Universidade Federal de Uberlândia - UFU
Faculdade de Matemática - FAMAT
Coordenação dos Cursos de Bacharelado e Licenciatura em Matemática

Trabalho de Conclusão de Curso

Códigos Algébricos Geométricos

Aluno: João Antonio Camargo Neto

Orientador(a): Alonso Sepúlveda Castellanos

João Antonio Camargo Neto

Códigos Algébricos Geométricos

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de licenciado em matemática

Universidade Federal de Uberlândia – UFU

Faculdade de Matemática

Orientador: Prof. Dr. Alonso Sepúlveda Castellanos

Uberlândia-MG

2019

João Antonio Camargo Neto

Códigos Algébricos Geométricos

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de licenciado em matemática

Trabalho aprovado. Uberlândia-MG, ***data***:

Prof. Dr. Alonso Sepúlveda Castellanos
Orientador

Prof. Dr. Germano Abud de Rezende

Prof. Dr. Guilherme Chaud Tizziotti

Uberlândia-MG
2019

Agradecimentos

Agradeço a Deus por me sustentar e me ajudar a seguir em frente, todas as vezes que tudo ficava difícil, Ele foi para mim a voz que me guiou e trouxe ordem quando tudo se tornava caos.

Agradeço também aos meus maiores incentivadores em todos os sentidos, minha família - em especial meus pais Marildo José Martins e Gleidis de Camargo Martins - que me proporcionou e continua proporcionando o privilégio de viver os sonhos que tenho, me dando suporte em todas as áreas para que consiga manter o foco e chegar até o fim.

Agradeço ao meu orientador, Profº Dr. Alonso Sepúlveda Castellanos, que me acompanhou durante todo o período da graduação e, foi essencial na minha caminhada acadêmica até aqui. Se hoje concluo esta fase, é porque ele foi para mim não somente um orientador, como também, um amigo.

Agradeço aos meus colegas de curso, que durante muitos momentos me ajudaram.

Agradeço a Universidade Federal de Uberlândia por todas as portas que foram abertas para que tivesse diversas experiências. Cito também o Programa de Iniciação Científica PICME ligado ao CNPQ, ao qual fiz parte durante 3 anos e meio, que me incentivou a vivenciar a pesquisa científica, me desenvolvendo como acadêmico.

"Agrada-te do Senhor e, Ele
satisfará os desejos do teu coração."
(Salmo 37:4)

Resumo

Neste trabalho estudamos códigos algébricos geométricos (códigos AG), que são códigos lineares construídos sobre curvas algébricas em corpos finitos. Para isso, introduzimos algumas noções básicas da teoria de corpos finitos e de corpos de funções. Estudamos a teoria de códigos lineares corretores de erros para a compreensão e fundamentação da construção dos códigos AG. No final, construímos códigos AG sobre a Curva Hermitiana e exibimos os parâmetros dos códigos.

Palavras-chave: Corpos Finitos. Códigos Lineares. Curvas Algébricas. Códigos AG. Teoria de códigos corretores de erros. Curva hermitiana.

Abstract

In this work, we study geometric algebraic codes (AG codes), which are linear codes built on algebraic curves in finite fields. To do so, we introduce some basic notions of finite fields theory and function fields. We study a theory of error-correcting linear codes to understand and substantiate the construction of AG codes. In the end, we build AG codes over a Hermitian Curve and display the code parameters.

Keywords: Algebra. Theory of Error-Correcting Codes. Hermitian Curve.

Sumário

Introdução

A teoria dos códigos corretores de erros é um campo de pesquisa muito ativo na atualidade em diversas áreas do conhecimento: matemática, computação, engenharia elétrica, estatística e entre outras. Na transmissão de dados, na vida real, às vezes ocorrem problemas, como interferências eletromagnéticas ou erros humanos (por exemplo, erros de digitação) que chamamos de ruído e que fazem com que a mensagem recebida seja diferente daquela que foi enviada. O objetivo da teoria de códigos corretores de erros é desenvolver métodos que permitam detectar e corrigir estes erros.

A teoria de códigos corretores de erros lineares sobre curvas algébricas (códigos algébricos geométricos (códigos AG) passou a ser desenvolvida desde o trabalho de Goppa e Tsfasman, Vladut e Zink em 1981-1982.

Para a construção dos códigos AG são utilizados divisores das curvas algébricas que são construídos por meio dos pontos racionais (ou lugares de grau 1) da curva. Dessa forma, é importante que a curva possua uma grande quantidade de pontos racionais para que os códigos construídos apresentem parâmetros como: dimensão e distância mínima satisfatórios.

Com isso, torna-se vantajoso utilizar as chamadas curvas maximais, que tem como característica atingir a cota superior de Hasse-Weil, que estabelece o maior número de pontos racionais de uma curva de gênero g, sobre um corpo finito. Em particular construiremos um código AG sobre uma curva maximal, chamada curva Hermitiana.

No capítulo 1, abordamos a teoria inicial dos códigos corretores de erros, definindo importantes conceitos que permearão os nossos resultados no decorrer do trabalho. Também iremos enunciar e mostrar alguns resultados chaves no desenvolvimento da teoria.

No capítulo 2, estudamos noções básicas de corpos finitos, extensões de corpos e as aplicações Norma e Traço, além de algumas de suas propriedades.

O capítulo 3 será destinado a teoria de corpos de funções, imprescindível para construção dos códigos AG, pois nele, iremos definir lugares, divisores, valorização e enunciar o principal resultado que iremos utilizar na estrutura do códigos AG, que é o Teorema de Riemann-Roch.

No capitulo 4, mostramos a construção dos códigos AG, suas propriedades e exibimos os chamados códigos.

1 Códigos Corretores de Erros

Os códigos corretores de erros participam do nosso cotidiano de diferentes formas, como, por exemplo, quando assistimos programas de TV, falamos ao telefone, ouvimos um CD ou navegamos pela internet. Nestas situações estamos utilizando informações digitalizadas. [2]

Um código corretor de erros é, em essência, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar, que permita ao recuperar a informação, detectar e corrigir erros.

A Teoria de Códigos Corretores de Erros foi fundada pelo matemático Claude Elwood Shannon, matemático estadunidense conhecido como pai da teoria da informação, que publicou um trabalho intitulado *A Mathematical Theory of Communication* em 1948, no qual abordava qual a melhor forma de se codificar a informação que um emissor queira transmitir para um receptor.

Inicialmente, os maiores interessados em Teoria dos Códigos foram os matemáticos, que a desenvolveram consideravelmente nas décadas de 50 e 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros.

1.1 Código do Robô

Vejamos um exemplo, o qual chamaremos de código do Robô, para ilustrar os princípios desta teoria. Suponha que tenhamos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (Leste, Oeste, Norte e Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando. Podemos codificar os comandos, como elementos de $\{0,1\} \times \{0,1\}$, da seguinte forma:

$$\begin{array}{rcl} Leste & \mapsto & 00 \\ Oeste & \mapsto & 01 \\ Norte & \mapsto & 10 \\ Sul & \mapsto & 11 \end{array}$$

A coluna da direita é chamada *código da fonte*. Agora suponhamos que os pares ordenados devem ser transmitidos por rádio e que o sinal sofra uma interferência no caminho, em decorrência deste ruído na informação, a mensagem 00 pode ser recebida como 01. Com isso, o robô ao invés de ir para o Leste, iria para o Oeste. Para que isso não

aconteça, introduzimos redundâncias nas palavras, recodificando-as, para que seja possível identificar e corrigir os erros.

Podemos recodificar nosso código da seguinte forma:

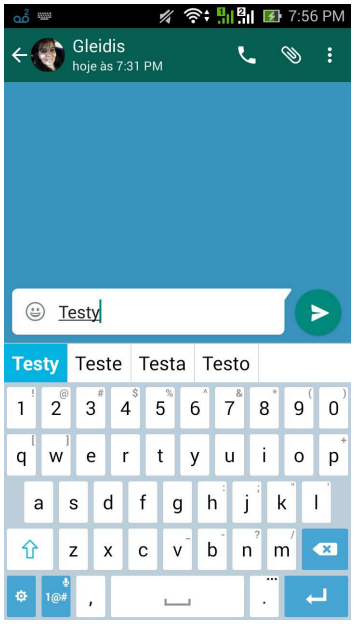
$$\begin{aligned} \textit{Leste} &\mapsto 00 \mapsto 00000 \\ \textit{Oeste} &\mapsto 01 \mapsto 01011 \\ \textit{Norte} &\mapsto 10 \mapsto 10110 \\ \textit{Sul} &\mapsto 11 \mapsto 11101 \end{aligned}$$

Veja que nesta recodificação, as duas primeiras posições reproduzem o código da fonte e os três números introduzidos são as redundâncias. Este novo código será chamado de **Código de canal**.

Suponha que se tenha introduzido um erro ao transmitirmos, por exemplo, a palavra 10110, de modo que a mensagem recebida seja 11110. Comparando essa mensagem com as palavras do código, notamos que não lhe pertence e, portanto detectamos erros. A palavra do código mais próxima da palavra introduzida (a que tem menos coordenadas distintas) é 10110, que é precisamente a palavra transmitida.

O nosso estudo consiste, então, em transformar o código da fonte em um código de canal, sendo possível a detecção e correção de forma mais eficiente.

Outro exemplo para ilustrar a teoria de códigos corretores de erros, é o corretor de celular, muito criticado pelos usuários de smartfones. Note que as palavras do código que o corretor analisa são neste caso as palavras da língua portuguesa, portanto, veja o seguinte caso:



Perceba que a palavra introduzida *testy* não existe na língua portuguesa e, portanto são sugeridas algumas opções para a correção, porém notem que todas as opções dadas

possuem apenas uma letra distinta da palavra errada introduzida, impossibilitando uma correção certeira se deixada de forma automática.

Concluímos que a língua portuguesa é um péssimo alfabeto para utilizarmos, já que as palavras são muito próximas, em questão de apenas uma letra introduzida errada, pode equivaler a várias palavras com sentido distinto. Isso nos leva a crer que é mais interessante pensar em alfabetos algébricos.

1.2 Métrica de Hamming

Seja A um conjunto finito, o qual chamaremos de Alfabeto. O número de elementos de A será denotado por $|A| = q$. Um código corretor de erros é um subconjunto próprio qualquer de $A^n = \{(x_1, x_2, \ldots, x_n) : x_i \in A; i = 1, 2, \ldots, n\}$, para $n \in \mathbb{N}$. Até agora utilizamos a noção intuitiva de proximidade entre palavras, porém vamos definir uma forma de medir essa distância.

Definição 1.1. Dados dois elementos $u, v \in A^n$, a distância de Hamming entre u e v é definida como

$$d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|.$$

Para exemplificar esta definição, considere $A = \{0, 1\}$ e $n = 4$:

$$d(0010, 1111) = 3$$

$$d(1010, 0101) = 4$$

$$d(1001, 1101) = 1$$

Proposição 1.2. *Dados $u, v, w \in A^n$, valem as seguintes propriedades:*

i) Positividade: $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.

ii) Simetria: $d(u, v) = d(v, u)$.

iii) Desigualdade Triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

Demonstração. i) Temos por definição que $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$, logo, temos que a distância será a quantidade de elementos deste conjunto, desta forma $d(u, v) \geq 0$.

ii) Quando calculamos a distância de Hamming, comparamos coordenada a coordenada das palavras, dessa forma, independe a ordem que comparamos a i-ésima coordenada das palavras, ou seja, os conjuntos $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$ e $d(v, u) = |\{i; v_i \neq u_i, 1 \leq i \leq n\}|$ são equivalentes.

iii) A contribuição das i-ésimas coordenadas de u e v para $d(u.v)$ é igual a 0 se $u_i = v_i$, e igual a 1 se $u_i \neq v_i$. No caso em que a contribuição é zero, certamente a contribuição das i-ésimas coordenadas de $d(u, v)$ é menor igual a das i-ésimas coordenadas de $d(u, w) + d(w, v)$ (= 0, 1 ou 2).

No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, a contribuição das i-ésimas coordenadas a $d(u, v) + d(w, v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas de $d(u, v)$.

□

A Proposição 1 nos garante que a distância de Hamming, como definimos é uma métrica.

Dado um elemento $a \in A^n$ e um número real $t \geq 0$, definimos o disco e a esfera de centro a e raio t como sendo, respectivamente, os conjuntos

$$D(a, t) = \{u \in A^n; d(u, a) \leq t\},$$
$$S(a, t) = \{u \in A^n; d(u, a) = t\}.$$

Como $d(u, a) \in \mathbb{N}$, os conjuntos acima são finitos e o próximo lema nos fornecerá as suas cardinalidades. Iremos a partir daqui utilizar a notação usual de números combinatórios:

$$\left(\begin{array}{c} n \\ i \end{array} \right) = \frac{n!}{i!(n-i)!}.$$

Lema 1.3. *Para todo $a \in A^n$ e todo número natural $r > 0$, temos que*

$$|D(a, r)| = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i.$$

Demonstração. Devemos mostrar que

$$|S(a, i)| = \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i$$

O resultado segue, observando que $S(a, i) \cap S(a, j) = \emptyset$ se $i \neq j$, e que

$$\bigcup_{i=0}^{r} S(a, i) = D(a, r).$$

□

Note que a cardinalidade de $D(a, r)$ depende apenas de n, q e r.

Definição 1.4. Seja C um código de A^n. A distância mínima de C é o número

$$d = min\{d(u, v); u, v \in C, u \neq v\}.$$

Por exemplo no código do robô, tínhamos $d = 3$.

Para calcularmos d, precisaríamos calcular $\binom{M}{2}$ distâncias, onde M é o número de palavras do código, o que tem um alto custo computacional. Veremos a seguir uma forma de calcular d, com baixo custo computacional, quando utilizamos uma estrutura algébrica adicional.

Dado um código C de A^n com distância miníma d, define-se $\kappa = \left[\frac{d-1}{2} \right]$, onde $[t]$ representa a parte inteira de $t \in \mathbb{R}$.

Lema 1.5. *Seja C um código com distância mínima d. Se c e c' são palavras distintas de C então*

$$D(c, \kappa) \cap D(c', \kappa) = \emptyset.$$

Demonstração. De fato, se $x \in C$ pertencesse a $D(c, \kappa) \cap D(c', \kappa)$, teríamos $d(x, c) \leq \kappa$ e $d(x, c') \leq \kappa$. Como $d(x, c) = d(c, x)$ pela desigualdade triangular temos que $d(c, c') \leq d(c, x) + d(x, c') \leq 2k$. Agora para $j, l \in \mathbb{Z}_+$ temos pelo algoritmo de euclides que existem $q, r \in \mathbb{Z}$ tais que $j = lq + r$ o que implica que $l \left[\frac{j}{l} \right] = j - r$ e daí segue que,

$$d(c, c') \leq d(c, x) + d(x, c') \leq 2\kappa \leq d - 1,$$

absurdo pois $d(c, c') \geq d$.

