UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Bacharelado em Matemática

Autor do trabalho: Luís Henrique da Silva Pinheiro

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann

Teorema da base normal

Breve introdução à elementos primitivos e normais em corpos finitos

UBERLÂNDIA

julho de 2020

Conteúdo

1 Origem

A teoria dos corpos finitos é um ramo da matemática que veio a tona nos últimos cinquenta anos por causa de suas diversas aplicações em vários segmentos da ciência, entre eles, análise combinatória, teoria dos códigos, criptografia, entre outros. Muitas figuras proeminentes na história da matemática contribuíram para o desenvolvimento desta teoria, entre eles podemos citar: Pierre de Fermat (1601- 1665); Leonhard Euler (1707-1783); Joseph-Louis Lagrange (1736-1813); AndrienMarie Legendre (1752-1833); entre outros. Além disso, segundo R. Lidil e H. Niederreiter, autores de uma das referências que utilizaremos [1], tal teoria começou com os trabalhos de Carl Friedrich Gauss (1777-1855) e Evariste Galois (1811- 1832), contudo, só veio a se tornar interessante para os matemáticos aplicados nas últimas décadas.

2 Conceitos principais

Para que se possa entender melhor este tema, explicaremos aqui mesmo, de forma breve, o significado destes conceitos. Começamos com a definição de corpo finito, este é qualquer coleção finita e não vazia de elementos, munida de duas operações binárias entre esses elementos, uma que se comporta como a adição, e outra que se comporta como a multiplicação, e quando falamos adição e multiplicação estamos nos referindo àquelas definidas entre números reais. Veremos no decorrer do trabalho, por exemplo, que se retirarmos de um corpo finito, o elemento neutro da adição, os elementos que sobram formam um grupo cíclico com a multiplicação, interessante não? Consequentemente, como todo grupo cíclico, ele passa a ter um gerador deste grupo. Ora, estes elementos, geradores destes grupos assim formados, são exatamente o que chamamos de "elementos primitivos". Já a definição de "elemento normal" é um pouquinho mais elaborada. Primeiro, começamos com um corpo finito de característica p, com q elementos (q é um natural não nulo). Veremos também que p deverá ser um número natural primo, e que o fato de p ser a característica deste corpo implica que a cardinalidade q deverá ser uma potência de p. Levando isso em conta, escolha um natural não nulo n, e considere uma extensão F de grau n do corpo inicial.

Da teoria de corpos finitos sabemos que esta extensão é um corpo que contém o primeiro, e que pode ser visto como um espaço vetorial de dimensão n (finita) sobre ele, é para a base deste espaço que olharemos agora. Um elemento x do corpo F é chamado "elemento normal" quando o conjunto $\{ x , x^q , x^{q^2} , ... , x^{q^{n-1}} \}$ é uma base para este espaço vetorial, estas bases assim formadas são chamadas bases normais sobre corpos finitos.

3 Relevância

O interesse de bases normais sobre corpos finitos decorre tanto da curiosidade puramente matemática quanto das aplicações práticas. Com o desenvolvimento da teoria de codificação e o surgimento de vários sistemas criptográficos utilizando corpos finitos, o trabalho nesta área resultou em vários projetos de implementação de hardware's e software's. Estes produtos são baseados em esquemas de multiplicação usando bases normais para representar corpos finitos, assim é necessário desenvolver uma aritmética de corpos finitos para que se possa construir os algorítimos apropriados. É claro que as vantagens de se utilizar uma representação de base normal são conhecidas há muitos anos. A complexidade do desenho de hardware de tais esquemas de multiplicação é fortemente dependente da escolha das bases normais usadas. Por isso, é essencial encontrar bases normais de baixa complexidade.

4 Metodologia

De forma sucinta, a metodologia consistiu em constante leitura, reflexão e resolução de exercícios. Os estudos avançaram seguindo como referência principal o livro [1, Finite fields], e como material de apoio os livros [2, Abstract algebra] e [3, Tópicos de álgebra], que eram consultados eventualmente para rever definições e demonstrações de teoremas, e ter uma visão sobre como o assunto estava sendo tratado por outros autores. E assim segui estudando os temas que posteriormente eu trouxe para o presente texto, tentando apresentar aqui uma

versão, além de traduzida para o português, também com vários comentários afim de clarear ideias e tornar o assunto um pouco mais acessível à estudantes de matemática a nível de graduação. Acho válido dizer também que, a linha de estudos cuja introdução está apresentada neste texto deve continuar, seguindo esta mesma metodologia na direção e sentido dos seguintes artigos: [4], [5], [6] e [7].

Obs: *Aqui, no sumário e ao longo de todo o texto o leitor poderá ver índices aparecendo em destaque, na cor verde ou azul. Clicando sobre eles você será redirecionado para a página e região da página para onde o "Link" está apontando, aproveite este recurso, muito útil na leitura de demonstroções mais extensas que fazem referência à lemas ou teoremas anteriores.*

5 Introdução ao texto técnico

O seguinte texto apresenta alguns dos principais conceitos e propriedades para qualquer um que deseja iniciar um estudo sobre Corpos finitos, e posteriormente sobre elementos primitivos e normais sobre corpos finitos. No primeiro capítulo definimos os corpos finitos, e o caracterizamos como um corpo de raízes de um polinômio específico associado. E também, apresentamos algumas das mais notáveis propriedades básicas envolvendo o tema, como por exemplo “O sonho de todos os estudantes” e o fato de que “Um certo grupo multiplicativo proveniente do corpo finito sempre será cíclico”.

No seguinte capítulo trabalhamos com raízes de polinômios irredutíveis sobre corpos finitos e resultados envolvendo os corpos de raízes desses polinômios. E também, introduzimos o conceito de “Conjugados” de um elemento do corpo finito, e a importância deles em todo este contexto.

E o último capítulo trata das bases normais repartindo-se basicamente em três trechos, no primeiro trecho definimos o “Traço” e desenvolvemos suas propriedades, no segundo trecho falamos sobre a “Norma” e suas propriedades, para então, só no final, falarmos efetivamente sobre as bases normais, definindo este conceito, demonstrando o “Lema de Artin”, e culminando no uso deste lema e de

resultados de álgebra linear para fazermos uma demonstração do "Teorema da base normal" finalizando por aqui.

6 Caracterização de corpos finitos

Sem mais delongas vamos ao que interessa. Como estamos estudando assuntos dentro da teoria de corpos finitos, nosso primeiro dever é definir e caracterizar os conceitos principais desta teoria, e exibir os resultados que necessitaremos para sermos capazes de demonstrar os resultados que constituem o objetivo deste texto, citados na visão geral dada anteriormente. Então vamos lá.

