para todo $\alpha \in \mathbb{F}_{q^n}$. Temos também que $\mathrm{Ord}(\chi)$ divide $X^n - 1$.

Proposição 3.26. *Seja f um divisor mônico de $X^n - 1$. Então*

$$\sum_{g|f} \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid Ord(\chi) = g\} = N(f).$$

Demonstração. Seja f um divisor mônico de $X^n - 1$. Defina o subgrupo aditivo $H = f \circ \mathbb{F}_{q^n} = \{f \circ \alpha \mid \alpha \in \mathbb{F}_{q^n}\}$ de $\mathbb{F}_{q^n}$. Temos então que o subgrupo $L := \{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \chi^f \equiv \chi_0\}$ do dual de $\mathbb{F}_{q^n}$ anula H. De fato, a inclusão $\mathrm{Ann}_{\widehat{\mathbb{F}_{q^n}}}(H) \subseteq L$ é clara. Seja $h \in H$. Temos que $h = f \circ \alpha$, para algum $\alpha \in \mathbb{F}_{q^n}$ e, se $\chi \in L$, então $\chi(h) = \chi(f \circ \alpha) = \chi^f(\alpha) = 1$. Assim, pela Proposição 3.12, temos que

$$L \simeq \frac{\mathbb{F}_{q^n}}{H} = \frac{\mathbb{F}_{q^n}}{f \circ \mathbb{F}_{q^n}}. \tag{3.8}$$

Em particular $|L| = \dfrac{|\mathbb{F}_{q^n}|}{|H|}$. Observe agora que f^σ é um endomorfismo do grupo aditivo $\mathbb{F}_{q^n}$ com núcleo $\mathrm{Ker}(f^\sigma) = \{\alpha \in \mathbb{F}_{q^n} \mid f \circ \alpha = f^\sigma(\alpha) = 0\}$, que possui $N(f)$ elementos, pois f^σ possui todas as suas raízes distintas. Logo, $\mathrm{Im}(f^\sigma) = f \circ \mathbb{F}_{q^n} = \dfrac{\mathbb{F}_{q^n}}{\mathrm{Ker}(f^\sigma)}$ que possui $\frac{q^n}{N(f)} = q^{n-\mathrm{grau}(f)}$ elementos. Assim, $|L| = q^{\mathrm{grau}(f)} = N(f)$. □

Proposição 3.27. *Se f é um divisor mônico de $X^n - 1$, então existem $\Phi(f)$ caráteres aditivos χ de $\mathbb{F}_{q^n}$ com $Ord(\chi) = f$.*

Demonstração. Usamos indução no grau de f. Se f é um divisor de grau 1 de $X^n - 1$, seus únicos divisores são 1 e f, assim

$$\begin{aligned} q = N(f) &= \sum_{g|f} \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = g\} \\ &= \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = 1\} + \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = f\} \\ &= 1 + \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = f\}. \end{aligned} \tag{3.9}$$

Portanto, concluímos que

$$\#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = f\} = q - 1 = \Phi(f).$$

Suponha agora que o resultado é válido para todo polinômio g divisor de $X^n - 1$ de grau menor que d. Seja f um polinômio de grau d tal que f divida $X^n - 1$. Temos que

$$\sum_{g|f} \Phi(g) = N(f) = \sum_{g|f, g\neq f} \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = g\} + \#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = f\}. \tag{3.10}$$

Pela hipótese de indução, $\#\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \mathrm{Ord}(\chi) = g\} = \Phi(g)$ para todo g divisor de f e diferente de f, cancelando os termos iguais, o resultado segue. □

Agora estamos aptos para construir a função característica para os elementos normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Para isso, uma nova definição é necessária.

Definição 3.28. Seja M um divisor de $X^n - 1$ em $\mathbb{F}_q[X]$ e $h \in \mathbb{F}_q[X]$ um divisor de M. Dizemos que $\alpha \in \mathbb{F}_{q^n}$ é M-livre se $\alpha = h \circ \beta$, onde $\beta \in \mathbb{F}_{q^n}$ sempre implicar $h = 1$.

Temos que α é normal sobre $\mathbb{F}_{q^n}$ se, e somente se, é $(X^n - 1)$-livre.

Observação 3.28.1. Neste caso, assim como no caso multiplicativo, temos que 0 não é M-livre, para nenhum M divisor de $X^n - 1$ visto que para qualquer $g \in \mathbb{F}_q[X]$, temos que $g \circ 0 = 0$.

Teorema 3.29. *Sejam $h \in \mathbb{F}_q[X]$ um divisor mônico de $X^n - 1$ e $\alpha \in \mathbb{F}_{q^n}$, defina a função*

$$V_h(\alpha) = \sum_{f|h} \frac{\mu(f)}{\Phi(f)} \sum_{\chi \in \widehat{\mathbb{F}_{q^n}}, Ord(\chi)=f} \chi(\alpha), \text{ para todo } \alpha \in \mathbb{F}_{q^n}.$$

Então

$$V_h(\alpha) = \begin{cases} 0, & \text{se } \alpha \text{ não é } h\text{-livre,} \\ \dfrac{N(h)}{\Phi(h)}, & \text{se } \alpha \text{ é } h\text{-livre.} \end{cases}$$

Demonstraremos um lema, análogo ao Lema 3.16 que será usado na prova do Teorema 3.29.

Lema 3.30. *Sejam $\mathbb{F}_{q^n}$ um corpo finito com q^n elementos e $\widehat{\mathbb{F}_{q^n}}$ seu dual. Valem as seguintes afirmações:*

a) Se $h \in \mathbb{F}_q[X]$ é um polinômio mônico e irredutível divisor de $X^n - 1$, então existem $\Phi(h) = N(h) - 1$ caráteres $\chi \in \widehat{\mathbb{F}_{q^n}}$ tais que $Ord(\chi) = h$.

b) Sejam $h_1 \neq h_2 \in \mathbb{F}_q[X]$ polinômios mônicos irredutíveis divisores de $X^n - 1$. Então todo caráter aditivo χ de $\mathbb{F}_{q^n}$ tal que $Ord(\chi) = h_1 h_2$ é o produto de um caráter de ordem h_1 com um caráter de ordem h_2. Reciprocamente, o produto de quaisquer caráteres de ordem h_1 e ordem h_2 resulta em um caráter de ordem $h_1 h_2$.

c) Para $\alpha \in \mathbb{F}_{q^n}$ e $h_1, h_2 \in \mathbb{F}_q[X]$, divisores mônicos irredutíveis de $X^n - 1$, temos que

$$\left(\sum_{Ord(\chi)=h_1} \chi(\alpha) \right) \left(\sum_{Ord(\chi)=h_2} \chi(\alpha) \right) = \left(\sum_{Ord(\chi)=h_1 h_2} \chi(\alpha) \right),$$

onde os somatórios percorrem todos os caráteres aditivos de $\mathbb{F}_{q^n}$ com dada ordem.

d) Se h é um divisor mônico irredutível de $X^n - 1$, e $\alpha \in \mathbb{F}_{q^n}$, então

$$\left(\sum_{Ord(\chi)=h} \chi(\alpha) \right) + 1 = \sum_{\substack{\chi \in \widehat{\mathbb{F}_{q^n}}, \\ \chi^h \equiv \chi_0}} \chi(\alpha),$$

onde o último somatório percorre todos os caráteres aditivos de $\mathbb{F}_{q^n}$ tais que $\chi^h = \chi_0$, i.e., $\chi(h \circ \alpha) = 0, \forall \alpha \in \mathbb{F}_{q^n}$.

Demonstração. O item a) é uma consequência direta da Proposição 3.27. Já o item b) é uma consequência Proposição 2.3, pois dois polinômios mônicos e irredutíveis distintos são necessariamente primos entre si. O item c) por sua vez é uma consequência do item b). Já o item d) segue do fato de que, como h é irredutível e mônico, temos que $\Phi(h) = h - 1$, ademais, se $\chi \in \widehat{\mathbb{F}_{q^n}}$ é um caráter tal que $\chi^h \equiv \chi_0$, então $\mathrm{Ord}(\chi)$ divide h (lembre-se que $\mathrm{Ord}(\chi)$ é o polinômio mônico gerador de $\mathrm{Ann}(\chi)$). Como h é irredutível, segue que χ é tal que $\mathrm{Ord}(\chi) = h$ ou $\mathrm{Ord}(\chi) = 1$. Como $\mathrm{Ord}(\chi) = 1$ se, e somente se $\chi \equiv \chi_0$, o resultado segue. □

Vamos agora à demonstração do Teorema 3.29.

Demonstração. A demonstração é análoga ao caso em que G é um grupo cíclico finito. Seja $h = t_1^{r_1} \cdots t_s^{r_s}$, t_i mônicos irredutíveis distintos e $r_i \geq 1$. Pelo Lema 3.30, podemos escrever $V_h(\alpha)$ da seguinte maneira:

$$V_h(\alpha) = \prod_{i=1}^{s} \left(1 - \frac{1}{N(t_i) - 1} \left(\sum_{\mathrm{Ord}(\chi) = t_i} \chi(\alpha) \right) \right),$$

disso decorre que

$$V_h(\alpha) = \prod_{i=1}^{s} \left(\frac{N(t_i)}{N(t_i) - 1} - \frac{1}{N(t_i) - 1} \left(\sum_{\mathrm{Ord}(\chi) = t_i} \chi(\alpha) + 1 \right) \right),$$

pelo Lema 3.30, como t_i é mônico e irredutível para todo $1 \leq i \leq s$, temos que

$$V_h(\alpha) = \prod_{i=1}^{s} \left(\frac{N(t_i)}{N(t_i) - 1} - \frac{1}{N(t_i) - 1} \sum_{\chi^{t_i} \equiv \chi_0} \chi(\alpha) \right).$$

Portanto, se α não é h-livre, então $\alpha = t_i \circ \beta$, para algum $1 \leq i \leq s$ e algum $\beta \in \mathbb{F}_{q^n}$. Logo,

$$\sum_{\chi^{t_i} \equiv \chi_0} \chi(\alpha) = \sum_{\chi^{t_i} \equiv \chi_0} \chi(t_i \circ \beta) = \sum_{\chi^{t_i} \equiv \chi_0} \chi^{t_i}(\beta) = \sum_{\chi^{t_i} \equiv \chi_0} 1 = N(t_i).$$

Portanto, existe um fator 0 no produtório, tornando $V_h(\alpha)$ zero. Se α é h-livre, então, para cada $1 \leq i \leq s$, temos que $\sum_{\chi^{t_i} \equiv \chi_0} \chi(\alpha) = 0$ pois, (3.8) implica que o conjunto $\{\chi \in \widehat{\mathbb{F}_{q^n}} \mid \chi^{t_i} \equiv \chi_0\} = \mathrm{Ann}(t_i \circ \mathbb{F}_{q^n})$ é isomorfo a $\dfrac{\mathbb{F}_{q^n}}{t_i \circ \mathbb{F}_{q^n}} \simeq \widehat{\dfrac{\mathbb{F}_{q^n}}{t_i \circ \mathbb{F}_{q^n}}}$, e α ser h-livre, implica em α ser t_i-livre para todo $1 \leq i \leq s$, assim $\alpha \neq 0$ em $\dfrac{\mathbb{F}_{q^n}}{t_i \circ \mathbb{F}_{q^n}}$ e o resultado segue como no Teorema 3.15. □

Definição 3.31. Seja h um divisor de $X^n - 1$. Definindo $\Theta(h) := \dfrac{\Phi(h)}{N(h)}$, temos que $\Theta(h)V_h$ é a função característica para os elementos h-livres de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Proposição 3.32. *Seja $1 \neq h \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. O número de elementos h-livres em $\mathbb{F}_{q^n}$ é $\Theta(h)q^n$.*

Demonstração. A demonstração é análoga à demonstração da Proposição 3.18. □

4 O Teorema da Base Normal e Primitiva

4.1 Introdução

Para provarmos o teorema da Base Normal e Primitiva, mostraremos que o número de elementos $\alpha \in \mathbb{F}_{q^n}$ satisfazendo simultaneamente $\mathrm{ord}(\alpha) = q^n - 1$ e $\mathrm{Ord}(\alpha) = X^n - 1$ é positivo. Para isso, as funções características que definimos anteriormente serão de extrema importância. Antes de atacarmos o problema, veremos que podemos procurar por elementos α com ordem multiplicativa menor que $q^n - 1$ e ainda assim garantir a validade do teorema. Ao longo desta seção, consideraremos $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$, um corpo finito de característica p com $q = p^r$ elementos.

Observe que, garantir a existência de um elemento *normal* e *primitivo* de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é equivalente a garantir a existência de um polinômio $f \in \mathbb{F}_q[X]$ *normal e primitivo* de grau n sobre $\mathbb{F}_q$.

A primeira demonstração do teorema da Base Normal e Primitiva foi devida a H. W. Lenstra e R. J. Schoof [23] em 1987, completando o trabalho de H. Davenport [13] de 1968, que provara o fato para extensões finitas do corpo primo $\mathbb{F}_p$. A demonstração de H. W. Lenstra e R. J. Schoof depende de um computador. Para um resultado de tamanha importância acerca dos corpos finitos, é interessante uma demonstração que não dependa do computador. Tal demonstração foi feita por S. D. Cohen e S. Huczynska [8] em 2003, no qual esta seção é majoritariamente baseada.

4.2 Reduções

Inicialmente, observe que em extensões da forma $\mathbb{F}_{q^2}|\mathbb{F}_q$, um elemento $\alpha \in \mathbb{F}_{q^2}$ tem como sua ordem aditiva um divisor de $X^2 - 1 = (X-1)(X+1)$. Se supusermos $\alpha \in \mathbb{F}_{q^2}$ primitivo, então α não pode ter ordem aditiva $X - 1$ nem $X + 1$. Portanto podemos supor $n \geq 3$ na extensão $\mathbb{F}_{q^n} \mid \mathbb{F}_q$.

Definição 4.1. Sejam m um divisor positivo de $q^n - 1$ e $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. Denotamos por $N(m, g)$ o número de elementos não nulos de $\mathbb{F}_{q^n}$ que são simultaneamente m-livres e g-livres em $\mathbb{F}_{q^n}$.

Observação 4.1.1. Como mencionado nas observações 3.17.1 e 3.28.1, todo elemento de $\mathbb{F}_{q^n}$ é 1-livre no sentido *multiplicativo* e todo elemento exceto o 0 é 1-livre no sentido *aditivo*. Portanto, temos que $N(1,1) = q^n - 1$. Devido à Proposição 3.18, se $m \in \mathbb{N}$ e $m \neq 1$, então $N(m,1) = \theta(m)(q^n - 1)$ e, se $g \in \mathbb{F}_q[X]$, $g \neq 1$, então, pela Proposição 3.32, $N(1,g) = \Theta(g)q^n$.

As seguintes proposições nos dizem que podemos reduzir o problema para obter informações sobre $N(m, g)$.

Lema 4.2. *Sejam m um divisor de $q^n - 1$, $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$ e $\alpha \in \mathbb{F}_{q^n}$.*

i) Seja k um divisor de m. Se α é m-livre, então α é k-livre.

ii) Seja h um divisor de g. Se α é g-livre, então α é h-livre.

Demonstração. Sejam m um divisor de $q^n - 1$, k um divisor de m e $\alpha \in \mathbb{F}_{q^n}$, m-livre. Seja d um divisor de k e suponha que $\alpha = \beta^d$ para algum $\beta \in \mathbb{F}_{q^n}$. Como d divide m, segue que $d = 1$. Portanto α é k-livre. A demonstração do caso aditivo é análoga. □

Lema 4.3. *Sejam m um divisor de $q^n - 1$ e m_0 sua parte livre de quadrados. Então, $\alpha \in \mathbb{F}_{q^n}$ é m-livre se, e somente se, é m_0-livre.*

Demonstração. Se α é m-livre, então é claro que é m_0-livre, pois qualquer divisor de m_0 é também um divisor de m. Reciprocamente, seja $\alpha \in \mathbb{F}_{q^n}$, m_0-livre e suponha que $\alpha = \beta^d$, onde d divide m. Podemos supor $m > 1$ e $m = p_1^{r_1} \dots p_s^{r_s}$ onde p_i é primo para $1 \leq i \leq s$, o que implica $m_0 = p_1 \dots p_s$. Se $d > 1$, então, após uma reordenação podemos escrever $d = p_1^{k_1} \dots p_w^{k_w}$ onde $1 \leq w \leq s$ e $1 \leq k_i \leq r_i$. Portanto,

$$\alpha = \beta^d = \beta^{p_1^{k_1} \dots p_w^{k_w}} = (\beta^{p_1^{k_1 - 1} \dots p_w^{k_w - 1}})^{p_1 \dots p_w}$$

e temos que $p_1 \dots p_w | m_0$. Logo, como α é m_0-livre, temos que $p_1 \dots p_w = 1$, o que implica $d = 1$, uma contradição. □

Temos um fato análogo para elementos $\alpha \in \mathbb{F}_{q^n}$ g-livres, $g \in \mathbb{F}_q[X]$.

Lema 4.4. *Sejam g um divisor de $X^n - 1$ e g_0 sua parte livre de quadrados. Então $\alpha \in \mathbb{F}_{q^n}$ é g-livre se, e somente se, é g_0-livre.*

Demonstração. A demonstração é idêntica ao caso anterior, visto que os argumentos só dependem do fato dos elementos em questão pertencerem a um Domínio de Fatoração Única. □

Um fato mais interessante no caso aditivo é o seguinte: se p é a característica de $\mathbb{F}_{q^n}$, escrevendo $n = p^b n^*$, onde p não divide n^*, temos o seguinte resultado.

Lema 4.5. *Um elemento $\alpha \in \mathbb{F}_{q^n}$ é $(X^n - 1)$-livre se, e somente se, é $(X^{n^*} - 1)$-livre.*

Demonstração. Se $\alpha \in \mathbb{F}_{q^n}$ é $(X^n - 1)$-livre, então, como n^* divide n, $X^{n^*} - 1$ divide $X^n - 1$, portanto α é $(X^{n^*} - 1)$-livre. Reciprocamente, sejam $\alpha \in \mathbb{F}_{q^n}$ um elemento $(X^{n^*} - 1)$-livre e $h \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. Devemos mostrar que, caso tenhamos $\alpha = h^\sigma(\beta) = h \circ \beta$ para algum $\beta \in \mathbb{F}_{q^n}$, devemos ter necessariamente $h = 1$. Observe que

$$x^n - 1 = x^{p^k n^*} - 1 = (x^{n^*} - 1)^{p^k}.$$

Se $x^{n^*} - 1 = f_1^{t_1} \cdots f_s^{t_s}$ onde f_i é irredutível para todo $1 \leq i \leq s$, então $x^n - 1 = f_1^{t_1 p^k} \dots f_s^{t_s p^k}$. Logo, se $h \neq 1$, após uma reordenação temos que $h = f_1^{t_1 p^k - r_1} \dots f_w^{t_w p^k - r_s}$, onde $1 \leq w \leq s$ e $0 \leq r_i < t_i p^k$, para $i = 1, \dots, w$. Portanto,

$$\alpha = h \circ \beta = (f_1 \dots f_w) \circ ((f_1^{t_1 p^k - r_1 - 1} \dots f_s^{t_w p^k - r_w - 1}) \circ \beta) = (f_1 \dots f_w) \circ \gamma,$$

onde $\gamma \in \mathbb{F}_{q^n}$. Como $f_1 \dots f_w$ divide $X^{n^*} - 1$ e, por hipótese, α é $(X^{n^*} - 1)$-livre, segue que $f_1 \dots f_w = 1$ uma contradição. □

Lema 4.6. *Sejam q e $n \in \mathbb{N}$ números naturais maiores que 1. Então $mdc(q - 1, q^{n-1} + \cdots + q + 1) = mdc(q - 1, n)$.*

Demonstração. Sejam $c = \text{mdc}(q - 1, q^{n-1} + \cdots + q + 1)$ e $d = \text{mdc}(q - 1, n)$. Temos que $q \equiv 1 \pmod{d}$, logo $q^{n-1} + \cdots + q + 1 \equiv 0 \pmod{d}$, portanto d divide c. Reciprocamente $q \equiv 1 \pmod{c}$, logo $n \equiv q^{n-1} + \cdots + q + 1 \equiv 0 \pmod{c}$. □

Lema 4.7. *Sejam $\gamma \in C = \{\gamma \in \mathbb{F}_{q^n}^* \mid \gamma^{q-1} \in \mathbb{F}_q\}$ e M um $\mathbb{F}_q[X]$-submódulo de $\mathbb{F}_{q^n}$. Então:*

i) γM *é um* $\mathbb{F}_q[X]$*-submódulo de* $\mathbb{F}_{q^n}$*.*

ii) Os $\mathbb{F}_q[X]$*-submódulos de* $\mathbb{F}_{q^n}$ *são permutados por* C*.*

Demonstração. i) Mostraremos que se $\gamma \in C$, $f \in \mathbb{F}_q[X]$ e $\gamma\alpha \in \gamma M$, então $f \circ (\gamma\alpha) \in \gamma M$. De fato, se $f = a_k X^k + \cdots + a_1 X + a_0$, então $f \circ (\gamma\alpha) = a_k(\gamma\alpha)^{q^k} + \cdots + a_1(\gamma\alpha)^q + a_0(\gamma\alpha)$. Temos que $X \circ (\gamma\alpha) = (\gamma\alpha)^q = \gamma\gamma^{q-1}(X \circ \alpha) \in \gamma M$, pois $\gamma^{q-1} \in \mathbb{F}_q^*$. Portanto, $X^j \circ (\gamma\alpha) = X^{j-1} \circ (X \circ (\gamma\alpha)) \in \gamma M$, o que mostra que $f \circ (\gamma\alpha) \in \gamma M$. Seja $\gamma \in C$. Para o item *ii)*, defina $\mathcal{M}$ como o conjunto de todos os $\mathbb{F}_q[X]$-submódulos de $\mathbb{F}_{q^n}$. Considere a função

$$\begin{aligned} P_\gamma : \mathcal{M} &\longrightarrow \mathcal{M} \\ M &\longmapsto \gamma M \end{aligned}$$

Mostraremos que P_γ é injetiva. De fato, se $M_1 \neq M_2$ são $\mathbb{F}_q[X]$-submódulos de $\mathbb{F}_{q^n}$, então $\gamma M_1 \neq \gamma M_2$. Para tal, seja $\alpha \in M_1 \setminus M_2$. Mostraremos que $\gamma\alpha \notin \gamma M_2$. De fato, suponha que $\gamma\alpha \in \gamma M_2$. Então $\alpha \in M_2$, pois $\gamma \in C$, uma contradição. Como $\mathcal{M}$ é um conjunto finito, temos que P_γ é uma bijeção. □

Proposição 4.8. *Definindo* $Q := \frac{q^n-1}{(q-1)mdc(n,q-1)}$*, se* $N(Q, x^n - 1) > 0$*, então* $N(q^n - 1, x^n - 1) > 0$*.*

Demonstração. Defina os seguintes conjuntos

$$A = \{\alpha \in \mathbb{F}_{q^n} \mid \mathrm{Ord}(\alpha) = X^n - 1\} \text{ e } B = \{\alpha \in \mathbb{F}_{q^n}^* \mid \mathrm{ord}(\alpha) = q^n - 1\}.$$

Temos que $\#A = \Phi(X^n - 1)$ e $\#B = \varphi(q^n - 1)$. Sendo assim, $N(q^n - 1, X^n - 1) > 0$ é equivalente a $A \cap B \neq \emptyset$. Considere agora o subgrupo $C < \mathbb{F}_{q^n}^*$ definido por

$$C = \{\gamma \in \mathbb{F}_{q^n}^* \mid \gamma^{q-1} \in \mathbb{F}_q\} = \{\gamma \in \mathbb{F}_{q^n}^* \mid \gamma^{(q-1)^2} = 1\}.$$

Temos que $\gamma \in C$ se, e somente se $\gamma^{(q-1)^2} = 1$ e $\gamma^{q^n-1} = 1$, o que implica que $\gamma^{\mathrm{mdc}((q-1)^2, q^n-1)} = 1$. Definindo $D := \mathrm{mdc}((q-1)^2, q^n - 1) = (q-1)\mathrm{mdc}(q-1, q^{n-1} + \ldots + q + 1) = (q-1)\mathrm{mdc}(n, q-1)$ o número de elementos $\gamma \in \mathbb{F}_{q^n}$ tais que $\gamma^D = 1$ é

$$\sum_{d|D} \varphi(d) = D.$$

O índice de C em $\mathbb{F}_{q^n}^*$ é

$$\#\left(\frac{\mathbb{F}_{q^n}^*}{C}\right) = \frac{q^n - 1}{(q-1)\mathrm{mdc}(n, q-1)} = Q.$$

Note que os elementos $\alpha \in A$, são exatamente aqueles que não pertencem a nenhum $\mathbb{F}_q[X]$-submódulo próprio de $\mathbb{F}_{q^n}$. Logo pelo Lema 4.7, $CA = A$, onde $CA = \{\gamma\alpha \mid \gamma \in C, \alpha \in A\}$.