□

A importância da distância mínima d de um código se dá pelo teorema a seguir.

Teorema 1.6. *Seja C um código de A^n com distância mínima d. Então C pode corrigir até $\kappa = \left[\frac{d-1}{2} \right]$ erros e detectar até $d - 1$ erros.*

Demonstração. Se ao transmitirmos uma palavra c do código cometermos t erros, com $t \leq \kappa$, recebendo a palavra r, então $d(r, c) = t \leq \kappa$; enquanto que, pelo Lema anterior, a distância de r a qualquer outra palavra do código é maior que κ. Isso determina c univocamente a partir de r. Por outro lado, dada uma palavra do código, podemos nela introduzir até $d - 1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível.

□

Por exemplo no código do robô como $d = 3$, é possível corrigir até $\kappa = \left[\frac{3-1}{2} \right] = 1$ erros e detectar até $d - 1 = 4 - 1 = 3$ erros.

Podemos concluir que um código terá maior capacidade de detecção e correção de erros quanto maior a sua distância mínima, portanto é fundamental que calculemos d e

que exista uma cota inferior para este parâmetro de qualidade do código, isto que iremos determinar a seguir.

Definição 1.7. Seja $C \subset A^n$ um código com distância mínima d e seja $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se

$$\bigcup_{c \in C} D(c, \kappa) = A^n.$$

Um código C sobre um alfabeto A possui três parâmetros fundamentais $[n, k, d]$, que são respectivamente, o seu comprimento, o número de elementos (veremos que em códigos lineares representa a dimensão do código) e sua distância mínima.

1.3 Códigos Lineares

A classe de códigos mais utilizada na prática é conhecida como códigos lineares, à qual iremos abordar no decorrer do trabalho.

Denotaremos por $\mathbb{F}_q$ um corpo finito com q elementos tomado como alfabeto. Temos, portanto, para cada $n \in \mathbb{N}$, existe um $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{F}_q, i = 1, 2, \ldots, n\}$ de dimensão n.

Sejam $u, v \in \mathbb{F}_q^n$ e $k \in \mathbb{F}_q$, onde $u = (u_1, u_2, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$. As operações definidas em $\mathbb{F}_q^n$ serão:

- **Soma:**

$$u + v = (u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n).$$

  Onde a soma de $u_i + v_i \in \mathbb{F}_q$, para $i = 1, 2, \ldots, n$ é a soma em $\mathbb{F}_q$.

- **Multiplicação por escalar:**

$$k \cdot u = k \cdot (u_1, u_2, \ldots, u_n) = (k \cdot u_1, k \cdot u_2, \ldots, k \cdot u_n)$$

  Note que $u_i \in \mathbb{F}_q; i = 1, 2, \ldots, n$, dessa forma a operação $k \cdot u_i \in \mathbb{F}_q$ é o produto usual de $\mathbb{F}_q$.

Definição 1.8. Todo subespaço $C \subset \mathbb{F}_q^n$ será chamado código linear sobre $\mathbb{F}_q$.

Sabemos que a imagem de uma transformação linear é um subespaço vetorial, portanto, podemos representar os códigos por meio de uma transformação linear injetora, veja um exemplo a seguir.

O código robô é um código linear, considerando o alfabeto $A = \mathbb{F}_2$, conhecido como corpo de Galois, e o código robô é subespaço vetorial de $\mathbb{F}_2^5$. A transformação linear que gera o código robô é

$$\begin{array}{rccc} T: & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & (x_1, x_2) & \mapsto & (x_1, x_2, x_1, x_1 + x_2, x_2) \end{array}$$

De fato, veja que:

$$\begin{aligned} T(0,0) &= (0,0,0,0,0) \\ T(0,1) &= (0,1,0,1,1) \\ T(1,0) &= (1,0,1,1,0) \\ T(1,1) &= (1,1,1,0,1) \end{aligned}$$

Todo código linear é por definição um espaço vetorial de dimensão finita. Portanto seja k a dimensão do código C e seja $(v_1, v_2, \ldots, v_k)$ uma de suas bases, portanto, todo $c \in C$, pode ser escrito como

$$c = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

onde $\lambda_i \in \mathbb{F}_q, i = 1, \ldots, k$. Segue daí que o número de palavras do código será $M = |C| = q^k$. E consequentemente,

$$\boxed{dim_K C = k = log_q q^k = log_q M.}$$

Definição 1.9. Seja $x \in \mathbb{F}_q^n$, dizemos que o peso de x é

$$\omega(x) = |\{i; x_i \neq 0)\}|.$$

Uma definição equivalente é $\omega(x) = d(x, 0)$.

Definição 1.10. O peso de um código linear C é

$$\omega(C) = min\{\omega(x); x \in C \backslash \{0\}\}.$$

Proposição 1.11. *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos que*

i) $\forall x, y \in \mathbb{F}_q^n$, $d(x, y) = \omega(x - y)$.

ii) $d = \omega(C)$.

Demonstração. i) Por definição temos que $\forall u, v \in \mathbb{F}_q^n$, $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$ e, $\forall u, v \in \mathbb{F}_q^n$ temos que, $\omega(u - v) = |\{i; u_i - v_i \neq 0, 1 \leq i \leq n\}|$, porém, podemos reescrever $u_i - v_i \neq 0$ como $u_i \neq v_i$, tornando assim os dois conjuntos iguais, logo, $\forall u, v \in \mathbb{F}_q^n$, $d(u, v) = \omega(u - v)$.

ii) Para todo par de elementos $x, y \in C$, com $x \neq y$, tem-se que $z = x - y \in C\backslash\{0\}$ e $d(x, y) = \omega(z)$, logo a distância mínima será o menor peso de um elemento z assim construído do código.

□

1.4 Matriz Geradora de um Código

Considere $\mathbb{F}_q$ o corpo finito com q elementos e $C \subset \mathbb{F}_q^n$ um código linear. Chamaremos de *parâmetros do código linear* C à terna de inteiros $[n, k, d]$ onde k é a dimensão de C sobre $\mathbb{F}_q$ e d representa a distância mínima de C, que é também igual ao peso de $\omega(C)$ do código C. Note que o número de elementos M de C é igual a q^k.

Seja $\beta = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, isto é:

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}$$

A matriz G é chamada de *matriz geradora* de C associada a base β.

Considere a transformação linear definida por:

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}$$

Se $x = (x_1, \ldots, x_k)$, temos que

$$T(x) = xG = x_1 v_1 + \cdots + x_k v_k$$

Logo $T(\mathbb{F}_q^k) = C$. Podemos, então, considerar $\mathbb{F}_q^n$ como sendo o código da fonte, C, o código de canal e a transformação T, uma codificação.

Note que a matriz G depende da escolha da base, dessa forma não é univocamente determinada por C.

Podemos também considerar o processo inverso e construir códigos a partir de matrizes geradoras. Para isso, basta tomar uma matriz cujas linhas são linearmente independentes e definir um código como sendo a imagem da transformação linear:

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}$$

Definição 1.12. Diremos que uma matriz geradora G de um código C está na forma padrão se tivermos

$$G = (Id_k | A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

O teorema a seguir nos garante a existência da matriz na forma padrão de qualquer matriz geradora de um código C, e podemos obtê-la por meio de operações elementares e permutação de colunas.

Teorema 1.13. *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração. A demonstração pode ser vista em [2] nas páginas 92-93. □

1.5 Código Dual

Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$, defini-se o produto de u e v sendo:

$$\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n.$$

Essa operação possui as propriedades usuais de um produto interno, ou seja, é simétrica

$$\langle u, v \rangle = \langle v, u \rangle$$

e bilinear

$$\begin{aligned} \langle u + \lambda w, v \rangle &= \langle u, v \rangle + \lambda \langle w, v \rangle \\ \langle u, v + \lambda w \rangle &= \langle u, v \rangle + \lambda \langle w, v \rangle \\ \langle \lambda u, v \rangle &= \langle u, \lambda v \rangle = \lambda \langle u, v \rangle \end{aligned}$$

para todo $\lambda \in \mathbb{F}_{_{11}}$.

Seja $C \subset \mathbb{F}_q^n$ um código linear, defini-se:

$$C^{\perp} = \{v \in \mathbb{F}_q^n; \langle u, v \rangle = 0, \forall u \in C\}.$$

Lema 1.14. *Se $C \subset \mathbb{F}_q^n$ é um código linear, com matriz geradora G, então*

i) $C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$.

ii) $x \in C^{\perp} \Leftrightarrow Gx^t = 0$.

Demonstração. i) Considere $u, v \in C^{\perp}$ e $\lambda \in \mathbb{F}_q$. Temos que para todo $x \in C$

$$\langle u + \lambda v, x \rangle = \langle u, x \rangle + \lambda \langle v, x \rangle = 0$$

e portanto, $u + \lambda v \in C^{\perp}$, provando que $C^{\perp}$ é um subespaço vetorial de $\mathbb{F}_q^n$.

ii) $x \in C^{\perp} \Leftrightarrow x$ é ortogonal a todos os elementos de $C \Leftrightarrow x$ é ortogonal a todos os elementos de uma base de C, o que é equivalente a dizer que $Gx^t = 0$ pois as linhas de G são uma base de C.

□

O subespaço vetorial $C^{\perp}$ de $\mathbb{F}_q^n$, ortogonal a C, é também um código linear que será chamado **código dual** de C.

2 Corpos finitos

Nos apêndices deste trabalho, são abordados conceitos relacionados a introdução a corpos, extensões de corpos e polinômios, que são importantes para a compreensão dos resultados abordados nesta seção.

Neste capítulo iremos caracterizar os corpos finitos, para isso, enunciaremos e provaremos alguns resultados importantes para que saibamos manipular as curvas que serão trabalhadas no decorrer do trabalho. Para maiores detalhes ver [1].

2.1 Caracterização de Corpos Finitos

Lema 2.1. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então F contém q^m elementos, onde $m = [F : K]$.*

Demonstração. F é um espaço vetorial sobre K, e uma vez que F é finito, ele é um espaço de dimensão finita sobre K. Se $[F : K] = m$, então F tem uma base sobre K consistindo de m elementos, digamos $b_1, b_2, ..., b_m$. Logo, cada elemento de F pode ser unicamente representado na forma $a_1b_1 + \cdots + a_mb_m$, onde $a_1, ..., a_m \in K$. Como cada a_i pode assumir q valores, F tem exatamente q^m elementos. □

Teorema 2.2. *Seja F um corpo finito. Então F tem p^n elementos, onde o primo p é a característica de F e n é o grau de F sobre seu subcorpo primo.*

Demonstração. Uma vez que F é finito, sua característica é um primo p. Assim o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ e, portanto, contém p elementos. O resultado segue do Lema 2.1. □

Começando dos corpos primos $\mathbb{F}_p$, podemos construir outros corpos finitos pelo processo de adjunção de raízes. Se $f \in \mathbb{F}_p[x]$ for um polinômio irredutível sobre $\mathbb{F}_p$ de grau n, então pela adjunção de uma raiz de f a $\mathbb{F}_p$, obtemos um corpo finito com p^n elementos. Além disso, veremos que existe apenas um corpo (a menos de isomorfismo) com uma dada quantidade de elementos.

Lema 2.3. *Se F for um corpo finito com q elementos, então todo $a \in F$ satisfaz $a^q = a$.*

Demonstração. A identidade $a^q = a$ é trivial para $a = 0$. Por outro lado, os elementos não-nulos de F formam um grupo multiplicativo de ordem $q-1$. Então, $a^{q-1} = 1$ para todo $a \in F$ com $a \neq 0$, e multiplicando ambos os lados por a, obtemos o resultado desejado. □

Lema 2.4. *Se F for um corpo finito com q elementos e K for um subcorpo de F, então o polinômio $x^q - x \in K[x]$ se fatora em $F[x]$ como*

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

e F é um corpo de decomposição de $x^q - x$ sobre K.

Demonstração. O polinômio $x^q - x$ de grau q tem, no máximo q raízes em F. Pelo Lema 2.3, sabemos q tais raízes (todos os elementos de F). Assim, o polinômio dado se divide em F da maneira indicada, e não pode se dividir em nenhum corpo menor. □

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

Demonstração. (Existência) Para $q = p^n$, considere $x^q - x$ em $\mathbb{F}_p[x]$ e seja F seu corpo de decomposição sobre $\mathbb{F}_p$. Esse polinômio tem q raízes distintas em F, uma vez que sua derivada é $qx^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$ e, dessa maneira, não tem nenhuma raiz em comum com $x^q - x$. Seja $S = \{a \in F : a^q - a = 0\}$. Então, S é um subcorpo de F, já que:
(i) S contém 0 e 1;
(ii) $a, b \in S$ implica $a - b \in S$ $((a-b)^q = a^q - b^q = a - b)$;
(iii) $a, b \in S$, $b \neq 0$ implica $ab^{-1} \in S$ $((ab^{-1})^q = a^q b^{-q} = ab^{-1})$.
Mas, por outro lado, $x^q - x$ deve se dividir em S, uma vez que S contém todas as suas raízes. Logo, $F = S$ e, uma vez que S tem q elementos, F é um corpo finito com q elementos.

(Unicidade) Seja F um corpo finito com $q = p^n$ elementos. Então F tem característica p pelo Teorema 2.2 e, assim, contém $\mathbb{F}_p$ como subcorpo. Segue do Lema 2.4 que F é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Então, o resultado desejado é uma consequência da unicidade (a menos de isomorfismo) dos corpos de decomposição. □

Podemos concluir que o único (a menos de isomorfismo) corpo finito com $q = p^n$ elementos é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. A seguir, veremos quais são todos os subcorpos $\mathbb{F}_r$ de um dado corpo $\mathbb{F}_q$. Não basta que $\mathbb{F}_r$ esteja contido em $\mathbb{F}_q$, precisamos que todos os elementos $x \in \mathbb{F}_r$ satisfaçam a condição $x^q = x$ em $\mathbb{F}_r$. Por exemplo,

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\} \subset \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{F}_7,$$

mas, em $\mathbb{F}_5$, $2^7 = 3$, mostrando que $\mathbb{F}_5$ não é subcorpo de $\mathbb{F}_7$.