Definição 6.1 (Corpo)**.** *Um corpo é um conjunto não vazio munido de duas operações, conforme indica a notação* $(\mathbb{F}, +, *)$ *, de modo que, uma delas, a representada pelo símbolo* $+$ *é chamada de adição e a outra, representada pelo símbolo* $*$ *é chamada de multiplicação, e para que possamos chamar esta estrutura de corpo, estas duas operações precisam satisfazer as seguintes propriedades:*

- *Adição:* $+$
  - *(Neutro)* $\exists 0 \in \mathbb{F} \ tq \ \forall u \in \mathbb{F} \ 0 + u = u$
  - *(Simétrico)* $\forall u \in \mathbb{F} \ \exists -u \in \mathbb{F} \ tq \ u + (-u) = 0$
  - *(Associativa)* $\forall u, v, w \in \mathbb{F} \ (u + v) + w = u + (v + w)$
  - *(Comutativa)* $\forall u, v \in \mathbb{F} \ u + v = v + u$
- *Multiplicação:* $*$
  - *(Neutro)* $\exists 1 \in \mathbb{F} \ tq \ \forall u \in \mathbb{F} \, 1 * u = u$
  - *(Inverso)* $\forall u \in \mathbb{F} \ \exists u^{-1} \ tq \ u * u^{-1} = 1$
  - *(Associativa)* $\forall u, v, w \in \mathbb{F} \ (u * v) * w = u * (v * w)$
  - *(Comutativa)* $\forall u, v \in \mathbb{F} \ u * v = v * u$
- *Juntas devem satisfazer*
  - *(Distributiva)* $\forall u, v, w \in \mathbb{F} \ u * (v + w) = u * v + u * w$

Definição 6.2 (Corpo Finito)**.** *Um corpo finito é um corpo com uma quantidade finita de elementos. Dado* $q \in \mathbb{N} \setminus \{0\}$ *(Conjunto dos números naturais, zero excluso), para representar um corpo com* q *elementos utilizamos a notação* $\mathbb{F}_q$ *.*

Agora vejamos alguns resultados básicos sobre os corpos finitos, tais resultados constituem as noções essenciais que deveremos manter em mente ao longo de todo o texto.

Sabemos da teoria de corpos que todo corpo tem uma característica p , que por sua vez, é zero ou um número natural primo, que está associado ao corpo e a todos os corpos dentro da mesma "Torre de Corpos", que começa no subcorpo primo $\mathbb{F}_p$ e ascende até atingir seu fecho algébrico. Neste texto não explicaremos estes conceitos, consideramos que o leitor já foi exposto ao menos uma vez às teorias de anéis e corpos. Nosso foco nesta seção é trazer as propriedades que dizem respeito aos corpos finitos a partir dos conceitos e resultados básicos sobre corpos em geral. Apenas para efeito de relembrar, a característica de um corpo é definida como sendo a quantidade mínima de vezes que devemos somar a unidade (elemento neutro da multiplicação) do corpo afim de obter zero (elemento neutro da adição). No caso em que esta quantidade não existe, a característica é definida como sendo o $0 \in \mathbb{N}$. Outro ponto de interesse, que vale a pena ser mencionado agora, é sobre a dimensão nas extensões de corpos. Como já dissemos, uma "Torre de Corpos" mencionada anteriormente, deve ser vista como uma família de corpos encadeados pela relação de inclusão ($\subseteq$), todos possuindo a mesma característica p , de modo que esta relação vem a ser uma ordem total nesta família, tendo $\mathbb{F}_p$ como o mínimo dos membros, e o fecho algébrico como o máximo nesta ordem. Quando a característica é zero, o subcorpo primo é o corpo dos números racionais e o fecho algébrico é o corpo dos números complexos, já quando a característica é um número primo p , o subcorpo primo é $\mathbb{F}_p$ e o fecho algébrico também existirá normalmente. Mas, não só estão uns contidos em outros, como temos uma estrutura muito mais poderosa, uma vez que, se um corpo está contido em um segundo, o maior (que contém) pode ser visto como um espaço vetorial sobre o menor (que está contido). Novamente, não definiremos aqui noções de álgebra linear, também esperamos que o leitor já tenha familiaridade com esta teoria. Bem, da álgebra linear, sabemos que os espaços vetoriais pos-

suem dimensão, que por sua vez, é a quantidade de vetores que aparece em uma base para o espaço. Assim, dados dois corpos $\mathbb{F} \subseteq \mathbb{E}$, podemos ver $\mathbb{E}$ como um espaço vetorial sobre $\mathbb{F}$, e a dimensão de $\mathbb{E}$ sobre $\mathbb{F}$ é denotada por $[\mathbb{E}|\mathbb{F}]$, que em geral pode nem ser finita. Após esta discussão já podemos enunciar um importante resultado sobre corpos finitos.

Teorema 6.1 (Sobre a quantidade de elementos dos corpos finitos)**.** *Seja* $\mathbb{F}_q$ *um corpo finito de característica* p. *Então* $q = p^n$ *onde* $n = [\mathbb{F}_q|\mathbb{F}_p]$.

Demonstração. Sejam $\mathbb{K} \subseteq \mathbb{F}_q$ corpos finitos. Uma vez que o "maior deles" é finito, segue obviamente da teoria de corpos que ele deve ser de dimensão finita sobre o primeiro. (Pois o corpo todo já é finito, e a base está contida nele). Seja $n \in \mathbb{N}$ a quantidade de vetores em uma dessas bases. Então, há n vetores numa base, e todos os elementos de $\mathbb{F}_q$ são as combinações lineares dos elementos de uma dessas bases com coeficientes provenientes de $\mathbb{K}$. Como $\mathbb{K}$ também é finito, a quantidade de combinações lineares existente é exatamente $(\#\mathbb{K})^n$. Consequentemente $q = (\#\mathbb{K})^n$. Mas, pela discussão que tivemos antes de enunciar este teorema, dado qualquer corpo finito $\mathbb{F}_q$, ele terá sua característica p, que é diferente de zero, e será uma extensão de $\mathbb{F}_p$. Portanto, deverá ocorrer $q = p^n$ onde $n = [\mathbb{F}_q|\mathbb{F}_p]$. □

Antes de partirmos para o próximo teorema só precisamos de um resultado importante. Gosto de chamar este resultado de "O Sonho de Todos os Estudantes" (Não foi invenção minha), pois qualquer aluno que esteja aprendendo a fazer o desenvolvimento do binômio de Newton pela primeira vez, sonharia em poder aplicar a propriedade a seguir.

Lema 6.1 (O Sonho de Todos os Estudantes)**.** $\forall a, b \in \mathbb{F}_q$ *temos* $(a+b)^q = a^q + b^q$.