Temos $A \cap B \neq \emptyset$ se, e somente se, $A \cap (BC) \neq \emptyset$, pois, se $\alpha \in A, \beta \in B$ e $\gamma \in C$, são tais que $\alpha = \beta\gamma \in A \cap (BC)$, então $\beta = \gamma^{-1}\alpha \in (CA) \cap B = A \cap B$. Logo, $A \cap B$ é não-vazio se, e somente se, $A \cap (BC)$ é não-vazio.

Considere agora o homomorfismo sobrejetivo

$$\Psi : \mathbb{F}_{q^n}^* \longrightarrow \frac{\mathbb{F}_{q^n}^*}{C},$$

tal que $\Psi(\alpha) = \alpha C$. O conjunto B é o conjunto dos geradores de $\mathbb{F}_{q^n}^*$. Como Ψ é um homomorfismo sobrejetivo, em particular Ψ induz uma sobrejeção entre os geradores de $\mathbb{F}_{q^n}$ e $\frac{\mathbb{F}_{q^n}^*}{C}$. Logo

$$BC = \{\beta \in \mathbb{F}_{q^n}^* \mid \beta C \text{ gera o grupo } \frac{\mathbb{F}_{q^n}^*}{C}\}.$$

Temos que o conjunto BC é exatamente o conjunto dos elementos Q-livres, bastando aplicar o Teorema 3.15 ao grupo $\frac{\mathbb{F}_{q^n}^*}{C}$ (que possui cardinalidade Q) e observar que $V_Q(\alpha) \neq 0$ apenas para os elementos $\alpha \in BC$. Portanto $\alpha \in A \cap (BC)$ é equivalente a α ser normal sobre $\mathbb{F}_q$ e Q-livre. Logo se $N(Q, X^n - 1) > 0$, então $N(q^n - 1, X^n - 1) > 0$. □

Portanto, para garantir que $N(q^n - 1, X^n - 1) > 0$ basta mostrar que $N(Q_1, X^n - 1) > 0$, onde Q_1 é a parte livre de quadrados de $Q = \dfrac{q^n - 1}{(q-1)\text{mdc}(n, q-1)}$. Os próximos resultados nos permitem, em alguns casos, substituir Q e $X^n - 1$ por valores ainda menores.

Lema 4.9. *Suponha que um primo ℓ divida n. Defina $k := \frac{n}{\ell}$ e $\ell_0 := mdc(\ell, q^k - 1)$. Se $P := \frac{q^n-1}{\ell_0(q^k-1)}$ for um número primo, então $N(Q, X^n - 1) = N(Q/P, X^n - 1)$.*

Demonstração. Se $\alpha \in \mathbb{F}_{q^n}$ é Q-livre, então α é Q/P-livre. Suponha agora que $\alpha \in \mathbb{F}_{q^n}$ seja Q/P-livre e $(X^n - 1)$-livre, mas não seja Q-livre, ou seja, existe $d \neq 1$ um divisor de Q e $\tau \in \mathbb{F}_{q^n}$ tal que $\alpha = \tau^d$. Se $d \mid Q/P$, então, por α ser Q/P-livre, teríamos $d = 1$, uma contradição. Se $d \nmid Q/P$, como P é primo e α não é Q-livre, necessariamente $P \mid d$, ou seja, $\alpha = \beta^P$ para algum $\beta \in \mathbb{F}_{q^n}$. Temos então que

$$\alpha^{\ell_0} = \left(\beta^{\frac{q^n-1}{\ell_0(q^k-1)}}\right)^{\ell_0} = \beta^{\frac{q^n-1}{q^k-1}}$$

é tal que

$$\left(\alpha^{\ell_0}\right)^{q^k-1} = \beta^{q^n-1} = 1.$$

Portanto $\alpha^{\ell_0} \in \mathbb{F}_{q^k}$ e podemos escrever $\alpha^{q^k} = \gamma\alpha$ onde $\gamma = \alpha^{q^k-1}$ satisfaz $\gamma^{\ell_0} = 1$ e $\gamma \in \mathbb{F}_{q^k}$. Portanto, se $\gamma = 1$, temos que $\alpha^{q^k} - \alpha = 0$, ou seja $(X^k - 1) \circ \alpha = 0$, o que implica que $\text{Ord}(\alpha) \mid X^k - 1$, um absurdo, pois $\text{Ord}(\alpha) = X^n - 1$. Se $\gamma \neq 1$, temos que $\ell_0 \neq 1$, logo $\ell_0 = \ell$. Como ℓ é primo, temos então que γ é uma raiz primitiva da unidade de ordem ℓ em $\mathbb{F}_{q^k}$. Como $\alpha^{q^k} = \gamma\alpha$, e $\gamma \in \mathbb{F}_{q^k}$, temos que

$$\begin{aligned}
0 &= (1 + \gamma + \gamma^2 + \cdots + \gamma^{\ell-1})\alpha \\
&= \alpha + \gamma\alpha + \gamma^2\alpha + \cdots + \gamma^{\ell-1}\alpha \\
&= \alpha + \alpha^{q^k} + \alpha^{q^{2k}} + \cdots + \alpha^{q^{(\ell-1)k}} \\
&= (1 + X^k + \cdots + X^{(\ell-1)k}) \circ \alpha,
\end{aligned}$$

novamente uma contradição com o fato de α ser $(X^n - 1)$-livre. Concluímos então que, caso α seja Q/P-livre e $(X^n - 1)$-livre, α necessariamente é Q-livre. □

No exemplo a seguir, mostramos algumas aplicações do Lema 4.9 que nos serão úteis.

Exemplo 4.1. Para os pares (q, n), onde q é a cardinalidade do corpo finito base e n o grau da extensão sobre $\mathbb{F}_q$, temos os seguintes resultados, onde detalhamos as contas nos primeiros itens, os outros podem ser facilmente verificados.

i) $(2,6) : \ell = \ell_0 = 3$; temos que $k = 6/3 = 2$, $P = \frac{2^6-1}{3(2^2-1)} = 7$,$Q = \frac{q^n-1}{\mathrm{mdc}(n,q-1)(q-1)} = 2^6 - 1 = 63$, sua parte livre de quadrados é $Q_1 = 21$ e $Q_1/P = 3$. Logo $N(21, X^3 - 1) = N(3, X^3 - 1)$.

ii) $(2,n)$, onde $n = 3, 5$ ou 7: $\ell = n$, $\ell_0 = 1$; temos que $k = 1$, $P = 2^n - 1$, nesse caso, consideramos $Q = 2^n - 1$ ao invés de sua parte livre de quadrados. Portanto $Q/P = 1$ e então $N(2^n - 1, X^n - 1) = N(1, X^n - 1)$.

iii) $(3,3) : \ell = 3, \ell_0 = 1; N(13, X^3 - 1) = N(1, X^3 - 1)$.

iv) $(3,4) : \ell = \ell_0 = 2; N(10, X^4 - 1) = N(2, X^4 - 1)$.

v) $(3,8) : \ell = \ell_0 = 2; N(1640, X^8 - 1) = N(410, X^8 - 1) = N(10, X^8 - 1)$.

vi) $(4,3) : \ell = \ell_0 = 3; N(7, X^3 - 1) = N(1, X^3 - 1)$.

vii) $(5,4) : \ell = \ell_0 = 2; N(39, X^4 - 1) = N(3, X^4 - 1)$.

viii) $(5,8) : \ell = \ell_0 = 2; N(2 \cdot 3 \cdot 13 \cdot 313, X^8 - 1) = N(78, X^8 - 1)$.

O próximo lema nos permite, em alguns casos, reduzir o polinômio $X^n - 1$ em $N(Q, X^n - 1)$.

Lema 4.10.

i) Se $n = 4$ e $q \equiv 3 \pmod 4$, então $N(Q, X^4 - 1) = N(Q, X^2 - 1)$.

ii) Se $n = 3$ e $q \equiv 2 \pmod 3$, então $N(Q, X^3 - 1) = N(Q, X - 1)$.

Demonstração. i) Para o caso $n = 4$, é claro que se $\alpha \in \mathbb{F}_{q^4}$ é $(X^4 - 1)$-livre então ele é $\big(X^2 - 1\big)$-livre, pois $\big(X^2 - 1\big) \mid \big(X^4 - 1\big)$. Suponha que $\alpha \in \mathbb{F}_{q^n}$ é Q-livre e $\big(X^2 - 1\big)$-livre, mas não $\big(X^4 - 1\big)$-livre. Observe que a hipótese $q \equiv 3 \pmod 4$ implica que $\big(X^2 + 1\big)$ é irredutível sobre $\mathbb{F}_q$. Assim, se $\alpha \in \mathbb{F}_{q^4}$ não é $\big(X^4 - 1\big)$-livre, como $X^4 - 1 = \big(X^2 + 1\big)\big(X^2 - 1\big)$, necessariamente existe $\beta \in \mathbb{F}_{q^4}$ tal que $\alpha = \big(X^2 + 1\big) \circ \beta = \beta^{q^2} + \beta$. Como $\alpha^{q^2} = \alpha$, temos que $\alpha^{q^2-1} = 1$. Como $\mathrm{mdc}(q^4 - 1, q^2 + 1) = q^2 + 1$, pela Proposição 2.10, segue que $\alpha = \gamma^{q^2+1}$, contradizendo o fato de α ser Q-livre.

ii) Se $n = 3$, como $q \equiv 2 \pmod 3$, temos que $X^2 + X + 1$ é irredutível sobre $\mathbb{F}_q$. Similarmente, suponha $\alpha \in \mathbb{F}_{q^3}$, Q-livre e $(X - 1)$-livre, mas não $\big(X^3 - 1\big)$-livre. Assim, $\alpha = \beta^{q^2} + \beta^q + \beta$, para algum $\beta \in \mathbb{F}_{q^3}$ e, portanto $\alpha^q = \alpha$, logo $\alpha^{q-1} = 1$. Como nesse caso $Q = \frac{q^3-1}{q-1}$, pois $\mathrm{mdc}(n, q - 1) = 1$, segue então pela Proposição 2.10 que $\alpha = \gamma^Q$, novamente um absurdo. A prova está completa. □

4.3 Uma expressão para $N(m, g)$

Sejam $Q := Q(q, n) := \dfrac{q^n - 1}{(q - 1)\mathrm{mdc}(n, q - 1)}$, $m \in \mathbb{N}$ um divisor de Q e $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. Estamos aptos a encontrar uma expressão para o número de elementos simultaneamente m-livres e g-livres. Adotaremos a seguinte convenção.

Sejam λ o caráter aditivo canônico em $\mathbb{F}_q$, χ o caráter aditivo canônico em $\mathbb{F}_{q^n}$ e χ_δ o caráter definido por $\chi_\delta = \chi(\delta\alpha)$, para todo $\alpha, \gamma, \in \mathbb{F}_{q^n}$. Para um divisor mônico $h \in \mathbb{F}_q[X]$ de $X^n - 1$, defina

$$\Delta_h = \{\delta \in \mathbb{F}_{q^n} \mid \mathrm{Ord}(\chi_\delta) = h\}.$$

Escrevemos χ_{δ_h}, onde $\delta_h \in \Delta_h$ para representar um caráter de ordem h, e temos pela Proposição 3.27 que $\#\{\chi_{\delta_h} \in \widehat{\mathbb{F}_{q^n}} \mid \delta_h \in \Delta_h\} = \Phi(h)$. Observe que $\Delta_1 = \{\chi_0\}$, o caráter trivial em $\mathbb{F}_{q^n}$ e $\delta_1 = 0$, pois, em função do caráter canônico de $\mathbb{F}_{q^n}$, temos que $\chi_0 = \chi(0 \cdot \alpha)$. Vamos mostrar que Δ_h é invariante por elementos de $\mathbb{F}_q^*$.

Proposição 4.11. *Seja Δ_h como definido anteriormente. Então $\mathbb{F}_q^*\Delta_h = \Delta_h$.*

Demonstração. É claro que $\Delta_h \subseteq \mathbb{F}_q^*\Delta_h$. Sejam $\delta \in \Delta_h$ e $c \in \mathbb{F}_q^*$ e considere $c\delta$. Vamos mostrar que $\mathrm{Ord}(\chi_{c\delta}) = h$. Temos que

$$\chi_{c\delta}(h \circ \alpha) = \chi_\delta(ch \circ \alpha) = \chi_\delta(h \circ c\alpha),$$

pois $c^{q^i} = c$, para todo $i \in \mathbb{N}$. Defina $\beta := c\alpha$. Então β permuta os elementos de $\mathbb{F}_{q^n}$. Logo $\chi_{c\delta}(h \circ \beta) = 1$, para todo $\beta \in \mathbb{F}_{q^n}$ e h é mínimo com tal propriedade. Portanto a ordem de $\chi_{c\delta}$ é h, sendo assim $c\delta \in \Delta_h$. Concluímos que $\mathbb{F}_{q^n}^*\Delta_h = \Delta_h$. □

Consideramos agora as funções características dos elementos $\alpha \in \mathbb{F}_{q^n}$ que são m-livres e g-livres sobre $\mathbb{F}_q$. Usaremos a notação definida em [8] para simplificar a expressão das funções características dos elementos m-livres e g-livres sobre $\mathbb{F}_q$.

i) A função característica dos elementos $\alpha \in \mathbb{F}_{q^n}^*$ que são m-livres.

Para m um divisor de Q, defina a função em $\mathbb{F}_{q^n}$

$$\int_{d|m} \eta_d := \sum_{d|m} \frac{\mu(d)}{\varphi(d)} \sum_{d|m} \eta_d,$$

onde η_d é definido na Definição 3.20. Note que esta expressão aparece recorrentemente nas fórmulas para a função característica dos elementos m-livres. Observe também que apenas divisores d livres de quadrados importam. Com essa nova notação, a função característica para os elementos m-livres em $\mathbb{F}_{q^n}^*$ toma a forma

$$\theta(m)V_m(\alpha) = \theta(m) \int_{d|m} \eta_d(\alpha), \text{ para } \alpha \in \mathbb{F}_{q^n}^*.$$

ii) A função característica dos elementos $\alpha \in \mathbb{F}_{q^n}$ que são g-livres sobre $\mathbb{F}_q$.

Seja $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$, defina função em $\mathbb{F}_{q^n}$

$$\int_{h|g} \chi_{\delta_h} := \sum_{h|g} \frac{\mu(h)}{\Phi(h)} \sum_{\delta_h \in \Delta_h} \chi_{\delta_h},$$

onde a soma interior percorre todos os $\Phi(h)$ elementos δ_h de Δ_h. Novamente, apenas os elementos livres de quadrados importam. Assim, a função característica para os elementos g-livres se torna

$$\Theta(g)V_g(\alpha) = \Theta(g) \int_{h|g} \chi_{\delta_h}(\alpha), \text{ para } \alpha \in \mathbb{F}_{q^n}.$$

Agora estamos aptos a encontrar uma expressão explícita para $N(m, g)$.

Proposição 4.12. *Seja m um divisor de Q e $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. Então*

$$N(m,g) = \theta(m)\Theta(g)\left(q^n - \epsilon_g + \int_{d(\neq 1)|m}\int_{h(\neq 1)|g} G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right),$$

onde $\epsilon_g = 1$ se $g = 1$, e 0 caso contrário. A barra em $\overline{\eta_d(\delta_h)}$ significa conjugação complexa, χ representa o caráter aditivo canônico de $\mathbb{F}_{q^n}$ e $\delta_h \in \Delta_h$.

Demonstração. Pela Observação 4.1.1, o resultado é claro quando $m = 1$ ou $g = 1$. Podemos então supor que $m \neq 1$ e $g \neq 1$, logo $\epsilon_g = 0$. Sejam $\theta(m)V_m$ e $\Theta(g)V_g$ as funções características dos elementos m-livres e g-livres respectivamente (Definições 3.17 e 3.31).

Temos então que

$$\begin{aligned} N(m,g) = \sum_{\alpha\in\mathbb{F}_q} \theta(m)V_m(\alpha)\Theta(g)V_g(\alpha) &= \sum_{\alpha\in\mathbb{F}_q}\left(\theta(m)\int_{d|m}\eta_d(\alpha)\right)\left(\Theta(g)\int_{h|g}\chi_{\delta_h}(\alpha)\right) \\ &= \theta(m)\Theta(g)\left(\int_{d|m}\int_{h|g}\sum_{\alpha\in\mathbb{F}_q}\eta_d(\alpha)\chi_{\delta_h}(\alpha)\right). \end{aligned}$$

Logo

$$\begin{aligned} N(m,g) = \theta(m)\Theta(g)\Bigg(\int_{h|g}\sum_{\alpha\in\mathbb{F}_q}\eta_1(\alpha)\chi_{\delta_h}(\alpha) + \int_{d(\neq 1)|m}\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d(\alpha)\chi_{\delta_1}(\alpha) \\ + \int_{d(\neq 1)|m}\int_{h(\neq 1)|g}\sum_{\alpha\in\mathbb{F}_q}\eta_d(\alpha)\chi_{\delta_h}(\alpha)\Bigg). \end{aligned}$$

Como $\chi_{\delta_1} \equiv \chi_0$ temos que $\chi_{\delta_1}(\alpha) = 1$ e $d \neq 1$ implica que

$$\sum_{\alpha\in\mathbb{F}_q}\eta_d(\alpha) = 0,$$

pela Proposição 3.23. Portanto

$$N(m,g) = \theta(m)\Theta(g)\left(\int_{h|g}\sum_{\alpha\in\mathbb{F}_q}\chi_{\delta_h}(\alpha) + \int_{d(\neq 1)|m}\int_{h(\neq 1)|g}\sum_{\alpha\in\mathbb{F}_q}\eta_d(\alpha)\chi_{\delta_h}(\alpha)\right).$$

Se χ_{δ_h} não é o caráter trivial, então

$$\sum_{\alpha\in\mathbb{F}_q}\chi_{\delta_h}(\alpha) = 0,$$

pela Proposição 3.23. Se $\chi_{\delta_h} \equiv \chi_0$ então

$$\sum_{\alpha\in\mathbb{F}_q}\chi_{\delta_h}(\alpha) = q^n.$$

Como $\chi_{\delta_h} \equiv \chi_0$ se e somente se $h = 1$, temos que

$$N(m,g) = \theta(m)\Theta(g)\left(q^n + \int_{d(\neq 1)|m}\int_{h(\neq 1)|g}\sum_{\alpha\in\mathbb{F}_q}\eta_d(\alpha)\chi(\delta_h\alpha)\right).$$

Onde $\chi(\alpha\delta_h) = \chi_{\delta_h}(\alpha)$. Como já descartamos o caso $h = 1$, que implica em $\delta_1 = 0$, podemos substituir α por α/δ_h. Logo

$$N(m,g) = \theta(m)\Theta(g)\left(q^n + \int_{d(\neq 1)|m}\int_{h(\neq 1)|g}\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d(\alpha)\chi(\alpha)\overline{\eta_d(\delta_h)}\right),$$

onde o termo $\overline{\eta_d(\delta_h)}$ vem do fato de que $\eta_d(\delta_h^{-1}) = \overline{\eta_d(\delta_h)}$. O resultado segue pois

$$\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d(\alpha)\chi(\alpha)\overline{\eta_d(\delta_h)} = G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}.$$

□

Note que na expressão obtida para $N(m,g)$ o termo $G_n(\eta_d,\chi)$ aparece tantas vezes quanto os divisores livres de quadrado de m e g. Sendo assim, para $d \in D$ um domínio de ideais principais, defina $\omega(d)$ como o número de elementos irredutíveis distintos que aparecem na fatoração de d e $W(d) = 2^{\omega(d)}$ o número de divisores livres de quadrados de d.

Corolário 4.12.1. *Nas mesmas condições da Proposição 4.12, temos que*

$$N(m,g) \geq \theta(m)\Theta(g)\left(q^n - \epsilon_g - (W(m)-1)(W(g)-1)\,q^{n/2}\right).$$

Demonstração.

$$\begin{aligned} N(m,g) &\geq \theta(m)\Theta(g)\left(q^n - \epsilon_g - \left|\int_{d(\neq 1)|m}\int_{h(\neq 1)|g} G_n(\eta_d,\chi)\overline{\eta_d}(\delta_h)\right|\right) \\ &\geq \theta(m)\Theta(g)\left(q^n - \epsilon_g - \int_{d(\neq 1)|m}\int_{h(\neq 1)|g}|G_n(\eta_d,\chi)\overline{\eta_d}(\delta_h)|\right) \\ &\geq \theta(m)\Theta(g)\left(q^n - \epsilon_g - (W(m)-1)(W(g)-1)\,q^{\frac{n}{2}}\right), \end{aligned} \tag{4.1}$$

pois $|G_n(\eta_d,\chi)| = q^{\frac{n}{2}}$ e apenas os divisores livres de quadrados de m e g fornecem termos não nulos para as integrais. □

Para provarmos o Teorema da Base Normal e Primitiva em extensões do tipo $\mathbb{F}_{q^n}|\mathbb{F}_q$ precisamos garantir que $N(q^n-1, X^n-1) > 0$, que é equivalente a existência de pelo menos um elemento $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$ e primitivo. Pela Proposição 4.8, é suficiente mostrar que $N(Q, X^n-1) > 0$. Escrevendo $q = p^b$ e $n = p^j n^*$ onde $p \nmid n^*$ e p é um número primo, a demonstração é dividida em 7 casos:

- Caso 1: Pares (q,n) tais que $n^* \leq 4$, com $q \equiv 2 \pmod 3$ se $n^* = 3$ e $q \equiv 3 \pmod 4$ se $n^* = 4$.
- Caso 2: Pares (q,n), onde $n^* = q - 1 > 2$.

- Caso 3: Pares (q, n), onde $2 < n^* \mid (q-1)$ e $n^* \neq (q-1)$.
- Caso 4: Pares (q, n) com $n^* = l \geq 5$, onde l é primo ou $l = q+1$, com q par.
- Caso 5: Pares (q, n), com $n^* = 2l \geq 6$, onde l é primo ou $l = \frac{1}{2}(q+1)$ e $q \equiv 3 \pmod 4$.
- Caso 6: Pares (q, n), onde $q \geq 5$ e $n^* \geq 8$.
- Caso 7: Pares (q, n), onde $q < 5$ e $n^* \geq 8$.

Vejamos que os 7 casos acima de fato cobrem todos os pares (q, n). Note que os casos 6 e 7 cobrem todos os pares (q, n) onde $n^* \geq 8$. Vejamos que os outros casos cobrem os pares restantes. O caso 1 cobre os casos $n^* \leq 4$ com exceção dos casos

- $q \equiv 1 \pmod 3$, se $n^* = 3$,
- $q \equiv 1 \pmod 4$, se $n^* = 4$,

que são cobertos pelos casos 2 e 3. Portanto, os 3 primeiros casos cobrem todos os pares (q, n), onde $n^* \leq 4$. O caso 4 cobre em particular os casos (q, n) onde $n^* = 5$ e $n^* = 7$, já o caso 5 cobre em particular o caso $n^* = 6$, esgotando, assim, todos os casos. As condições extras que aparecem nos casos 4 e 5 e não foram usados na argumentação acima, aparecem para cobrir alguns pares particulares (q, n) na demonstração dos casos 6 e 7. Vamos mostrar os casos 2 e 7 que englobam toda a teoria desenvolvida para demonstrar o Teorema. Os casos restantes podem ser encontrados em [8].