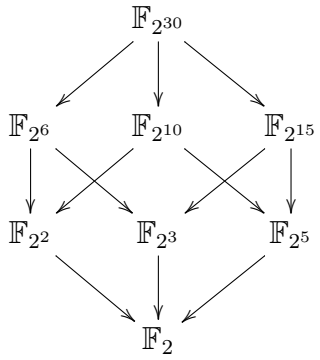
Teorema 2.6 (Critério para subcorpos)**.** *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então todo subcorpo de $\mathbb{F}_q$ tem p^m elementos, onde m é um divisor positivo de n. Inversamente, se m for um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. É fácil ver que um subcorpo K de $\mathbb{F}_q$ tem ordem p^m para algum inteiro positivo $m \leq n$. O Lema 2.1 mostra que $q = p^n$ deve ser uma potência de p^m, logo m é, necessariamente, um divisor de n.

Inversamente, se m for um divisor positivo de n, então $p^m - 1$ divide $p^n - 1$, e assim $x^{p^m} - 1$ divide $x^{p^n} - 1$ em $\mathbb{F}_p[x]$. Consequentemente, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ em $\mathbb{F}_p[x]$. Logo, toda raiz de $x^{p^m} - x$ é uma raiz de $x^q - x$ e, portanto, pertence a $\mathbb{F}_q$. Segue que $\mathbb{F}_q$ deve conter como subcorpo um corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$, e como vimos na prova do Teorema 2.5, tal corpo de decomposição tem ordem p^m. Se existissem dois tais subcorpos de ordem p^m em $\mathbb{F}_q$, eles conteriam, juntos, mais que p^m raízes de $x^{p^m} - x$ em $\mathbb{F}_q$, uma contradição óbvia. □

A prova do Teorema 2.6 mostra que o único subcorpo de $\mathbb{F}_{p^n}$ de ordem p^m, onde m é um divisor positivo de n, consiste precisamente das raízes do polinômio $x^{p^m} - x \in \mathbb{F}_p[x]$ em $\mathbb{F}_{p^n}$.

Exemplo 2.7. Os subcorpos do corpo finito $\mathbb{F}_{2^{30}}$ podem ser determinados listando todos os divisores positivos de 30. As relações de contingência entre esses vários subcorpos estão dispostas no seguinte diagrama.



Pelo Teorema 2.6, as relações de contingência são equivalentes às relações de divisibilidade entre os divisores positivos de 30.

Para um corpo finito $\mathbb{F}_q$, denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo dos elementos não-nulos de $\mathbb{F}_q$. Uma propriedade muito importante de tal grupo é a seguinte:

Teorema 2.8. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

Demonstração. Podemos assumir $q > 3$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para cada $i, 1 \leq i \leq m$, o polinômio $x^{\frac{h}{p_i}} - 1$ tem, no máximo, $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Uma vez que $\frac{h}{p_i} < h$, segue que existem elementos não-nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um tal elemento e defina $b_i = a_i^{h \backslash p_i^{r_i}}$. Então $b_i^{p_i^{r_i}} = 1$, logo a ordem de b_i é um divisor de $p_i^{r_i}$ e é, com isso, da forma $p_i^{s_i}$ com

$0 \leq s_i \leq r_i$. Por outro lado,

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

e, assim, a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. Suponha, do contrário, que a ordem de b é um divisor próprio de h e é, portanto, um divisor de, no mínimo, um dos m inteiros $\frac{h}{p_i}, 1 \leq i \leq m$, digamos de $\frac{h}{p_1}$. Então, temos

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

Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide $\frac{h}{p_1}$, e, assim, $b_1^{\frac{h}{p_1}} = 1$. Isso implica que a ordem de b_1 deve dividir $\frac{h}{p_1}$, o que é impossível, já que a ordem de b_1 é $p_i^{r_i}$. Logo, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 2.9. Um gerador para o grupo cíclico $\mathbb{F}_q^*$ é chamado um **elemento primitivo** de $\mathbb{F}_q$.

Teorema 2.10. *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ um corpo finitamente estendido. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ pode servir como um elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

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

Corolário 2.11. *Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n, existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Demonstração. Seja $\mathbb{F}_r$ o corpo estendido de $\mathbb{F}_q$ de ordem q^n, então $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 2.10, temos $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ para algum $\zeta \in \mathbb{F}_r$. Então, o polinômio minimal de ζ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n. □

Com os resultados apresentados nesse capítulo, podemos enxergar um corpo finito $\mathbb{F}_q$ de característica p como o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p = \mathbb{Z}_p$, temos um critério para subcorpos e sabemos encontrar extensões de corpos de qualquer grau.

Veremos a seguir resultados importantes a respeito dos chamados polinômios irredutíveis que determinam curvas algébricas. Além disso, definiremos funções importantes envolvendo corpos finitos, as quais serão utilizadas na construção do código AG sobre a curva hermitiana, que pode ser vista como uma relação entre as funções traço e norma.

2.2 Raízes de polinômios irredutíveis

Lema 2.12. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre um corpo finito $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão de corpos de $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$, nós temos $h(\alpha) = 0$ se, e só se, f dividir h.*

Demonstração. Basta usar o algoritmo da divisão em $\mathbb{F}_q[x]$. A partir dele, obtemos

$$h(x) = q(x)f(x) + r(x).$$

"Aplicando" α nessa expressão, encontramos $h(\alpha) = r(\alpha)$ e o resultado segue. □

Lema 2.13. *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 só se, m dividir n.*

Demonstração. Suponha que $f(x)$ divida $x^{q^n} - x$. 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 $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, sabemos que m divide n pelo Teorema A.31.

Inversamente, se m dividir n, o Teorema 2.6 implica que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como subcorpo. Se α for uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}(\alpha) : \mathbb{F}_q] = m$, e, então, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Consequentemente, nós temos $\alpha \in \mathbb{F}_{q^n}$, logo $\alpha^{q^n} = \alpha$, e, portanto, α é uma raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Nós temos como consequência então pelo Lema 2.12 que $f(x)$ divide $x^{q^n} - x$. □

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

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, e, em particular, $\alpha \in \mathbb{F}_{q^m}$. Em seguida, nós mostraremos que se $\beta \in \mathbb{F}_{q^m}$ for uma raiz de f, então β^q é também uma raiz de f. Escreva $f(x) = a_0 + a_1x + \cdots + a_mx^m$, com $a_i \in \mathbb{F}_q$. Logo, usando o Lema 2.3, temos

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

Portanto, os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são raízes de f. Resta provar que esses elementos são distintos. Suponha, do contrário, que $\alpha^{q^j} = \alpha^{q^k}$, para inteiros j e k com $0 \leq j < k \leq m - 1$. Elevando essa identidade à potência q^{k-j}, obtemos

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

Segue, então, do Lema 2.12, que $f(x)$ divide $x^{q^{m-k+j}} - x$. Pelo Lema 2.13, isso só é possível se m dividir $m - k + j < m$, e então chegamos em uma contradição. □

Corolário 2.15. *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. Usando o Teorema 2.14, vemos facilmente que f se decompõe em $\mathbb{F}_{q^m}$. Além disso, $\mathbb{F}_q(\alpha, \alpha^q, ..., \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ para uma raiz α em $\mathbb{F}_{q^m}$, onde a segunda identidade é tirada da prova do Teorema 2.14. □

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

Assim, vimos que o corpo de decomposição de um polinômio irredutível pode ser obtido quando conhecemos uma de suas raízes. Além disso, nós conseguimos mostrar que, se soubermos uma raiz α de um polinômio irredutível de grau m, saberemos todas as outras raízes (que são exatamente as potências $\alpha^q, \alpha^{q^2}, ..., \alpha^{q^m}$). Essas potências recebem uma nomenclatura especial.

Definição 2.17. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então os elementos $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ são chamados **conjugados** de α com respeito a $\mathbb{F}_q$.

Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito a $\mathbb{F}_q$ são distintos se, e só se, o polinômio minimal de α sobre $\mathbb{F}_q$ tiver grau m. Do contrário, o grau d do polinômio minimal será um divisor próprio de m, e, assim, os conjugados de α com respeito a $\mathbb{F}_q$ serão os elementos distintos $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$, cada um repetido $\frac{m}{d}$ vezes.

Teorema 2.18. *Os conjugados de $\alpha \in \mathbb{F}_{q^m}^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ têm a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Seja $\mathbb{F}_d$ um subcorpo de $\mathbb{F}_q$ e a a ordem de α no grupo $\mathbb{F}_q^*$. Sabemos que d é uma potência da característica de $\mathbb{F}_q$ e, portanto, é coprimo com a ordem $q-1$ de $\mathbb{F}_q^*$. Um outro resultado bem conhecido da teoria de grupos é que a ordem de α^d em $\mathbb{F}_q^*$ é igual a $\frac{a}{mdc(d,q-1)} = a$. Logo, a ordem de α^d em $\mathbb{F}_q^*$ é igual à ordem de α nesse grupo. Analogamente, prova-se para os outros conjugados e temos o resultado desejado. □

Corolário 2.19. *Se α for um elemento primitivo de $\mathbb{F}_{q^m}$, então todos os seus conjugados com respeito a qualquer subcorpo de $\mathbb{F}_q$ também o são.*

Exemplo 2.20. Seja $\alpha \in \mathbb{F}_{16}$ uma raiz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Então os conjugados de α com respeito a $\mathbb{F}_2$ são $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ e $\alpha^8 = \alpha^2 + 1$, cada um deles é um elemento primitivo de $\mathbb{F}_{16}$. Os conjugados de α com respeito a $\mathbb{F}_4$ são α e $\alpha^4 = \alpha + 1$.

Existe uma relação íntima entre elementos conjugados e certos automorfismos de um corpo finito. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$. Por um **automorfismo** de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, nós denotamos um automorfismo σ de $\mathbb{F}_{q^m}$ que fixa os elementos de $\mathbb{F}_q$. Portanto, em detalhes,

nós exigimos que σ seja um mapa injetor de $\mathbb{F}_{q^m}$ nele mesmo com $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$ e $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ para todos $\alpha,\beta\in\mathbb{F}_{q^m}$ e $\sigma(a)=a$ para todo $a\in\mathbb{F}_q$.

Teorema 2.21. *Os distintos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente os mapas $\sigma_0,\sigma_1,...,\sigma_{m-1}$ definidas por $\sigma_j(\alpha)=\alpha^{q^j}$ para $\alpha\in\mathbb{F}_{q^m}$ e $0\leq j\leq m-1$.*

Demonstração. Para cada σ_j e todos $\alpha,\beta\in\mathbb{F}_{q^m}$ é simples notar que temos $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$ e $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$, de forma que σ_j é um endomorfismo de $\mathbb{F}_{q^m}$. Além disso, $\sigma_j(\alpha)=0$ se, e só se, $\alpha=0$, logo σ_j é injetor. Uma vez que $\mathbb{F}_{q^m}$ é um conjunto finito, σ_j é sobrejetor e, portanto, um automorfismo de $\mathbb{F}_{q^m}$. Além disso, temos $\sigma_j(a)=a$ para todo $a\in\mathbb{F}_q$ pelo Lema 2.3, e, então, cada σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Os mapas $\sigma_0,\sigma_1,...,\sigma_{m-1}$ são distintos, uma vez que atribuem valores distintos aos elementos primitivos de $\mathbb{F}_{q^m}$.

Agora, suponha que σ é um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Seja β um elemento primitivo de $\mathbb{F}_{q^m}$ e seja $f(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_0\in\mathbb{F}_q[x]$ seu polinômio minimal sobre $\mathbb{F}_q$. Então

$$0=\sigma(\beta^m+a_{m-1}\beta^{m-1}+\cdots+a_0)=\sigma(\beta)^m+a_{m-1}\sigma(\beta)^{m-1}+\cdots+a_0,$$

de forma que $\sigma(\beta)$ é uma raiz de f em $\mathbb{F}_{q^m}$. Segue do Teorema 2.14 que $\sigma(\beta)=\beta^{q^j}$ para algum $0\leq j\leq m-1$. Uma vez que σ é um homomorfismo, $\sigma(\alpha)=\alpha^{q^j}$ para todo $\alpha\in\mathbb{F}_{q^m}$. □

Assim, finalizamos essa seção ressaltando a importância de se conhecer as raízes de polinômios irredutíveis: a partir de uma dessas raízes, pode-se obter todas as outras tomando seus conjugados e o corpo de decomposição desse polinômio pode ser obtido adjuntando-se ao corpo base uma raiz encontrada.

2.3 Traço e Norma

Vamos agora introduzir uma importante aplicação de $\mathbb{F}=\mathbb{F}_{q^m}$ em $\mathbb{K}=\mathbb{F}_q$, a qual será linear. Mais resultados envolvendo as funções que serão definidas a seguir, podem ser encontrados em [3].

Definição 2.22. Para $\alpha\in\mathbb{F}=\mathbb{F}_{q^m}$ e $\mathbb{K}=\mathbb{F}_q$, o traço de α sobre $\mathbb{K}$ é definido por

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

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

Teorema 2.23. *Seja $\mathbb{K}=\mathbb{F}_q$ e $\mathbb{F}=\mathbb{F}_{q^m}$. Então a função traço $Tr_{\mathbb{F}/\mathbb{K}}$ satisfaz as seguintes propriedades:*

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

ii) $Tr_{\mathbb{F}/\mathbb{K}}(c\alpha) = cTr_{\mathbb{F}/\mathbb{K}}(\alpha)$, $\forall c \in \mathbb{K}, \forall \alpha \in \mathbb{F}$.

iii) $Tr_{\mathbb{F}/\mathbb{K}}$ *é uma transformação linear de* $\mathbb{F}$ *em* $\mathbb{K}$*, onde ambos são vistos como espaço vetorial sobre* $\mathbb{K}$.

iv) $Tr_{\mathbb{F}/\mathbb{K}}(a) = ma; \forall a \in \mathbb{K}$.

v) $Tr_{\mathbb{F}/\mathbb{K}}(\alpha^q) = Tr_{\mathbb{F}/\mathbb{K}}(\alpha); \forall \alpha \in \mathbb{F}$.

Demonstração. i) Sejam $\alpha, \beta \in \mathbb{F}$, temos que

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

Obs: Note que usamos o fato da característica de $\mathbb{F}$ ser q, isto nos permitiu utilizar a seguinte igualdade

$$(\alpha+\beta)^q = \alpha^q+\beta^q$$

ii) Sejam $c \in \mathbb{K}$ e $\alpha \in \mathbb{F}$, então:

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

iii) As propriedades (i) e (ii) juntamente com o fato de $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) \in \mathbb{K}, \forall \alpha \in \mathbb{F}$, nos garante que $Tr_{\mathbb{F}/\mathbb{K}}$ é uma transformação linear de $\mathbb{F}$ em $\mathbb{K}$. Basta mostrar que $\exists \alpha \in \mathbb{F}$, tal que, $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) \neq 0$.