Demonstração. No desenvolvimento do binômio de Newton $(a+b)^q$, a primeira parcela é a^q, a última parcela é b^q, e cada uma das demais parcelas, conforme triângulo de Pascal, aparecem uma quantidade de vezes igual a C_i^q (Combinação de q tomados i a i) para cada $1 \leq i \leq q-1$. Ou seja, C_i^q é o coeficiente da i-ésima parcela no desenvolvimento do binômio inicial. De análise combinatória e teoria dos números sabemos que $q|C_i^q$. Como $p|q$, segue que $p|C_i^q$. Consequentemente, as parcelas do meio desaparecem após filtrarmos pela congruência

módulo p, sobrando apenas as duas parcelas extremas, que ocorrem quando $i \in \{0, q\}$. □

O próximo teorema é sobre a existência e unicidade dos corpos finitos, para compreende-lo é preciso lembrar do conceito de corpo de decomposição. Dado um polinômio $p(x)$ sobre um corpo $\mathbb{K}$, o corpo de decomposição deste polinômio é o "menor" corpo na "torre" de $\mathbb{K}$, relativamente a ordem total $\subseteq$ desta família, que contém $\mathbb{K}$ e todas as raízes de $p(x)$. Lembrando que, da teoria de corpos e da teoria dos polinômios sobre corpos, sabemos que todas as raízes do polinômio $p(x)$ pode ser encontrada dentro desta mesma "torre". Tal corpo de decomposição existe, é único para cada par $\{\mathbb{K}, p(x)\}$ e será denotado por $\mathbb{K}(p)$.

Lema 6.2 ($a \in \mathbb{F}_q \implies a^q = a$). *Se $\mathbb{F}$ é um corpo finito com q elementos, então para todo $a \in \mathbb{F}$ temos que $a^q = a$.*

Demonstração. A identidade $a^q = a$ é trivial para $a = 0$. Por outro lado, os elementos não nulos de $\mathbb{F}$ formam um grupo de ordem $q-1$ sob a multiplicação. Logo $a^{q-1} = 1$ para todo $a \in \mathbb{F}$ com $a \neq 0$, e a multiplicação por a nos traz o resultado desejado. □

Teorema 6.2 (Existência e Unicidade dos Corpos Finitos). *Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. E todo corpo finito $\mathbb{F}_q$ é isomorfo ao corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. (Existência) Considere $x^q - x \in \mathbb{F}_p[x]$ e $\mathbb{F} := \mathbb{F}_p(x^q - x)$. Como a derivada de $x^q - x$ é $qx^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$, todas as raízes de $x^q - x$ têm multiplicidade 1. (Pois o polinômio e sua derivada não têm raízes comuns). Ponha então $\mathbb{S} := \{a \in \mathbb{F} \ tq. \ a^q - a = 0\}$. Note que $\mathbb{S}$ é um corpo pois: (i) $\mathbb{S}$ possui 0 e 1. (ii) $\forall a, b \in \mathbb{S}$ temos $(a-b)^q = a^q - b^q = a - b \in \mathbb{S}$. (Lema anterior) E (iii) $\forall a, b \in \mathbb{F}$ com $b \neq 0$, $(ab^{-1})^q = a^q(b^{-1})^q = a(b^q)^{-1} = ab^{-1}$. Logo $ab^{-1} \in \mathbb{S}$. Dessa forma $\mathbb{S}$ é um subcorpo de $\mathbb{F}$ que contém $\mathbb{F}_p$ e todas as raízes de $x^q - x$. Como $\mathbb{F}$ é o menor com estas propriedades, $\mathbb{F} = \mathbb{S}$.

(Unicidade) Agora tome $\mathbb{F}_q$ e seja p sua característica. Então, pelo teorema 6.1 pág 6, $q = p^n$ e $\mathbb{F}_q$ é extensão de seu subcorpo primo $\mathbb{F}_p$. Agora seja $a \in \mathbb{F}_q$. Se $a = 0$ a identidade $a^q - a$ ocorre trivialmente. Caso $a \neq 0$, o conjunto

destes elementos, denotado por $\mathbb{F}_q^*$ forma um grupo multiplicativo de ordem $q-1$ uma vez que $\forall a, b \in \mathbb{F}_q^*$ temos $ab^{-1} \in \mathbb{F}_q^*$ obviamente. Consequentemente, da teoria de grupos podemos concluir que $a^{q-1} = 1$. Logo $a^q - a = 0$. Em outras palavras, acabamos de demonstrar que $\mathbb{F}_q^*$ é também o conjunto das raízes de $x^q - x \in \mathbb{F}_p[x]$. Assim, $\mathbb{F}_p(x^q - x) \subseteq \mathbb{F}_q^* \cup \{0\}$. Mas, como $\mathbb{F}_q^*$ é exatamente o conjunto das raízes de $x^q - x$, nenhum subcorpo próprio de $\mathbb{F}_q$ poderia ser o corpo de decomposição de $x^q - x$, pois qualquer um destes viria com raízes faltando. Portanto, $\mathbb{F}_q = \mathbb{F}_p(x^q - x)$. □

A parte da unicidade na demonstração acima serve para justificar a nossa fala, quando falamos sobre "o" corpo finito (ou corpo de Galois) com q elementos, ou sobre o corpo finito (ou corpo de Galois) de ordem q.

Teorema 6.3 (Critério dos subcorpos)**.** *Considere o corpo finito com q elementos $\mathbb{F}_q$ onde $q = p^n$ e p é a característica desta torre. Então todo subcorpo de $\mathbb{F}_q$ tem ordem p^m onde m é um divisor positivo de n. Reciprocamente, se m é um divisor positivo de n, então existe exatamente um divisor positivo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. É claro que um subcorpo $\mathbb{K}$ de $\mathbb{F}_q$ tem ordem p^m para algum inteiro positivo $m \leq n$. O teorema 6.1 mostra que $q = p^n$ precisa ser uma potência de p^m, e então m é necessariamente um divisor de n.

Reciprocamente, se m é um divisor positivo de n, então $p^m - 1$ divide $p^n - 1$, e então $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1 \in \mathbb{F}_p[x]$. Reciprocamente, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x \in \mathbb{F}_p[x]$. Logo, toda raiz de $x^{p^m} - x$ é uma raiz de $x^q - x$ e portanto pertence a $\mathbb{F}_q$. Daí segue que $\mathbb{F}_q$ tem que conter como um subcorpo o corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$, e como vimos na demonstração do teorema 6.2, este corpo decomposição deve ter ordem p^m. Se houvessem dois subcorpos distintos de ordem p^m contidos em $\mathbb{F}_q$, eles juntos possuiriam mais do que p^m raizes de $x^{p^m} - x$ em $\mathbb{F}_q$, o que é obviamente uma contradição. □

O próximo teorema é de extrema importância em todo o resto do texto, ele é a base para as principais proposições que sustentam os resultados mais interessantes que apresentaremos, então vejamo-o com atenção.