A primeira abordagem ao problema, feita por Lenstra e Schoof em [23] mostra que $N(Q, X^n - 1)$ é positivo utilizando o Corolário 4.12.1 para $m = Q$ e $g = X^n - 1$, exceto para alguns pares (q, n), fazendo detalhadas considerações acerca dos divisores de Q. O método de Cohen e Huczynska em [8] no entanto é focado na parte *aditiva* de $\mathbb{F}_{q^n}$, ou seja, nos divisores de $X^n - 1$ (mais precisamente em sua parte livre de quadrados) ou em valores menores, utilizando resultados como a Proposição 4.10. O seguinte resultado fornece uma cota superior para $W(m)$.

Proposição 4.13. *Sejam m e a inteiros positivos. Então:*

$$W(m) \leq c_m m^{1/a},$$

onde $c_m = 2^s/(p_1, \ldots p_s)^{1/a}$ e $p_1, \ldots, p_s$ são os primos distintos menores que 2^a que dividem m.

Demonstração. Seja $m = p_1^{t_1} \ldots p_s^{t_s} p_{s+1}^{t_{s+1}} \ldots p_k^{t_k}$ a sua fatoração única em $\mathbb{Z}$, onde $p_{s+1}, \ldots, p_k$ são os primos distintos maiores que 2^a. Assim, temos $m \geq p_1 \ldots p_s 2^{a(k-s)}$, ou seja

$$2^{ak} \leq \frac{2^{as} m}{p_1 \ldots p_s}.$$

Segue que

$$W(m) = 2^k \leq \frac{2^s m^{1/a}}{(p_1 \ldots p_s)^{1/a}} = c_m m^{1/a}.$$

□

Observação 4.13.1. Embora o resultado acima seja válido para $a \in \mathbb{N}$, o caso $a = 4$ é suficiente para os fins da demonstração do Teorema da Base Normal e Primitiva.

Corolário 4.13.1. *Seja m um inteiro positivo. Então*

$$W(m) \leq c_m m^{1/4}, \tag{4.2}$$

onde $c_m < 4.9$ para todo $m \in \mathbb{N}$ e $c_m < 2.9$ para m ímpar.

Demonstração. Nos resta mostrar apenas as cotas superiores para c_m. Temos que c_m assume seu máximo quando todos os primos menores que $2^4 = 16$ aparecem na fatoração de m, ou seja

$$c_m = \frac{2^6}{(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13)^{1/4}} < 4.9,$$

já no caso m ímpar, basta remover um fator 2 no numerador e no denominador da expressão acima. □

Note que, caso tenhamos mais informações sobre os primos menores que 16 que aparecem na fatoração de m, podemos aprimorar a cota para c_m.

4.4 Uma desigualdade de redução

Nesta seção é descrita uma forma de obter informações sobre $N(Q, X^n - 1)$ a partir de informações acerca dos divisores de Q e $X^n - 1$. Mais precisamente, para um par (q, n), seja $f \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. Sejam $f_1, \ldots, f_r$, $r \geq 2$, fatores de f. O conjunto $\{f_1, \ldots f_r\}$ é chamado de um *conjunto de divisores complementares* de f com divisor comum f_0 se $mmc(f_1, \ldots, f_r) = f$ e $\text{mdc}(f_i, f_j) = f_0$, para todo $i \neq j$.

Proposição 4.14. *Para m um divisor de Q e $f \in \mathbb{F}[X]$ um divisor de $X^n - 1$, seja $\{f_1, \ldots, f_r\}$, $r \geq 2$ um conjunto de divisores complementares de f com divisor comum f_0. Então*

$$N(m, f) \geq \left(\sum_{i=1}^{r} N(m, f_i) \right) - (r-1) N(m, f_0). \tag{4.3}$$

Demonstração. Sejam $f \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$ e $\{f_1, \ldots, f_r\}$, $r \geq 2$, um conjunto de divisores complementares de f com divisor comum f_0. Usamos indução em r. Se $r = 2$, devemos mostrar que

$$N(m, f) \geq N(m, f_1) + N(m, f_2) - N(m, f_0).$$

Para $g \in \mathbb{F}_q[X]$, defina S_g como o conjunto dos elementos que são m-livres e g-livres. Então $N(m, f) = S_f$ e é claro que

$$\#\left(S_{f_1} \cup S_{f_2}\right) = \#S_{f_1} + \#S_{f_2} - \#\left(S_{f_1} \cap S_{f_2}\right).$$

Como f_0 divide f_1 e f_2, temos que $S_{f_1} \cup S_{f_2} \subseteq S_{f_0}$. Como $f = mmc(f_1, f_2)$, segue que $S_{f_1} \cap S_{f_2} = S_f$. Logo $\#S_{f_1} + \#S_{f_2} - \#S_f \leq S_{f_0}$ e o resultado é válido. Suponha agora o resultado válido para $k = r - 1$. Como o conjunto $\{f_1, \ldots f_r\}$ é um conjunto de divisores complementares de f com divisor comum f_0, então definindo $f' = f_1 \cdots f_{r-1}$, temos que o conjunto $\{f', f_r\}$ também é um conjunto de divisores complementares de f com divisor comum f_0. Pelo caso $r = 2$, temos que

$$N(m, f) \geq N(m, f') + N(m, f_r) - N(m, f_0) \geq N(m, f_r) + \sum_{i=1}^{r-1} N(m, f_i) - (r-2) N(m, f_0) + N(m, f_0),$$

onde usamos a hipótese de indução na última desigualdade. O resultado segue. □

Note que, definindo um conjunto de divisores complementares de m com divisor comum m_0 de maneira análoga à definida para polinômios, obtemos um resultado análogo à proposição 4.14. Este fato será explorado mais adiante.

Para aplicarmos a Proposição 4.14, precisamos de informações acerca dos divisores de $X^{n^*}-1$. Um caso particular é quando n^* divide $q-1$, assim todas as raízes da unidade de ordem n^* pertencem a $\mathbb{F}_q$, portanto $X^{n^*}-1$ é o produto de n^* fatores lineares distintos em $\mathbb{F}_q[X]$. Consideramos agora o caso $n^* = q-1$, que é o Caso 2.

Caso 2. Os pares (q,n) onde $n^* = q-1 > 2$. Neste caso $Q(q,n) = Q = \frac{q^n-1}{(q-1)^2} < \frac{q^n}{(q-1)^2}$. Pelo Corolário 4.13.1, $W(Q) < \frac{c_Q q^{n/4}}{\sqrt{q-1}}$.

i) Suponha que q é ímpar, logo n^* é par. Defina $k = \frac{q-1}{2}$ e considere os polinômios coprimos $f_1 = X^k - 1$ e $f_2 = X^k + 1$. Temos que $\{f_1, f_2\}$ é um conjunto de divisores complementares de f com divisor comum 1. Pela Proposição 4.14, temos que

$$N(Q, X^n - 1) = N(Q, X^{n^*} - 1) \geq N(Q, X^k - 1) + N(Q, X^k + 1) - N(Q, 1).$$

Note que $\Theta(X^k - 1) = \Theta(X^k + 1)$ e $W(X^k + 1) = W(X^k - 1) = 2^k$. Pelo Corolário 4.12.1 aplicado em $N(Q, X^k - 1), N(Q, X^k + 1)$ e $N(Q, 1)$, temos que

$$\begin{aligned} N(Q, X^{n^*} - 1) &\geq 2\theta(Q)\Theta(X^k + 1)\left(q^n - (W(Q) - 1)(W(X^k + 1) - 1)\right) q^{n/2} - \theta(Q)(q^n - 1) \\ &\geq 2\theta(Q)\Theta(X^k + 1)\left(q^n - (W(Q) - 1)(W(X^k + 1) - 1)\right) q^{n/2} - \theta(Q)q^n \\ &\geq \theta(Q)\left(2\Theta(X^k + 1)\left(q^n - (2^k - 1)(W(Q) - 1)q^{n/2}\right) - q^n\right), \end{aligned} \tag{4.4}$$

Temos que $\Theta(X^k + 1) = \dfrac{\Phi(X^k + 1)}{N(X^k + 1)} = \dfrac{(q-1)^k}{q^k} = \left(1 - \dfrac{1}{q}\right)^k$, pois $X^k + 1$ é o produto de k fatores lineares distintos em $\mathbb{F}_q[X]$. Logo

$$N(Q, X^{n^*} - 1) \geq \theta(Q)\left(2\left(1 - \frac{1}{q}\right)^k \left(q^n - (2^k - 1)(W(Q) - 1)q^{n/2}\right) - q^n\right).$$

Portanto $N(Q, X^{n^*} - 1)$ é positivo quando

$$2\left(1 - \frac{1}{q}\right)^k \left(q^n - (2^k - 1)(W(Q) - 1)q^{n/2}\right) > q^n,$$

$$2\left(1 - \frac{1}{q}\right)^k q^n - q^n > 2\left(1 - \frac{1}{q}\right)^k (2^k - 1)(W(Q) - 1)q^{n/2},$$

$$q^{n/2} > \frac{2\left(1 - \frac{1}{q}\right)^k (2^k - 1)(W(Q) - 1)}{2\left(1 - \frac{1}{q}\right)^k - 1},$$

ou seja, sempre que

$$q^{n/2} > \frac{2(2^k-1)(W(Q)-1)}{2-\left(1-\frac{1}{q}\right)^{-k}}. \tag{4.5}$$

Note que $(1-\frac{1}{q})^{2k} = (1-\frac{1}{q})^{q-1}$ é uma função decrescente em q que converge para $1/e$. Portanto $\dfrac{2}{2-(1-\frac{1}{q})^{-k}}$ converge para $\dfrac{2}{2-\sqrt{e}} < 5.7$. Sendo assim, $N(Q, X^{n^*}-1)$ é positivo quando

$$\frac{q^{n/4}}{2^{(q-1)/2}} > \frac{5.7c_Q}{\sqrt{q-1}}. \tag{4.6}$$

Observe que a função

$$\frac{q^{n/4}\sqrt{q-1}}{2^{(q-1)/2}}$$

é uma função crescente tanto em q quanto em n, sendo assim, se (4.6) é valida para um par (q_0, n_0), ela também será válida para qualquer par (q, n), com $q \geq q_0$ e $n \geq n_0$. Portanto, escrevemos (q_0+, n_0+) para denotar qualquer par (q, n) tal que $q \geq q_0$ e $n \geq n_0$. No entanto, (q_0+, n_0+) significa que n_0 é o menor inteiro positivo n tal que (4.6) vale numericamente quando $q = q_0$, apesar do par (q_0, n_0) não necessariamente satisfazer a condição do Caso 2. Portanto, a notação (q_0+, n_0+) não fornece informação sobre o par (q_0, n_0). Isto é necessário para cobrir todos os casos.

Retornando à análise de (4.6), temos que ela vale para $(5+, 10+)$ (observe que o par $(5, 10)$ não pertence ao Caso 2), pois neste caso, $Q(5, 10)$ é par. Faltam os casos $(9, 8)$, $(7, 6)$ e $(5, 4)$. Para o caso $(9, 8)$, temos que $Q(9, 8)$ é ímpar e claramente 3 não divide $Q(9, 8)$. Logo podemos considerar $c_Q < 2$ e com isso (4.6) é satisfeita. Quanto ao par $(7, 6)$, $Q(7, 6) = 2 \cdot 19 \cdot 43$, portanto na desigualdade (4.5), temos que

$$\frac{2(2^k-1)(W(Q)-1)}{2-(1-\frac{1}{q})^{-k}} = \frac{2(2^3-1)(W(2\cdot 19\cdot 43)-1)}{2-(1-\frac{1}{7})^{-3}} < 238 < 7^3 = q^{n/2}.$$

Para o caso $(5, 4)$, pelo Exemplo 4.1, $N(Q, X^4-1) = N(3, X^4-1)$ e

$$\begin{aligned} N(3, X^4-1) \geq & \theta(3)\Theta(X^4-1)(5^4-(W(3)-1)(W(X^4-1)-1)5^2) \\ = & \theta(3)\Theta(X^4-1)(5^4-(2^4-1)5^2) \\ = & \theta(3)\Theta(X^4-1)(5^4-3\cdot 5^3), \end{aligned} \tag{4.7}$$

pelo Corolário 4.12.1. É claro que

$$\theta(3)\Theta(X^4-1)(5^4-3\cdot 5^3) > 0.$$

ii) O caso em que q é par é similar. Definimos $k = (q-1)/2$ e consideramos como conjunto de divisores complementares de $X^{n^*}-1$ qualquer par de polinômios coprimos com grau $k+\frac{1}{2}$ e $k-\frac{1}{2}$. Analogamente ao caso anterior, obtemos:

$$\frac{q^{n/4}}{2^{(q-1)/2}} > \frac{6.04c_Q}{\sqrt{q-1}}. \tag{4.8}$$

O resultado segue de maneira semelhante ao caso anterior. Os cálculos serão omitidos, mas podem ser encontrados em [8, Example 4.2].

Para garantir a existência de um elemento normal e primitivo na extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$ para qualquer par (q,n), pela Proposição 4.14 é necessário analisar a fatoração de $X^{n^*}-1$. Para isso, defina $s(q,n)=s:=\mathrm{ord}_{n^*}(q)$ ou seja, s é o menor inteiro positivo tal que $q^s\equiv 1 \pmod{n^*}$. Portanto, $\mathbb{F}_{q^s}$ é a menor extensão de $\mathbb{F}_q$ que contém todas as n^*-ésimas raízes da unidade. Temos também que s divide $\varphi(n^*)$. Cada fator irredutível de $X^{n^*}-1$ sobre $\mathbb{F}_q[X]$ possui como grau um divisor de s pois s é o grau da extensão $\mathbb{F}_{q^s}|\mathbb{F}_q$. Sendo assim, escreva $X^{n^*}-1=gG$, onde G é o produto dos fatores irredutíveis de $X^{n^*}-1$ de grau s e g é o produto dos fatores irredutíveis de $X^{n^*}-1$ de grau menor que s. Se $s=1$, definimos $g=1$. Definimos também $r(q,n)=r$, como sendo o número de fatores irredutíveis de $G=\prod_{i=1}^{r}G_i$, e $m(q,n)=m:=\mathrm{grau}(g)$. Note que $rs+m=n^*$. Consideramos o conjunto $\{g_1,\dots g_r\}$, onde $g_i=gG_i$. Como $X^{n^*}-1$ é livre de quadrados, segue que $\{g_1,\dots,g_r\}$ é um conjunto de divisores complementares de $X^{n^*}-1$ com divisor comum g. Com isso, mostramos a seguinte proposição.

Proposição 4.15. *Com a mesma notação anterior, temos que $N(Q,X^n-1)>0$ sempre que*

$$q^{\frac{n}{2}}>(W(Q)-1)\left(W(g)\left(\frac{(n^*-m)(q^s-1)}{sq^s-(n^*-m)}+1\right)-1\right). \tag{4.9}$$

Demonstração. Como $\{g_1,\dots,g_r\}$ é um conjunto de divisores complementares de $X^{n^*}-1$ com divisor comum g, a Proposição 4.14 nos dá

$$N(Q,X^n-1)=N(Q,X^{n^*}-1)\geq\left(\sum_{i=1}^{r}N(Q,g_i)\right)-(r-1)N(Q,g). \tag{4.10}$$

Pela Proposição 4.12, para $i=1,\dots,r$ temos que

$$\begin{aligned}N(Q,g_i)&=\theta(Q)\Theta(g_i)\left(q^n+\int_{d(\neq 1)|Q}\int_{h(\neq 1)|g_i}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right)\\&=\theta(Q)\Theta(g_i)\left(q^n+\int_{d(\neq 1)|Q}\int_{h(\neq 1)|g}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}+\int_{d(\neq 1)|Q}\int_{h|g_i,h\nmid g}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right).\end{aligned} \tag{4.11}$$

Como $g_i=gG_i$ e G_i é um polinômio irredutível de grau s e G_i é primo com g, segue que $\Theta(g_i)=\Theta(g)\Theta(G_i)=\Theta(g)\left(1-\frac{1}{q^s}\right)$. Portanto,

$$\begin{aligned}\sum_{i=1}^{r}N(Q,g_i)&=\theta(Q)\Theta(g)r\left(1-\frac{1}{q^s}\right)\left(q^n+\int_{d(\neq 1)|Q}\int_{h(\neq 1)|g}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right)\\&\quad+\theta(Q)\Theta(g)\left(1-\frac{1}{q^s}\right)\sum_{i=1}^{r}\int_{d(\neq 1)|Q}\int_{h|g_i,h\nmid g}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\end{aligned} \tag{4.12}$$

Temos também que

$$N(Q,g)=\theta(Q)\Theta(g)\left(q^n+\int_{d(\neq 1)|Q}\int_{h(\neq 1)|g}G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right). \tag{4.13}$$

Sendo assim, por (4.10), (4.12) e (4.13) obtemos

$$N(Q, X^n-1) \geq \theta(Q)\Theta(g)\Bigg(\left(r\left(1-\frac{1}{q^s}\right)-(r-1)\right)\left(q^n + \int_{d(\neq 1)|Q}\int_{h(\neq 1)|g} G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\right) \\ + \left(1-\frac{1}{q^s}\right)\sum_{i=1}^{r}\int_{d(\neq 1)|Q}\int_{h|g_i, h\nmid g} G_n(\eta_d,\chi)\overline{\eta_d(\delta_h)}\Bigg) \tag{4.14}$$

Note que, pela definição dos g_i, temos que $W(g_i) = 2W(g)$, assim $W(g_i) - W(g) = W(g)$. Logo, o número de $h \in \mathbb{F}_q[X]$ livres de quadrado tais que $h \mid g_i$ e $h \nmid g$ é $W(g_i) - W(g) = W(g)$. Portanto, como no Corolário 4.12.1, temos que

$$\frac{N(Q, X^n-1)}{\theta(Q)\Theta(g)} \geq \Bigg(\left(r\left(1-\frac{1}{q^s}\right)-(r-1)\right)\left(q^n - (W(Q)-1)(W(g)-1)q^{\frac{n}{2}}\right) \\ - r\left(1-\frac{1}{q^s}\right)(W(Q)-1)W(g)q^{\frac{n}{2}}\Bigg). \tag{4.15}$$

Ou seja,

$$\frac{N(Q, X^n-1)}{\theta(Q)\Theta(g)q^{\frac{n}{2}}} \geq \left(1-\frac{r}{q^s}\right)\left(q^{\frac{n}{2}} - (W(Q)-1)(W(g)-1)\right) - r\left(1-\frac{1}{q^s}\right)(W(Q)-1)W(g), \tag{4.16}$$

portanto, $N(Q, X^n-1)$ é positivo quando

$$q^{\frac{n}{2}} > \frac{(W(Q)-1)W(g)r(q^s-1)}{q^s-r} + (W(Q)-1)(W(g)-1) \\ > (W(Q)-1)\left(W(g)\left(\frac{r(q^s-1)}{q^s-r}+1\right)-1\right). \tag{4.17}$$

Lembramos que r é o número de fatores irredutíveis de $G = \prod_{i=1}^{r} G_i$, m é o grau do polinômio g, $X^{n^*}-1 = gG$ e todo fator irredutível de G tem grau s. Portanto temos que $rs + m = n^*$, sendo assim $N(Q, X^n-1)$ é positivo quando

$$q^{\frac{n}{2}} > (W(Q)-1)\left(W(g)\left(\frac{(n^*-m)(q^s-1)}{sq^s-(n^*-m)}+1\right)-1\right), \tag{4.18}$$

o que completa a prova. □

Para trabalhar com a desigualdade (4.9) é necessário encontrar boas cotas para $W(g)$. Para tal, são necessárias mais algumas notações. Relembramos que s é o menor inteiro positivo tal que $q^s \equiv 1 \pmod{n^*}$, g é o produto dos fatores irredutíveis de grau menor que s e $\omega(g)$ é o número de fatores irredutíveis distintos de g sobre $\mathbb{F}_q$. Note que $\omega(g)$ depende de q e n, por isso escrevemos $\omega(g) := \omega(q,n) := \omega$. Defina a razão $\rho := \rho(q,n) = \omega(q,n)/n$. Vamos encontrar cotas para $\rho(q,n)$. Pela definição do polinômio g, segue que $\omega(q,n) = \omega(q,n^*)$, portanto é suficiente encontrar cotas quando $p \nmid n$. Finalmente, para todo divisor d de $s(q,n)$, defina $n_d := \mathrm{mdc}(q^d-1, n)$. Com essa definição temos que $n_s = n^*$. O seguinte resultado técnico fornece cotas para ρ.

Proposição 4.16. *Suponha que $n > 4$ e $p \nmid n$. Então:*

i) Se $n = 2n_1$ e q é ímpar, então $\rho = 1/2$;

se $n = 4n_1$ *e* $q \equiv 1 \pmod 4$, *então* $\rho = 3/8$;
se $n = 6n_1$ *e* $q \equiv 1 \pmod 6$, *então* $\rho = 13/36$;
caso contrário $\rho(q,n) \leq 1/3$.

ii) $\rho(4,9) = 1/3$, $\rho(4,45) = 11/45$, *caso contrário* $\rho(4,n) \leq 1/5$.

iii) $\rho(3,16) = 5/16$, *caso contrário* $\rho(3,n) \leq 1/4$.

iv) $\rho(2,5) = 1/5$, $\rho(2,9) = 2/9$, $\rho(2,21) = 4/21$, *caso contrário* $\rho(2,n) \leq 1/6$.

Demonstração. A prova pode ser encontrada em [8, Section 7]. □

Para o Caso 7, note que devido aos casos anteriores, podemos supor $n^* > 4$, $n^* \nmid (q-1)$ e $s > 1$. Pelo Corolário 4.13.1, temos que

$$W(Q) < c_Q \left(\frac{q^n}{n_1(q-1)} \right)^{1/4}, \tag{4.19}$$

onde $n_1 = \mathrm{mdc}(q-1, n)$, como definido anteriormente. Seja

$$\beta(q,n) := 2^{\omega(g)} \left(\frac{(n^* - m)(q^s - 1)}{sq^s - (n^* - m)} + 1 \right) - 1. \tag{4.20}$$

Pela Proposição 4.15, temos que $N(Q, X^n - 1) > 0$ se

$$q^{\frac{n}{2}} > (W(Q) - 1)\beta(q,n). \tag{4.21}$$

Para o Caso 7, a seguinte cota para $\beta(q,n)$ é suficiente.

Lema 4.17. *Seja* ρ_0 *um número positivo tal que* $\rho_0 \leq \frac{1}{3}$. *Suponha que* $\rho(q,n^*) = \omega(q,n^*)/n^* \leq \rho_0$. *Então*

$$\beta(q,n) < 2^{\rho_0 n^*} \left(\frac{n^*}{\frac{s}{1-\rho_0} - 1} + 1 \right). \tag{4.22}$$

Demonstração. [8, Lemma 6.3]. □

Se $\rho(q,n^*) \leq 1/3$, junto com a Proposição 4.15, o Lema 4.17 e (4.19) temos que $N(Q, X^n - 1)$ é positivo se

$$q^{\frac{n}{2}} > c_Q \left(\frac{q^n}{n_1(q-1)} \right)^{1/4} 2^{\rho_0 n^*} \left(\frac{n^*}{\frac{s}{1-\rho_0} - 1} + 1 \right).$$

Como $n^* \leq n$, temos que $N(Q, X^n - 1)$ é positivo sempre que

$$\frac{(q^n n_1(q-1))^{1/4}}{2^{\rho_0 n}} > c_Q \left(\frac{n}{\frac{s}{1-\rho_0} - 1} + 1 \right). \tag{4.23}$$

Estamos aptos a mostrar o Caso 7.