Temos que $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) = 0$ se, e somente se, α é raiz de $x^{q^{m-1}}+\cdots+x^q+x \in \mathbb{K}[x]$ em $\mathbb{F}$. Mas como esse polinômio possui no máximo q^{m-1} raizes em $\mathbb{F}$ e como $\mathbb{F}$ possui q^m, podemos garantir que pelo menos um elemento de $\mathbb{F}$ não é raíz do polinômio, o que equivale a dizer que $\exists \alpha \in \mathbb{F}$, tal que,$Tr_{\mathbb{F}/\mathbb{K}}(\alpha) \neq 0$.

iv) Seja $a \in \mathbb{K}$, temos que:

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

v) Para $\alpha \in \mathbb{F}$, temos que $\alpha^{q^m} = \alpha$, e então, $Tr_{\mathbb{F}/\mathbb{K}}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^m} = Tr_{\mathbb{F}/\mathbb{K}}(\alpha)$.

□

A função $Tr_{\mathbb{F}/\mathbb{K}}$ serve para descrever todas as transformações lineares de $\mathbb{F}$ para $\mathbb{K}$.

Teorema 2.24. *Seja $\mathbb{F}$ uma extensão finita do corpo finito $\mathbb{K}$, ambos são espaços vetoriais sobre $\mathbb{K}$. Então as transformações lineares de $\mathbb{F}$ para $\mathbb{K}$ são exatamente os mapeamentos $L_\beta.\beta \in F$, onde $L_\beta(\alpha) = Tr_{\mathbb{F}/\mathbb{K}}(\beta\alpha)$, $\forall \alpha \in \mathbb{F}$. Além disso, temos que $L_\beta \neq L_\gamma$, onde β e γ são elementos distintos de $\mathbb{F}$.*

Demonstração. Cada mapeamento L_β é uma transformação linear de $\mathbb{F}$ para $\mathbb{K}$ pelo teorema 2.23(iii). Para $\beta, \gamma \subset \mathbb{F}$ com $\beta \neq \gamma$, temos que $L_\beta - L_\gamma = Tr_{\mathbb{F}/\mathbb{K}}(\beta\alpha) - Tr_{\mathbb{F}/\mathbb{K}}(\gamma\alpha) = Tr_{\mathbb{F}/\mathbb{K}}((\beta - \gamma)\alpha) \neq 0$ para um $\alpha \in F$ adequado, $Tr_{\mathbb{F}/\mathbb{K}}$ mapeia $\mathbb{F}$ sobre $\mathbb{K}$, e $L_\beta \neq L_\gamma$. Se $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$, então existem q^m diferentes transformações lineares L_β de $\mathbb{F}$ para $\mathbb{K}$. Por outro lado, toda transformação linear de $\mathbb{F}$ para $\mathbb{K}$ pode ser obtida atribuindo elementos arbitrários de $\mathbb{K}$ aos m elementos da base de $\mathbb{F}$ sobre $\mathbb{K}$. Isto pode ser feito de q^m diferentes formas, o mapeamento L_β percorre portanto todas as possibilidades de transformação linear de $\mathbb{F}$ para $\mathbb{K}$. □

Teorema 2.25. *Seja $\mathbb{F}$ uma extensão finita de $\mathbb{K} = \mathbb{F}_q$. Então para $\alpha \in \mathbb{F}$ nós temos $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q - \beta$ para algum $\beta \in \mathbb{F}$.*

Demonstração. ($\Leftarrow$) A demonstração é direta, considerando o item (v) do Teorema 2.23, já que se $Tr_{\mathbb{F}/\mathbb{K}}(\beta^q) = Tr_{\mathbb{F}/\mathbb{K}}(\beta)$ teremos pelo item (i) do mesmo Teorema $Tr_{\mathbb{F}/\mathbb{K}}(\beta^q - \beta) = Tr_{\mathbb{F}/\mathbb{K}}(\beta^q) - Tr_{\mathbb{F}/\mathbb{K}}(\beta) = Tr_{\mathbb{F}/\mathbb{K}}(\beta) - Tr_{\mathbb{F}/\mathbb{K}}(\beta)$.

($\Rightarrow$) Suponha $\alpha \in \mathbb{F} = \mathbb{F}_{q^m}$ com $Tr_{\mathbb{F}/\mathbb{K}}(\alpha) = 0$ e seja β uma raíz de $x^q - x - \alpha$ em alguma extensão de $\mathbb{F}$. Então $\beta^q - \beta = \alpha$ e

$$\begin{aligned} 0 &= Tr_\alpha = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta \end{aligned}$$

Portanto, $\beta \in \mathbb{F}$.

□

A composição da função traço segue uma regra que iremos mostrar no teorema a seguir.

Teorema 2.26. *Sejam $\mathbb{K}$ um corpo finito, $\mathbb{F}$ uma extensão de $\mathbb{K}$ e $\mathbb{E}$ uma extensão de $\mathbb{F}$. Então*

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

Demonstração. Sejam $\mathbb{K} = \mathbb{F}_q$, $[\mathbb{F} : \mathbb{K}] = m$ e $[\mathbb{E} : \mathbb{F}] = n$, então $[\mathbb{F} : \mathbb{K}] = mn$ pelo Teorema A.31 Então para $\alpha \in \mathbb{E}$ temos

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

□

Agora vamos definir outra aplicação linear importante para o nosso trabalho.

Definição 2.27. Para $\alpha \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, a norma $N_{\mathbb{F}/\mathbb{K}}(\alpha)$ de α sobre $\mathbb{K}$ é definido por

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

Esta aplicação possui algumas propriedades que veremos no teorema a seguir.

Teorema 2.28. *Sejam $\mathbb{K} = \mathbb{F}_q$ e $\mathbb{F} = \mathbb{F}_{q^m}$. Então a função norma $N_{\mathbb{F}/\mathbb{K}}$ satisfaz as seguintes propriedades:*

i) $N_{\mathbb{F}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{F}/\mathbb{K}}(\alpha)N_{\mathbb{F}/\mathbb{K}}(\beta); \forall \alpha, \beta \in \mathbb{F}$.

ii) $N_{\mathbb{F}/\mathbb{K}}$ *mapeia* $\mathbb{F}$ *em* $\mathbb{K}$ *e* $\mathbb{F}^*$ *para* $\mathbb{K}^*$.

iii) $N_{\mathbb{F}/\mathbb{K}}(\alpha) = a^m; \forall \alpha \in \mathbb{K}$.

iv) $N_{\mathbb{F}/\mathbb{K}}(\alpha^q) = N_{\mathbb{F}/\mathbb{K}}(\alpha); \forall \alpha \in \mathbb{F}$.

Demonstração. i)

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

como $\alpha, \beta \in \mathbb{F}_q$ e, $\mathbb{F}_q$ tem característica q, vale a igualdade:

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

ii) Pela propriedade i) temos que $N_{\mathbb{F}/\mathbb{K}}$ é um homomorfismo de grupo entre os grupos multiplicativos. Os elementos do núcleo de $N_{\mathbb{F}/\mathbb{K}}$ são exatamente as raízes do polinômio $x^{(q^m-1)\backslash(q-1)} - 1 \in \mathbb{K}[x]$ em $\mathbb{F}$, a ordem d do núcleo satisfaz $d \leq (q^m - 1)\backslash(q - 1)$. A imagem de $N_{\mathbb{F}/\mathbb{K}}$ tem ordem $q^m - 1\backslash(q - 1) \geq (q - 1)$. Segue que $N_{\mathbb{F}/\mathbb{K}}$ mapeia $\mathbb{F}^*$ para $\mathbb{K}^*$ e $\mathbb{F}$ para $\mathbb{K}$.

iii) Como $\alpha \in \mathbb{K}$, vale que $\alpha^q = \alpha$ (os conjugado de α em K são iguais a α), com isso pelo definição teremos

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

iv) Pelo item i) temos que $N_{\mathbb{F}/\mathbb{K}}(\alpha^q) = N_{\mathbb{F}/\mathbb{K}}(\alpha)^q = N_{\mathbb{F}/\mathbb{K}}(\alpha)$, isto porque $N_{\mathbb{F}/\mathbb{K}}(\alpha) \in \mathbb{K}$.

□

Teorema 2.29. *Sejam $\mathbb{K}$ um corpo finito e $\mathbb{F}$ uma extensão de $\mathbb{K}$ e $\mathbb{E}$ uma extensão de $\mathbb{F}$. Então*

$$N_{\mathbb{E}/\mathbb{K}}(\alpha) = N_{\mathbb{F}/\mathbb{K}} N_{\mathbb{E}/\mathbb{F}}(\alpha)); \forall \alpha \in \mathbb{E}.$$

Demonstração. Seja $\alpha \in \mathbb{E}$.

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

□

3 Corpo de Funções Algébricas

Neste capítulo, apresentamos as definições e resultados básicos da teoria da campos de funções algébricas: valorizações, lugares, divisores, o gênero de uma função campo, adeles, diferenciais de Weil e o teorema de Riemann-Roch [6].

Neste capítulo iremos denotar por K um corpo finito qualquer.

3.1 Lugares

Definição 3.1. Um corpo de funções F/K de uma variável sobre K é uma extensão $F \supseteq K$, tal que, F é uma extensão finita de $K(x)$ para algum elemento $x \in F$, onde x é transcendente em K [3].

Iremos utilizar a notação F/K para denotar os corpos de funções. Obviamente o conjunto $\bar{K} = \{z \in F | z \text{ é algébrico sobre } K\}$ é um subcorpo de F, pois a soma, produto e inversos de elementos algébricos são algébricos. $\bar{K}$ é chamado **corpo das constantes** de F/K. Temos que $K \subseteq \bar{K} \subsetneq F$ e, $F/\bar{K}$ é corpo de funções sobre $\bar{K}$. Dizemos que K é algebricamente fechado em F se $\bar{K} = K$.

Exemplo 3.2. O exemplo mais simples de corpo de funções é o corpo de funções racionais. F/K é chamado de racional se $F = K(x)$ para algum $x \in F$ transcende sobre K. Cada elemento $z \neq 0 \in K(x)$ possui uma representação única

$$z = a \prod_i p_i(x)^{n_i},$$

onde $a \neq 0 \in K$, os polinômios $p_i(x) \in K[x]$ são mônicos, distintos dois a dois, irredutíveis e $n_i \in \mathbb{Z}$.

Um corpo de funções arbitrário é frequentemente representado como uma extensão algébrica simples de um corpo de funções racionais $K(x)$, isto é, $F = K(x, y)$, onde $\phi(y) = 0$, para algum $\phi(T) \in K(x)[T]$ irredutível.

Iremos ver a seguir decomposições de elementos de um corpo de funções qualquer. Para isso iremos introduzir os conceitos de anel de valorização e lugares do corpo de funções. Além de zeros e polos dos elementos de um corpo de funções racionais.

Definição 3.3. Um anel de valorização do corpo de funções F/K é um anel $O \subset F$ que satisfaz as seguintes propriedades

i) $K \subsetneq O \subsetneq F$.

ii) $\forall z \in F$, $z \in O$ ou $z^{-1} \in O$.

Com esta definição, podemos construir o seguinte conjunto em $F = K(x)$. Seja $p(x) \in K[x]$ irredutível, defina:

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}$$

Veja que $\frac{f(x)}{p(x)}$, onde $f(x)$,$p(x)$ são elementos não nulos de $K[x]$, pertence a $K(x)$, mas tal elemento não pertence a $O_{p(x)}$ se $p(x)$ não divide $f(x)$. Além disso, seja $g(x) \in K[x]$ tal que $g(x)$ é irredutível e $mdc(g(x), p(x)) = 1$, então $\frac{1}{g(x)} \in O_{p(x)}/K$.

Portanto, $K \subsetneq O_{p(x)} \subsetneq F$.

Seja $z = \frac{f(x)}{g(x)} \in F = K(x)$ não nulo, então se $z \notin O_{p(x)} \Rightarrow p(x)|g(x)$. E como já podemos supor que $f(x)$ e $g(x)$ são relativamente primos, temos que $p(x)$ não divide $f(x)$; logo, $z^{-1} = \frac{g(x)}{f(x)} \in O_{p(x)}$.

Portanto $O_{p(x)}$ é um anel de valorização de $K(x)$.

Note ainda que se $p(x)$ e $g(x)$ são polinômios irredutíveis de $K[x]$ distintos, temos $O_{p(x)} \neq O_{g(x)}$, pois $\frac{1}{g(x)} \in O_{p(x)}$ e $\frac{1}{g(x)} \notin O_{g(x)}$.

Proposição 3.4. *Seja O um anel de valorização do corpo de funções F/K. Então:*

i) O tem um único ideal maximal $P = O/O^*$, onde

$$O^* = \{x \in O | \exists z \in O \text{ onde } x.z = 1\}.$$

ii) Para $x \in F$, não nulo, temos: $x \in P \Leftrightarrow x^{-1} \in O$.

iii) Para $\bar{K}$ o corpo de constantes de F/K, temos $\bar{K} \subseteq O$ e $\bar{K} \cap P = \{0\}$.

Demonstração. i) Primeiro seja $x \in P$ e $z \in O$, se $zx \in O^* \Rightarrow \exists w \in O$ onde $zxw = 1 \Rightarrow x(zw) = 1 \Rightarrow x \in O^*$.

Agora sejam $x, y \in P$. Considere $\frac{x}{y} \in F$, então $\frac{x}{y} \in O$ ou $\frac{y}{x} \in O$.

Se $\frac{x}{y} \in O \Rightarrow 1 + \frac{x}{y} \in O \Rightarrow x + y = y(1 + \frac{x}{y}) \in P$. Se $\frac{y}{x} \in O$ é análogo.

Portanto $x + y \in P$ onde temos que P é um ideal.

Mostremos agora que P é maximal.

Seja J um ideal onde $P \subsetneq J \subseteq O$. Tome $x \in J/P$. Então $x \in O^*$, pois $P = O \backslash O^*$, assim $xx^{-1} \in J$, pois J é um ideal. Logo $1 \in J \Rightarrow O \subset J \Rightarrow J = O$. Portanto P é maximal.

P é o único ideal maximal de O. De fato, seja J ideal maximal de O. Se J não contém unidades de O, então $J \subseteq P \Rightarrow J = P$, pois J é maximal. Agora se J possui uma unidade, então $J = O$.

Portanto P é o único ideal maximal próprio de O.

ii) $x \in P \Leftrightarrow x \in O/O^* \Leftrightarrow x \notin O^* \Leftrightarrow x^{-1} \notin O^*$.

iii) Seja $z \in \bar{K}$. Suponha que $z \notin O$. Então $z^{-1} \in O$ pois O é um anel de valorização. Como z^{-1} é algébrico sobre K, existem elementos $a_1, \ldots, a_r \in K$ com $a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 = 0$, consequentemente $z^{-1}(a_r(z^{-1})^{r-1} + \cdots + a_1) = -1$. Portanto $z = -(a_r(z^{-1})^{r-1} + \cdots + a_1 \in K[z^{-1}] \subseteq O$ então $z \in O$. Temos uma contradição pois assumimos que $z \notin O$. Mostramos assim que $\bar{K} \subseteq O$. A intersecção $\bar{K} \cap P = \{0\}$ é trivial.