Teorema 6.4 (O Grupo Multiplicativo proveniente do corpo finito é Cíclico)**.** *Para todo corpo finito* $\mathbb{F}_q$ *, o grupo multiplicativo* $(\mathbb{F}_q^*, *)$ *é cíclico.*

Demonstração. Para $q = 2$ é trivial. Assuma $q \geq 3$. Seja $h := q - 1$ e permita que $h = \prod_{i=1}^{m} {p_i}^{r_i}$ seja sua decomposição primária em $\mathbb{F}_q^*$. Para todo $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes em $\mathbb{F}_q$. Uma vez que $h/p_i < h$ segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes deste polinômio. Seja a_i um destes elementos e ponha $b_i = a_i^{h/p_i^{r_i}}$. Assim temos $b_i^{p_i^{r_i}} = 1$ uma vez que a ordem de b_i é um divisor de $p_i^{r_i}$ e portanto é da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Por outro lado $b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$ logo a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b := \prod_{i=1}^{m} b_i$ tem ordem h . Suponha o contrário, que a ordem de b seja um divisor próprio de h e é portanto divisor de pelo menos um dos m inteiros h/p_i com $1 \leq i \leq m$, digamos que seja menor do que h/p_1 . Então nós temos $1 = b^{h/p_1} = \prod_{i=1}^{m} b_i^{h/p_i}$. Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h/p_1 , e consequentemente $b_i^{h/p_1} = 1$. Portanto $b_1^{h/p_1} = 1$. Isto implica que a ordem de b_1 tem que dividir h/p_1 , o que é impossível uma vez que a ordem de b_1 é $p_1^{r_1}$. Portanto, $\mathbb{F}_q^*$ é um grupo cíclico gerado por b . □

Agora já podemos definir o primeiro protagonista desta história.

Definição 6.3 (Elemento Primitivo)**.** *Um gerador do grupo* $(\mathbb{F}_q^*, *)$ *é chamado de* ***elemento primitivo*** *de* $\mathbb{F}_q$.

7 Raízes de polinômios irredutíveis

A teoria dos polinômios sobre corpos finitos é importante tanto para investigar a estrutura algébrica dos corpos finitos como também para muitas outras aplicações. Nesta seção coletamos algumas informações a respeito do conjunto das raízes de um polinômio irredutível sobre um corpo finito.

Lema 7.1 (Divisibilidade vs. Inclusão de Raízes)**.** *Seja* $f \in \mathbb{F}_q[x]$ *um polinômio irredutível sobre um corpo finito* $\mathbb{F}_q$ *e seja* α *uma raíz de* f *em uma extensão de* $\mathbb{F}_q$ *. Então para um polinômio* $h \in \mathbb{F}_q[x]$ *nós temos* $h(\alpha) = 0$ *se, e somente se,* f *divide* h *.*

Demonstração. Seja a o coeficiente líder de f e defina $g(x) = a^{-1}f(x)$. Então g é um polinômio mônico irredutível em $\mathbb{F}_q[x]$ com $g(\alpha) = 0$ e, portanto, é o polinômio minimal de α sobre $\mathbb{F}_q$. O restante segue das propriedades do polinômio minimal. □

Lema 7.2 (Relação entre f irredutível e o polinômio $x^{q^n} - x$). *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se, e somente se, m divide n.*

Demonstração. Suponha que $f(x)$ divide $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, logo $\alpha \in \mathbb{F}_{q^n}$. Segue que $\mathbb{F}_q(\alpha)$ é um subcorpo de $\mathbb{F}_{q^n}$. Mas, uma vez que $[\mathbb{F}(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, e considerando que uma extensão de um corpo pode ser vista como um espaço vetorial sobre o corpo de baixo, segue da teoria de espaços vetoriais que m divide n.

Por outro lado, se m divide n, o teorema 6.3 implica que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como um subcorpo. Se α é uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Consequentemente, temos que $\alpha \in \mathbb{F}_{q^n}$, assim $\alpha^{q^n} = \alpha$, e então α é uma raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Deduzimos então a partir do Lema 7.1 que $f(x)$ divide $x^{q^n} - x$. □

Teorema 7.1 (Raizes de um polinômio irredutível sobre um corpo finito). *Se f é um polinômio irredutivel em $\mathbb{F}_q[x]$ de grau m, então f tem uma raiz $\alpha \in \mathbb{F}_{q^m}$. Além disso, todas as raizes de f são simples e são dadas pelos m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então temos que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, portanto $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, e em particular temos que $\alpha \in \mathbb{F}_{q^m}$. Em sequida mostramos que se $\beta \in \mathbb{F}_{q^m}$ é uma raiz de f, então β^q também é uma raiz de f. Escreva $f(x) = \sum_{i=0}^{m} a_i x^{qi}$ com $a_i \in \mathbb{F}_q$ para $0 \leq i \leq m$. Então usando o Lema 6.2 e o Teorema 6.1, nós temos:

$$f(\beta^q) = \sum_{i=0}^{m} a_i \beta^{qi} = \sum_{i=0}^{m} {a_i}^q \beta^{qi} = \sum_{i=0}^{m} (a_i \beta^i)^q = f(\beta)^q = 0$$

Portanto esses elementos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ são raizes de f. Resta então provar que esses elementos são distintos. Suponha,por absurdo, que $\alpha^{q^j} = \alpha^{q^k}$

para algum j e k com $0 \leq j \leq k \leq m-1$. Ao elevar essa identidade a potência q^{m-k}, nós temos:

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

Seque então do Lema **??** que f divide $\alpha^{q^{m-k+j}} - x$. Pelo Lema 7.1, isso só é possivel se m divide $m-k+j$. Mas nós temos que $0 < m-k+j < m$, chegando assim a uma contradição. □

Corolário 7.2 ($f \in \mathbb{F}_q[x]$ irredutível $\implies \mathbb{F}_{q^{\delta(f)}} = \mathbb{F}_q(f)$)**.** *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m. Então o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.*

Demonstração. O Teorema 7.1 mostra que f se decompõe em $\mathbb{F}_{q^m}$. Além disso, $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ para uma raiz α de f em $\mathbb{F}_{q^m}$, onde a segunda identidade é tirada da demonstração do Teorema 7.1. □

Corolário 7.3 (Dois polinômios irredutíveis, mesmo corpo de decomposição)**.** *Quaisquer dois polinômios irredutiveis em $\mathbb{F}_q[x]$ de mesmo grau tem corpos de decomposição isomórficos.*

Introduzimos uma terminologia conveniente para os elementos que aparecem no Teorema 7.1, independentemente do $\alpha \in \mathbb{F}_{q^m}$ ser uma raiz do polinômio irredutivel em $\mathbb{F}_q[x]$ de grau m ou não.