Caso 7: Pares (q,n), com $q = 2, 3$ ou 4 e $n^* \geq 8$. Suponha que $q = 4$. Então $Q(4,n)$ é ímpar. Se $n \neq n^*$, então $n^* \leq n/2$. Portanto, $\rho(4,n) \leq \frac{1}{2}\rho(4,n^*) \leq 1/6 < 1/5$, pela Proposição 4.16. Se $n = n^*$, temos que $\rho(4,n) \leq 1/5$ se $n = n^* \neq 9, 45$. Sendo assim, para $n \neq 9, 45$, por (4.23) com $q = 4, \rho_0 = 1/5$ e como $s \geq 2$,

o resultado é válido se

$$(3n_1)^{\frac{1}{4}}2^{\frac{3n}{10}} > c_Q\left(\frac{2n}{3}+1\right). \tag{4.24}$$

Note que como $q = 4$ e $n^* \geq 8$, temos que $n \geq 17$. O caso $n = n^* = 17$ é garantido pelo Caso 4. Como Q é ímpar, temos que $c_Q < 2.9$ e (4.24) vale para $n \geq 18$ com $n_1 = 1$. Para $n = 15$, temos que $n_1 = \text{mdc}(q-1, n) = 3$ e (4.24) também vale. Para o caso $n^* = 45$ não coberto pela Equação (4.24), temos que $\rho(4, 45) = 11/45 < 1/4$ e $s = 6$. Sendo assim, tomando $\rho_0 = 1/4$ no Lema 4.17, temos que o resultado é válido se

$$(3n_1)^{\frac{1}{4}}2^{\frac{n}{4}} > c_Q\left(\frac{n}{7}+1\right), \tag{4.25}$$

que é claramente válido para $n \geq 45$ com $n_1 = 1$. Quanto ao caso restante $n^* = 9$, temos que $s = 3$ e $\rho(4, 9) = 1/3$. Logo, o resultado é válido se

$$(3n_1)^{\frac{1}{4}}2^{\frac{n}{6}} > c_Q\left(\frac{2n}{7}+1\right), \tag{4.26}$$

que é válido se $n \geq 24$ e $n_1 = 1$, ou seja, resta o caso $n = 9$. Se $n = 9$, então $Q(4, 9) = 3 \cdot 7 \cdot 19 \cdot 73$ e usando a Equação (4.21) e observando que $m \geq \omega = 3$, temos que $(W(Q) - 1)\beta(4, 9) < 349 < 4^{\frac{9}{2}}$. Os casos restantes, $n = 10, 11, 12, 13, 14$ são cobertos pelos casos anteriores, sendo $n = 10, 12, 14$ pois $n^* < 8$ e $n = n^* = 11, 13$ pelo Caso 4, completando o caso $q = 4$.

Suponha, agora, $q = 3$. Se $s = 2$, então $3^2 \equiv 1 \pmod{n^*}$, ou seja $n^* = 2, 4$ ou 8. Os casos $n^* \leq 4$ são cobertos pelo Caso 1, restando apenas o caso $n = n^* = 8$. Se $s = 3$, então $n^* = 13$ ou 26. O caso $n = n^* = 13$ é coberto pelo Caso 4 enquanto o caso $n = n^* = 26 = 2 \cdot 13$ é coberto pelo Caso 5. Portanto todos os casos com $s < 4$ exceto $n = n^* = 8$ estão cobertos. Suponha agora $s \geq 4$. Pela Proposição 4.16, $\rho(3, n^*) \leq 5/16$. Se $n \neq n^*$, ou seja, $n^* \leq n/3$, temos que com $\rho = 5/16$ no Lema 4.17 obtemos que

$$\beta(3, n) < 2^{\frac{5n^*}{16}}\left(\frac{11n^*}{53}+1\right). \tag{4.27}$$

Como $n^* \leq n/3$, segue que

$$\beta(3, n) < 2^{\frac{5n}{48}}\left(\frac{11n}{159}+1\right) < 2^{\frac{5n}{48}}\left(\frac{n}{13}+1\right), \tag{4.28}$$

ou seja, o resultado é válido se

$$\frac{(2n_1)^{\frac{1}{4}}3^{\frac{n}{4}}}{2^{\frac{5n}{48}}} > c_Q\left(\frac{n}{13}+1\right), \tag{4.29}$$

que vale com $n_1 = 1$ para $n \geq 24$ e note que 24 é o menor valor tal que $n \neq n^*$, pois $n^* \geq 8$. Suponha então $n = n^*$. Se $n^* \neq 16$, então $\rho(q, n^*) \leq 1/4$, sendo assim, por (4.23) com $\rho_0 = 1/4$, temos que o resultado é válido se

$$(2n_1)^{\frac{1}{4}}(3/2)^{\frac{n}{4}} > c_Q\left(\frac{3n}{4s-3}+1\right). \tag{4.30}$$

Com $c_Q < 3.2$ (3 não divide Q), $n_1 = 1$ e $s \geq 4$, (4.30) é válida para $n \geq 40$ e com $s \geq 6$, (4.30) é válido para $n \geq 25$. Restam os casos $n = 8, 9, 10, \ldots, 23$. Observe que $n = 9, 12, 15, 18, 21$, são tais que $n^* < 8$, cobertos pelos casos anteriores. Quando $n = n^* = 10, 14, 22$ o resultado vale pelo Caso 5. Se $n = n^* = 11, 13, 17, 19, 23$, o resultado é válido pelo Caso 4. Restam agora os casos $n = 8$ ($s = 2$) e $n = 16, 20$ ($s = 4$). Se $n = n^* = 16$, temos que $s = 4$, $m \geq \omega = 5$ e $Q(3, 16) = 2 \cdot 5 \cdot 17 \cdot 41 \cdot 193$, portanto $(W(Q) - 1)\beta(3, 16) < 3751 < 3^{\frac{16}{2}}$ e (4.21) vale. Se $n = 20$, temos que $s = 2$, $n_1 = 2$ e $Q =$

$2^2 \cdot 5^2 \cdot 11^2 \cdot 61 \cdot 1181$, logo $c_Q < 2.9$ e (4.30) é satisfeita. Se $n = 8$, então, pelo Exemplo 4.1, temos que $N(Q(3,8), X^8 - 1) = N(10, X^8 - 1)$. Temos também que $s = 2$. Sobre $\mathbb{F}_3$, o polinômio $X^8 - 1$ se fatora como $X^8 - 1 = (X-1)(X+1)(X^2+1)(X^2+X+2)(X^2+2X+2)$, logo $m = \text{grau}(g) = 2$ e $\omega(g) = 2^2$ (g é o produto de todos os polinômios de grau menor que $s = 2$ que são fatores de $X^8 - 1$). Logo, $(W(2 \cdot 5) - 1)\beta(3,8) = 57 < 3^4$. Portanto o resultado vale por (4.20) e (4.21), encerrando o caso $q = 3$.

Para o caso $q = 2$, temos que $Q = 2^n - 1$ é ímpar, logo $c_Q < 2.9$. Suponha que n é par, então $n^* \leq n/2$. Note que todo $n < 30$ exceto $n = 18$ está coberto pelos casos anteriores. Pela Proposição 4.16, temos que $\rho(2, n^*) \leq 1/6$, logo, pelo Lema 4.17,

$$\beta(2,n) < 2^{\frac{n^*}{6}} \left(\frac{5n^*}{6s-5} + 1 \right), \tag{4.31}$$

ou seja,

$$\beta(2,n) < 2^{\frac{n}{12}} \left(\frac{5n}{2(6s-5)} + 1 \right). \tag{4.32}$$

Logo, o resultado é válido se

$$2^{\frac{n}{6}} > c_Q \left(\frac{5n}{2(6s-5)} + 1 \right). \tag{4.33}$$

Com $c_Q < 2.9$ e $s \geq 4$, (4.33) é válida para todo $n \geq 30$. O caso $s < 4$ é coberto pelos casos anteriores. Para $n = 18$, os únicos fatores primos menores que 16 que aparecem na fatoração de $Q(2,18)$ são 3 e 7, logo $c_Q < 1.9$. Como neste caso $s = 6$, a desigualdade (4.33) é satisfeita, completando o caso n par. Suponha agora n ímpar, ou seja, $n = n^*$. Se $s = 4$, o caso que falta é $n = 15$. Se $s = 5$, então $n = 31$, sendo este coberto pelo Caso 4. Se $s = 6$, então $n = 9, 21, 63$. Se $s = 7$, então $n = 127$, coberto pelo Caso 4. Se $l < 16$ é um número primo ímpar, a ordem de 2 módulo l só é ímpar se $l = 7$. Portanto o único primo menor que 16 que pode aparecer na fatoração de $Q(2,n) = 2^n - 1$ se n é ímpar é 7. Sendo assim, $c_Q < 1.23$. Se $n \neq 9, 21$, então, por (4.23) com $\rho_0 = 1/6$, temos que

$$2^{\frac{n}{12}} > c_Q \left(\frac{5n}{6s-5} + 1 \right), \tag{4.34}$$

que é satisfeita com $c_Q < 1.23$ e $s \geq 10$ para $n \geq 25$ e $n \geq 39$ se $s \geq 6$. Agora restam apenas os casos $n = 9, 21$ e $n = 15$. Se $n = 21$, então $Q(2,21) = 49 \cdot 127 \cdot 337$ e $X^{21} - 1$ se fatora como 1 fator linear, 1 fator quadrático, 2 fatores cúbicos e 2 fatores de grau 6. Portanto $W(Q) = 8$ e $W(X^{21} - 1) = 64$ e portanto $N(Q, X^2 1 - 1) > 0$ pelo Corolário 4.12.1. Se $n = 15$, então $Q = 7 \cdot 31 \cdot 151$ e $X^{15} - 1 = (X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$, logo $m = 3$, $\omega = 2$. Portanto $(W(Q) - 1)\beta(2,15) < 118 < 2^{\frac{15}{2}}$ e o resultado vale por (4.21). Para $n = 9$, $Q = 7\dot{7}3$, $X^9 - 1 = (X+1)(X^2+X+1)(X^6+X^3+1)$, logo $m = 3$, $\omega = 2$ e $(W(Q) - 1)\beta(2,9) = 21 < 2^{\frac{9}{2}}$, encerrando o caso $q = 2$.

A prova do Teorema da Base Normal e Primitiva está completa.

5 A Existência de Elementos Normais e Primitivos com Norma e Traço Prescritos

5.1 Introdução

O Teorema da Base Normal e Primitiva, provado por Lenstra e Schoof [23] em 1987 garante a existência de um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que α é primitivo e gera uma base normal sobre $\mathbb{F}_q$. Equivalentemente, para cada $n \in \mathbb{N}$, existe um polinômio normal e primitivo de grau n sobre $\mathbb{F}_q$. Em 1994, Mullen [25] conjecturou o seguinte resultado.

Conjectura 5.1. [25, Conjecture 1] Sejam $2 \leq n \in \mathbb{N}$ e $0 \neq a \in \mathbb{F}_q$. Então existe um polinômio normal e primitivo de grau n sobre $\mathbb{F}_q$ com traço a.

Esta conjectura foi provada por Cohen et al. em [6]. Seja $f \in \mathbb{F}_q[X]$ o polinômio mínimo de um elemento $\alpha \in \mathbb{F}_{q^n}$. Escrevendo

$$f = X^n + \sigma_{n-1}X^{n-1} + \cdots + \sigma_1 X + \sigma_0, \tag{5.1}$$

temos que $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = -\sigma_{n-1}$, ou seja, a Conjectura 5.1 é equivalente à existência de um polinômio normal e primitivo com o coeficiente σ_{n-1} prescrito. Portanto, é natural perguntar-se se é possível prescrever mais coeficientes de um polinômio normal e primitivo. Como temos que $\sigma_0 = (-1)^n \mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ em (5.1), uma escolha natural para o próximo coeficiente prescrito é σ_0. Com isso, Cohen propõe a seguinte questão, que é resolvida em [5] (completando o trabalho de Cohen et al., em [7]). Note que, se $\beta \in \mathbb{F}_{q^n}$ é primitivo, então $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\beta) \in \mathbb{F}_q$ também é primitivo.

Problema PFNT. Dados uma extensão finita $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ e $a, b \in \mathbb{F}_q^*$ com b primitivo, existe um elemento $\alpha \in \mathbb{F}_{q^n}$, primitivo e normal sobre $\mathbb{F}_q$, tal que $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$ e $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$? Caso a pergunta seja afirmativa para todo par (a, b), então o par correspondente (q, n) é chamado de um par PFNT.

O termo PFNT introduzido por Cohen et al. [7] é uma abreviação de *primitive, free, norm, trace*. O problema PFNT foi resolvido para $n \geq 5$ em [7] e [5]. Os casos $n = 3$ e $n = 4$ foram resolvidos em [9] e [10]

Nesta seção, damos uma prova do seguinte resultado.

Teorema 5.2. *[5, Theorem 1.1] Sejam $\mathbb{F}_{q^n}|\mathbb{F}_q$ uma extensão finita de corpos finitos, $b \in \mathbb{F}_q$ primitivo e $a \in \mathbb{F}_q$ não nulo. Para todo q e todo $n \geq 5$, existe um elemento $\alpha \in \mathbb{F}_{q^n}$ tal que α é primitivo, normal sobre $\mathbb{F}_q$ e é tal que $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$ e $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$.*

Tal prova é devida a Cohen [5], onde foi desenvolvida uma técnica intitulada *sieve technique*, para lidar com casos onde q e n são pequenos.

5.2 Reduções

Para mostrarmos o Teorema 5.2, mostraremos que o número de elementos $\alpha \in \mathbb{F}_{q^n}$ que satisfazem simultaneamente as seguintes condições

i) $\mathrm{ord}(\alpha) = q^n - 1$, ou seja, α é $(q^n - 1)$-livre,

ii) $\mathrm{Ord}(\alpha) = X^n - 1$, ou seja, α é $(X^n - 1)$-livre,

iii) $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$ e

iv) $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$

é positivo. Para tal, os próximos resultados nos mostram que podemos reduzir o problema a encontrar elementos com ordens multiplicativa e aditivas estritamente menores que $q^n - 1$ e $X^n - 1$.

Seja $m = m(q, n)$ o maior divisor de $q^n - 1$ primo com $q - 1$.

Lema 5.3. *Seja $\alpha \in \mathbb{F}_{q^n}$. Então α é primitivo se, e somente se, α é m-livre e $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ é primitivo em $\mathbb{F}_q$.*

Demonstração. Se $\alpha \in \mathbb{F}_{q^n}$ é primitivo, é claro que m divide $\mathrm{ord}(\alpha) = q^n - 1$ e também $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ é primitivo em $\mathbb{F}_q$ pois $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ é um homomorfismo sobrejetor de grupos cíclicos. Suponha então $\alpha \in \mathbb{F}_{q^n}$ m-livre e $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ primitivo em $\mathbb{F}_q$. Se $q = 2$, segue que $m = 2^n - 1$ e o resultado é válido pois m-livre é equivalente a ser primitivo. Suponha então $q > 2$ e sejam d um divisor de $q^n - 1$ e $\beta \in \mathbb{F}_{q^n}$ tal que $\alpha = \beta^d$. Precisamos mostrar que $d = 1$. Se $\mathrm{mdc}(d, m) = r$, então escrevemos $d = rs$, onde $\mathrm{mdc}(s, m) = 1$. Logo $\alpha = \beta^d = (\beta^s)^r$, como α é m-livre, então $r = 1$. Logo $\mathrm{mdc}(d, m) = 1$ e como m divide $q^n - 1$, segue que d divide $\frac{q^n-1}{m}$. Sendo assim, qualquer divisor primo de d é um divisor de $q - 1$ pois m é o maior divisor de $q^n - 1$ primo com $q - 1$. Como $q > 2$, $\mathrm{mdc}(d, q - 1) = d$. Agora $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\beta^d) = \mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\beta)^d$. Como, por hipótese, $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ é primitivo em $\mathbb{F}_q$, segue que $1 = \mathrm{mdc}(d, q - 1) = d$. O resultado segue. □

Um fato análogo vale no o caso aditivo. Sejam $q = p^b$, $n = p^j n^*$ onde $p \nmid n^*$ e $M = M(q, n) \in \mathbb{F}_q[X]$ o divisor mônico de $X^n - 1$, de grau máximo, tal que M é primo com $X - 1$. Neste caso,

$$M = \frac{X^n - 1}{X^{p^j} - 1}.$$

Lema 5.4. *Seja $\alpha \in \mathbb{F}_{q^n}$. Então α é normal sobre $\mathbb{F}_q$ se, e somente se $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)$ é diferente de 0 e α é M-livre sobre $\mathbb{F}_q$.*

Demonstração. Se $\alpha \in \mathbb{F}_{q^n}$ é normal sobre $\mathbb{F}_q$, então α é $(X^n - 1)$-livre e, em particular, M-livre. Isto implica que $\mathrm{Ord}(\alpha) = X^n - 1$, logo

$$\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = (1 + X + \cdots + X^{n-1}) \circ \alpha = \left(\frac{X^n - 1}{X - 1}\right) \circ \alpha \neq 0.$$

Suponha, agora, que $\alpha \in \mathbb{F}_{q^n}$ é M-livre sobre $\mathbb{F}_q$ e $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) \neq 0$. Sejam $g \in \mathbb{F}_q[X]$ um divisor de M e $\beta \in \mathbb{F}_{q^n}$ tais que $\alpha = g \circ \beta$, mostraremos que $g = 1$. Se $\mathrm{mdc}(g, M) = h$, então $M = ht$, onde $\mathrm{mdc}(t, M) = 1$. Logo, $\alpha = g \circ \beta = (ht) \circ \beta = h \circ (t \circ \beta)$, o que implica que $h = 1$, pois h divide M. Sendo assim, $g = 1$, ou $g = (X - 1)^k$, para $k \geq 1$. Se $g = 1$ o resultado vale, caso contrário,

$$\alpha = g \circ \beta = (X - 1)^k \circ \beta = (X - 1) \circ \big((X - 1)^{k-1} \circ \beta\big) = (X - 1) \circ \gamma,$$

onde $\gamma = (X - 1)^{k-1} \circ \beta \in \mathbb{F}_{q^n}$. Portanto,

$$\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = \frac{X^n - 1}{X - 1} \circ \alpha = \frac{X^n - 1}{X - 1} \circ ((X - 1) \circ \gamma) = (X^n - 1) \circ \gamma = 0,$$

um absurdo pois $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) \neq 0$ por hipótese. Logo $g = 1$ e o resultado está provado. □

Definição 5.5. Sejam t um divisor de $m = m(q, n)$, $T \in \mathbb{F}_q[X]$ um divisor de $M = M(q, n)$ e $a, b \in \mathbb{F}_q^*$ com b primitivo. Defina $N(t, T, a, b) := N(t, T)$ o conjunto dos elementos $\alpha \in \mathbb{F}_{q^n}$ tais que

i) α é t-livre,

ii) α é T-livre sobre $\mathbb{F}_q$,

iii) $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$ e

iv) $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$,

onde $b \in \mathbb{F}_q$ é um elemento primitivo e $a \in \mathbb{F}_q^*$. Defina $\pi(t,T) = q(q-1)N(t,T)$.

Temos que, pelos Lemas 5.3 e 5.4, para garantir a existência de um elemento $\alpha \in \mathbb{F}_{q^n}$ normal sobre $\mathbb{F}_q$ e primitivo é suficiente mostrar que $N(m,M) > 0$.

5.3 As funções características para traço e norma

Vamos, agora, construir as funções características para $\alpha \in \mathbb{F}_{q^n}$, tais que $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$ e $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$.

i) A função característica dos elementos $\alpha \in \mathbb{F}_{q^n}$ tais que $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b \in \mathbb{F}_q^*$.

A função característica pode ser expressa do seguinte modo

$$\frac{1}{q-1} \sum_{\nu \in \widehat{\mathbb{F}_q^*}} \nu(\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) b^{-1}), \text{ para } \alpha \in \mathbb{F}_{q^n}. \tag{5.2}$$

Se $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$, então o somatório retorna $q-1$ enquanto se $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) \neq b$, como $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) b^{-1} \neq 1$, o somatório retorna 0 pela Proposição 3.6.

ii) A função característica dos elementos $\alpha \in \mathbb{F}_q$ tais que $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$.

Seja $\lambda \in \widehat{\mathbb{F}_q}$ o caráter aditivo canônico, a função característica pode ser expressa por

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \lambda(c(\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) - a)), \text{ para } \alpha \in \mathbb{F}_{q^n}. \tag{5.3}$$

Novamente, se $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$, então o somatório retorna q, enquanto se $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) \neq a$, o somatório retorna 0 pela Proposição 3.6.

Se χ e λ são, respectivamente, os caráteres aditivos canônicos de $\mathbb{F}_{q^n}$ e $\mathbb{F}_q$, eles estão conectados pela expressão

$$\chi(\alpha) = \lambda(\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)), \text{ para } \alpha \in \mathbb{F}_{q^n}, \tag{5.4}$$

por (3.5). Para $h \in \mathbb{F}_q[X]$ um divisor de M, relembramos o conjunto

$$\Delta_h = \{\delta \in \mathbb{F}_{q^n} \mid \mathrm{Ord}(\chi_\delta) = h\},$$

definido no início da Seção 3.3.

Proposição 5.6. *Seja $1 \neq h \in \mathbb{F}_q[X]$ um divisor de M. Então $\Delta_h \cap \mathbb{F}_q = \emptyset$.*

Demonstração. Suponha, por absurdo, que exista $c \in \Delta_h \cap \mathbb{F}_q$. Então $\mathrm{Ord}(\chi_c) = h$, logo por (5.4), temos que $\chi_c(\alpha) = \chi(c\alpha) = \lambda(c\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha))$, para todo $\alpha \in \mathbb{F}_{q^n}$. Como $c \in \mathbb{F}_q$, segue que $c\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = d \in \mathbb{F}_q$, logo

$$\chi_c^{X-1}(\alpha) = \lambda((X-1) \circ d) = \lambda(d^q - d) = \lambda(0) = 1,$$

para todo $\alpha \in \mathbb{F}_{q^n}$, logo $h = \mathrm{Ord}(\chi_c)$ divide $X-1$, um absurdo pois h divide M que é primo com $X-1$. □

Corolário 5.6.1. *Sejam $h \in \mathbb{F}_q[X]$ um divisor de M e $c \in \mathbb{F}_q$. Se $\delta_h \in \Delta_h$, então $\delta_h + c = 0$ se, e somente se $h = 1$ e $c = 0$.*

Demonstração. Se $c = 0$, então $\delta_h = 0$ o que é equivalente a $h = 1$. Reciprocamente, se $\delta_h + c = 0$, então $\delta_h \in \mathbb{F}_q$. Pela Proposição 5.6, isso só acontece se $h = 1$, ou seja $\delta_h = 0$. □

Se ν é um caráter multiplicativo de $\mathbb{F}_q^*$, podemos estender ν para um caráter $\widehat{\nu} \in \widehat{\mathbb{F}_{q^n}^*}$ definindo $\widehat{\nu}(\alpha) = \nu(\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha))$. É claro que a ordem de $\widehat{\nu}$ em $\widehat{\mathbb{F}_{q^n}^*}$ é a mesma que a ordem de ν em $\widehat{\mathbb{F}_q}$, ou seja $\mathrm{ord}(\widehat{\nu})$ divide $q-1$. Com isso, podemos mostrar o seguinte resultado, relembramos que ν_1 é o caráter multiplicativo trivial de $\mathbb{F}_q$ enquanto η_1 é o caráter multiplicativo trivial de $\mathbb{F}_{q^n}$.