□

Para mostrarmos o Teorema que virá a seguir, iremos considerar o seguinte lema, que não iremos provar.

Lema 3.5. *Sejam O um anel de valorização de F/K, P o ideal maximal de O e $x \in P$, tal que, $x \neq 0$. Sejam $x_1, \ldots, x_n \in P$, tais que, $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, \ldots, n-1$. Então $n \leq [F : K(x)] < \infty$.*

Teorema 3.6. *Seja O um anel de valorização do corpo de funções F/K e P o único ideal maximal de O. Então:*

i) P é ideal principal.

ii) Se $P = tO$, então $\forall z \in F$ $(z \neq 0)$, existe uma única representação na forma $z = t^n u$, para algum $n \in \mathbb{Z}$ e $u \in O^*$.

iii) O é um domínio de ideais principais. Mais que isso: se $P = tO$ e $\{0\} \neq I \subseteq O$ é um ideal, então $I = t^n O$, para algum $n \in \mathbb{Z}$.

Demonstração. i) Suponha que P não é principal e escolha $x_1 \in P$ não nulo. Como $P \neq x_1 O$, então existe $x_2 \in P \backslash x_1 O$. Então $x_2 x_1^{-1} \notin O$, pois $x_2 x_1^{-1} \in O \Rightarrow x_2 x_1^{-1} = o \Rightarrow x_2 = o x_1^{-1} \Rightarrow x_2 \in x_1 O$.

Isso implica que $x_2^{-1} x_1 \in P$ (Pela proposição 3.4, item ii)), onde temos $x_1 \in x_2 P$. Por indução temos uma sequência infinita $x_1, x_2, \cdots \in P$, tal que, $x_i \in x_{i+1}P, \forall i \geq 1$, contrariando o lema 3.5.

ii) Seja $z \in F$ $(z \neq 0)$, como $z \in O$ ou $z^{-1} \in O$, então podemos supor que $z \in O$, pois caso contrário basta fazer o mesmo raciocínio para $z^{-1} \in O$.

Se $z \in O^* \Rightarrow z = t^0 z$.

Se $z \notin O^* \Rightarrow z \in P$.

Como $z \in P = tO$, então temos que o conjunto $A = \{m \geq 1; z \in t^m O\} \neq \{\emptyset\}$.

Seja $m = maxA$. Veja que $m < \infty$, caso contrário iria contradizer o lema 3.5.

Assim $z \in t^m O \Rightarrow z = t^m u$, onde $u \in O^*$, pois se $u \notin O^*$, teríamos $u \in P \Rightarrow u = tw$, onde $w \in O \Rightarrow z = t^{m+1}w \in t^{m+1}O$. Contrariando a maximalidade de m.

Suponha agora que $z = t^m u = t^n v$, onde $m, n \in \mathbb{Z}$ e $u, v \in O^*$. Temos:

$$t^m u = t^n v \Rightarrow t^n(u - t^{n-m}v) = 0$$
$$\Rightarrow u = t^{n-m}v \Rightarrow t^{n-m} = uv^{-1} \in O^*$$

Portanto se $m \neq n$, temos $t \in O^*$ e assim $t \notin P$, gerando um absurdo. Assim $m = n$, e também $u = v$. Onde temos a unicidade da representação.

iii) Seja $\{0\} \neq I \subset O$ um ideal.

O conjunto $A = \{r \in \mathbb{N}; t^r \in I\} \neq \{\emptyset\}$ pois se $0 \neq x \in I$, então $x = t^r u$, com $u \in O^*$, assim $t^r = xu^{-1} \in I$.

Defina $n = minA$. Temos $I = t^n O$:

$I \supset t^n O$: como $t^n \in I \Rightarrow t^n O \subset I$.

$I \subset t^n O$: seja $y \in I$, não nulo, então $y = t^s w$ onde $w \in O^*$ e $s \geq 0$. Assim $t^s = yw^{-1} \in I$, logo, pela minimalidade de n, temos que, $s \geq n$. Portanto $y = t^n t^{s-n} w \in t^n O$.

□

Definição 3.7. 1. Um lugar P de um corpo de funções F/K é o ideal maximal de algum anel de valorização O de F/K. Todo $t \in P$ tal que $P = tO$ é chamado de um elemento primo de P (outras notações são parâmetro local ou variável uniforme).

2. $\mathbb{P}_F = \{P; P \text{ é um lugar de } F/K\}$.

Pelo item ii) da proposição 3.4, temos que dado O um anel de valorização de F/K e P seu ideal maximal, O é unicamente determinado por $P : O = \{z \in F; z^{-1} \notin P\}$. Assim $O_P = O$ é chamado de anel de valorização do lugar P.

Definição 3.8. Uma valorização discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

i) $v(x) = \infty \Leftrightarrow x = 0$.

ii) $v(xy) = v(x) + v(y), \forall x, y \in F$.

iii) $v(x + y) \geq min\{v(x), v(y)\}, \forall x, y \in F$.

iv) $\exists z \in F$, tal que , $v(z) = 1$.

v) $v(a) = 0, \forall a \in K$ não nulo.

Definição 3.9. Para todo lugar $P \in \mathbb{P}_F$ associamos uma função $v_p : F \to \mathbb{Z} \cup \{\emptyset\}$. Escolha t um elemento primo de P. Então para todo $z \in F$ não nulo, temos uma única representação $z = t^n u$ com $u \in O^*$ e $n \in \mathbb{Z}$. Defina $v_P(z) = n$ e $v_P(0) = \infty$.

Veja que a definição acima depende apenas de P, e não do t escolhido.

Teorema 3.10. *Seja F/K um corpo de funções:*

i) Para todo lugar $P \in \mathbb{P}_F$, a função v_P é uma valorização discreta de F/K. Mais que isso:

$$\begin{aligned} O_P &= \{z \in F; v_P(z) \geq 0\} \\ O_P^* &= \{z \in F; v_P(z) = 0\} \\ P &= \{z \in F; z > 0\} \end{aligned}$$

Um elemento $x \in F$ é primo de P, se e somente se, $v_P(x) = 1$.

ii) Recíprocamente, se v é uma valorização discreta de F/K, então o conjunto $P = \{z \in F; v(z) > 0\}$ é um lugar de F/K, e $O_P = \{z \in F; v(z) \geq 0\}$ é o seu anel de valorização correspondente.

iii) Qualquer anel de valorização O de F/K é um subanel maximal próprio de F.

Demonstração. i) Temos que v_P é bem definido.

A propriedade 1, segue da definição.

A propriedade 2 de valorização discreta, segue do fato que $v_p(xy) = v_P(t^n u_1 t^m u_2) = v_P(t^{n+m} u_1 u_2) = n + m = v_P(x) + v_P(y)$.

A propriedade 3: sejam $x, y \in F$ com $v_P(x) = n$ e $v_P(y) = m$. Sem perda de generalidade podemos supor $n \leq m \leq \infty$. Assim, temos $x = t^n u_1$ e $y = t^m u_2$, com $u_1 u_2 \in O_P^*$. Então $x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n} u_2) = t^n z$, com $z \in O_P$.

Se $z = 0$: $v_P(x + y) = \infty > min\{n, m\} = min\{v_P(x), v_P(y)\}$.

Se $z \neq 0 : z = t^k u$, com $0 \leq k \in \mathbb{Z}$ e $u \in O^*$. Então,

$$v_P(x + y) = v_P(t^{n+k} u) = n + k \geq n = min\{v_P(x), v_P(y)\}.$$

Agora se $x = 0$ ou $y = 0$, então $v_P(x + y) = v_P(y) = min\{v_P(x), v_P(y)\}$, quando $y \neq 0$, e $v_P(x + y) = v_P(x) = min\{v_P(x), v_P(y)\}$, quando $x \neq 0$.

Quanto a propriedade 4 de valorização discreta, observe que pela definição $v_P(t) = 1$.

Por último a propriedade 5: seja $0 \neq a \in K \subset O^* \subset O$. Então $v_P(a) = v_P(t^0 a) = 0$.

Quanto aos conjuntos temos:

$O_P = \{z \in F; v_P(z) \geq 0\}$: se $z \in O_P$, então, se z é nulo temos $v_P(z) = \infty > 0$, e se z é não nulo temos $v_P(z) = v_p(t^n u) = n$ onde $0 \leq n \in \mathbb{Z}$ e $u \in O^*$. Se $z \in F$ e $v_P(z) \geq 0$, temos:

($\star$) se $v_P(z) = 0 \Leftrightarrow z \in O^*$.

($\star\star$) se $v_P(z) = \infty \Leftrightarrow z = 0 \in P \subset O_P$ e se $v_P(z) = n > 0 \Leftrightarrow z = t^n u$, $0 < n \in \mathbb{Z}$ e $u \in O^* \Leftrightarrow z \in tO = P \subset O_P$.

Observe que $O_P^* = \{z \in F; v_P(z) = 0\}$ segue de ($\star$).

E $P = \{z \in F; v_P(z) > 0\}$ segue de ($\star\star$).

Se $x \in F$ é primo em P, então vimos que a definição independe do parâmetro local t, onde temos que $v_P(x) = v_P(t) = 1$.

ii) Segue da verificação das propriedades desses conjuntos e usando que se $x \in F$ então $v_P(x) = -v_P(x^{-1})$.

iii) Sejam O um anel de valorização, P seu ideal maximal, v_P a valorização discreta de P e $z \in F/O$.

Seja também $y \in F$. Como $z \notin O \Rightarrow z^{-1} \in O$, além disso, $z^{-1} \notin O^* \Rightarrow v_P(z^{-1}) > 0$.

Veja que $v_P(yz^{-k}) = v_P(y) + kv_P(z^{-1})$.

Assim para $k \geq 0$ suficientemente grande, $v_P(yz^{-k}) \geq 0 \Rightarrow yz^{-k} \in O$. Defina $w = yz^{-k} \in O$, temos assim $y = wz^k \Rightarrow F = O[z]$.

Portanto O é maximal.

□

Definição 3.11. Seja $P \in \mathbb{P}_F$.

1. $F_P = \frac{O_P}{P}$ é o corpo das classes residuais módulo P. A aplicação $x \mapsto x(P)$ de F e $F_P \cup \{\infty\}$ é chamada aplicação classe residual com respeito a P. E também podemos denotar $x + P = x(P), \forall x \in O_P$.

2. $gr(P) = [F_P : K]$ é chamado grau de P.

Proposição 3.12. *Se P é um lugar de F/K e $0 \neq x \in P$, então:*

$$gr(P) \leq [F : K(x)] < \infty.$$

Demonstração. Temos que $x \in P$ não nulo é transcendente, pois $\bar{K} \cap P = \{0\}$ segue que $[F : K(x)] < \infty$.

Sejam $z_1, \ldots, z_n \in O_P$ tais que $z_1(P), \ldots, z_n(P) \in \frac{O_P}{P}$ sejam linearmente independentes sobre K . Mostremos que $z_1, \ldots, z_n \in F$ são linearmente independentes sobre $K(x)$.

Suponhamos que sejam linearmente dependentes, assim tomemos uma combinação linear não trivial:

$$0 = \sum_{i=1}^{n} \Phi_i z_i, \text{ onde } \Phi_i \in K(x), i = 1, 2, \ldots, n$$

Sem perda de generalidade, podemos supor que $\Phi_i \in K[x], \forall i$, e que x não divide Φ_i, ou seja, $\exists j \in \{1, \ldots, n\}$ onde $\Phi_j = a_j + xg_j$ com $a_j \in K$ não nulo.

Como $x \in P$ e $g_i \in K[x] \subset O_P$, então, $\forall i$, temos:

$$\Phi_i(P) = a_i(P) + xg_i(P) = a_i(P) + 0(P) = a_i(P) = a_i.$$

Assim

$$0 = 0(P) = (\sum_{i=1}^{n} \Phi_i z_i)(P) = \sum_{i=1}^{n} \Phi_i(P) z_i(P) = \sum_{i=1}^{n} a_i(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P)$$

onde os a_i não são todos nulos.

Temos que $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K, gerando uma contradição. Portanto $gr(P) = [F_P : K] \leq [F : K(x)] < \infty$. □

Corolário 3.13. *O corpo das constantes $\bar{K}$ de F/K é uma extensão corpos finita de K, ou seja, $[\bar{K} : K] < \infty$.*

No caso em que $gr(P) = 1$, temos que $F_P = K$, e a aplicação classe residual leva F em $K \cup \{\infty\}$. Em particular, se K é algebricamente fechado, então todo lugar de F tem grau 1. De fato, se K é algebricamente fechado, então toda extensão algébrica é trivial $\Rightarrow [F_P : K] = 1, \forall P \in \mathbb{P}_F$.

Assim podemos ver $z \in F$ como a função

$$z : \mathbb{P}_F \to K \cup \{\infty\}, \text{ tal que } P \mapsto z(P)$$

Daí o porquê F/K é chamado corpo de funções. Os elementos de K visto como funções do tipo acima são funções constantes, pois se, $P_1, P_2 \in \mathbb{P}_F$, então $k(P_1) = k(P_2) = k$. Por isso K é chamado corpo de constantes de F.

Definição 3.14. Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se, e somente se, $v_P(z) > 0$. P é um polo de z se, e somente se, $v_P(z) < 0$. Se $v_P(z) = m > 0$ P é dito um zero de z de ordem m. Se $v_P(z) = -m < 0$, P é dito polo de z de ordem m.

Com isso, definimos os conceitos e enunciamos os resultados que utilizaremos para construção dos códigos algébricos geométricos.

3.2 Corpo de Funções Racionais

Nesta seção iremos investigar o corpo de funções racionais $F = K(x)$, onde x é transcendente sobre K.

Considere um polinômio mônico e irredutível $p(x) \in K[x]$ e o anel de valorização:

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}$$

de $K(x)/K$ com seu ideal maximal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) | f(x), p(x) \text{ não divide } g(x) \} \right\}$$

No caso de $p(x)$ linear, isto é, $p(x) = x - \alpha$ com $\alpha \in K$, escrevemos $P_\alpha = P_{p(x)} \in \mathbb{P}_F$. Existe outro anel de valorização de $K(x)/K$:

$$O_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], gr(f(x)) \leq gr(g(x)) \right\}$$

com ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], gr(f(x)) < gr(g(x)) \right\}$$

P_∞ é chamado lugar infinito de $K(x)$. Observe que este rótulo depende da escolha do elemento gerador $x \in K(x)$. Por exemplo, $K(x) = K(\frac{1}{x})$ pois $x^{-1} = \frac{1}{x}$, e o lugar infinito com respeito a $\frac{1}{x}$ é o lugar P_0 com respeito a x.