Definição 7.1 (Conjugados)**.** *Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então os elementos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ são chamados de conjugados de α em relação a $\mathbb{F}_q$.*

Teorema 7.4 (Conjugados tem a mesma ordem no grupo multiplicativo)**.** *Os conjugados de $\alpha \in \mathbb{F}_q^*$ em relação a qualquer subcorpo de $\mathbb{F}_q$ tem a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Uma vez que $\mathbb{F}_q^*$ é um grupo cíclico, pelo Teorema 6.4, o resultado segue de resultados da teoria de grupos, e do fato de que toda potência da característica de $\mathbb{F}_q$ é coprima com a ordem $q-1$ de $\mathbb{F}_q^*$. □

Corolário 7.5 (α primitivo $\implies$ seus conjugados também são). *Se* α *é um elemento primitivo de* $\mathbb{F}_q$ *, então todos os seus conjugados com relação ao subcorpo* $\mathbb{F}_q$ *também o são.*

Teorema 7.6 (Descrição dos automorfismos entre corpos finitos). *Os automorfismos distintos de* $\mathbb{F}_{q^m}$ *em* $\mathbb{F}_q$ *são exatamente as funções* $\sigma_0, \sigma_1, ..., \sigma_{m-1}$ *definidas por* $\sigma_j(\alpha) = \sigma^{q^j}$ *para cada* $\alpha \in \mathbb{F}_{q^m}$ *e* $0 \leq j \leq m-1$.

Demonstração. Para cada σ_j e $\alpha, \beta \in \mathbb{F}_{q^m}$ nós temos obviamente $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ e também $\sigma_j(\alpha+\beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ devido o teorema 6.1, logo α_j é um endomorfismo de $\mathbb{F}_{q^m}$. Além disso, $\sigma_j(\alpha) = 0$ se e somente se $\alpha = 0$, consequentemente σ_j é injetora. Uma vez que $\mathbb{F}_{q^m}$ é um conjunto finito, σ_j é um epimorfismo, e portanto, um automorfismo de $\mathbb{F}_{q^m}$. Mais ainda, temos $\sigma_j(a) = a$ para todo $a \in \mathbb{F}_q$ pelo lema 6.2, e então cada σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. As funções $\sigma_0, \sigma_1, ..., \sigma_{m-1}$ são distintas uma vez que elas produzem valores distintos quando aplicadas em um mesmo elemento primitivo de $\mathbb{F}_{q^m}$.

Agora suponha que σ é um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Seja *beta* um elemento primitivo de $\mathbb{F}_{q^m}$ e digamos que $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0 \in \mathbb{F}_q[x]$ seja seu polinômio minimal sobre $\mathbb{F}_q$. Então $0 = \sigma(\ (\sum_{i=0}^{m-1} a_i\beta^i) + \beta^m\ ) = (\ \sum_{i=0}^{m-1} a_i\sigma(\beta)^i\ ) + \sigma(\beta)^m$ consequentemente $\sigma(\beta)$ é uma raiz de f em $\mathbb{F}_{q^m}$. Assim, segue do teorema 7.1 que $\sigma(\beta) = \beta^{q^j}$ para algum j tal que $0 \leq j \leq m-1$. Uma vez que σ é um homomorfismo, concluímos que $\sigma(\alpha) = \alpha^{q^j}$ para todo $\alpha \in \mathbb{F}_{q^m}$. □

8 Traços, Normas e Bases

Neste capítulo falaremos um pouco sobre os conceitos de traço e norma sobre corpos finitos, para que possamos contruir e definir o que vem a ser uma base normal, e por fim elemento normal.

Definição 8.1 (Traço). *Seja* $\alpha \in \mathbb{F}_{q^m}$ *e ponha* $\mathbb{F} := \mathbb{F}_{q^m}$ *e* $\mathbb{K} := \mathbb{F}_q$ *. O traço de* α *sobre* $\mathbb{K}$ *é definido por* $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) := \sum_{k=0}^{m-1} \alpha^{q^k}$.

Repare que, por definição concluímos que o traço é exatamente a soma de α com seus conjugados. Uma outra descrição do traço pode ser conseguida a partir do polinômio minimal de α . Pelo que vimos na seção anterior, se $f \in \mathbb{F}_q[x]$ é o

polinômio minimal de α então seu grau divide m. Definindo $g(x) := f(x)^{m/\delta(f)}$ como sendo o polinômio característico de α onde $\delta(f)$ representa o grau de f, segue da seção anterior que α e seus conjugados constituem exatamente as raízes de g. Consequentemente, da teoria de polinômios podemos concluir que o traço pode ser encontrado a partir dos coeficientes de g da seguinte forma: Se $g(x) = \sum_{i=0}^{\delta(g)} a_i x^i$ então $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -a_{\delta(g)-1}$. Ou seja, é o simétrico do próximo coeficiente após o líder uma vez ordenados segundo a ordem decrescente das potências dos termos associados no polinômio característico de α.

Teorema 8.1 (Propriedades do traço)**.** *Sejam $\mathbb{F} = \mathbb{F}_{q^m}$ e $\mathbb{K} = \mathbb{F}_q$. Então, a função $Tr_{\mathbb{F}/\mathbb{K}} : \mathbb{F} \to \mathbb{K}$ satsfaz as seguintes propriedades:*

(i) (Preserva a soma) $\forall \alpha, \beta \in \mathbb{F}\ Tr_{\mathbb{F}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{F}/\mathbb{K}}(\alpha) + Tr_{\mathbb{F}/\mathbb{K}}(\beta)$

(ii) (Preserva o produto por escalar) $\forall a \in \mathbb{K}\ \forall \alpha \in \mathbb{F}\ Tr_{\mathbb{F}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{F}/\mathbb{K}}(\alpha)$

(iii) (Transformação linear) $Tr_{\mathbb{F}/\mathbb{K}} : \mathbb{F} \to \mathbb{K}$ *é uma transformação linear sobrejetora quando tanto* $\mathbb{F}$ *quanto* $\mathbb{K}$ *são vistos como espaços vetoriais sobre* $\mathbb{K}$

(iv) (Traço em $\mathbb{K}$*)* $\forall a \in \mathbb{K}\ Tr_{\mathbb{F}/\mathbb{K}}(a) = ma$

(v) (Traço absorve potências por q*)* $\forall \alpha \in \mathbb{F}\ Tr_{\mathbb{F}/\mathbb{K}}(\alpha^q) = Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$

Demonstração. (i) Para $\alpha, \beta \in \mathbb{F}$ usamos o teorema 6.1 para obter $Tr_{\mathbb{F}/\mathbb{K}}(\alpha+\beta) = \sum_{i=0}^{m-1} (\alpha+\beta)^{q^i} = \sum_{i=0}^{m-1} (\alpha^{q^i} + \beta^{q^i}) = \sum_{i=0}^{m-1} \alpha^{q^i} + \sum_{i=0}^{m-1} \beta^{q^i} = Tr_{\mathbb{F}/\mathbb{K}}(\alpha) + Tr_{\mathbb{F}/\mathbb{K}}(\beta)$.