Proposição 5.7. *Sejam d um divisor de m, $\eta_d \in \widehat{\mathbb{F}_{q^n}^*}$ um caráter multiplicativo de ordem d e $\nu \in \widehat{\mathbb{F}_q^*}$. Então $\eta_d\widehat{\nu} = \eta_1$, o caráter trivial de $\mathbb{F}_{q^n}^*$ se, e somente se $d = 1$ e $\widehat{\nu} = \eta_1$.*

Demonstração. É claro que se $\eta_d = \widehat{\nu} = \eta_1$, então o produto $\eta_d\widehat{\nu}$ também é o caráter trivial. Reciprocamente, se $\eta_d\widehat{\nu} = \eta_1$ então, como $\mathrm{ord}(\eta_d) = d$ divide m, $k := \mathrm{ord}(\widehat{\nu})$ divide $q-1$ e m é o maior divisor de $q^n - 1$ primo com $q-1$, temos que $\mathrm{mdc}(d,k) = 1$ e $\mathrm{ord}(\eta_d\widehat{\nu}) = \mathrm{ord}(\eta_d)\mathrm{ord}(\widehat{\nu}) = dk = 1$. □

Proposição 5.8. *Seja η um caráter multiplicativo de $\mathbb{F}_{q^n}$ de ordem d. Então a restrição de η a $\mathbb{F}_q$ é um caráter multiplicativo de ordem $\dfrac{d}{mdc(d,n)}$.*

Demonstração. Seja η um caráter multiplicativo de ordem d em $\mathbb{F}_{q^n}^*$. Se $g \in \mathbb{F}_{q^n}$ gera $\mathbb{F}_{q^n}^*$, então $\eta(g)$ é uma d-ésima raiz primitiva da unidade e $\mathrm{ord}(\eta) = \mathrm{ord}(\eta(g))$. Como g gera $\mathbb{F}_{q^n}^*$, então definindo $N = \frac{q^n-1}{q-1}$, temos que g^N gera $\mathbb{F}_q^*$. Seja η^* a restrição de η a $\mathbb{F}_q^*$. Então

$$\mathrm{ord}(\eta^*) = \mathrm{ord}(\eta^*(g^N)) = \mathrm{ord}(\eta(g)^N) = \frac{d}{\mathrm{mdc}(d,N)} = \frac{d}{\mathrm{mdc}(d,(q^n-1)/(q-1))},$$

pois $\eta(g)$ é uma d-ésima raiz primitiva da unidade, logo $\eta(g)$ gera um grupo cíclico de ordem d. O resultado segue pois $\mathrm{mdc}(d,(q^n-1)/(q-1)) = \mathrm{mdc}(d,n)$. □

Como consideramos caráteres $\eta_d \in \widehat{\mathbb{F}_{q^n}^*}$ tais que d divide $m(q,n)$, pela Proposição 5.8, temos que η_d restrito a $\mathbb{F}_q^*$ é o caráter multiplicativo trivial de $\mathbb{F}_q^*$.

Da mesma maneira que estendemos um caráter multiplicativo ν de $\mathbb{F}_q^*$ para um caráter $\widehat{\nu} \in \widehat{\mathbb{F}_{q^n}^*}$, podemos restringir este mesmo caráter para obtermos $\nu^* \in \widehat{\mathbb{F}_q^*}$. Contudo, não temos necessariamente $\nu = \nu^*$. Mais precisamente, temos o seguinte resultado.

Corolário 5.8.1. *Se η é um caráter multiplicativo de $\mathbb{F}_q$ de ordem d, então:*

i) η^* tem ordem $\dfrac{d}{mdc(d,n)}$.

ii) $\eta^* = \eta_1$ se e somente se d divide n.

iii) Existem $mdc(n, q-1)$ *caráteres multiplicativos* η *de* $\mathbb{F}_q$ *tais que* $\eta^* = \eta_1$.

Demonstração. O item *i)* é uma reformulação da Proposição 5.8 e o item *ii)* segue diretamente do item *i)*. Quanto ao item *iii)*, note que, se η é um caráter multiplicativo de $\mathbb{F}_q$ de ordem m, então m divide $q-1$, pelo item *ii)*, $\eta^* = \eta_1$ se e somente se m divide n. Portanto $\eta^* = \eta_1$ se e somente se m divide $\mathrm{mdc}(n, q-1)$. □

Teorema 5.9. *Sejam* m *o maior divisor de* $q^n - 1$ *primo com* $q-1$, $M \in \mathbb{F}_q[X]$ *o divisor mônico de* $X^n - 1$ *de maior grau, primo com* $X-1$, $a \in \mathbb{F}_q^*$ *e* $b \in \mathbb{F}_q$ *um elemento primitivo. Então, para qualquer divisor* t *de* m *e* $T \in \mathbb{F}_q[X]$ *divisor de* M, *temos que*

$$\pi(t,T) = q(q-1)N(t,T) = \theta(t)\Theta(T)\left(q^n + A + B - C)\right), \tag{5.5}$$

onde

$$A = \int_{d|t}\int_{D|T} \sum_{\substack{\nu \in \widehat{\mathbb{F}_q^*} \\ \nu^* \neq \nu_1}} \nu^*(a)\widehat{\nu}(b)\overline{\eta_d\widehat{\nu}(\delta_D+1)G_1(\nu^*,\lambda)}G_n(\eta_d\widehat{\nu},\chi),$$

$$B = \int_{d|t}\int_{D(\neq 1)|T} \sum_{\substack{\nu \in \widehat{\mathbb{F}_q^*} \\ \nu^* = \nu_1, \eta_d\widehat{\nu} \neq \eta_1}} \overline{\nu(b)}\left(\overline{\eta_d\widehat{\nu}(\delta_D)} - \overline{\eta_d\widehat{\nu}(\delta_D+1)}\right) G_n(\eta_d\widehat{\nu},\chi),$$

$$C = \int_{d|t} \sum_{\substack{\nu \in \widehat{\mathbb{F}_q^*} \\ \nu^* = \nu_1, \eta_d\widehat{\nu} \neq \eta_1}} \overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi).$$

Demonstração. Temos que $N(t,T)$ é o número de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que α é t-livre, T-livre sobre $\mathbb{F}_q$, tem traço a e norma b. Abreviando $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ por Tr e $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ por N e levando em conta as funções características de tais elementos, temos que $N(t,T)$ é igual a

$$\sum_{\alpha\in\mathbb{F}_{q^n}} \left(\theta(t)\int_{d|t}\eta_d(\alpha)\right)\left(\Theta(T)\int_{D|T}\chi_{\delta_D}(\alpha)\right)\left(\frac{1}{q-1}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\nu(N(\alpha)b^{-1})\right)\left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\lambda(c(\mathrm{Tr}(\alpha)-a))\right). \tag{5.6}$$

Como $\nu(N(\alpha)b^{-1}) = \overline{\nu(b)}\nu(N(\alpha)) = \overline{\nu(b)}\widehat{\nu}(\alpha)$ e $\lambda(c(\mathrm{Tr}(\alpha)-a)) = \overline{\lambda(ca)}\lambda(c\mathrm{Tr}(\alpha)) = \overline{\lambda(ca)}\chi_c(\alpha)$, temos que

$$N(t,T) = \frac{1}{q(q-1)}\theta(t)\Theta(T)\int_{d|t}\int_{D|T}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)\lambda(ca)}\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d(\alpha)\widehat{\nu}(\alpha)\chi_c(\alpha)\chi_{\delta_D}(\alpha). \tag{5.7}$$

Escrevendo $\eta_d(\alpha)\widehat{\nu}(\alpha) = \eta_d\widehat{\nu}(\alpha)$ e $\chi_c(\alpha)\chi_{\delta_D}(\alpha) = \chi_{\delta_D+c}(\alpha)$, obtemos

$$\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d\widehat{\nu}(\alpha)\chi_{\delta_D+c} = G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}).$$

Portanto

$$\pi(t,T) = \theta(t)\Theta(T)\int_{d|t}\int_{D|T}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)\lambda(ca)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}). \tag{5.8}$$

Mas,

$$|G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c})| = \begin{cases} q^n, & \text{se } \eta_d\widehat{\nu}=\nu_1 \text{ e } \chi_{\delta_D+c}=\chi_0, \\ q^{\frac{n}{2}}, & \eta_d\widehat{\nu}\neq\nu_1 \text{ e } \chi_{\delta_D+c}\neq\chi_0, \\ 0, & \text{caso contrário.} \end{cases}$$

Note que $\chi_{\delta_D+c}=\chi_0$ apenas quando $\delta_D=c=0$. Portanto, aparte do caso em que $\eta_d\widehat{\nu}=\eta_1$ e $\chi_{\delta_D+c}=\chi_0$, $G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c})\neq 0$ se, e somente se

$$\eta_d\widehat{\nu}\neq\eta_1 \text{ e } (c=0 \text{ ou } \delta_D=0).$$

Como $\delta_D=0$ se, e somente se $D=1$, podemos separar os termos da seguinte maneira: uma parte com o termo referente a D qualquer e $c\neq 0$ e outra parte com os termos referentes a $c=0$ e $D\neq 1$, sendo assim, podemos escrever $\pi(t,T)$ como

$$\theta(t)\Theta(T)\left(q^n+\int_{d|t}\int_{D|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)\lambda(ca)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c})+\int_{d|t}\int_{D(\neq 1)|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D})\right). \tag{5.9}$$

O termo

$$\int_{d|t}\int_{D(\neq 1)|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D}) \tag{5.10}$$

é tal que $\delta_D\neq 0$, portanto, na Soma de Gauss

$$G_n(\eta_d\widehat{\nu},\chi_{\delta_D})=\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d\widehat{\nu}(\alpha)\chi_{\delta_D}(\alpha), \tag{5.11}$$

podemos substituir α por α/δ_D, obtendo

$$\sum_{\alpha\in\mathbb{F}_{q^n}}\overline{\eta_d\widehat{\nu}(\delta_D)}\eta_d\widehat{\nu}(\alpha)\chi(\alpha)=\overline{\eta_d\widehat{\nu}(\delta_D)}G_n(\eta_d\widehat{\nu},\chi). \tag{5.12}$$

Logo

$$\int_{d|t}\int_{D(\neq 1)|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D})=\int_{d|t}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi)\int_{D(\neq 1)|T}\overline{\eta_d\widehat{\nu}(\delta_D)}, \tag{5.13}$$

e observe que, pela Proposição 4.11, como $\mathbb{F}_q^*\Delta_D=\Delta_D$,

$$\int_{D(\neq 1)|T}\overline{\eta_d\widehat{\nu}(\delta_D)}=\sum_{D|T}\frac{\mu(D)}{\Phi(D)}\sum_{\delta_D\in\Delta_D}\overline{\eta_d\widehat{\nu}(\delta_D)}=\frac{1}{q-1}\int_{D(\neq 1)|T}\sum_{c\in\mathbb{F}_q^*}\overline{\eta_d\widehat{\nu}(c\delta_D)}. \tag{5.14}$$

Como d divide t, em particular d divide $\frac{q^n-1}{q-1}$, então, pela Proposição 5.8, η_d restrito a $\mathbb{F}_q^*$ é o caráter trivial

de $\mathbb{F}_q^*$, portanto

$$\int_{D(\neq 1)|T} \sum_{c\in\mathbb{F}_q^*} \overline{\eta_d\widehat{\nu}(c\delta_D)} = \frac{1}{q-1}\int_{D(\neq 1)|T} \overline{\eta_d\widehat{\nu}(\delta_D)} \sum_{c\in\mathbb{F}_q^*} \overline{\nu^*(c)}, \tag{5.15}$$

e temos que

$$\sum_{c\in\mathbb{F}_q^*} \overline{\nu^*(c)} \neq 0, \tag{5.16}$$

somente quando $\nu^* = \nu_1$. Logo

$$\int_{d|t}\int_{D(\neq 1)|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D}) = \int_{d|t}\int_{D(\neq 1)|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}} \overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D}) =: X. \tag{5.17}$$

Quanto ao termo

$$\int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \sum_{c\in\mathbb{F}_q^*} \overline{\nu(b)\lambda(ca)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}) = \int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \sum_{c\in\mathbb{F}_q^*} \overline{\nu(b)\lambda(ca)} \sum_{\alpha\in\mathbb{F}_{q^n}} \eta_d\widehat{\nu}(\alpha)\chi((\delta_D+c)\alpha), \tag{5.18}$$

novamente como $\mathbb{F}_q^*\Delta_D = \Delta_D$, podemos substituir δ_D por $c\delta_D$, e também, como $c\neq 0$, podemos substituir α por $\alpha/(c(\delta_D+1))$, obtendo

$$\int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \sum_{c\in\mathbb{F}_q^*} \overline{\nu(b)\lambda(ca)\eta_d\widehat{\nu}(c(\delta_D+1))}G_n(\eta_d\widehat{\nu},\chi). \tag{5.19}$$

Como η_d é trivial em $\mathbb{F}_q^*$, $\eta_d(c)=1$. Portanto obtemos

$$\int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \sum_{c\in\mathbb{F}_q^*} \overline{\nu(b)\lambda(ca)\widehat{\nu}(c)\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi). \tag{5.20}$$

Como $\widehat{\nu}(c)=\nu^*(c)$ e escrevendo $\overline{\nu^*(c)} = \overline{\nu^*(c)\nu^*(a)}\nu^*(a)$, temos que,

$$\int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \overline{\nu(b)}\nu^*(a)\ \overline{\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi) \sum_{c\in\mathbb{F}_q^*} \overline{\lambda(ca)\nu^*(ca)}. \tag{5.21}$$

Para termos uma soma de Gauss no último somatório em (5.21), precisamos adicionar o termo $c=0$, ou seja, somar e subtrair o seguinte termo

$$\int_{d|t}\int_{D|T} \sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1}} \overline{\nu(b)\nu^*(a)\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi)\overline{\lambda(0)\nu^*(0)}. \tag{5.22}$$

Obtemos que (5.21) é igual a

$$\begin{aligned}&\int_{d|t}\int_{D|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \nu^*\neq\nu_1}}\overline{\nu(b)}\nu^*(a)\overline{\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi)\overline{G_1(\lambda,\nu^*)}\\ &-\int_{d|t}\int_{D|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}}\overline{\nu(b)}\nu^*(0)\ \overline{\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi).\end{aligned}\tag{5.23}$$

A condição $\nu^*\neq\nu_1$ aparece no primeiro termo, pois $G_1(\lambda,\nu^*)$ é diferente de 0 somente quando ν^* é não trivial, pois λ é o caráter aditivo canônico de $\mathbb{F}_q$. No segundo termo, o fator $\nu^*(a)$ desaparece pois $\nu^*(0)\nu^*(a)=\nu^*(0)$ e $\nu^*(0)$ só é diferente de 0 quando $\nu^*=\nu_1$, pela convenção feita sobre os caráteres multiplicativos no 0. Note que

$$\int_{d|t}\int_{D|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \nu^*\neq\nu_1}}\overline{\nu(b)}\nu^*(a)\overline{\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi)\overline{G_1(\nu^*,\lambda)}=A.\tag{5.24}$$

Separando os fatores em $D=1$ e $D\neq1$, o segundo termo no somatório em (5.23) pode ser reescrito como

$$\begin{aligned}-\int_{d|t}\int_{D|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=-\nu_1}}\overline{\nu(b)\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi)&=-\int_{d|t}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi)\\ &-\int_{d|t}\int_{D(\neq1)|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}}\overline{\nu(b)\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi),\end{aligned}\tag{5.25}$$

sendo o termo

$$\int_{d|t}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi)=C\tag{5.26}$$

e o termo

$$-\int_{d|t}\int_{D(\neq1)|T}\sum_{\substack{\nu\in\widehat{\mathbb{F}_{q^n}^*}\\ \eta_d\widehat{\nu}\neq\eta_1,\nu^*=\nu_1}}\overline{\nu(b)\eta_d\widehat{\nu}(\delta_D+1)}G_n(\eta_d\widehat{\nu},\chi)=Y,\tag{5.27}$$

é tal que $X+Y=B$, onde X foi definido em (5.17). A prova está completa. □

Corolário 5.9.1. *Nas condições do Teorema 5.9, definindo $e=mdc(n,q-1)$, temos que*

$$\pi(t,T)\geq\theta(t)\Theta(T)\left(q^n-(q-1-e)W(t)W(T)q^{\frac{n+1}{2}}-(eW(t)-1)(2W(T)-1)q^{\frac{n}{2}}\right).\tag{5.28}$$

Demonstração. Com argumentação análoga ao Corolário 4.12.1 e como temos $e=\mathrm{mdc}(n,q-1)$ caráteres $\nu\in\widehat{\mathbb{F}_q^*}$ tais que $\nu^*=\nu_1$, obtemos que

$$|A|\leq W(t)W(T)(q-1-e)q^{\frac{n}{2}}q^{\frac{1}{2}}=W(t)W(T)(q-1-e)q^{\frac{n+1}{2}}.$$

Quanto ao termo B, temos que $\eta_d\widehat{\nu} \neq \eta_1$ quando $d \neq 1$ ou $\widehat{\nu} \neq \eta_1$, o que implica $\nu \neq \nu_1$. Logo

$$|B| \leq 2\left((W(t)-1)(W(T)-1)e + W(t)(W(T)-1)(e-1)\right) q^{\frac{n}{2}}, \tag{5.29}$$

onde o termo 2 aparece por conta da diferença $\overline{\eta_d\widehat{\nu}(\delta_D)} - \overline{\eta_d\widehat{\nu}(\delta_D+1)}$. Analogamente o termo C é tal que

$$|C| \leq \left((W(t)-1)e + (e-1)\right) q^{\frac{n}{2}}.$$

O resultado segue pois

$$\pi(t,T) \geq \theta(t)\Theta(T)\left(q^n - |A| - |B| - |C|\right).$$

□

Corolário 5.9.2. *Nas mesmas condições do Teorema 5.9, $\pi(t,T)$ é positivo quando*

$$q^{\frac{n-3}{2}} > \left(1 - \frac{e+1}{q}\right) W(t)W(T) + \frac{1}{q^{\frac{3}{2}}}(eW(t)-1)(2W(T)-1), \tag{5.30}$$

e, portanto, quando

$$q^{\frac{n-3}{2}} > \left(1 - \frac{1}{q}\right) W(t)W(T),\ q \geq 4. \tag{5.31}$$

Demonstração. A desigualdade (5.30) segue diretamente do Corolário 5.9.1. Quanto à desigualdade (5.31), note que

$$\left(1 - \frac{e+1}{q}\right) W(t)W(T) + \frac{1}{q^{\frac{3}{2}}}(eW(t)-1)(2W(T)-1) \leq \left(1 - \frac{e+1}{q}\right) W(t)W(T) + \frac{2e}{q\sqrt{q}}W(t)W(T).$$

Como $q \geq 4$, temos que $\frac{2}{\sqrt{q}} \leq 1$; logo

$$\left(1 - \frac{e+1}{q}\right) W(t)W(T) + \frac{1}{q\sqrt{q}}2eW(t)W(T) \leq \left(1 - \frac{e+1}{q}\right) W(t)W(T) + \frac{e}{q}W(t)W(T),$$

completando a prova. □

Mostraremos que a condição (5.31), com $t = m$ e $T = M$ é satisfeita para todo $n \geq 7$ com a exceção de 14 pares (q,n). Para tal, precisaremos de cotas para $W(m) = 2^{\omega(m)}$ e $W(M) = 2^{\omega(M)}$. Começamos com cotas para $\omega(m)$.

Lema 5.10. *Seja m um inteiro positivo e $\omega(m)$ o número de fatores primos distintos de m. Seja $\ell > 1$ um inteiro e Λ um conjunto de números primos menores que ℓ que contenha todos os fatores primos de m menores que ℓ. Defina também $L = \prod_{r\in\Lambda} r$. Então*

$$\omega(m) \leq \frac{\ln m - \ln L}{\ln \ell} + \#\Lambda. \tag{5.32}$$

Demonstração. Sejam m, ℓ e Λ como no enunciado e seja Γ o conjunto de divisores primos de m. Logo

$\#\Gamma = \omega(m)$ e se $r \in \Gamma - \Lambda$, então $r \geq \ell$. Portanto,

$$m \geq \prod_{r\in\Gamma} r = \frac{\left(\prod_{r\in\Lambda} r\right)\left(\prod_{r\in\Gamma-\Lambda} r\right)}{\left(\prod_{r\in\Lambda-\Gamma} r\right)} \geq \left(\prod_{r\in\Lambda} r\right)\ell^{\#(\Gamma-\Lambda)-\#(\Lambda-\Gamma)} = L\cdot\ell^{\#\Gamma-\#\Lambda} = L\cdot\ell^{\omega(m)-\#\Lambda},$$

ou seja

$$\ln m \geq \ln L + (\omega(m) - \#\Lambda)\ln\ell$$

e o resultado segue. □

Cotas para $\omega(M(q,n))$ podem ser obtidas através do próximo lema. Como temos que $\omega(M(q,n)) = \omega(\frac{X^n-1}{X-1}) = \omega(\frac{X^{n^*}-1}{X-1})$, é suficiente obter cotas para $\omega(M(q,n))$ para o caso em que p não divide n.

Lema 5.11 ([6], Lemma 4.3)**.** *Seja n primo com q e seja $M = M(q,n)$ o maior divisor de $X^n - 1$ primo com $X-1$, como definido anteriormente. Neste caso, $M(q,n) = \frac{X^n-1}{X-1}$. Então*

i) $\omega(M) \leq \frac{1}{2}(n + mdc(n, q-1)) - 1$. *Em particular* $\omega(M) \leq n-1$, *com igualdade se, e somente se, n divide $q-1$. Ademais,* $\omega(M) \leq \frac{3}{4}n - 1$ *se n não divide $q-1$.*

ii) $\omega(M) \leq \frac{1}{3}n + 5$, *se* $q = 5$,

iii) $\omega(M) \leq \frac{1}{3}n + 1$, *se* $q = 4$ *e* $n \neq 15$,

iv) $\omega(M) \leq \frac{1}{3}n + \frac{1}{3}$, *se* $q = 3$ *e* $n \neq 4, 8, 16$.

Note que todas as cotas para $\omega(M)$ são da forma $\omega(M) \leq \alpha n + \beta$. Sendo assim, consideramos o caso geral $\omega(M) \leq \alpha n + \beta$ e junto com o Lema 5.10 obtemos o seguinte resultado.

Lema 5.12. *Se para alguma escolha de ℓ, Λ como no Lemma 5.10 e $\alpha > 0$, β números racionais tais que $\omega(M) \leq \alpha n + \beta$, então o par (q,n) satisfaz (5.31) se*

$$\left(\frac{n-3}{\ln 4} - \frac{n}{\ln\ell}\right)\ln q \geq \alpha n + \beta + |\Lambda| - \frac{\ln L}{\ln\ell} \text{ ou} \tag{5.33}$$

$$\left(\frac{\ln q}{\ln 4} - \frac{\ln q}{\ln\ell} - \alpha\right) n \geq \frac{3\ln q}{2\ln 2} + \beta + |\Lambda| - \frac{\ln L}{\ln\ell}. \tag{5.34}$$

Demonstração. As duas desigualdades são equivalentes. Para obtê-las basta observar que $m(q,n) = m \leq q^n$ e como

$$\left(1 - \frac{1}{q}\right) W(m)W(M) < W(M)W(m) = 2^{\omega(M)+\omega(m)},$$

segue que (5.31) é satisfeita se

$$q^{\frac{n-3}{2}} < 2^{\omega(M)}2^{\omega(m)},$$

que é equivalente a

$$q^{n-3} < 4^{\omega(M)+\omega(m)}.$$

O resultado segue aplicando o logaritmo, usando a estimativa do Lema 5.10 e $\omega(M) \leq \alpha n + \beta$. □

Estamos aptos a mostrar o seguinte resultado.

Teorema 5.13. *Seja (q, n) onde $q \geq 4$ é uma potência de um primo p e $n \geq 7$ um número inteiro. Então (5.31) é satisfeita, exceto para os 14 pares listados a seguir*

$$(4,9),(4,15),(5,8),(5,12),(7,8),(7,12),(8,7),(9,8),$$

$$(11,10),(13,8),(13,12),(16,15),(17,8),(25,8)$$

Demonstração. A demonstração necessita de alguns cálculos, que podem ser feitos usando alguma plataforma algébrica, como o SAGE, por exemplo. Os algoritmos usados durante a argumentação encontram-se no Apêndice. O Lema 5.12 nos fornece uma condição suficiente para que (5.31) seja satisfeita, contudo sua expressão é mais simples para encontrar cotas para q ou n.

Caso 1: Suponha inicialmente que $n \geq 10$ e que $q \geq 11$. Escolhemos $\ell = 72$ e como $m(q, n)$ é sempre ímpar, escolhemos Λ como o conjunto de todos os primos ímpares menores que 72.