3.3 Divisores

O corpo de constantes $\tilde{K}$ de F/K é uma extensão finita de K, e F pode ser visto como corpo de funções sobre $\tilde{K}$. Iremos agora utilizar a notação F/K para denotar um corpo de funções de uma variável tal que $\tilde{K} = K$.

Definição 3.15. O grupo de divisores de F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K, denotado por $Div(F)$. Os elementos de $Div(F)$ são chamados divisores de F/K. Ou seja, um divisor é uma soma

$$D = \sum_{P \in \mathbb{P}_F} n_P P$$

com $n_P \in \mathbb{Z}$, quase todos nulos.

Definição 3.16. O suporte de D é definido como

$$supp(D) = \{P \in \mathbb{P}_F | n_p \neq 0\}.$$

Podemos também escrever o divisor como

$$D = \sum_{P \in S} n_P P,$$

onde $S \subseteq \mathbb{P}_F$ é finito com $supp(D) \subseteq S$.

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado **divisor primo**. Considere $D = \sum n_P P$ e $D' = \sum n'_P P$ a soma de divisores é definida como

$$D + D' = \sum (n_P + n'_P) P$$

O elemento neutro do grupo de divisores $Div(F)$ é o divisor $0 = \sum_{P\in\mathbb{P}_F} r_P P$, onde $r_p = 0, \forall P \in \mathbb{P}_F$.

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P\in\mathbb{P}_F} n_P P \in Div(F)$, definimos $v_Q(D) = n_Q$. Assim $supp(D) = \{P \in \mathbb{P}_F | v_P(D) \neq 0\}$ e $D = \sum_{P\in\mathbb{P}_F} v_P(D)P$.

Com isso definimos uma ordem parcial para os divisores de F:

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2), \forall P \in \mathbb{P}_F.$$

Definição 3.17. Um divisor $D \geq 0$ é chamado positivo ou **efetivo**.

Definição 3.18. O grau de um divisor é definido por $gr(D) = \sum_{P\in\mathbb{P}_F} v_P(D)gr(P)$.

Um elemento $x \in F$ não nulo tem somente uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Assim podemos definir:

Definição 3.19. Sejam $x \neq 0 \in F$ e Z(respectivamente N) o conjunto de zeros(respectivamente pólos) de x em $\mathbb{P}_F$. Definimos

$$(x)_0 = \sum_{P\in Z} v_P(x)P, \text{ o divisor de zeros de } x.$$

$$(x)_\infty = \sum_{P\in N} (-v_P(x))P, \text{ o divisor de pólos de} x.$$

$$(x) = (x)_0 - (x)_\infty \text{ o divisor principal de } x.$$

Veja que $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e $(x) = \sum_{P\in\mathbb{P}_F} v_P(x)P$.

Definição 3.20. O conjunto dos divisores $Princ(F) = \{(x)/0 \neq x \in F\}$ é chamado de *conjunto de divisores principais* de F/K.

Note que $(xy) = (x) + (y), \forall x, y \in F$ não nulos, temos então que $Princ(F)$ é subgrupo de $Div(F)$.

Dois divisores $D, D' \in Div(F)$ são chamados de *divisores equivalentes* se $D = D' + (x)$, para algum $(x) \in Princ(F)$.

Definição 3.21. Para um divisor $A \in Div(F)$, definimos o espaço de Riemann-Roch associado a A por:

$$\mathcal{L}(A) = \{x \in F | (x) \geq -A\} \cup \{0\}.$$

Podemos interpretar essa definição analogamente como o conjunto de $(x) \in F$, tal que, $(x) + A$ é efetivo.

Teorema 3.22. *Seja $A \in Div(F)$, então:*

i) $\mathcal{L}(A)$ *é um espaço vetorial sobre* K*.*

ii) Se $A^{'}$ *é um divisor equivalente a* A*, então* $\mathcal{L}(A) \cong \mathcal{L}(A^{'})$*. (Isto é, são isomorfos como espaços vetoriais sobre* K*.)*

Demonstração. i) Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$, temos $v_P(x+y) \geq min\{v_P(x), v_P(y)\} \geq -v_P(A)$ e $v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A), \forall P \in \mathbb{P}_F$, logo, $x + y \in \mathcal{L}(A)$ e $ax \in \mathcal{L}(A)$.

ii) Como $A \equiv A^{'} \Rightarrow A - A^{'} \in Princ(F)$, logo existe $z \in F$ não nulo onde $A = A^{'} + (z)$. Assim considere a aplicação $\phi : \mathcal{L}(A) \to F$, onde, $x \mapsto \phi(x) = zx$. Veja que se $x, y \in \mathcal{L}(A)$ e $a \in K$ então $\phi(x + ay) = (x + ay)z = xz + ayz = \phi(x) + a\phi(y)$. Logo ϕ é K-linear. Veja que $\phi(x) \in \mathcal{L}(A^{'})$. De fato,

$$x \in \mathcal{L}(A) \Rightarrow (x) \geq -A \Rightarrow (x) \geq -(A^{'} + (z)) \Rightarrow (x) \geq -A^{'} - (z) \Rightarrow$$
$$\Rightarrow v_P(x) \geq -v_P(A^{'} + (z)), \forall P \in \mathbb{P}_F \Rightarrow v_P(x) \geq -v_P(A^{'}) - v_P(z), \forall P \in \mathbb{P}_F$$

Logo, $v_P(xz) = v_P(x) + v_P(z) \geq -v_P(A^{'}) - v_P(z) + v_P(z) = -v_P(A^{'}), \forall P \in \mathbb{P}_F$. Portanto $xz \in \mathcal{L}(A^{'})$. De forma análoga definindo $\phi^{'} : \mathcal{L}(A^{'}) \to F$, tal que, $x \mapsto xz^{-1}$, temos $\phi^{'}$ K-linear e $\phi^{'}(\mathcal{L}(A^{'})) \subset \mathcal{L}(A)$. Como ϕ e $\phi^{'}$ são inversas, temos que ϕ estabelece um isomorfismo entre $\mathcal{L}(A)$ e $\mathcal{L}(A^{'})$.

□

Lema 3.23. *i)* $\mathcal{L}(0) = K$*.*

ii) Se $A < 0$*, então* $\mathcal{L}(A) = \{0\}$*.*

Demonstração. i) Veja que $\forall x \in K$ não nulo, $(x) = 0 \Rightarrow (x) \geq -0 = 0 \Rightarrow x \in \mathcal{L}(0) \Rightarrow K \subset \mathcal{L}(0)$. A última implicação acontece pelo fato de que $0 \in \mathcal{L}(0)$. Seja agora $x \neq 0 \in \mathcal{L}(0) \Rightarrow (x) \geq -0 = 0$, ou seja, $v_P(x) \geq 0, \forall P \in \mathbb{P}_F \Rightarrow x$ não tem pólos, isto é, $x \in \tilde{K} = K \Rightarrow \mathcal{L}(0) \subset K$.

Portanto, $\mathcal{L}(0) = K$.

ii) Suponha por absurdo que $\exists x \in \mathcal{L}(A)$ não nulo. Assim $(x) \geq -A \Rightarrow (x) > 0$. Daí, $v_P(x) > 0, \forall P \in \mathbb{P}_F$, ou seja, x tem zeros mas não tem pólos, absurdo!

□

A partir daqui enunciaremos alguns resultados para construção da teoria, porém omitiremos algumas demonstrações, que podem ser encontradas em [3].

Lema 3.24. *Sejam* $A, B \in Div(F)$ *com* $A \leq B$*. Então* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e* $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq gr(B) - gr(A)$*.*

Proposição 3.25. *Para cada divisor $A \in Div(F)$, $\mathcal{L}(A)$ é um espaço vetorial de dimensão finita sobre K.*

Definição 3.26. Seja $A \in Div(F)$, o inteiro $l(A) = dim(\mathcal{L}(A))$ é chamado de dimensão do divisor A.

Teorema 3.27. *Todo divisor principal tem grau zero. Mais precisamente: seja $x \in F/K$ e $(x)_0$, respectivamente $(x)_\infty$, o divisor de zeros, respectivamente o divisor de polos de x. Então: $gr(x)_0 = gr(x)_\infty = [F : K(x)]$.*

Definição 3.28. O gênero g de F/K é definido por

$$g = max\{gr(A) - l(A) + 1; A \in Div(F)\}.$$

Corolário 3.29. *O gênero de F/K é não negativo.*

Demonstração. veja que $gr(0) - l(0) + 1 = 0 \Rightarrow g \geq 0$. □

Exemplo 3.30. Em um corpo de funções racionais $K(x)/K$, temos que $g = 0$.

Sejam P_∞ polo de x e $r \geq 0$ inteiro, considere o espaço vetorial $\mathcal{L}(rP_\infty)$. Veja que $\{1, x, \ldots, x^r\} \subset \mathcal{L}(rP_\infty)$, daí $1 + r \leq l(rP_\infty) = gr(rP_\infty) + 1 - g$, para r suficientemente grande. Temos $g \leq 0$, e portanto pelo corolário acima $g = 0$.

3.4 Teorema de Riemann-Roch

Nesta seção, F/K denota um corpo de funções algébricas de gênero g. Mais detalhes podem ser vistos em [5]

Definição 3.31. Para $A \in Div(F)$, o inteiro

$$i(A) = l(A) - gr(A) + g - 1$$

é chamado **índice de especialidade** de A.

O teorema de Riemann nos diz que $i(A)$ é um inteiro não negativo e que $i(A) = 0$ para $gr(A)$ suficientemente grande.

Definição 3.32. Um *adele* de F/K é uma aplicação $\alpha : \mathbb{P}_F \to F$, $P \mapsto \alpha_P$, tal que $\alpha_P \in O_P$ para quase todo $P \in \mathbb{P}_\mathbb{F}$.

Consideramos um adele como um elemento do produto direto $\prod_{P \in \mathbb{P}_\mathbb{F}} F$ e portanto usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_\mathbb{F}}$, ou ainda menor, $\alpha = (\alpha_P)$.

O conjunto $\mathcal{A}_F = \{\alpha; \alpha$ é um adele de $F/K\}$ é chamado de espaço adele de F/K. Este conjunto é considerado um espaço vetorial sobre K. O adele principal de um elemento

$x \in F$ é o adele cuja totalidade das componentes são iguais a x, o qual faz sentido, pois x tem no máximo finitos polos.

A definição de adele principal nos fornece um mapeamento $F \mapsto \mathcal{A}_F$, e a função valorização v_p de F/K é naturalmente extendida para $\mathcal{A}_F$ por $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a P-componente do adele α. Por definição, temos $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

Definição 3.33. Para $A \in Div(F)$ definimos:

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F; v_P(\alpha) \geq -v_P(A), \forall P \in \mathbb{P}_F$$

o K-espaço de $\mathcal{A}_F$.

Teorema 3.34. *Para cada $A \in Div(F)$, o índice de especialidades de A é dado por:*

$$i(A) = dim(\mathcal{A}_F/\mathcal{A}_F(A) + F).$$

Demonstração. Ver em [6, Pags. 35-36]. □

Corolário 3.35.

$$g = dim(\mathcal{A}_F/\mathcal{A}_F(0) + F).$$

Demonstração.

$$dim(\mathcal{A}_F/\mathcal{A}_F(0) + F) = i(0) = l(0) - gr(0) + g - 1 = g$$

isto porque $l(0) = 1$ e $gr(0) = 0$. □

Podemos então escrever:

$$l(A) = gr(A) + 1 - g + dim(\mathcal{A}_F/\mathcal{A}_F(A) + F)$$

4 Códigos Algébricos Geométricos

Os códigos algébricos geométricos, que chamaremos de códigos AG, foram introduzidos por Valerii Denisovich Goppa em seu livro *Geometry and codes* publicado em 1988. Esta classe de códigos é muitas vezes chamada de códigos de Goppa.Como uma motivação para a construção desses códigos, primeiro consideramos Reed-Solomon códigos sobre o corpo finito $\mathbb{F}_q$, onde q é uma potência de um primo. Essa importante classe de códigos é bem conhecida na teoria dos códigos. Os códigos algébricos geométricos são uma generalização natural do Código de Reed-Solomon [3].

4.1 Códigos AG

Vamos primeiramente construir o Reed-Solomon generalizado, através de uma aplicação linear, sobre um corpo finito $\mathbb{F}_q$.

Sejam $n = q - 1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^*$, isto é, $\mathbb{F}_q^\times = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Para um inteiro k com $1 \leq k \leq n$ considere o k-dimensional espaço vetorial

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[X] | gr(f) \leq k - 1\}$$

e a aplicação avaliação, **ev**: $\mathcal{L}_k \to \mathbb{F}_q^n$, definida como

$$ev(f) = (f(\beta), f(\beta^2), \ldots, f(\beta^n)) \in \mathbb{F}_q^n.$$

Note que esta aplicação é $\mathbb{F}_q$-linear, basta mostrar que $ev(f + g) = ev(f) + ev(g)$ onde $f, g \in \mathbb{F}_q[X]$ e que $ev(\alpha f) = \alpha ev(f)$ com $\alpha \in \mathbb{F}_q$. A primeira igualdade acontece pelo fato de que em $\mathbb{F}_q[X]$ vale $(f + g)(x) = f(x) + g(x)$, portanto, basta que separemos termo a termo e reorganizemos obtendo $ev(f) + ev(g)$, já a segunda igualdade ocorre pelo fato de $(\alpha f)(x) = \alpha f(x)$, portanto colocando α em evidência concluímos que valem as duas igualdades e portanto a aplicação ev é, de fato, $\mathbb{F}_q$-linear.

Além disso a aplicação é também injetiva, isto porque um polinômio não nulo $f \in \mathbb{F}_q[X]$ de grau $< n$ possui menos que n raízes distintas. Com isso garantimos que a aplicação ev define um $[n, k]$-código

$$C_k = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) | f \in \mathcal{L}_k\}.$$

Este código é um RS código (Reed-Solomon código). O peso das palavras $c \neq 0 = ev(f) \in C_k$ é dado por

$$\begin{aligned} \omega(c) &= n - |\{i \in \{1, \ldots, n\}; f(\beta^i) = 0\}| \\ &\geq n - gr(f) \geq n - (k - 1). \end{aligned}$$

Portanto a distância mínima d de C_k satisfaz $d \geq n+1-k$, por outro lado, a cota de Singleton nos garante que $d \leq n+1-k$ portanto $d = n+1-k$, sendo dessa forma um código MDS sobre $\mathbb{F}_q$.