(ii) Dado $c \in \mathbb{K}$ nós temos $c^{q^j} = c\ \forall j \geq 0$ pelo Lema 6.2. Portanto $\forall \alpha \in \mathbb{F}$ obtemos $Tr_{\mathbb{F}/\mathbb{K}}(c\alpha) = \sum_{i=0}^{m-1} (c\alpha)^{q^i} = \sum_{i=0}^{m-1} c^{q^i}\alpha^{q^i} = \sum_{i=0}^{m-1} c\alpha^{q^i} = c\sum_{i=0}^{m-1} \alpha^{q^i} = cTr_{\mathbb{F}/\mathbb{K}}(\alpha)$.

(iii) As propriedades (i) e (ii) junto com o fato $\forall \alpha \in \mathbb{F}\ Tr_{\mathbb{F}/\mathbb{K}}(\alpha) \in \mathbb{K}$ mostram que $Tr_{\mathbb{F}/\mathbb{K}}$ é uma transformação linear de $\mathbb{F}$ em $\mathbb{K}$. Agora, sabemos de álgebra linear que, para uma transformação linear ser sobrejetora, só basta que ela não seja identicamente nula. Então provemos que existe $\alpha \in \mathbb{F}$ tal que $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) \neq 0$. Com efeito, dado $\alpha \in \mathbb{F}$ temos que $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) = 0 \iff \alpha$ é uma raíz do polinômio $\sum_{i=0}^{m-1} x^{q^i}$. Como este polinômio pode ter no máximo q^{m-1} raízes e existem q^m elementos em $\mathbb{F}$ segue que pelo menos um elemento deste corpo não pode

ser raíz deste polinômio. Nomeando-o(s) de β deve ocorrer $Tr_{\mathbb{F}/\mathbb{K}}(\beta) \neq 0$.

(iv) Seja $a \in \mathbb{K}$. Aplicando novamente o Lema 6.2 obtemos imediatamente $Tr_{\mathbb{F}/\mathbb{K}}(a) = \sum_{i=0}^{m-1} a^{q^i} = \sum_{i=0}^{m-1} a = ma$.

(v) Seja $\alpha \in \mathbb{F}$. Aplicando mais uma vez o Lema 6.2 obtemos $\alpha^{q^m} = \alpha$. Assim $Tr_{\mathbb{F}/\mathbb{K}}(\alpha^q) = \sum_{i=0}^{m-1} (\alpha^q)^{q^i} = \sum_{i=0}^{m-1} \alpha^{q^{i+1}} = \alpha^{q^m} + \sum_{i=1}^{m-1} \alpha^{q^i} = \alpha + \sum_{i=1}^{m-1} \alpha^{q^i} = \sum_{i=0}^{m-1} \alpha^{q^i} = Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$. □

O traço não é apenas uma transformação linear de $\mathbb{F}$ em $\mathbb{K}$, como também nos ajuda a descrever todas as transformações lineares de $\mathbb{F}$ em $\mathbb{K}$, e o melhor de tudo é que isto acontece de forma independente da base escolhida.

Teorema 8.2 (Descrição das Transformações Lineares)**.** *Seja $\mathbb{F}$ uma extensão finita do corpo finito $\mathbb{K}$. Então, as transformações lineares de $\mathbb{F}$ em $\mathbb{K}$ são exatamente as funções L_β, $\beta \in \mathbb{F}$ onde $L_\beta(\alpha) = Tr_{\mathbb{F}/\mathbb{K}}(\beta\alpha)$ para todo $\alpha \in \mathbb{F}$. Alem disso, $L_\alpha \neq L_\beta$ sempre que α e β são elementos distintos de $\mathbb{F}$.*

Demonstração. Cada função L_β é uma transformação linear de $\mathbb{F}$ em $\mathbb{K}$ pelo teorema 8.1 item (iii). Para $\beta, \gamma \in \mathbb{F}$ com $\beta \neq \gamma$, nós temos $L_\beta(\alpha) - L_\gamma(\alpha) = Tr_{\mathbb{F}/\mathbb{K}}(\beta\alpha) - Tr_{\mathbb{F}/\mathbb{K}}(\gamma\alpha) = Tr_{\mathbb{F}/\mathbb{K}}(\beta\alpha - \gamma\alpha) = Tr_{\mathbb{F}/\mathbb{K}}((\beta-\gamma)\alpha) = L_{\beta-\gamma}(\alpha)$. Como $L_{\beta-\gamma}$ não pode ser identicamente nula, como já vimos, segue que $L_\beta \neq L_\gamma$. Se $\mathbb{F} = \mathbb{F}_q^m$ e $\mathbb{K} = \mathbb{F}_q$ então $\#\{L_\alpha \,/\, \alpha \in \mathbb{F}\} = q^m$. Por outro lado, cada transformação linear de $\mathbb{F}$ em $\mathbb{K}$ pode ser obtida associando cada elemento de uma base dada de $\mathbb{F}$ sobre $\mathbb{K}$, a um único elemento de $\mathbb{K}$. Isto pode ser feito de exatamente q^m maneiras. Ou seja, existem exatamente q^m transformações lineares de $\mathbb{F}$ em $\mathbb{K}$. Portanto o conjunto $\{L_\alpha \,/\, \alpha \in \mathbb{F}\}$ possui todas elas. □

Quando temos uma cadeia de estensões de corpos, a composição de traços satisfaz uma propriedade bem simples.

Teorema 8.3 (Transitividade do traço)**.** *Seja $\mathbb{K}$ um corpo finito, $\mathbb{F}$ uma extensão finita de $\mathbb{K}$ e $\mathbb{E}$ uma extensão finita de $\mathbb{F}$. Então $Tr_{\mathbb{E}/\mathbb{K}} = Tr_{\mathbb{F}/\mathbb{K}} \circ Tr_{\mathbb{E}/\mathbb{F}}$.*

Demonstração. Seja $\mathbb{K} = \mathbb{F}_q$ e $m = [\mathbb{F}|\mathbb{K}]$ e $n = [\mathbb{E}|\mathbb{F}]$. Logo, de álgebra linear segue que $[\mathbb{E}|\mathbb{K}] = mn$. Então, para $\alpha \in \mathbb{E}$ nós temos $Tr_{\mathbb{F}/\mathbb{K}}(Tr_{\mathbb{E}/\mathbb{F}}(\alpha)) =$

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

□

Há uma outra função interessante que pode ser definida a partir de um corpo finito em algum de seus subcorpos, ela é formada fazendo o produto de um elemento com seus conjugados relativos a este subcorpo.