Caso 1a: Suponha que n divide $q-1$, sendo assim $X^n - 1$ se fatora como n fatores lineares distintos e, portanto $\omega(M) = n - 1$. Escolha então $\alpha = 1$, $\beta = -1$. Se (q, n) não satisfaz (5.31), então com $q \geq 11$, (5.33) implica que $n \leq 52$. Contudo, se $n \geq 21$, então $q \leq 21$, não podendo ser tal que n divida $q - 1$. Sendo assim, para cada $n \in \{10, 11, \ldots, 21\}$, usamos a Equação (5.34) para obter cotas inferiores para q, por exemplo, quando $n = 10$, $q \leq 160$, para cada q neste espectro (existem 43 potências de primos entre 11 e 160, sendo que apenas 10 destas são tais que 10 divide $q - 1$), usamos a Equação (5.31) para verificar cada caso. Para $n = 11$, temos $q \leq 100$ e neste espectro apenas 3 se enquadram no Caso 1. Continuamos o processo e obtemos três pares que não satisfazem a Equação (5.31):

$$(11,10),(13,12),(16,15).$$

Caso 1b: Suponha que n não divida q e $\mathrm{mdc}(n, q) = 1$. Pelo Lema 5.11, podemos tomar $\alpha = 3/4$ e $\beta = -1$, obtendo desta vez $n \leq 21$. Procedendo igualmente ao caso anterior, obtemos que todos os pares satisfazem (5.31). Se $\mathrm{mdc}(q, n) \neq 1$, então, $n^* \leq \frac{n}{2}$. Como $\omega(M(q, n)) = \omega(M(q, n^*)) \leq \frac{3}{4}n^* - 1$, pelo Lema 5.11, segue-se que $\omega(M(q, n)) \leq \frac{3}{8}n - 1$. Sendo assim, com $\alpha = \frac{3}{8}$ e $\beta = -1$, obtemos que todos os pares (q, n) satisfazem (5.31).

Caso 2: Consideramos agora os casos $n \geq 10$ com $q = 9, 8, 7, 5, 4$.

Caso $q = 9$: Se n divide $q - 1 = 9$, então, como supomos $n \geq 7$, o caso que nos resta é $(9, 8)$, que não satisfaz (5.31). Suponha que n não divida $q-1$. Se 3 não divide n, então novamente podemos escolher $\alpha = \frac{3}{4}$ e $\beta = -1$ e usando (5.33), supondo que $(9, n)$ não satisfaz (5.31), obtemos $n \leq 26$. Verificando todos os pares, vemos que todos satisfazem (5.33). Se 3 divide n, então $\omega(M) \leq \frac{1}{4}n - 1$ e tomamos $\alpha = \frac{1}{4}$ e $\beta = -1$ e procedendo como anteriormente, vemos que todos os pares considerados satisfazem (5.33).

Caso $q = 8$: Se n divide $q - 1 = 7$, então o único par possível é $(8, 7)$, que não satisfaz (5.31). Se n não divide $q - 1$, procedendo de maneira semelhante aos casos anteriores, vemos que nenhum par falha.

Caso $q = 7$: Neste caso usamos $\ell = 200$. Se n divide $q - 1 = 6$, então $n \leq 7$, não sendo considerado. Suponha que n não divida $q - 1$. Se 7 não divide n, então usamos $\alpha = \frac{3}{4}$ e $\beta = -1$ e (5.34) para obtermos $n \geq 44$, destes o único que falha a (5.31) é o par $(7, 12)$. Se 7 divide n, todos os pares considerados satisfazem (5.33).

Caso $q = 5$: Continuamos com $\ell = 200$. Como no caso anterior, nenhum par tal que n divida $q - 1 = 4$ é considerado, portanto suponha n não divide $q - 1$. Se 5 não divide n, pelo Lema 5.11, usamos $\alpha = \frac{1}{3}$ e $\beta = 5$ na Equação (5.34) e obtemos que $n \geq 34$. O único par que não satisfaz (5.31) é o par $(5, 12)$. Se 5 divide n, usamos $\alpha = \frac{1}{15}$ e $\beta = 5$, todos os pares considerados satisfazem (5.31).

Caso $q = 4$: Também usamos $\ell = 200$. Podemos supor que n não divide $q - 1$. Suponha n ímpar. Pelo Lema (5.11), se $n \neq 15$, podemos escolher $\alpha = \frac{1}{3}$ e $\beta = 1$. Vemos que todos os pares satisfazem (5.31). Se $n = 15$, $(4, 15)$, não satisfaz (5.31). Se n é par, então podemos escolher $\alpha = \frac{1}{6}$ e $\beta = 1$, sendo neste caso o único par que não satisfaz (5.33) é $(4, 10)$, que satisfaz a Equação (5.31).

Caso 3: Consideramos agora $n = 9, 8, 7$ e $q \geq 4$. Usamos $\ell = 72$.

Caso $n = 9$: Suponha que 9 divida $q - 1$. Então $\alpha = 1$, $\beta = -1$. Sendo assim, a Equação (5.33) nos leva a $q \leq 310$, destes, todos satisfazem (5.31). Suponha que n não divida q. Se $\mathrm{mdc}(q, n) = 1$, então $\alpha = \frac{3}{4}$ e $\beta = -1$ e obtemos que $q \leq 112$, destes, apenas o par $(4, 9)$ não satisfaz (5.31). Se $\mathrm{mdc}(q, n) \neq 1$, então podemos escolher $\alpha = \frac{3}{8}$ e $\beta = -1$ e então $q \leq 24$. Todos os pares considerados satisfazem (5.33).

Caso $n = 8$: Se 8 divide $q - 1$, consideramos $\alpha = 1$, $\beta = -1$ e obtemos que $q \leq 875$. Destes, os pares que não satisfazem (5.31) são $(9, 8)$ e $(17, 8)$. Suponha que 8 não divida $q - 1$. Usamos então $\alpha = \frac{3}{4}$ e $\beta = -1$, obtemos a condição $q \leq 276$ e vemos que o único par que não satisfaz (5.31) é $(5, 8)$. Se $\mathrm{mdc}(8, q) \neq 1$, então consideramos $\alpha = \frac{3}{8}$ e $\beta = -1$, obtendo $q \leq 49$. Todos os pares satisfazem (5.31).

Caso $n = 7$: Se 7 divide $q - 1$, novamente $\alpha = 1$, $\beta = -1$ e obtemos $q \leq 5535$ (neste espectro temos 774 potências de primo, sendo 128 pertinentes ao caso). Vemos que apenas o par $(8, 7)$ não satisfaz (5.31). Suponha que 7 não divide $q - 1$. Se $\mathrm{mdc}(q, 7) = 1$, então escolhemos $\alpha = \frac{3}{4}$ e $\beta = -1$, obtendo $q \leq 276$ e todos os pares satisfazem (5.31). Se $\mathrm{mdc}(7, q) \neq 1$, então $\alpha = \frac{3}{8}$ e $\beta = 1$ e encontramos $q \leq 166$, todo par considerado satisfaz (5.31). A prova está completa. □

Corolário 5.13.1. *Dada uma extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$, onde $q \geq 4$ e $n \geq 7$ para todo $a \in \mathbb{F}_q^*$ e para todo $b \in \mathbb{F}_q$ primitivo, existe $\alpha \in \mathbb{F}_{q^n}$, normal sobre $\mathbb{F}_q$ e primitivo, tal que $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$ e $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$, exceto para os casos excepcionais*

$$(4, 9), (4, 15), (5, 8), (5, 12), (7, 8), (7, 12), (8, 7), (9, 8)$$

$$(11, 10), (13, 8), (13, 12), (16, 15), (17, 8), (25, 8).$$

Como os casos excepcionais com $n \geq 7$ são finitos, podemos desenvolver um algorítimo que verifica se cada um dos pares no Corolário 5.13.1 é de fato um par PFNT, contudo, como lidaremos também como os casos $n = 6, 5$, necessitamos aprimorar cotas inferiores para $N(m, M)$, em particular o que faremos na próxima seção engloba também tais casos excepcionais.

5.4 Os casos excepcionais e $n = 5, 6$.

Para lidar com os casos excepcionais no problema PFNT, é necessário um método de redução semelhante à redução feita no Teorema da Base Normal e Primitiva, dada pela Proposição 4.14. Seja $\Gamma = \Gamma(q, n)$ o conjunto dos produtos formais tT tais que t é um divisor de $m(q, n)$ e $T \in \mathbb{F}_q[X]$ é um divisor de $M(q, n)$. Para $\tau \in \Gamma$, definimos $\Theta(\tau) := \theta(t)\Theta(T)$ e $\pi(\tau) := \pi(t, T)$. Esta definição tem a finalidade de unificar o tratamento dado aos divisores t de m e T de M. Um divisor τ_0 de τ é um produto $\tau_0 = t_0 T_0$ tal que t_0 divide t e T_0 divide T.

Sejam $r \geq 2$ e $\tau_1, \ldots, \tau_r$ divisores de τ. Diremos que $\{\tau_1, \ldots, \tau_r\}$ é um conjunto de divisores complementares de τ com divisor comum τ_0 se $mmc(\tau_1, \ldots, \tau_r) = \tau$ e $\mathrm{mdc}(\tau_i, \tau_j) = \tau_0$, para todo $i \neq j$.

Proposição 5.14. *Sejam $\tau \in \Gamma$ e $\{\tau_1, \ldots, \tau_r\}$, $r \geq 2$, um conjunto de divisores complementares de τ com divisor comum τ_0. Então*

$$\pi(\tau) \geq \left(\sum_{i=1}^{r} \pi(\tau_i) \right) - (r-1)\pi(\tau_0). \tag{5.35}$$

Demonstração. A prova é idêntica à prova da Proposição 4.14. □

Para trabalhar com a Proposição 5.14, é necessário generalizar o termo $\Theta(\tau)$. Dado $\{\tau_1, \ldots, \tau_r\}$, $r \geq 2$, um conjunto de divisores complementares de τ com divisor comum τ_0, defina

$$\Theta := \Theta(\tau_1, \ldots, \tau_r) := \left(\sum_{i=1}^{r} \Theta(\tau_i) \right) - (r-1)\Theta(\tau_0). \tag{5.36}$$

Exemplo 5.1. Suponha que n divida $q-1$. Sendo assim $M(q,n) = \frac{X^n-1}{X-1} = M_1 \cdots M_{n-1}$, onde M_i, para $i = 1, \ldots, n$ são polinômios lineares distintos. Então o conjunto $\{mM_i\}_{i=1,\ldots,n-1}$, (onde $m = m(q,n)$) é um conjunto de divisores complementares de mM com divisor comum m. Portanto

$$\Theta(mM_1, \ldots, mM_{n-1}) = \left(\sum_{i=1}^{n-1} \theta(m)\Theta(M_i) \right) - (n-2)\theta(m),$$

como M_i é linear, segue que $\Theta(M_i) = \Theta(M_j) = \frac{q-1}{q} = 1 - \frac{1}{q}$, portanto

$$\Theta(mM_1, \ldots, mM_{n-1}) = \theta(m)(n-1)\left(1 - \frac{1}{q}\right) - (n-2)\theta(m) = \theta(m)\left(1 - \frac{n-1}{q}\right). \tag{5.37}$$

E se consideramos o conjunto $\{M_1, \ldots, M_{n-1}, m\}$, que possui divisor comum 1, obtemos

$$\Theta(M_1, \ldots, M_{n-1}, m) = \theta(m) - \frac{n-1}{q}. \tag{5.38}$$

Proposição 5.15. *Sejam q uma potência de um primo e $n \geq 4$ um inteiro. Fixados elementos $a \in \mathbb{F}_q^*$ e $b \in \mathbb{F}_q$ primitivo, suponha que $\tau_1 = t_1 T_1, \ldots \tau_r = t_r T_r$ são divisores complementares de $\tau = mM$ com divisor comum $\tau_0 = m_0 M_0$. Suponha $\Theta = \Theta(\tau_1, \ldots, \tau_r)$ positivo. Então $\pi(\tau)$ é positivo se*

$$q^{\frac{n-3}{2}} \geq R - S + \Theta^{-1} \sum_{i=1}^{r} \Theta(\tau_i)(U_i - V_i), \tag{5.39}$$

onde, com $e = mdc(n, q-1)$,

$$R = \left(1 - \frac{e+1}{q} + \frac{2e}{q^{\frac{3}{2}}}\right) W(\tau_0),$$

$$S = \frac{1}{q^{\frac{3}{2}}}(eW(m_0) + 2W(M_0) - 1),$$

$$U_i = \left(1 - \frac{e+1}{q} + \frac{2e}{q^{\frac{3}{2}}}\right)(W(\tau_i) - W(\tau_0)),$$

$$V_i = \frac{1}{q^{\frac{3}{2}}}(e(W(m_i) - W(m_0)) + 2(W(M_i) - W(M_0))).$$

Em particular, $\pi(\tau)$ é positivo se

$$q^{\frac{n-3}{2}} > \left(1 - \frac{1}{q}\right)\left(W(\tau_0) + \Theta^{-1}\sum_{i=1}^{r}\Theta(\tau_i)(W(\tau_i) - W(\tau_0))\right),\ q \geq 4. \tag{5.40}$$

Demonstração. Defina a quantidade

$$\Theta_0 = \frac{\Theta}{\Theta(\tau_0)}.$$

Sejam $\tau_1 = t_1T_1, \ldots \tau_r = t_rT_r$, divisores complementares de $\tau = mM$ com divisor comum $\tau_0 = m_0M_0$. Então, pela Proposição 5.14, temos que

$$\pi(\tau) \geq \left(\sum_{i=1}^{r}\pi(\tau_i)\right) - (r-1)\pi(\tau_0).$$

Como

$$\Theta_0 = \frac{\Theta}{\Theta(\tau_0)} = \frac{(\sum_{i=1}^{r}\Theta(\tau_i)) - (r-1)\Theta(\tau_0)}{\Theta(\tau_0)},$$

podemos escrever

$$(r-1) = \frac{\sum_{i=1}^{r}\Theta(\tau_i)}{\Theta(\tau_0)} - \Theta_0.$$

Portanto

$$\pi(\tau) \geq \left(\sum_{i=1}^{r}\pi(\tau_i)\right) + \left(\Theta_0 - \frac{\sum_{i=1}^{r}\Theta(\tau_i)}{\Theta(\tau_0)}\right)\pi(\tau_0).$$

Pelo Teorema 5.9

$$\pi(\tau_i) = \Theta(\tau_i)\left(q^n + A_i + B_i - C_i\right),$$

para $i = 0, \ldots, r$. Portanto,

$$\pi(\tau) \geq \left(\sum_{i=1}^{r}\Theta(\tau_i)(q^n + A_i + B_i - C_i)\right) + \Theta_0\pi(\tau_0) - \left(\sum_{i=1}^{r}\Theta(\tau_i)\right)(q^n + A_0 + B_0 - C_0),$$

ou seja

$$\pi(\tau) \geq \left(\sum_{i=1}^{r}\Theta(\tau_i)\Big((A_i - A_0) + (B_i - B_0) - (C_i - C_0)\Big)\right) + \Theta_0\pi(\tau_0).$$

Quanto aos termos $(A_i - A_0)$ etc., analisaremos o caso $(C_i - C_0)$, os casos restantes são análogos.

$$\begin{aligned} C_i - C_0 = &\int_{d|t_i} \sum_{\substack{\nu \in \widehat{\mathbb{F}_q^*} \\ \nu^* = \nu_1, \eta_d\widehat{\nu} \neq \eta_1}} \overline{\nu(b)}G_n(\eta_d\widehat{\nu}, \chi) \\ &- \int_{d|t_0} \sum_{\substack{\nu \in \widehat{\mathbb{F}_q^*} \\ \nu^* = \nu_1, \eta_d\widehat{\nu} \neq \eta_1}} \overline{\nu(b)}G_n(\eta_d\widehat{\nu}, \chi), \end{aligned} \tag{5.41}$$

ou seja

$$C_i - C_0 = \int_{\substack{d|t_i \\ d\nmid t_0}} \sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*} \\ \nu^*=\nu_1,\eta_d\widehat{\nu}\neq\eta_1}} \overline{\nu(b)} G_n(\eta_d\widehat{\nu},\chi),$$

logo

$$|C_i - C_0| \leq q^{\frac{n}{2}} \left(W(t_i) - W(t_0)\right) e. \tag{5.42}$$

A desigualdade (5.39) segue como no Corolário 5.9.2. A desigualdade (5.40) segue do fato que

$$q^{\frac{n-3}{2}} \geq R - S + \Theta^{-1}\sum_{i=1}^{r}\Theta(\tau_i)(U_i - V_i) > R + \Theta^{-1}\sum_{i=1}^{r}\Theta(\tau_i)(U_i),$$

usando que $\frac{2}{\sqrt{q}} \leq 1$ se $q \geq 4$.

□

Corolário 5.15.1. *Nas mesmas condições da Proposição 5.15, suponha que n divida $q-1$ e escreva $M = M_1 \cdots M_{n-1}$, com $M_i \in \mathbb{F}_q[X]$ um polinômio linear para todo $i = 1, \ldots, n-1$. Então $\pi(m, M)$ é positivo quando*

$$q^{\frac{n-3}{2}} > Q_M(q)W(m), \tag{5.43}$$

onde

$$Q_M(q) = \frac{(q-1)(nq - 2(n-1))}{q(q-n+1)}. \tag{5.44}$$

Demonstração. Considere os divisores complementares $\tau_1, \ldots, \tau_{n-1}$ como em (5.37).

Como $W(\tau_i) = W(M_i)W(m) = 2W(m)$, pois M é linear, então $W(\tau_i) - W(\tau_0) = W(\tau_0) = W(m)$. Por (5.37) e (5.40), temos que

$$q^{\frac{n-3}{2}} > \left(1 - \frac{1}{q}\right)\left(W(m) + \frac{\sum_{i=1}^{n-1}\theta(\tau_i)W(m)}{\theta(m)\left(1 - \frac{n-1}{q}\right)}\right) = \left(1 - \frac{1}{q}\right)\left(1 + \frac{(n-1)\left(1 - \frac{1}{q}\right)}{\left(1 - \frac{n-1}{q}\right)}\right)W(m), \tag{5.45}$$

que é equivalente a $Q_M(q)W(m)$. □

Antes de começarmos o estudo de caso, vejamos dois resultados que podem simplificar o problema em alguns casos.

Lema 5.16. *Seja q uma potência de um primo e n um inteiro positivo. Se $q-1$ divide n, então (q, n) é um par PFNT.*

Demonstração. Veja [7, Proposition 4.1] □

Ou seja, temos que $(2, n)$ é um par PFNT para todo n e $(3, n)$ é um par $PFNT$ quando n é par. Os casos excepcionais $(4, 9), (11, 10), (5, 12), (7, 12), (9, 8), (13, 12), (16, 15)$ são cobertos também pelo Lema 5.16.

Lema 5.17. *Suponha que, para um par (q, n), $M(q, n) \in \mathbb{F}_q[X]$ é irredutível. Então $\pi(m, M)$ é positivo se e somente se $\pi(m, 1)$ é positivo.*

Demonstração. É claro que $\pi(m, M) > 0$ implica em $\pi(m, 1) > 0$. Suponha então $\alpha \in \mathbb{F}_{q^n}$ m-livre com traço e norma prescritos. Como a norma de α está prescrita e é primitiva, pelo Lema 5.3, α é primitivo, portanto $0 \neq \alpha^q - \alpha = (X-1) \circ \alpha$. Logo α é M-livre, pois M é irredutível. Pelo Lema 5.4, α é normal sobre $\mathbb{F}_q$. $\square$

Estamos aptos a mostrar os casos restantes. Podemos sempre supor $q > 2$ ou $q > 3$ se n for par, pelo Lema 5.16. Denotamos por $\omega = \omega(m)$, onde $m(q, n)$ é o maior divisor de $q^n - 1$ primo com $q - 1$. Detalhamos aqui o caso $n = 5$, o caso $n = 6$ e os casos excepcionais do Corolário 5.13.1 são análogos. Os cálculos detalhados podem ser encontrados em [5, Section 4]

Caso $n = 5$: Primeiramente, observe que $m(5, n)$ divide $\frac{q^5-1}{q-1}$ e é primo com $q - 1$. Ademais, $\frac{q^5-1}{q-1}$ é múltiplo de 5 se, e somente se $q \equiv 1 \pmod 5$. Em todos os casos, temos $\text{mdc}(5, m) = 1$. Sendo assim, como m é sempre ímpar, os primos possíveis na fatoração de m estão no conjunto $S_5 := \{11, 31, 41, 61, ...\}$, que é o conjunto dos primos l tais que $l \equiv 1 \pmod{10}$. Denotamos por P_r o produto dos primeiros r primos em S_5.

Caso 1: $q \equiv 1 \pmod 5$. Como $m \leq \dfrac{q^5 - 1}{5(q-1)}$, segue que $5m \leq q^4 + q^3 + q^2 + q + 1 \leq (q+1)^4$, logo $q > (5m)^{1/4} - 1 > (5P_\omega)^{1/4} - 1 =: R_\omega$. Pelo Corolário 5.15.1, temos que o resultado vale se

$$q > 2^\omega Q_M(q), \tag{5.46}$$

onde, neste caso

$$Q_M(q) = \frac{(q-1)(5q-8)}{q(q-4)},$$

uma função que decresce para 5. Portanto, é suficiente mostrar que

$$R_\omega > 2^\omega Q_M(q),\ q \geq R_\omega. \tag{5.47}$$

A função

$$\frac{R_\omega}{2^\omega Q_M(q)}$$

é uma função crescente em ω. Portanto, se (5.47) vale para ω_0, valerá para todo $\omega \geq \omega_0$. Para $\omega = 6$ temos que $R_6 = (5P_6)^{1/4}) - 1 > 417 > 322 > 2^6 Q_M(417)$, logo (5.46) vale para todo $\omega \geq 6$. Se $\omega = 5$, então $R_5 > 130$. Entretanto, $2^5 Q_M(165) < 162$, sendo assim (5.47), é válida exceto se $131 \leq q < 165$. Neste intervalo, existem 7 potências de primo, sendo apenas duas pertinentes ao caso, 131 e 151, mas $\omega(m(131, 5)) = 2 \neq 5$ e $\omega(m(151, 5)) = 1$. Se $\omega = 4$, $R_4 > 44$ e $2^4 Q_M(81) < 81$, logo (5.47) é satisfeita a não ser que $44 < q < 81$, que nos leva a $q = 61$ ou $q = 71$, mas $\omega(m(61, 5)) = 2$ e $\omega(m(71, 5)) = 3$. Se $\omega = 3$, então $R_3 > 5$ e $2^3 Q_M(43) < 42$, portanto $16 \leq q \leq 43$, sendo os únicos casos possíveis $q = 16$ ou $q = 41$, mas $\omega(m(41, 5)) = 1$.

Se $q = 16$, $m = 11 \cdot 31 \cdot 41$. e $\omega(\tau) = \omega(m) + \omega(M) = 7$. Considerando o conjunto de divisores complementares $M_1, \ldots, M_4, 11, 31, 41$, com divisor comum 1, temos que

$$\Theta(M_1, M_2, \ldots, 11, 31, 41) = \Theta = \sum_{i=1}^{4} \Theta(M_i) + \theta(11) + \theta(31) + \theta(41) - 6 = 4(1 - \frac{1}{16}) + \frac{10}{11} + \frac{30}{31} + \frac{40}{41} - 6 < 0.6024.$$

Por (5.40), temos que

$$\left(1 - \frac{1}{16}\right)\left(1 + 0.6024^{-1}\left(4\left(1 - \frac{1}{16}\right) + \frac{10}{11} + \frac{30}{31} + \frac{40}{41}\right)\right) < 11.3 < 16,$$

satisfazendo (5.47). Se $\omega = 2$, então a condição (5.37) implica $q < 21$, que não contem nenhum primo relevante. Se $\omega = 1$, obtemos $q \leq 11$, sendo 11 o único primo relevante. Neste caso, $m(11, 5)$ é primo e escolhemos o conjunto de divisores complementares $mM_1, \ldots, mM_4$, com divisor comum m. O resultado segue aplicando (5.39) com $e = 5$.