Para introduzirmos a noção de códigos algébricos geométricos, fixaremos as seguintes notações:

- $F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
- $P_1, P_2, \ldots, P_n$ são lugares distintos dois a dois de $F\backslash\mathbb{F}_q$ de grau 1.
- $D = P_1 + P_2 + \cdots + P_n$.
- G é um divisor de $F/\mathbb{F}_q$, tal que, supp$G \cap$ supp$D = \emptyset$.

Definição 4.1. Um código algébrico geométrico (ou código AG) $C_{\mathcal{L}}(D, G)$ associado aos divisores D e G é definido por

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Note que esta definição faz sentido, pois para $f \in \mathcal{L}(G)$ temos $v_{P_i}(f) \geq 0$ $(i = 1, \ldots, n)$, pois supp $G \cap$ supp $D = \emptyset$. A classe residual $f(P_i)$ de f módulo P_i é um elemento do corpo da classe residual de P_i. Como $gr(P_i) = 1$, esse corpo de classes residuais é $\mathbb{F}_q$, portanto $f(P_i) \in \mathbb{F}_q$.

Assim como no exemplo inicial, consideremos a aplicação avaliação $\mathbf{ev}_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ dada por

$$ev_D(x) = (x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n.$$

Esta aplicação é $\mathbb{F}_q$-linear, analogamente ao que fizemos no caso do Reed-Solomon e, $C_{\mathcal{L}}(D, G)$ é a imagem de $\mathcal{L}(G)$ sob esta aplicação. Veja que a construção do código de Reed-Solomon generalizado é um caso particular desta definição, escolhendo apropriadamente o corpo de funções e os divisores. O teorema a seguir nos mostrará porque estes códigos são interessantes, pois podemos calcular seus parâmetros através do Teorema de Riemann-Roch e, além disso, conseguimos obter uma cota inferior para a distância mínima.

Teorema 4.2. *$C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código com parâmetros*

$$k = l(G) - l(G - D) \text{ e } d \geq n - gr(G).$$

Demonstração. A aplicação avaliação é um mapeamento linear e sobrejetivo de $\mathcal{L}(G)$ para $C_{\mathcal{L}}(D, G)$ com núcleo

$$Nuc(ev_D) = \{f \in \mathcal{L}(G) | v_{P_i}(f) > 0 \text{ para } i = 1, \ldots, n\} = \mathcal{L}(G - D).$$

Segue do *teorema do núcleo e da imagem* que $k = \dim C_{\mathcal{L}}(D,G) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D) = l(G) - l(G-D)$. A afirmação sobre a distância mínima d faz sentido somente se considerarmos $C_{\mathcal{L}}(D,G) \neq 0$, portanto assumiremos isto. Tome um elemento $f \in \mathcal{L}(G)$ com $\omega(ev_D(f)) = d$. Então exatos $n-d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ no suporte de D são zeros de f, então

$$f \neq 0 \in \mathcal{L}(G - (P_{i_1}, \ldots, P_{i_{n-d}})).$$

Concluímos então que

$$0 \leq gr(G - (P_{i_1}, \ldots, P_{i_{n-d}})) = gr(G) - n + d$$

Portanto $d \geq n - gr(G)$. □

Corolário 4.3. *Suponha que o $gr(G) < n$. Então a avaliação $\boldsymbol{ev}_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ é injetora, e temos:*

i) $C_{\mathcal{L}}(D,G)$ é um $[n,k,d]$-código com

$$d \leq n - gr(G) \text{ e } k = l(G) \geq gr(G) + 1 - g$$

Portanto

$$k + d \geq n + 1 - g.$$

ii) Se $2g - 2 < gr(G) < n$ então $k = gr(G) + 1 - g$.

iii) Se $\{f_1, f_2, \ldots, f_n\}$ é uma base de $\mathcal{L}(G)$ então a matriz

$$M = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \ldots & \ldots & \ddots & \ldots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{pmatrix}$$

é a matriz geradora do código $C_{\mathcal{L}}(D,G)$.

4.2 Curvas Planas Maximais

Antes de falarmos sobre os códigos Hermitianos, é necessário definir o que é a curva Hermitiana, mostrando porque ela é uma curva maximal. Para isso, iremos definir alguns conceitos da teoria de geometria algébrica, para que mostremos que, de fato, estaremos trabalhando com uma curva maximal, o que torna nosso trabalho mais interessante. Para maiores informações sobre este tipo de curva ver [4], [8], [3].

Nesta seção denotaremos por $\bar{K}$ o fecho algébrico de K.

Definição 4.4. Uma curva algébrica plana é o lugar dos pontos cujas coordenadas cartesianas satisfazem uma equação do tipo:

$$f(x_1, \ldots, x_n) = 0$$

Onde f é um polinômio não constante.

Definição 4.5. Um polinômio $K(x, y)$ é homogêneo se todos os seus monômios possuírem mesmo grau, ou seja,

$$K(x, y) = \sum_{i=0}^{m} \alpha_i x^i y^{m-i},$$

onde $\alpha_i \in K$, para, $i = 0, 1, \ldots, m$.

Definição 4.6. Uma curva algébrica projetiva é o lugar dos pontos cujas coordenadas satisfazem uma equação do tipo:

$$F(x_1 : \cdots : x_n : x_{n+1}) = 0.$$

Onde F é um polinômio homogêneo não constante.

Definição 4.7. Considere uma curva projetiva C, definida por um polinômio $F \in \mathbb{F}_q[X, Y]$, dizemos que C é não-singular se para qualquer $P \in C$, $F_X(P)$ ou $F_Y(P)$, as derivadas parciais de F, não se anulam simultaneamente.

Seja C uma curva algébrica projetiva não-singular definida sobre um corpo finito $K = \mathbb{F}_q$. Um resultado de Weil [7], diz que vale a seguinte desigualdade:

$$|C(\mathbb{F}_q)| \leq 1 + q + 2g\sqrt{q}$$

onde g é o gênero da curva C. Quando há igualdade, dizemos que a curva é maximal.

Exemplo 4.8. A curva hermitiana é uma curva maximal. De fato:

Considere a curva projetiva associada ao polinômio $f(X, Y) = Y^q + Y - X^{1+q} \in \mathbb{F}_q[X, Y]$, onde $\mathbb{F}_q$ é o corpo finito de cardinalidade $q = p^{2n}$ com $n \in \mathbb{N}$.

O polinômio homogêneo associado $F(X, Y, Z)$ é dado por

$$F(X, Y, Z) = Z\dot{Y}^q + Z^q\dot{Y} - X^{1+q}.$$

Podemos verificar que C é não-singular. Primeiramente devemos calcular as derivadas parciais do polinômio homogêneo acima.

$$\begin{array}{rcccl} F_X(X, Y, Z) & = & -(1+q)X^q & = & -X^q \\ F_Y(X, Y, Z) & = & qZY^{q-1} + Z^q & = & Z^q \\ F_Z(X, Y, Z) & = & Y^q + qZ^{q-1}Y & = & Y^q \end{array}$$

Para verificarmos se todos os pontos da curvas são não-singular, devemos resolver o seguinte sistema

$$\begin{cases} -(1+q)X^q &= 0 \quad (1) \\ qZY^{q-1} + Z^q &= 0 \quad (2) \\ Y^q + qZ^{q-1}Y &= 0 \quad (3) \end{cases}$$

Observe que da equação (1), temos que $X = 0$. Da equação (2) temos que $Z = 0$, pois como a curva é definida em $\mathbb{F}_q$, temos que, $qZY^{q-1} = 0$. Analogamente, de (3) concluímos que $Y = 0$. Portanto a curva é não-singular.

Em [9] encontramos uma fórmula para o gênero de curvas de grau d não-singulares, sendo ela

$$g = \frac{(d-1)(d-2)}{2} = \frac{p^n\dot{(}p^n - 1)}{2} = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$$

Para contarmos os pontos da curva, primeiramente olhamos para a sua parte afim, denotaremos por $C_a(\mathbb{F}_q)$ o conjunto dos pontos afins da curva.

Com isso, os pontos que satisfazem $f(X,Y) = 0$ são os pontos tais que $Tr(y) = N(x)$, onde Tr e N são as funções traço e norma, de $\mathbb{F}_{p^{2n}}$ para $\mathbb{F}_{p^n}$, respectivamente. Usando o fato de que a função traço e norma tem como imagem o corpo $\mathbb{F}_{p^n}$ e como o traço é $\mathbb{F}_{p^n}$-linear e satisfaz que $|Tr^{-1}(y)| = p^n, \forall y \in \mathbb{F}_{p^n}$, obtemos

$$\begin{aligned} |C_a(\mathbb{F}_q)| &= \textstyle\sum_{x\in\mathbb{F}_q} |\{y \in \mathbb{F}_q | Tr(y) = x^{1+p^n}\}| \\ &= \textstyle\sum_{x\in\mathbb{F}_q} |Tr^{-1}(x^{1+p^n})| \\ &= \textstyle\sum_{x\in\mathbb{F}_q} p^n = p^{2n}p^n = p^{3n} \end{aligned}$$

A curva hermitiana possui apenas o ponto $(0:1:0)$ no infinito. De fato, se tomarmos $Z = 0$ na equação da curva e fizermos $F(X,Y,Z) = 0$, teremos que $-X^{1+q} = 0 \Rightarrow X = 0$, e dessa forma Y é arbitrário. Portanto, temos que

$$|C(\mathbb{F}_q)| = 1 + p^{3n}$$

Como

$$1 + q + 2g\sqrt{q} = 1 + p^{3n}$$

Com isso concluímos que a curva hermitiana é maximal sobre $\mathbb{F}_q$ com $q = p^{2n}$.

Podemos estabelecer uma equivalência entre os lugares de grau 1 com os pontos racionais de uma curva algébrica. Dessa forma, os lugares no infinito definidos na seção anterior, serão equivalentes aos pontos no infinito denotados nesta seção. Esta equivalência está verificada em [11].

4.3 Códigos AG sobre a curva Hermitiana

Nesta seção iremos mostrar uma construção de códigos algébricos geométricos sobre uma classe especial de curvas chamadas curvas Hermitianas. Esta classe de códigos são exemplos interessantes de códigos AG, porque a curva Hermitiana é uma curva maximal, e este tipo de curvas tem se mostrado fundamentais para a obtenção de códigos AG com bons parâmetros [3].

Primeiramente, vamos relembrar algumas propriedades do corpo de funções $\mathcal{H}$ da curva Hermitiana. $\mathcal{H}$ é o corpo de funções sobre $\mathbb{F}_{q^2}$ e pode ser representado por

$$\mathcal{H} = \mathbb{F}_{q^2}(x, y)$$

com equação afim dada por

$$y^q + y = x^{q+1}$$

O gênero de $\mathcal{H}$ é $g = q(q-1)/2$, e $\mathcal{H}$ tem $N = 1 + q^3$ lugares de grau um, sendo eles:

1. O único polo comum Q_∞ de x e y.
2. Os pares $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, com isso há um único lugar $P_{\alpha,\beta} \in \mathbb{P}_H$ tal que $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.
3. $v_{P_\infty}(x) = -(q)$ e $v_{P_\infty}(y) = -(q+1)$.

Observe que para todo $\alpha \in \mathbb{F}_{q^2}$, existe q elementos distintos $\beta \in \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, este número é a fibra da função norma. Portanto o número de lugares $P_{\alpha,\beta}$ é q^3.

Definição 4.9. Para $r \in \mathbb{Z}$ definimos o código

$$C_r = C_{\mathcal{L}}(D, rQ_\infty),$$

onde

$$D = \sum_{\beta^q + \beta = \alpha^{q+1}} P_{\alpha,\beta}$$

é a soma de todos os lugares de grau um (exceto Q_∞) do corpo de funções Hermitiano $\mathcal{H}/\mathbb{F}_{q^2}$. Os códigos C_r são chamados códigos Hermitianos.

Os códigos Hermitianos possuem comprimento $n = q^3$ sobre o corpo $\mathbb{F}_{q^2}$. Para $r \leq s$ nós temos, claramente, que $C_r \subseteq C_s$. Primeiramente vejamos alguns casos triviais. Para $r < 0$, $\mathcal{L}(rQ_\infty) = 0$ e consequentemente $C_r = 0$. Para $r > q^3 + q^2 - q - 2 = q^3 + (2g-2)$, o teorema 4.2 e o teorema de Riemann-Roch nos garante que

$$\begin{aligned} dim\ C_r &= l(rQ_\infty) - l(rQ_\infty - D) \\ &= (r+1-g) - (r-q^3+1-g) = q^3 = n \end{aligned}$$

Dessa forma, nos resta estudar o caso onde $0 \leq r \leq q^3+q^2-q-2$

Proposição 4.10. *O código dual de C_r é*

$$C_r^\perp = C_{q^3+q^2-q-2-r}.$$

Portanto C_r é auto-ortogonal se $2r \leq q^3+q^2-q-2$, e C_r é auto-dual para $r = (q^3+q^2-q-2)/2$.

Demonstração. Ver em [3, Pag. 294]. □

Agora vamos determinar os parâmetros de C_r. Consideremos o conjunto I dos polos de Q_∞, isto é:

$$I = \{n \geq 0 | z \in \mathcal{H}; (z)_\infty = nQ_\infty\}.$$

Para $s \geq 0$ defina

$$I(s) = \{n \in I | n \leq s\}.$$

Então $|I(s)| = l(sQ_\infty)$, e pelo teorema de Riemann-Roch

$$|I(s)| = s + 1 - q(q-1)/2$$

para $s \geq 2g-1 = q(q-1)-1$.

Podemos ainda descrever $I(s)$ da seguinte forma:

$$I(s) = \{n \leq s | n = iq + j(q+1) \text{ com } i \geq 0 \text{ e } 0 \leq j \leq q-1\}.$$

Portanto,

$$|I(s)| = |\{(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 | j \leq q-1 \text{ e } iq + j(q+1) \leq s\}|.$$

Isto se deve ao seguinte resultado:

Lema 4.11. *Para $r \geq 0$, os elementos $x^i y^j$ com $0 \leq i$, $0 \leq j \leq q-1$ e $iq + j(q+1) \leq r$ formam uma base de $\mathcal{L}(rQ_\infty)$.*

Proposição 4.12. *Suponha que $0 \leq r \leq q^3+q^2-q-2$. Então segue que:*

i) A dimensão de C_r é dada por

$$dim\ C_r = \begin{cases} |I(r)| & para \quad 0 \leq r < q^3 \\ q^3 - |I(s)| & para \quad q^3 \leq r \leq q^3+q^2-q-2 \end{cases}$$

onde $s = q^3+q^2-q-2-r$ e $I(r) = \{n \in I | n \leq r\}$.

ii) Para $q^2 - q - 2 < r < q^3$, temos que

$$dim\ C_r = r + 1 - q(q-1)/2.$$

iii) A distância mínima d de C_r, satisfaz

$$d \geq q^3 - r$$

Demonstração. i) Para $0 \leq r < q^3$ o corolário 4.3 nos garante que

$$dim C_r = dim \mathcal{L}(rQ_\infty) = |I(r)|.$$

Para $q^3 \leq r \leq q^3+q^2-q-2$, temos que $s = q^3+q^2-q-2$. Então $0 \leq s \leq q^2-q-2 < q^3$. Pela proposição 4.8, obtemos:

$$dim C_r = q^3 - dim C_s = q^3 - |I(s)|.$$

ii) Para $q^2 - q - 2 = 2g - 2 < r < q^3$, pelo corolário 4.3, temos

$$dim C_r = r + 1 - g = r + 1 - q(q-1)/2.$$

iii) A desigualdade $d \geq q^3 - r$ segue do teorema 4.3.