Definição 8.2 (Norma). *Dado* $\alpha \in \mathbb{F} = \mathbb{F}_{q^m}$ *e* $\mathbb{K} = \mathbb{F}_q$, *a norma* $N_{\mathbb{F}/\mathbb{K}}(\alpha)$ *de* α *sobre* $\mathbb{K}$ *é definida por* $N_{\mathbb{F}/\mathbb{K}}(\alpha) = \prod_{i=0}^{m-1} \alpha^{q^i} = \alpha^{(q^m-1)/(q-1)}$.

Assim como o traço pode ser expresso a partir dos coeficientes do polinômio característico, a norma também pode. Utilizando alguns resultados da teoria dos polinômios, e comparando coeficientes conseguimos obter $N_{\mathbb{F}/\mathbb{K}}(\alpha) = (-1)^m a_0$ onde a_0 é o termo constante do polinômio característico de α. Antes de ler o enunciado do teorema a seguir, é importante saber também que estamos adotando a notação $f|_S$ para representar a restrição de uma função f a um subconjunto S de seu domínio original.

Teorema 8.4 (Propriedades da Norma). *Seja* $\mathbb{F} = \mathbb{F}_{q^m}$ *e* $\mathbb{K} = \mathbb{F}_q$. *Então a função norma satisfaz as seguintes propriedades:*

(i) (Preserva o Produto) $\alpha, \beta \in \mathbb{F}$ $N_{\mathbb{F}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{F}/\mathbb{K}}(\alpha)N_{\mathbb{F}/\mathbb{K}}(\beta)$

(ii) $N_{\mathbb{F}/\mathbb{K}}$ *é uma função sobrejetora de* $\mathbb{F}$ *em* $\mathbb{K}$ *e* $N_{\mathbb{F}/\mathbb{K}}|_{\mathbb{F}^*}$ *é sobrejetora em* $\mathbb{K}^*$

(iii) (Norma em $\mathbb{K}$*)* $\forall a \in \mathbb{K}$ $N_{\mathbb{F}/\mathbb{K}}(a) = a^m$

(iv) (Norma absorve potências por q*)* $\forall \alpha \in \mathbb{F}$ $N_{\mathbb{F}/\mathbb{K}}(\alpha^q) = N_{\mathbb{F}/\mathbb{K}}(\alpha)$

Demonstração. (i) Segue imediatamente da definição de norma. Já vimos que $N_{\mathbb{F}/\mathbb{K}}$ é uma função de $\mathbb{F}$ em $\mathbb{K}$. Uma vez que $N_{\mathbb{F}/\mathbb{K}}(\alpha) = 0 \iff \alpha = 0$, $N_{\mathbb{F}/\mathbb{K}}$ mapeia $\mathbb{F}^*$ em $\mathbb{K}^*$. A propriedade (i) mostra que $N_{\mathbb{F}/\mathbb{K}}$ é um homomorfismo de grupos entre estes grupos multiplicativos. Uma vez que os elementos do núcleo de $N_{\mathbb{F}/\mathbb{K}}$ são exatamente as raízes do polinômio $x^{(q^m-1)/(q-1)} - 1 \in \mathbb{K}[x]$ em $\mathbb{F}$, a ordem d do núcleo satisfaz $d \leq (q^m-1)/(q-1)$. Pelo de homomorfismos de grupos, a imagem de $N_{\mathbb{F}/\mathbb{K}}$ tem ordem $(q^m-1)/d$, o qual é $\geq q-1$. Portanto, $N_{\mathbb{F}/\mathbb{K}}$ mapeia $\mathbb{F}^*$ em $\mathbb{K}^*$ e também $\mathbb{F}$ em $\mathbb{K}$, ambas de forma sobrejetiva. A propriedade (iii) segue da definição de norma e do fato de que, para $a \in \mathbb{K}$, os

conjugados de a relativos a $\mathbb{K}$ se resumem a apenas a. Finalmente, nós temos $N_{\mathbb{F}/\mathbb{K}}(\alpha^q) = N_{\mathbb{F}/\mathbb{K}}{}^q = N_{\mathbb{F}/\mathbb{K}}(\alpha)$ por causa de (i) e $N_{\mathbb{F}/\mathbb{K}}(\alpha) \in \mathbb{K}$, e assim (iv) está demonstrado. □

Teorema 8.5 (Transitividade da Norma). *Seja $\mathbb{K}$ um corpo finito, $\mathbb{F}$ uma extensão finita de $\mathbb{K}$ e $\mathbb{E}$ uma extensão finita de $\mathbb{F}$. Então $N_{\mathbb{E}/\mathbb{K}}(\alpha) = N_{\mathbb{F}/\mathbb{K}}(N_{E/\mathbb{F}}(\alpha))$ para todo $\alpha \in \mathbb{E}$.*

Demonstração. Com a mesma notação que usamos na demonstração do Teorema 8.3, nós temos que, para todo $\alpha \in \mathbb{E}$, $N_{\mathbb{F}/\mathbb{K}}(N_{\mathbb{E}/\mathbb{F}}(\alpha)) = N_{\mathbb{F}/\mathbb{K}}(\alpha^{(q^{mn}-1)/(q^m-1)}) = (\alpha^{(q^{mn}-1)/(q^m-1)})^{(q^m-1)/(q-1)} = \alpha^{(q^{mn}-1)/(q-1)} = N_{\mathbb{E}/\mathbb{K}}(\alpha)$. □

Definição 8.3 (Base Normal). *Sejam $\mathbb{K} = \mathbb{F}_q$ e $\mathbb{F} = \mathbb{F}_q^m$. Então uma base de $\mathbb{F}$ sobre $\mathbb{K}$ da forma $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$, consistindo de um certo elemento $\alpha \in \mathbb{F}$ e seus conjugados com relação a $\mathbb{K}$, é chamado uma base normal de $\mathbb{F}$ sobre $\mathbb{K}$.*

Nesse momento é bom relembrarmos alguns fatos e conceitos de álgebra linear. Se T é um operador linear no espaço vetorial de dimensão finita $\mathbb{V}$ sobre o corpo (arbitrário) $\mathbb{K}$, então dizemos que um polinômio $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ aniquila T quando $\sum_{i=0}^{n} a_i T^i = 0$ (lembrando que $T^0 = I$) onde I é o operador identidade e 0 o operador nulo sobre $\mathbb{V}$. O polinômio mônico unicamente determinado de menor grau positivo com esta propriedade é chamado de polinômio minimal de T. Ele divide qualquer outro polinômio em $\mathbb{K}[x]$ que aniquile T. Em particular, o polinômio minimal para T divide o polinõmio característico $g(x)$ de T (Teorema de Cayley-Hamilton), que é dado por $der(xI - T)$ e é um polinômio mônico de grau igual a dimensão de $\mathbb{V}$. Um vetor $\alpha \in \mathbb{V}$ é dito vetor cíclico de T quando os vetores $\{T^k(\alpha)\}_{k=0,1,2,...}$ geram o espaço $\mathbb{V}$. O seguinte lema é um resultado padrão de álgebra linear.