Caso 2: $n = 5$ e $q \equiv -1 \pmod 5$. Note que, no caso atual, o polinômio $X^5 - 1$ só possui uma raiz em $\mathbb{F}_q$. Temos que $X^5 - 1 = (X - 1)Q_5$, onde Q_5 é o polinômio ciclotômico de ordem 5 sobre $\mathbb{F}_q$. Como a ordem de q módulo 5 é 2 neste caso e $\text{mdc}(5, q) = 1$, Q_5 se fatora em $\varphi(5)/2 = 2$ fatores mônicos irredutíveis distintos sobre $\mathbb{F}_q$. Logo $M(q, 5) = M_1 M_2$, onde M_1 e M_2 são polinômios quadráticos. Como na prova do Corolário 5.15.1, escolhemos $\{mM_1, mM_2\}$ como conjunto de divisores complementares com divisor comum m, sendo assim

$$\Theta(mM_1, mM_2) = \Theta = \theta(m)\left(1 - \frac{1}{q^2}\right),$$

aplicando (5.40), obtemos a condição suficiente

$$q > \left(1 - \frac{1}{q}\right)\left(W(m) + \frac{\left(2 - \frac{2}{q^2}\right)W(m)}{\left(1 - \frac{2}{q^2}\right)}\right) = \frac{(q-1)(3q^2-4)}{q(q^2-2)}W(m) \tag{5.48}$$

e redefinimos

$$Q_M(q) := \frac{(q-1)(3q^2-4)}{q(q^2-2)}.$$

Note que $Q_M(q) < 3$ para $q \geq 2$. Portanto tomamos, $Q_M = 3$ e obtemos a condição suficiente

$$q > 3W(m) = 3 \cdot 2^\omega. \tag{5.49}$$

Como, agora, $m \leq \dfrac{q^5 - 1}{q - 1}$, redefinimos $R_\omega = P_\omega^{1/4} - 1$ e temos que $q > R_\omega$. Como $R_6 > 278 > 192 \geq 2^6 Q_M$, temos que o resultado vale para todo $\omega \geq 6$. Para os casos $\omega = 1, 3, 4, 5$ não existem potências de primos relevantes entre R_w e $2^\omega \cdot 3$. Para o caso $\omega = 2$, temos $q > 4 \cdot 3 = 12$, portanto os primos que falham com $\omega = 2$ são $q = 4$ e $q = 9$. Se $q = 4$, $m(4, 5) = 11 \cdot 31$ e tomamos como divisores complementares com divisor comum 1 o conjunto $\{M_1, M_2, 11, 31\}$. Aplicando (5.39) com $e = 1$, o resultado segue. O caso $q = 9$ é similar, agora $m = 11 \cdot 671$ e como neste caso $q > 4$, podemos usar (5.40).

Caso 3: $n = 5$ e $q \equiv \pm 2 \pmod 5$ ou q uma potência de 5.

Se $q \equiv \pm 2 \pmod 5$, então $M(q, 5)$ é um polinômio irredutível de grau 4. Pelo Lema 5.17, é suficiente mostrar que $\pi(m, 1)$ é positivo. Caso $q = 5^j$, então $M = 1$, portanto a análise de $\pi(m, 1)$ é suficiente para ambos os casos. Por (5.31), o resultado é válido se

$$q > \left(1 - \frac{1}{q}\right)W(m) = \left(1 - \frac{1}{q}\right)2^\omega, \ q \geq 4.$$

Novamente, se a condição vale para ω_0, então valerá para todo $\omega \geq \omega_0$, portanto fixe $\omega = 3$. Então a condição se torna

$$q > \left(1 - \frac{1}{q}\right)8,$$

que é equivalente a

$$\frac{q^2}{q-1} > 8.$$

Portanto o resultado vale se $q > 8$. Restam os casos $q = 5, 7, 8$, contudo para tais casos $\omega = 2$ e temos a condição suficiente

$$q > 4\left(1 - \frac{1}{q}\right),$$

que é satisfeita para $q = 5, 7, 8$. Resta-nos o caso $q = 3$, que não é coberto pelo Lema 5.16, pois neste caso n é ímpar. Se $q = 3$, então $\omega = 1$ e como $q < 4$, usamos (5.30), completando todos os casos.

Caso $n = 6$: Como dito anteriormente, os cálculos não serão detalhados aqui por serem análogos ao caso $n = 5$, contudo uma pequena observação faz-se necessária: diferente do caso $n = 5$, qualquer primo ímpar pode ser fator de $m(q, 6)$, sendo assim, o conjunto de primos usado é o conjunto dos primos ímpares. O resultado segue analogamente ao caso $n = 5$, dividindo a demonstração nos mesmos sub-casos, analisando a fatoração de M e tomando os correspondentes divisores complementares de M e m. Os casos excepcionais com $n \geq 7$ também seguem analogamente, completando a prova.

6 Sobre a Existência de Elementos 1-normais e Primitivos com Norma Prescrita

Uma generalização do conceito de elemento normal em extensões de corpos finitos foi desenvolvida por Huczynska et al. [21] em 2013. Nesta seção introduzimos o conceito de elementos k-normais e mostramos um resultado sobre a existência de elementos 1-normais e primitivos com norma prescrita.

Seja $\alpha \in \mathbb{F}_{q^n}$. Um critério clássico para determinar se α é normal sobre $\mathbb{F}_q$ é o seguinte.

Proposição 6.1. *Seja $\alpha \in \mathbb{F}_{q^n}$. Considere o polinômio $g_\alpha = \alpha X^{n-1} + \alpha^q X^{n-2} + \cdots + \alpha^{q^{n-2}} X + \alpha^{q^{n-1}} \in \mathbb{F}_{q^n}[X]$. Então α é normal sobre $\mathbb{F}_q$ se, e somente se $mdc(g_\alpha, X^n - 1) = 1$.*

Demonstração. Veja [24, Theorem 2.39, p. 62] □

Motivado por tal fato, a seguinte generalização dos elementos normais foi proposta.

Definição 6.2. Sejam $\alpha \in \mathbb{F}_{q^n}$ e g_α como definido anteriormente. Dizemos que α é k-normal sobre $\mathbb{F}_q$ se $\mathrm{mdc}(g_\alpha, X^n - 1)$ é um polinômio de grau k.

Como motivação adicional ao estudo dos elementos k-normais, é mencionado em [21] que tais elementos aparecem implicitamente na construção de bases *quase normais*. Tais bases oferecem uma multiplicação eficiente em $\mathbb{F}_{q^n}$.

Neste mesmo artigo é estudada a caracterização dos elementos k-normais com a noção de $\mathbb{F}_q$-ordem aditiva, assim como é fornecida uma fórmula para o número dos elementos k-normais de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, entretanto tal fórmula depende de se conhecer determinados fatores do polinômio $X^n - 1 \in \mathbb{F}_q[X]$ (ver [21, Theorem 3.5]), o que é bem difícil em geral. Também são estudadas cotas para o número de elementos k-normais. É provado também um resultado sobre a existência de elementos 1-normais e primitivos, que será enunciado posteriormente.

6.1 Resultados existentes

Nesta seção, enunciamos os principais resultados acerca dos elementos k-normais que nos serão úteis. O próximo teorema relaciona k-normalidade com a ordem aditiva de um elemento $\alpha \in \mathbb{F}_{q^n}$.

Teorema 6.3. *Seja $\alpha \in \mathbb{F}_{q^n}$. As seguintes condições são equivalentes:*

i) α é k-normal sobre $\mathbb{F}_q$,

ii) $Ord(\alpha)$ é um polinômio de grau $n - k$.

Demonstração. Ver [21, Theorem 3.2]. □

Focamos aqui nos elementos 1-normais e primitivos sobre $\mathbb{F}_q$. Neste caso é possível aplicar os métodos usados até agora para obtermos resultados sobre a existência de tais elementos em extensões de corpos finitos.

Relembramos um fato mencionado no final da Seção 2: se um elemento $\alpha \in \mathbb{F}_{q^n}$ é tal que $\mathrm{Ord}(\alpha) = g$, então existe $\beta \in \mathbb{F}_{q^n}$ tal que $\alpha = \left(\frac{X^n - 1}{g}\right) \circ \beta$.

Proposição 6.4. *Seja $\alpha \in \mathbb{F}_{q^n}$ e $g \in \mathbb{F}_q[X]$ um divisor de $X^n - 1$. As seguintes afirmações são equivalentes:*

i) α *é g-livre sobre* $\mathbb{F}_q$,

ii) $mdc\left(g, \dfrac{X^n-1}{Ord(\alpha)}\right) = 1$.

Demonstração. Veja [21, Theorem 5.4] □

Proposição 6.5. *Suponha que p, a característica de* $\mathbb{F}_q$ *não divida n. Seja* $\alpha \in \mathbb{F}_{q^n}$. *Então*

$$Ord(\alpha) = \frac{X^n-1}{X-1} \text{ se, e somente se } \alpha \text{ não é normal sobre } \mathbb{F}_q \text{ e é } \left(\frac{X^n-1}{X-1}\right)\text{-livre.}$$

Demonstração. Suponha $\mathrm{Ord}(\alpha) = \dfrac{X^n-1}{X-1}$, então α não é normal sobre $\mathbb{F}_q$. Como $\mathrm{mdc}(\dfrac{X^n-1}{X-1}, X-1) = 1$ (pois p não divide n), pela Proposição 6.4 temos o resultado. Reciprocamente, se α não é normal, então $\mathrm{Ord}(\alpha) \neq (X^n-1)$. Suponha que $\mathrm{Ord}(\alpha) \neq \left(\dfrac{X^n-1}{X-1}\right)$, ou seja, $\mathrm{Ord}(\alpha) = \dfrac{X^n-1}{t}$ onde $t \neq (X-1)$. Portanto, existe $\beta \in \mathbb{F}_{q^n}$ tal que $\alpha = t \circ \beta$. Como t divide $\left(\dfrac{X^n-1}{X-1}\right)$, temos $t = 1$, pois α é $\left(\dfrac{X^n-1}{X-1}\right)$-livre, um absurdo pois α não é normal sobre $\mathbb{F}_q$.

□

6.2 Resultados sobre a existência de elementos 1-normais e primitivos

Pelo Teorema 6.3, um elemento $\alpha \in \mathbb{F}_{q^n}$ 1-normal sobre $\mathbb{F}_q$ é tal que o grau de sua $\mathbb{F}_q$-ordem é $n-1$. Se a característica de $\mathbb{F}_q$ não divide n, os elementos que não são normais sobre $\mathbb{F}_q$ e são $\left(\frac{X^n-1}{X-1}\right)$-livres são 1-normais sobre $\mathbb{F}_q$. Como evidenciado pela Proposição 5.4, elementos $\alpha \in \mathbb{F}_{q^n}$ tais que $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = 0$ nunca são normais. Portanto, se $\mathrm{mdc}(q,n) = 1$, um subconjunto de elementos $\alpha \in \mathbb{F}_{q^n}$ 1-normais sobre $\mathbb{F}_q$ e primitivos é constituído pelos elementos primitivos, com traço 0 e $\left(\frac{X^n-1}{X-1}\right)$-livres. Em [21], foi obtido o seguinte resultado.

Teorema 6.6. *Considere a extensão* $\mathbb{F}_{q^n}|\mathbb{F}_q$, *onde* $mdc(q,n) = 1$. *Suponha que* $n \geq 6$ *se* $q \geq 11$ *e* $n \geq 3$ *se* $3 \leq q \leq 9$. *Então existe um elemento* $\alpha \in \mathbb{F}_{q^n}$, 1*-normal sobre* $\mathbb{F}_q$ *e primitivo.*

Em Outubro de 2017, foi obtido o resultado geral para o Teorema 6.6 [28]:

Teorema 6.7 (Teorema da base 1-normal e primitiva)**.** *Considere a extensão* $\mathbb{F}_{q^n}|\mathbb{F}_q$, *onde* $n \geq 3$. *Então existe um elemento* $\alpha \in \mathbb{F}_{q^n}$, 1*-normal sobre* $\mathbb{F}_q$ *e primitivo. Ademais, se* $n = 2$, *não existem elementos* 1*-normais e primitivos na extensão* $\mathbb{F}_{q^2}|\mathbb{F}_q$.

Mostraremos aqui que, em alguns casos, é possível prescrever a norma de um elemento 1-normal e primitivo. Para tal, suponha $\mathrm{mdc}(q,n) = 1$ e seja $N(q,n)$ o número de elementos $\alpha \in \mathbb{F}_{q^n}$ tais que:

i) α é $\left(\frac{X^n-1}{X-1}\right)$-livre,

ii) α é primitivo,

iii) $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = 0$,

iv) $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$, com b primitivo.

Em particular, se $N(q,n) > 0$ então existem elementos 1-normais e primitivos com norma prescrita na extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$.

Teorema 6.8. *Considere a extensão $\mathbb{F}_{q^n}|\mathbb{F}_q$, onde $mdc(q,n)=1$ e $b\in\mathbb{F}_q$ um elemento primitivo. Seja $M=\dfrac{X^n-1}{X-1}$ e m o maior divisor de q^n-1 primo com $q-1$. Então definindo $\pi(q,n)=q(q-1)N(q,n)$, temos que*

$$\pi(q,n)=\theta(m)\Theta(M)\left(q^n+A+B+C+D\right), \tag{6.1}$$

onde

$$A=\int_{d(\neq 1)|m}\int_{D(\neq 1)|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}\ G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}),$$

$$B=\int_{d(\neq 1)|m}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_c),$$

$$C=\int_{D(\neq 1)|M}\sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \nu\neq 1}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}\ G_n(\widehat{\nu},\chi_{\delta_D+c}),$$

$$D=\sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \nu\neq 1}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)}\ G_n(\widehat{\nu},\chi_c).$$

Demonstração. Note que, como estamos a considerar elementos $\alpha\in\mathbb{F}_{q^n}$ primitivos com $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)=b$, um elemento primitivo de $\mathbb{F}_q$, pela Proposição 5.3 isto é equivalente a procurar por elementos m-livres com norma b. Temos então que $N(q,n)$ é o número de elementos $\alpha\in\mathbb{F}_{q^n}$ tais que α é m-livre, M-livre sobre $\mathbb{F}_q$, tem traço 0 e norma b. Abreviando $\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ por Tr e $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ por N, temos que $N(q,n)$ é igual a

$$\sum_{\alpha\in\mathbb{F}_{q^n}}\left(\theta(m)\int_{d|m}\eta_d(\alpha)\right)\left(\Theta(M)\int_{D|M}\chi_{\delta_D}(\alpha)\right)\left(\frac{1}{q-1}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\nu(N(\alpha)b^{-1})\right)\left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\lambda(c(\mathrm{Tr}(\alpha)))\right). \tag{6.2}$$

Como $\nu(N(\alpha)b^{-1})=\overline{\nu(b)}\nu(N(\alpha))=\overline{\nu(b)}\widehat{\nu}(\alpha)$ e $\lambda(c(\mathrm{Tr}(\alpha)))=\lambda(c\mathrm{Tr}(\alpha))=\chi_c(\alpha)$, temos que

$$N(q,n)=\frac{1}{q(q-1)}\theta(m)\Theta(M)\int_{d|m}\int_{D|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d(\alpha)\widehat{\nu}(\alpha)\chi_c(\alpha)\chi_{\delta_D}(\alpha). \tag{6.3}$$

Escrevendo $\eta_d(\alpha)\widehat{\nu}(\alpha)=\eta_d\widehat{\nu}(\alpha)$ e $\chi_c(\alpha)\chi_{\delta_D}(\alpha)=\chi_{\delta_D+c}(\alpha)$, temos que

$$\sum_{\alpha\in\mathbb{F}_{q^n}}\eta_d\widehat{\nu}(\alpha)\chi_{\delta_D+c}(\alpha)=G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}),$$

portanto

$$N(q,n)=\frac{1}{q(q-1)}\theta(m)\Theta(M)\int_{d|m}\int_{D|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}). \tag{6.4}$$

Temos que

$$|G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c})|=\begin{cases}q^n, & \text{se } \eta_d\widehat{\nu}=\nu_1 \text{ e } \chi_{\delta_D+c}=\chi_0,\\ q^{\frac{n}{2}}, & \eta_d\widehat{\nu}\neq\nu_1 \text{ e } \chi_{\delta_D+c}\neq\chi_0,\\ 0, & \text{caso contrário.}\end{cases}$$

Pela Proposição 5.7, $\eta_d\widehat{\nu}$ é trivial se e somente se $d=1$ e ν é trivial. Pela Proposição 5.6.1, o caráter χ_{δ_D+c} é trivial, se e somente se $D=1$ ($\delta_D=0$) e $c=0$. Sendo assim, podemos escrever

$$\int_{d|m}\int_{D|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c}) \tag{6.5}$$

da seguinte maneira

$$\begin{aligned}\int_{d(\neq 1)|m}\int_{D(\neq 1)|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_{\delta_D+c})+\int_{d(\neq 1)|m}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_c)\\ +\int_{D(\neq 1)|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\widehat{\nu},\chi_{\delta_D+c})+\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\widehat{\nu},\chi_c).\end{aligned} \tag{6.6}$$

Como

$$\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\widehat{\nu},\chi_c)=\sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \nu\neq 1}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)}G_n(\widehat{\nu},\chi_c)+G_n(\eta_1,\chi_0), \tag{6.7}$$

onde η_1 e χ_0 denotam, respectivamente, os caráteres multiplicativo e aditivo triviais de $\mathbb{F}_{q^n}$, que ocorrem somente quando ν é trivial em $\mathbb{F}_q$ e $c=0$. Como $G_n(\eta_1,\chi_0)=q^n$ e

$$\sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \nu\neq 1}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)}G_n(\widehat{\nu},\chi_c)=D.$$

Resta-nos encontrar A, B e C, definidos no enunciado do presente Teorema. Note que no segundo termo da Equação (6.6),

$$\int_{d(\neq 1)|m}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_c),$$

como $d\neq 1$, $\eta_d\widehat{\nu}$ nunca é trivial e χ_c, é trivial somente quando $c=0$. Neste caso, $G_n(\eta_d\widehat{\nu},\chi_0)=0$ e podemos remover este termo obtendo

$$\int_{d(\neq 1)|m}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q^*}\overline{\nu(b)}G_n(\eta_d\widehat{\nu},\chi_c)=B.$$

Quanto ao terceiro termo da Equação (6.6),

$$\int_{D(\neq 1)|M}\sum_{\nu\in\widehat{\mathbb{F}_q^*}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\widehat{\nu},\chi_{\delta_D+c}),$$

como $D\neq 1$ temos que $\delta_D\neq 0$ e portanto χ_{δ_D+c} nunca é o caráter trivial. Temos também que $\widehat{\nu}$ é trivial somente quando ν é trivial, neste caso $G_n(\eta_1,\chi_{\delta_D+c})=0$ e podemos remover este termo da expressão, obtendo

$$\int_{D(\neq 1)|M}\sum_{\substack{\nu\in\widehat{\mathbb{F}_q^*}\\ \nu\neq 1}}\sum_{c\in\mathbb{F}_q}\overline{\nu(b)}G_n(\widehat{\nu},\chi_{\delta_D+c})=C.$$

O primeiro termo da Equação (6.6) é igual a A. A prova está completa observando que $\pi(q,n)=q(q-1)N(q,n)$. □

Corolário 6.8.1. *Nas mesmas condições do Teorema 6.8, temos que $\pi(q,n)$ é positivo quando*

$$\frac{q^{\frac{n}{2}}}{q(q-1)} > \left(W(M) - \frac{1}{q}\right)\left(W(m) - \frac{1}{q-1}\right). \tag{6.8}$$

Demonstração. É claro que

$$\frac{\pi(q,n)}{\theta(m)\Theta(M)} \geq q^n - |A| - |B| - |C| - |D|. \tag{6.9}$$

Procedendo de maneira análoga à demonstração do Corolário 4.12.1, apenas os divisores livres de quadrado de m e M importam. Cada Soma de Gauss que aparece em A, B, C e D tem norma $q^{\frac{n}{2}}$, portanto para a expressão

$$A = \int_{d(\neq 1)|m} \int_{D(\neq 1)|M} \sum_{\nu \in \widehat{\mathbb{F}_q^*}} \sum_{c \in \mathbb{F}_q} \overline{\nu(b)}\ G_n(\eta_d \widehat{\nu}, \chi_{\delta_D + c}),$$

como temos $q-1$ caráteres em $\widehat{\mathbb{F}_q^*}$ e q elementos em $\mathbb{F}_q$, segue que

$$|A| \leq q^{\frac{n}{2}}(W(m)-1)(W(M)-1)(q-1)q.$$

Os outros termos podem ser obtidos com mesma argumentação, encontrando $|B| \leq q^{\frac{n}{2}}(W(m)-1)(q-1)(q-1)$, $|C| \leq q^{\frac{n}{2}}(W(M)-1)(q-2)q$ e $|D| \leq q^{\frac{n}{2}}(q-2)(q-1)$. Portanto, $\pi(q,n)$ é positivo quando

$$q^n > q^{\frac{n}{2}}\Big((W(m)-1)(W(M)-1)(q-1)q + (W(m)-1)(q-1)(q-1) + (W(M)-1)(q-2)q + (q-2)(q-1)\Big), \tag{6.10}$$

que, após simplificação e divisão dos dois lados da desigualdade por $q(q-1)$, obtemos

$$\frac{q^{\frac{n}{2}}}{q(q-1)} > W(M)W(m) - \frac{W(m)}{q} - \frac{W(M)}{q-1} + \frac{1}{q-1} - \frac{1}{q} = (W(M) - \frac{1}{q})(W(m) - \frac{1}{q-1}),$$

encerrando a prova.

□

A desigualdade (6.8) pode ser resolvida com a mesma ideia e as mesmas cotas para $W(M)$ e $W(m)$ usadas para resolver o Teorema 5.13. Todavia, a mesma desigualdade é considerada em [7] e resolvida numericamente obtendo o seguinte resultado.

Proposição 6.9. *[7, Proposition 3.1] A desigualdade (6.8) é válida para todo $q \geq 4$ e todo $n \geq 7$ com a exceção de 18 pares, os quais são:*

$$(16,15),(13,12),(11,10),(4,15),(7,12),(5,12),(4,9),$$

$$(89,8),(41,8),(25,8),(17,8),(13,8),(9,8),(7,8),(5,8),$$

$$(64,7),(8,7),(4,7).$$

Uma verificação com um algorítimo em SAGE [29] constata que nenhum dos pares supracitados são exceções para nosso resultado. Pelo Teorema 6.7, sempre existem elementos 1-normais e primitivos para todo $n \geq 3$ em $\mathbb{F}_{q^n}|\mathbb{F}_q$. Se $q = 2$ ou $q = 3$, um elemento $\alpha \in \mathbb{F}_{q^n}$ primitivo só assume um único valor para sua

norma, pois tanto $\mathbb{F}_2$ quanto $\mathbb{F}_3$ possuem apenas um elemento primitivo, sendo assim mostramos o seguinte resultado.

Teorema 6.10. *Sejam $\mathbb{F}_{q^n}|\mathbb{F}_q$ uma extensão de corpos finitos tais que $mdc(q,n)=1$ e $b \in \mathbb{F}_q$ um elemento primitivo. Se $n \geq 7$, então existe um elemento $\alpha \in \mathbb{F}_{q^n}$ 1-normal sobre $\mathbb{F}_q$, primitivo e tal que $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$.*

7 Conclusões

Neste trabalho foi estudado o Teorema da Base Normal e Primitiva e também uma versão mais forte de tal resultado, que é a existência de elementos normais e primitivos com traço e norma prescritos. Também foi estudado sobre a existência de elementos 1-normais e primitivos, utilizando as mesmas técnicas aplicadas para resolver os dois primeiros problemas supracitados.

Mais precisamente, foram abordados os seguintes resultados.

Teorema 7.1 (Lenstra e Schoof). *Seja $\mathbb{F}_{q^n}|\mathbb{F}_q$ uma extensão de corpos finitos tal que $n \geq 2$. Então existe um elemento $\alpha \in \mathbb{F}_{q^n}$, normal sobre $\mathbb{F}_q$ e primitivo.*

Teorema 7.2 (Cohen). *Seja $\mathbb{F}_{q^n}|\mathbb{F}_q$, uma extensão de corpos finitos tal que $n \geq 5$. Para cada $a, b \in \mathbb{F}_q^*$, com b primitivo, existe $\alpha \in \mathbb{F}_{q^n}$, tal que α é normal sobre $\mathbb{F}_q$, primitivo e satisfaz $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$ e $Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = a$.*

A prova para o Teorema da Base Normal e Primitiva estudada aqui é devida a Cohen e Huczynska, enquanto a prova para a existência de elementos normais e primitivos com traço e norma prescrita é devida a Cohen. Além de ser usado o mesmo método para resolver as duas questões, faz-se uso de uma técnica intitulada *sieve technique* para reduzir o problema e evitar o uso computacional no caso do Teorema da Base Normal e Primitiva e para resolver os casos excepcionais e $n = 5, 6$ no caso da existência de elementos normais e primitivos com traço e norma prescritos.