Lema 8.1 (Lema de Artin). *Sejam $\phi_1, \phi_2, \phi_3, ..., \phi_m$ homomorfismos distindos de um grupo $\mathbb{G}$ no grupo multiplicativo $\mathbb{F}^*$ de um corpo harbitrário $\mathbb{F}$, e sejam $a_1, a_2, ..., a_m$ elementos de $\mathbb{F}$ nem todos nulos. Então, para algum $g \in \mathbb{G}$ nós temos $\sum_{i=1}^{m} a_i \phi_i(g) \neq 0$.*

Demonstração. Procedemos por indução em m. O caso $m = 1$ é trivial, assumimos que $m > 1$ e que a afirmação é verdadeira para qualquer coleção de $m-1$ ho-

momorfismos distintos. Agora tome $\phi_1, \phi_2, ..., \phi_m$ e $a_1, a_2, ..., a_m$ como no enunciado. Se $a_1 = 0$ a hipótese de indução nos traz o resultado procurado imediatamente. Logo, suponha $a_1 \neq 0$. Assim, supondo que tivéssemos $\sum_{i=1}^{m} a_i \phi_i(g) = 0$ (*) para todo $g \in \mathbb{G}$. Uma vez que $\phi_1 \neq \phi_m$, existiria $h \in \mathbb{G}$ com $\phi_1(h) \neq \phi_m(h)$. Então, subistituindo g por hg, obteríamos $\sum_{i=1}^{m} a_i \phi_i(g) = 0$ para todo $g \in \mathbb{G}$. Após multiplicarmos por $\phi_m(h)^{-1}$ obteríamos $\sum_{i=1}^{m} b_i \phi_i(g) = 0$ para todo $g \in \mathbb{G}$ onde $b_i = a_i \phi_i(h) \phi_m(h)^{-1}$ para todo $1 \leq i \leq m-1$. Subtraindo esta identidade de (*), chegaríamos em $\sum_{i=1}^{m-1} c_i \phi_i(g)$ para todo $g \in \mathbb{G}$ onde $c_i = a_i - b_i$ para $1 \leq i \leq m-1$. Mas $c_1 = a_1 - a_1 \phi_1(h) \phi_m(h)^{-1} \neq 0$ e finalmente chegaríamos na condição da hipótese de indução, o que conclui a demonstração. □

Lema 8.2 (Critério para existir vetor cíclico)**.** *Seja T um operador linear sobre o espaço vetorial de dimensão finita V. Então T tem um vetor cíclico se, e somente se, os polinômios característico e minimal de T são idênticos.*

Teorema 8.6 (Teorema da Base Normal)**.** *Para todo corpo finito $\mathbb{K}$ e toda extensão finita $\mathbb{F}$ de $\mathbb{K}$, existe uma base normal de $\mathbb{F}$ sobre $\mathbb{K}$.*

Demonstração. Sejam $\mathbb{K} = \mathbb{F}_q$ e $\mathbb{F} = \mathbb{F}_{q^m}$ com $m \geq 2$. Do Teorema 7.6 e das considerações após ele, sabemos que os distintos automorfismos de $\mathbb{F}$ sobre $\mathbb{K}$ são dados por $\epsilon, \sigma, \sigma^2, ..., \sigma^{m-1}$, onde ϵ é a função identidade em $\mathbb{F}$, $\sigma(\alpha) = \alpha^q$ para todo $\alpha \in \mathbb{F}$, e uma potência σ^j refere-se a j-ésima composição de σ consigo mesma. Uma vez que $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$ para todo $\alpha, \beta \in \mathbb{F}$ e $c \in \mathbb{K}$, a função σ também pode ser considarada um operador linear no espaço vetorial $\mathbb{F}$ sobre $\mathbb{K}$. Uma vez que $\sigma^m = \epsilon$, o polinômio $x^m - 1 \in \mathbb{K}[x]$ aniquila σ. O Lema 8.1 aplicado a $\epsilon, \sigma, \sigma^q, ..., \sigma^{q^{m-1}}$ vistos como endomorfismos de $\mathbb{F}^*$ mostra que, polinômios não nulos de $\mathbb{K}[x]$ de grau menor do que m aniquila σ. Consequentemente, o polinômio $x^m - 1$ é o polinômio minimal para o operador linear σ. Uma vez que o polinômio característico de σ é um polinômio mônico de grau m que é múltiplo do polinômio minimal de σ, segue que o polinômio característico de σ também é dado por $x^m - 1$. O lema 8.2 implica então a existência de um elemento $\alpha \in \mathbb{F}$ tal que $\alpha, \sigma(\alpha), \sigma^2(\alpha), ...$ gera o espaço vetorial $\mathbb{F}$. Descartando os elementos repetidos, vemos que $\alpha, \sigma(\alpha), \sigma^2(\alpha), ..., \sigma^{m-1}(\alpha)$ gera $\mathbb{F}$ e consequentemente forma uma

base de $\mathbb{F}$ sobre $\mathbb{K}$. Uma vez que esta base consiste α e seus conjugados com relação a $\mathbb{K}$, segue que esta é uma base normal de $\mathbb{F}$ sobre $\mathbb{K}$. □

Definição 8.4 (Elemento Normal)**.** *Dado um corpo finito* $\mathbb{F}_{q^m}$ *e um elemento* $\alpha \in \mathbb{F}_{q^m}$. *Dizemos que* α *é um elemento normal quando o conjunto* $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}\}$ *é uma base normal para o corpo* $\mathbb{F}_{q^m}$ *quando visto como um espaço vetorial sobre* $\mathbb{F}_q$.

A partir daqui, ainda há muita teoria a ser desenvolvida para um estudo mais profundo sobre elementos primitivos e normais, mas até aqui já temos vários dos conceitos básicos desta teoria, e ao menos já é possível compreender os significados destes conceitos.

Referências

[1] R. LIDL and H. Niederreiter, "Finite fields," *Cambridge University Press, Reino Unido*, 1997.

[2] P. A. Grillet, "Abstract algebra," *Springer, New York*, 2007.

[3] I. N. Hernstein, "Tópicos de álgebra," *Universidade de São Paulo, São Paulo*, 1970.

[4] H. W. Lenstra and R. J. Schoof, "Primitive normal bases for finite fields," *Mathematics of Computation*, 1987.

[5] S. D. Cohen, "Pairs of primitive elements in fields of even order," *Finite fields and their applications*, 2014.

[6] R. K. Sharma and Anju, "Existence of some special primitive normal elements over finite fields," *Finite Fields and Their Applications*, 2017.

[7] R. K. Sharma and Anju, "On primitive normal elements over finite fields," *Asian-European Journal of Mathematics*, 2018.