Ressaltamos que o resultado sobre a existência de elementos normais e primitivos com traço e norma prescritos é válido para qualquer extensão de $\mathbb{F}_q$ de grau $n \geq 3$. Entretanto, os casos $n = 3, 4$ são mais delicados e foram resolvidos por Cohen e Huczynska em [9] e [10]. É natural que, para n pequeno, o trabalho seja mais delicado, pois um polinômio normal e primitivo com traço e norma prescritos possui poucos graus de liberdade em tais casos.

Foi obtido também um resultado novo acerca dos elementos 1-normais e primitivos com norma prescrita.

Teorema 7.3. *Seja $\mathbb{F}_{q^n}|\mathbb{F}_q$, uma extensão de corpos finitos tais que $n \geq 7$ e $mdc(n, q) = 1$. Então para cada $b \in \mathbb{F}_q$ primitivo, existe um elemento $\alpha \in \mathbb{F}_{q^n}$, 1-normal sobre $\mathbb{F}_q$ e primitivo tal que $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$.*

É interessante notar que todas as questões consideradas neste trabalho estão diretamente conectadas com a fatoração de divisores de $q^n - 1$ e $X^n - 1$. Por exemplo, uma condição suficiente para a existência de elementos $\alpha \in \mathbb{F}_{q^n}$ normais sobre $\mathbb{F}_q$, primitivos, com traço e norma prescritos é dada pelo Corolário 5.9.2:

$$q^{\frac{n-3}{2}} > \left(1 - \frac{1}{q}\right) W(m)W(M), \quad q \geq 4.$$

Onde m denota o maior divisor de $q^n - 1$ primo com $q - 1$ e M é o maior divisor de $X^n - 1$ primo com $X - 1$.

O uso de funções características para encontrar elementos com propriedades fixadas é uma ferramenta bastante frutífera no escopo de corpos finitos, como pôde ser notado ao longo deste trabalho. O sucesso prático desta técnica foi primeiramente evidenciado no trabalho de Lenstra e Schoof [23]. Por ter se tornado uma técnica recorrentemente empregada, em trabalhos posteriores muitos autores referem-se a esta abordagem como o *método de Lenstra-Schoof*. Trabalhos onde a mesma técnica é empregada podem ser encontrados em [16], [17], por exemplo.

Entretanto, os resultados existenciais em geral se propõem apenas em mostrar que o número N de elementos com as propriedades desejadas é estritamente positivo, sendo assim, é natural indagar-se o seguinte.

Pergunta 1: Existem boas cotas para, por exemplo, o número N de elementos normais e primitivos com traço e norma prescritos em uma extensão de corpos finitos? Ou seja, para um par (q, n) fixado, é possível encontrar $l(q, n)$ e $L(q, n)$, tais que

$$l(q, n) \leq N \leq L(q, n)?$$

Esta pergunta se estende também ao número de elementos 1-normais e primitivos. Dada a validade do Teorema 6.7 e do Teorema 6.10, é natural propor também a seguinte pergunta.

Pergunta 2: Seja $\mathbb{F}_{q^n}|\mathbb{F}_q$, onde $n \geq 3$. Para cada $b \in \mathbb{F}_q$ primitivo, existe um elemento $\alpha \in \mathbb{F}_{q^n}$, 1-normal sobre $\mathbb{F}_q$ e primitivo tal que $N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = b$?

Como prescrever a norma de um elemento $\alpha \in \mathbb{F}_{q^n}$ é equivalente a prescrever o termo constante de seu polinômio mínimo sobre $\mathbb{F}_q$, também é válido propor o seguinte.

Pergunta 3: Para cada $n \geq 3$, é possível prescrever coeficientes de um polinômio 1-normal e primitivo de grau n sobre $\mathbb{F}_q$?

Note que no caso em que n é primo com q, o Teorema 6.10 é equivalente a prescrever o termo constante de tal polinômio.

8 Apêndice

Nesta seção constam os algoritmos usados para mostrar o Teorema 5.13 e verificar os casos excepcionais da Proposição 6.9. A plataforma algébrica usada é o SAGE [29].

8.1 Algoritmos para determinação de $\omega(m)$ e $\omega(M)$.

Para tal, é necessário encontrar e fatorar $m(q,n)$ e $M(q,n)$.

```
def m(q,n):
  fatores = list(factor(q-1)) #gera uma lista com os fatores de q-1.
  b = q^n-1
  for x in fatores: #este passo remove os fatores de q-1 de b
        while b in ZZ:
            b = b/x[0]
        b = b*x[0]
    return b
def M(q,n):
    x = PolynomialRing(GF(q),'x').gen()
    nast = n
    p = list(factor(q))[0][0] #encontra o primo p que divide q
    while nast/p in ZZ: #remove todos os fatores p de n
        nast = nast/p
    M = (x^n-1)/(x^(n/nast) -1) #encontra o polinomio M(q,n) pela definicao
    return M
def W(t): #retorna o numero de divisores livres de quadrado de t
  return 2^len(list(factor(t)))
```

8.2 Algorítimo para determinar potências de primos em intervalos fixados

```
def listar_potencias_primo(i,q): #retorna uma lista com as potencias de primo entre i e q
    a = []
    for x in range(i, q+1):
        if is_prime_power(x) == True:
            a.append(x)
    return a
```

8.3 Algoritmos para verificar e resolver desigualdades

A seguir encontram-se os algoritmos para verificar a Equação (5.31) e resolver numericamente a Equação (5.33) para q e n.

```
def verificar_eq_principal(q,n): #verifica a eq (5.31) para dados q e n
    if (q^((n-3)/2)) > (1-q^(-1))*W(m(q,n))*W(M(q,n)):
        return True
    return False
```

Os parâmetros nos códigos a seguir significam: $l = \ell$, L, $d = |\Lambda|$, $a = \alpha$ e $b = \beta$ como no Lema 5.12.

```
def resolve_eq533_n(q,l,L,d,a,b): #resolve a eq. (5.33) para um q fixado
    n = var('n')
```

```
    eq1 = ((n-3)/ln(4) - (n)/log(l))*log(q) - (a*n + b + d - log(L)/log(l)) == 0
    return int(solve(eq1,n)[0].rhs())

def resolve_eq533_q(n,l,L,d,a,b): #resolve a eq (5.33) para um n fixado
    q = var('q')
    eq1 = ((n-3)/ln(4) - (n)/log(l))*log(q) - (a*n + b + d - log(L)/log(l)) == 0
    return int(solve(eq1,q)[0].rhs())
```

8.4 O Caso 1

```
l = 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71 #o produto de todos os primos
                                                    impares menores que 72.

def verificar_caso_1a(q,n): #para dados q e n, verifica a eq. (5.31) para todo q' <= q e n
                                                    fixado, retorna uma lista com os valores de (q
                                                    ,n) que se enquadram no Caso 1a e tais que a
                                                    eq. (5.31) falha.
    a = []
    b = []
    for x in listar_potencias_primo(1,q):
        if verificar_eq_principal(x,n) == False:
            if (x-1)/n in ZZ:
                a.append(x)
    if a == []:
        return []
    for x in a:
        b.append((x,n))
    return b

def resolve_caso_1a(): #retorna os valores (q,n) que a eq (5.31) falha no Caso 1a.
    n = resolve_eq533_n(11,72,1,19,1,-1)
    u = range(10,n+1)
    m = []
    for x in u:
        j = resolve_eq533_q(x,72,1,19,1,-1)
        if verificar(j,x) != []:
            print verificar(j,x)
    return 'Fim'

def verificar_caso_1b1(q,n): #para dados q e n, verifica a eq. (5.31) para todo q' < q e n
                                                    fixado, retorna uma lista com os valores de (q
                                                    ,n) que se enquadram na primeira parte do Caso
                                                     1b e tais que a eq. (5.31) falha.
    a = []
    b = []
    for x in listar_potencias_primo(1,q):
        if verificar_eq_principal(x,n) == False:
            if (x-1)/n not in ZZ:
                if gcd(n,x) == 1:
                    if x > 10:
                        a.append(x)
    if a == []:
```

```
        return a
    for x in a:
        b.append((x,n))
    return b

def resolve_caso_1b_1(): #retorna os valores (q,n) que a eq (5.31) falha na primeira parte
                                                    do Caso 1b.
    n = resolve_eq533_n(11,1,19,3/4,-1)
    u = range(10,n+1)
    for x in u:
        j = resolve_eq533_q(x,72,1,19,3/4,-1)
        if verificar2(j,x) != []:
            print verificar2(j,x)
    return 'Fim'

def verifica_caso_1b_2(q,n): #para dados q e n, verifica a eq. (5.31) para todo q' < q e n
                                                    fixado, retorna uma lista com os valores de (q
                                                    ,n) que se enquadram na segunda parte do Caso
                                                    1b e tais que a eq. (5.31) falha.
    a = []
    b = []
    for x in listar_potencias_primo(1,q):
        if verificar_eq_principal(x,n) == False:
            if (x-1)/n not in ZZ:
                if gcd(n,x) != 1:
                    if x > 10:
                        a.append(x)
    if a == []:
        return a
    for x in a:
        b.append((x,n))
    return b

def resolvecaso1b2(): #retorna os valores (q,n) que a eq (5.31) falha na segunda parte do
                                                    Caso 1b.
    n = resolve_eq533_n(11,72,1,19,3/8,-1)
    u = range(10,n+1)
    for x in u:
        j = resolve_eq533_q(x,72,1,19,3/8,-1)
        if verifica_caso_1b_2(q,n) != []:
            print verifica_caso_1b_2(q,n)
    return 'Fim'
```

8.5 O Caso 2

O Caso $n \geq 10$ e $q = 9$.

```
l = 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71 #o produto de todos os primos
                                                    impares menores que 72.
def resolve_caso_2_q_9_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    primeira parte do caso q = 9.
    n = resolve_eq533_n(9,72,1,19,3/4,-1)
```

```
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(9,x) != True:
            if gcd(9,x) == 1:
                print (9,x)
    return 'Fim'

def resolve_caso_2_q_9_2(): #retorna os valores de (q,n) que falham para a eq (5.31) na
                                                segunda parte do caso q = 9.
    n = resolve_eq533_n(9,72,1,18,1/4,-1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(9,x) != True:
            if gcd(9,x) != 1:
                print (9,x)
    return 'Fim'
```

O Caso $n \geq 10$ e $q = 8$.

```
l = 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71 #o produto de todos os primos
                                                impares menores que 72.
def resolve_caso_2_q_8_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                primeira parte do caso q = 8.
    n = resolve_eq533_n(8,72,1,19,3/4,-1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(8,n) != True:
            if gcd(8,x) == 1:
                print (8,x)
    return 'Fim'

def resolve_caso_2_q_8_2(): #retorna os valores de (q,n) que falham para a eq (5.31) na
                                                segunda parte do caso q = 8.
    n = resolve_eq2_n(8,72,basico,19,3/8,-1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(8,x) != True:
            if gcd(8,x) != 1:
                print (8,x)
    return 'Fim'
```

O Caso $n \geq 10$ e $q = 7$.

```
l_2= 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71*73*79*83*89*97*101*103*107*109*
                                                113*127*131*137*139*149*151*157*163*167*173*
                                                179*181*191*193*197*199#neste caso, usamos
                                                todos os primos impares menores que 200.

def resolve_caso_2_q_7_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                primeira parte do caso q = 7.
    n = resolve_eq533_n(7,200,l_2,45,3/4,-1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(7,x) != True:
```

```
            if gcd(7,x) == 1:
                print (7,x)
    return 'Fim'

def resolve_caso_2_q_7_2(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    segunda parte do caso q = 7.
    n = resolve_eq533_n(7,200,l_2,45,3/28,-1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(7,x) != True:
            if gcd(7,x) != 1:
                print (7,x)
    return 'Fim'
```

O Caso $n \geq 10$ e $q = 5$.

```
l_2= 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71*73*79*83*89*97*101*103*107*109*
                                                    113*127*131*137*139*149*151*157*163*167*173*
                                                    179*181*191*193*197*199#neste caso, usamos
                                                    todos os primos impares menores que 200.
def resolve_caso_2_q_5_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    primeira parte do caso q = 5.
    n = resolve_eq533_n(5,200,l_2,45,1/3,5)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(5,x) != True:
            if gcd(5,x) == 1:
                print (5,x)
    return 'Fim'

def resolve_caso_2_q_5_2(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    segunda parte do caso q = 5.
    n = resolve_eq533_n(5,200,l_2,45,1/15,5)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(5,x) != True:
            if gcd(5,x) != 1:
                print (5,x)
    return 'Fim'
```

O Caso $n \geq 10$ e $q = 4$.

```
l_2= 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71*73*79*83*89*97*101*103*107*109*
                                                    113*127*131*137*139*149*151*157*163*167*173*
                                                    179*181*191*193*197*199#neste caso, usamos
                                                    todos os primos impares menores que 200.

def resolve_caso_2_q_4_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    primeira parte do caso q = 4.
    n = resolve_eq533_n(4,200,l_2,45,1/3,1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(4,x) != True:
            if gcd(4,x) == 1:
```

```
                print (4,x)
    return 'Fim'

def resolve_caso_2_q_4_2(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                primeira parte do caso q = 4.
    n = resolve_eq533_n(4,200,l_2,45,1/6,1)
    u = range(10,n+1)
    for x in u:
        if verificar_eq_principal(4,x) != True:
            if gcd(4,x) != 1:
                print (4,x)
    return 'Fim'
```

8.6 O Caso 3

O Caso $n = 9$.

```
l = 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71 #o produto de todos os primos
                                                impares menores que 72.

def resolve_caso_3_n_9_1():  #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                primeira parte do caso n = 9.
    q = resolve_eq1_q(9,72,l,19,1,-1)
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,9) != True:
            if (x-1)/9 in ZZ:
                print (x,9)
    return 'Fim'

def resolve_caso_3_n_9_2(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                segunda parte do caso n = 9.
    q = resolve_eq1_q(9,72,l,19,3/4,-1)
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,9) != True:
            if (x-1)/9 not in ZZ:
                if gcd(x,9) == 1:
                    print (x,9)
    return 'Fim'


def resolve_caso_3_n_9_3(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                terceira parte do caso n = 9.
    q = resolve_eq1_q(9,72,l,19,3/8,-1)
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,9) != True:
            if gcd(x,9) == 1:
                print (x,9)
    return 'Fim'
```

O Caso $n = 8$,

```
l = 3*5*7*11*13*17*19*23*29*31*37*41*43*47*53*59*61*67*71 #o produto de todos os primos
                                                    impares menores que 72.

def resolve_caso_3_n_8_1(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    primeira parte do caso n = 8.
    q = resolve_eq1_q(8,72,l,19,1,-1)
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,8) != True:
            if (x-1)/8 in ZZ:
                print (x,8)
    return 'Fim'

def resolve_caso_3_n_8_2(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    segunda parte do caso n = 8.
    q = resolve_eq1_q(8,72,l,19,3/4,-1)
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,8) != True:
            if (x-1)/8 not in ZZ:
                if gcd(x,8) == 1:
                    print (x,8)
    return 'Fim'

def resolve_caso_3_n_8_3(): #retorna os valores de (q,n) que falham para a eq. (5.31) na
                                                    terceira parte do caso n = 8.
    q = resolve_eq1_q(8,72,l,19,3/8,-1)
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,8) != True:
          if (x-1)/8 not in ZZ:
              if gcd(x,8) != 1:
                print (x,8)
    return 'Fim'
```

O Caso $n = 7$.

```
def resolve_caso_3_n_7_1():
    q = resolve_eq1_q(7,72,l,19,1,-1)
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,7) != True:
            if (x-1)/7 in ZZ:
              print (x,7)
    return 'Fim'

def resolve_caso_3_n_7_2():
    q = resolve_eq1_q(8,72,l,19,3/4,-1)
```

```
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,7) != True:
            if (x-1)/7 not in ZZ:
                if gcd(x,7) == 1:
                    print (x,7)
    return 'Fim'

def resolve_caso_3_n_7_3():
    q = resolve_eq1_q(7,72,1,19,3/8,-1)
    print q
    u = listar_potencias_primo(4,q+1)
    for x in u:
        if verificar_eq_principal(x,7) != True:
            if (x-1)/7 not in ZZ:
                if gcd(x,7) != 1:
                    print (x,7)
    return 'Fim'
```

8.7 Algorítimo para os casos excepcionais da Proposição 6.9

A seguir constam os códigos para verificar se os 18 casos excepcionais na Proposição 6.9, possuem ou não a existência de elementos 1-normais e primitivos com norma prescrita. Explicações sobre cada função será dada após o código.

```
def gpolinomio(q,n,y):
    x = PolynomialRing(GF(q^n),'x').gen()
    i = 0
    T = 0
    while i <= n-1:
        T = T + ((y^(q^i))*(x^(n-1-i)))
        i += 1
    return T

def verifica_1normal_primitivo(q,n,y):
    if y == 0:
        return False
    x = PolynomialRing(GF(q^n),'x').gen()
    H = gpolynomial(q,n,y).gcd(x^n-1)
    if H.degree() == 1:
        if y.multiplicative_order() == q^n - 1:
            return True
    return False

def verifica_prescreve_norma(q,n):
    a = []
    for y in GF(q^n):
        if verifica_1normal_primitivo(q,n,y) == True:
            t = y^((q^n-1)/(q-1))
            if t in a:
                pass
```

```
            else:
                a.append(t)
                if len(a) == euler_phi(q-1):

                    return True
    return False

a = [[16,15],[13,12],[11,10],[4,15],[7,12],[5,12],[4,9],[89,8],[41,8],[25,8],[17,8],[13,8],[
                                                    9,8],[7,8],[5,8],[64,7],[8,7],[4,7]]

def executar():
    for x in a:
        if verifica_prescreve_norma(x[0],x[1]) == True:
            print str(x) + ' possui elementos 1-normais e primitivos com norma prescrita'
        else:
            print str(x) + ' nao possui elementos 1-normais e primitivos com norma prescrita
                                                                    '
    return 'Fim'
```

A seguir, seguem os detalhamentos das funções construídas acima.

- gpolinomio(q,n,y): possui como entrada, q a potência de um primo, n o grau da extensão sobre $\mathbb{F}_q$ e y um elemento arbitrário de $\mathbb{F}_{q^n}$ e constrói o polinômio g_y como definido na Proposição 6.1.

- verifica_1normal_primitivo(q,n,y): Com as mesmas entradas de q e n e y como anteriormente, verifica se $y \in \mathbb{F}_{q^n}$ é 1-normal sobre $\mathbb{F}_q$ pela Definição 6.2 e também se é primitivo analisando sua ordem multiplicativa.

- verifica_prescreve_norma(q,n): Para cada y em $\mathbb{F}_{q^n}$, verifica se y é 1-normal sobre $\mathbb{F}_q$ e primitivo, caso não seja, ignora tal elemento. Caso y de fato seja 1-normal sobre $\mathbb{F}_q$ e primitivo, então calcula a norma de y sobre $\mathbb{F}_q$ pela fórmula usual e adiciona em uma lista nomeada a. É certificado que apenas elementos distintos sejam inclusos na lista a. Em seguida, é verificado quantos elementos possui a lista, caso este valor seja $\varphi(q-1)$ (o número de elementos primitivos em $\mathbb{F}_q$), então, como os valores da lista são todos distintos, todos os possíveis valores para $\mathrm{N}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(y)$ foram atingidos por elementos 1-normais e primitivos e a função retorna o valor verdade *True*. Caso contrário retorna o valor verdade *False*.

- executar(): Para os 18 pares na Proposição 6.9, utiliza a função anterior para verificar o resultado e imprimi-lo na tela.

Bibliografia

[1] Artin, M., *Algebra*, 2nd edition, Pearson, 2010.

[2] Atiyah, M. F. e Macdonalds, I. G., *Introduction to Commutative Algebra*, Addison-Wesley Series in Mathematics. University of Oxford, 1969.

[3] Carlitz, L. *Primitive roots in a finite field*, Trans. Amer. Math. Soc., 73:373-382, 1952.

[4] Carlitz, L. *Some problems involving primitive roots in a finite field*, Proc. Nat. Acad. Sci. U.S.A., 38:314-318, 1952.

[5] Cohen, S. D., *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen, 56:293-312, 2000.

[6] Cohen, S. D. e Hachenberger, D., *Primitive normal bases with prescribed trace*, Appl. Algebra Eng. Comm. Comput. 9, 383-403, 1999.

[7] Cohen, S. D. e Hachenberger, D., *Primitivity, freeness, norm and trace*, Disc. Math. 214:135-144, 2000.

[8] Cohen, S. D. e Huczynska, S., *The primitive normal basis theorem - without a computer*, J. London Math. Soc., 2(67):41-56, 2003.

[9] Cohen, S. D. e Huczynska, S. *Primitive free cubics with specified norm and trace*, Transactions of the American Mathematical Society, 355(8):3099-3116, 2003.

[10] Cohen, S. D. e Huczynska, S., *Primitive Free Quartics with Specified Norm and Trace*, Acta Arithmetica 109.4:359-385, 2003.

[11] Conway, J. H., *Tabulation of some information concerning finite fields*, Proc. Blaricum Conferente, 1966.

[12] Cox, D. A., *Galois Theory*, Pure and Applied Mathematics (New York). Wiley-Intersciente, John Willey & Sons, Hoboken, NJ, 2004.

[13] Davenport, H., *Bases for finite fields*, J. London Math Soc., 43:21-39, 1968.

[14] Dickson, L. E., *History of the Theory of Numbers*, Vol. I: *Divisibility and Primality*, Chelsea Publishing Co., New York, 1966.

[15] Eisenbud, D.,*Commutative Algebra with a view Toward Algebraic Geometry*, Springer, 1994.

[16] Fan, S., Han, W., Feng, K., Zhang, X., *Primitive normal polynomials with the first two coefficients prescribed: A revised p-adic method*, Finite Fields and Their Applications, 13:577-604, 2007.

[17] Fan, S., Han, W. e Feng, K., *Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result*, Finite Fields and Their Applications, 13:1029-1044, 2007.

[18] Fan, S., *Primitive normal polynomials with the last half coefficients prescribed*, Finite Fields and Their Applications, 15:604-614, 2009.

[19] Fan, S. e Wang, X., *Primitive Normal polynomials with a prescribed coefficient*, Finite Fields and Their Applications, 15:682-730, 2009.

[20] Galois, É., *Écrits em mémories mathématiques d'Évariste Galois*, editado por R. Bourgne e J. P. Azra, Gauthier-Villars, Paris, 1962.

[21] Huczynska, S., Mullen, G. L., Panario, D. e Thomson, D, *Existence and properties of k-normal elements over finite fields*, Finite Fields and Their Applications, 24:170-183, 2013.

[22] Huczynska, S., *Primitive Free Elements of Galois Fields*, PhD Thesis, University of Glasgow, 2002.

[23] Lenstra, H. W. e Schoof, R. J., *Primitive normal bases for finite fields*, Mathematics of Computation, 48:217-231, 1987.

[24] Lidl, R. e Niederreiter, H., *Finite Fields and its Applications*, Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2nd edition, 1997.

[25] Morgan, I. H. e Mullen, G. L., *Primitive normal polynomials over finite fields*, Math. Comp. 63:759-765, 1994.

[26] Mullen, G. L. e Panario, D., *Handbook of finite fields*, CRC Press, 2013.

[27] Ore, O., *Contribution to the theory of finite fields*, American Mathematical Society, 35:559-584, 1933.

[28] Reis, L. e Thomson, D., *Existence of primitive* 1*-normal elements in finite fields*, Finite Fields and Their Applications, 51:238-269, 2018.

[29] W. A. Stein, et al., *Sage Mathematics Software*, The Sage Development Team, http://www.sagemath.org, 2017.