□

Exemplo 4.13. Vamos construir a matriz geradora do código Hermitiano, sobre $\mathbb{F}_{3^2}$ e, tomaremos $r = 10$. Primeiramente vamos construir a extensão $\mathbb{F}_9$, para isso considere o polinômio $x^2 + x + 2 \in \mathbb{F}_3$ irredutível, seja α a raíz deste polinômio, os elementos de $\mathbb{F}_9$ serão portanto,

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

Para calcularmos os pontos do corpo que pertencem a curva Hermitiana, considere o seguinte quadro com a norma e o traço de cada elemento.

A curva hermitiana é definida por

$$y^q + y = x^{q+1}$$

Portanto queremos $(x, y) \in \mathbb{F}_{3^2}$ tal que $y^q + y = x^{q+1}$, isto é equivalente a encontrarmos elementos cujos traço e norma são iguais.

Dessa forma os pontos da curva são:

$$\begin{aligned}\mathcal{H} \;=\; & \{(0,0); (0,\alpha+1); (0,2\alpha+2); (1,2); (1,\alpha); (1,2\alpha+1); (2,2); (2,2\alpha+1); (2,\alpha);\\ & (\alpha,1); (\alpha,\alpha+2); (\alpha,2\alpha); (\alpha+1,2); (\alpha+1\alpha); (\alpha+1,2\alpha+1); (\alpha+2,1); (\alpha+2,\alpha+2);\\ & (\alpha+2,2\alpha); (2\alpha,1); (2\alpha,\alpha+2); (2\alpha,2\alpha); (2\alpha+1,1); (2\alpha+1,\alpha+2); (2\alpha+1,2\alpha);\\ & (2\alpha+2,2); (2\alpha+2,\alpha); (2\alpha+2,2\alpha+1)\} \cup \{P_\infty = (0:1:0)\}\end{aligned}$$

Elemento	Traço	Norma
0	0	0
1	1	2
2	1	1
α	2	1
$\alpha+1$	1	0
$\alpha+2$	2	2
2α	2	2
$2\alpha+1$	2	1
$2\alpha+2$	1	0

Devemos agora calcular o espaço de Riemann-Roch:

$$\mathcal{L}(10P_\infty) = \{f \in \mathbb{F}_q(X,Y) : (f) + 10P_\infty \geq 0\}$$

Utilizando as propriedades da valorização, obtemos o seguinte conjunto:

$$\mathcal{L}(10P_\infty) = \{1, x, y, x^2, y^2, xy, x^3, x^2y\}$$

Então, basta que apliquemos os pontos da curva nas funções encontradas. Considere o conjunto $\mathcal{H}$ como um conjunto ordenado dos pontos da curva:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & \dots & 2\alpha+1 & 2\alpha+1 & 2\alpha+2 & 2\alpha+2 & 2\alpha+2 \\ 0 & \alpha+1 & 2\alpha+2 & 2 & \alpha & \dots & \alpha+2 & 2\alpha & 2 & \alpha & 2\alpha+1 \\ 0 & 0 & 0 & 1 & 1 & \dots & 2\alpha+2 & 2\alpha+2 & 2 & 2 & 2 \\ 0 & \alpha+1 & 2\alpha+2 & 2 & \alpha & \dots & \alpha+2 & 2\alpha & 2 & \alpha & 2\alpha+1 \\ 0 & 0 & 0 & 2 & \alpha & \dots & \alpha+1 & 1 & \alpha+1 & \alpha+2 & \alpha \\ 0 & 0 & 0 & 1 & 1 & \dots & \alpha & \alpha & \alpha+1 & \alpha+1 & \alpha+1 \\ 0 & 0 & 0 & 2 & \alpha & \dots & 2\alpha & 2\alpha+1 & 1 & 2\alpha & \alpha+2 \end{pmatrix}$$

A matriz G é a *Matriz Geradora* do código Hermitiano sobre o corpo $\mathbb{F}_{3^2}$ com $r = 10$. Podemos também explicitar um intervalo para a distância mínima do código construído acima através das seguintes desigualdades vistas anteriormente:

$$\begin{aligned} d &\leq n - gr(G) \\ d &\geq q^3 - r. \end{aligned}$$

Como $n = 27$, $gr(G) = q + 1 = 4$, $q^3 = 3^3 = 27$ e $r = 10$, temos:

$$17 \leq d \leq 23.$$

5 Conclusão

Vimos neste trabalho que a construção de um código algébrico geométrico exige a abordagem de diversos conceitos das teorias de corpos de corpos finitos e corpos de funções, necessitando de uma gama de resultados. Através de propriedades das funções traço e norma e o fato da curva hermitiana ser maximal, pudemos obter uma importante classe de códigos, que possui ótimos parâmetros e é objeto de estudo constante na Teoria de Códigos Corretores de Erros.

Além disso, este trabalho possibilita uma base para a investigação de uma generalização dos códigos hermitianos, podendo ser encontrados códigos que melhorem os parâmetros máximos atuais.

Referências

[1] LIDL, R.; NIEDERREITER, H. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[2] HEFEZ, A.; Vilela, Maria Lúcia T. *Códigos Corretores de Erros, 2a. ediçao*. Rio de Janeiro: IMPA, 2008.

[3] STICHTENOTH, H. *Algebraic Functions Fields and Codes, 2a. edição*. Istanbul: Sabanci University, 2009.

[4] GARCIA, A. *Pontos Racionais em Curvas sobre Corpos Finitos*. Rio de Janeiro: IMPA, 1995.

[5] HODOLDT, T.; VAN LINT, J.; PELLIKAAN, R. *Algebraic Geometry Codes*. Elsevier, Amsterdam, 1998.

[6] VICENTIM, Steve S.. *Curvas algébricas sobre corpos finitos*. Universidade de São Paulo, São Carlos, 2012.

[7] WEIL, André.. *Courbes algébriques et variétés abéliennes*. Herman, Paris, 1971.

[8] COSSIDENTE, A. ; HIRSCHFELD, J. ; KORCHMAROS, G. ; TORRES, F. . *On Plane Maximal Curves*. Compositio Mathematica, 1998.

[9] HIRSCHFELD, J. ; KORCHMAROS, G. ; TORRES, F. . *The number of points on an algebraic curve over a finite field*.

[10] CASTELLANOS, A. S. ; *Estruturas Algébricas e Aplicações*. Universidade Federal de Uberlândia, Uberlândia, 2017.

[11] LI, W. C. WINNIE ; *Number Theory With Applications*. Departament of Mathematics,Pennsylvania State University, USA, 1998.

APÊNDICE A – Resultados preliminares

Nesse apêndice, começaremos com definições básicas, como grupos, anéis e corpos e finalizaremos com resultados importantes envolvendo polinômios irredutíveis e corpos de decomposição. Resultados iniciais podem ser vistos em [10].

A.1 Estruturas algébricas

Definição A.1. Um **grupo** é um conjunto G munido com uma operação $*$ tal que as seguintes propriedades são válidas:

1. $*$ é associativa, isto é, para quaisquer $a, b, c \in G$,

$$a * (b * c) = (a * b) * c.$$

2. Existe um elemento identidade (ou unidade) e em G tal que, para todo $a \in G$,

$$a * e = e * a = a.$$

3. Para cada $a \in G$, existe um elemento inverso a^{-1} em G tal que

$$a * a^{-1} = a^{-1} * a = e.$$

Se o grupo também satisfizer

4. Para todos $a, b \in G$,

$$a * b = b * a,$$

então o grupo será chamado de **abeliano** (ou **comutativo**).

Por fim, se o conjunto G for finito, o grupo será dito **finito** e o número de elementos de G é chamado **ordem**, e denotado por $|G|$.

Em particular, se a operação $*$ é chamada de adição, o grupo será dito aditivo e, se a operação $*$ é chamada de multiplicação, o grupo será dito multiplicativo. Ainda, se $H \subset G$ e a operação $*$ restrita a H conservar as propriedades acima, chamaremos H de **subgrupo** de G.

Vale, ainda, destacar uma classe de grupos importante: os **grupos cíclicos**. Dizemos que um grupo multiplicativo é cíclico se existir $a \in G$ tal que, para todo $b \in G$, existe um inteiro j tal que $b = a^j$, isto é, $G = \{a^m : m \in \mathbb{Z}\}$ (no caso de grupos aditivos, trocamos

potências por múltiplos). O elemento a é chamado **gerador** de G. É simples notar que todo grupo cíclico é abeliano.

Queremos definir um grupo muito importante: o grupo das classes de restos na divisão por um número n ($\mathbb{Z}_n$). Para isso, precisamos entender o que é uma classe. Dizemos que um subconjunto R de $S \times S$ é uma **relação de equivalência** em S se as três seguintes propriedades forem satisfeitas:

1. $(s, s) \in R$ para todo $s \in S$ (reflexiva).
2. Se $(s, t) \in R$, então $(t, s) \in R$ (simétrica).
3. Se $(s, t), (t, u) \in R$, então $(s, u) \in R$ (transitiva).

Se agruparmos todos os elementos de S equivalentes a um elemento $s \in S$ fixado, obteremos o que chamamos de **classe de equivalência** de s, denotado por

$$\bar{s} = \{t \in S : (s, t) \in R\}.$$

Note que $\bar{s} = \bar{t}$ se, e somente se, $(s, t) \in R$.

Definição A.2. Para inteiros arbitrários a, b e um natural n, dizemos que a é **congruente** a b no módulo n, e escrevemos $a \equiv b (\text{mod } n)$ se a diferença $a - b$ for múltipla de n.

Pode-se verificar facilmente que a "congruência módulo n" é uma relação de equivalência no conjunto dos inteiros $\mathbb{Z}$.

Definição A.3. O grupo formado pelo conjunto $\{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ de classes de equivalência módulo n com a operação

$$\bar{a} + \bar{b} = \overline{a + b}$$

é chamado **grupo de inteiros módulo** n e denotado por $\mathbb{Z}_n$.

Para finalizar o estudo dos grupos, precisamos definir o que seriam o normalizador de um conjunto, o centro de um grupo e apresentar a equação de classe. Para isso, tomando um subconjunto S de um grupo G, denotaremos por aSa^{-1} o conjunto

$$aSa^{-1} = \{asa^{-1} : s \in S\}$$

.

Definição A.4. Seja S um subconjunto não vazio de G. O **normalizador** de S em G é o conjunto $N(S) = \{a \in G : aSa^{-1} = S\}$.

Dizemos que dois elementos $a, b \in G$ são **conjugados** se existir um elemento $g \in G$ tal que $gag^{-1} = b$. Se agruparmos todos os elementos conjugados a um elemento fixado a, obteremos um conjunto chamado de **classe de conjugação** de a. Para certos elementos, essas classes de conjugação são unitárias, e isso vale exatamente para os elementos do centro do grupo G.

Definição A.5. Para um grupo G, o **centro** de G é o conjunto $C = \{c \in G : ac = ca, \text{para todo } a \in G\}$.

Por fim, precisamos apresentar a equação de classe. Embora a demonstração não seja muito complicada, assumiremos o seguinte teorema sem demonstrá-lo.

Teorema A.6 (Equação de classe)**.** *Seja G um grupo finito com centro C. Então,*

$$|G| = |C| + \sum_{i=1}^{k} |C_G(x_i)|,$$

onde $C_G(x_i)$ percorrem todas as classes de conjugação distintas e não-unitárias de G.

Agora, podemos definir anéis e corpos, uma "generalização" dos grupos. Para essas duas estruturas, porém, precisamos de duas operações.

Definição A.7. Um **anel** R é um conjunto R munido de duas operações, denotadas por $+$ e $\cdot$, tais que

1. R é um grupo abeliano com respeito a $+$.
2. $\cdot$ é associativa, isto é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todos $a, b, c \in R$.
3. A lei distributiva é valida, ou seja, para todos $a, b, c \in R$, temos $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

Denotamos por 0 o elemento identidade do grupo abeliano R com respeito à operação aditiva e por $-a$ o inverso aditivo de um elemento $a \in R$. Um exemplo bem conhecido de anel é o conjunto dos números inteiros $\mathbb{Z}$. Assim como no caso dos grupos, se tivermos $H \subset R$ e as propriedades acima ainda forem válidas em H, chamaremos H de **subanel** de R.

Definição A.8.

1. Um anel é chamado **anel com identidade** se o anel tiver um elemento identidade para a multiplicação, isto é, se existir um elemento e tal que $a \cdot e = e \cdot a = a$ para todo $a \in R$.
2. Uma anel é dito **comutativo** se a operação $\cdot$ for comutativa.
3. Um anel é chamado um **domínio de integridade** se for um anel comutativo com identidade $e \neq 0$ no qual $a \cdot b = 0$ implica $a = 0$ ou $b = 0$.

4. Um anel é chamado um **anel de divisão** se os elementos não-nulos de R formarem um grupo sob a multiplicação.

5. Um anel de divisão comutativo é chamado de **corpo**.

Denotaremos o elemento identidade da multiplicação (quando esse existir) por 1. Um **subcorpo** H do corpo F é um subconjunto H de F tal que H também é um corpo. Um exemplo importante de corpo é o conjunto dos números reais $\mathbb{R}$.

Se um dado anel R não for domínio de integridade, isto é se existirem $a, b \in R\backslash\{0\}$ tais que $ab = 0$, dizemos que R tem divisores de zero e, obviamente, a e b são esses divisores. Pode-se provar que todo corpo é um domínio de integridade e que todo domínio de integridade finito é um corpo. Usando esse fato, podemos mostrar o seguinte.

Teorema A.9. *$\mathbb{Z}_p$, o anel das classes de restos na divisão por um primo p, é um corpo.*

Demonstração. Como $\mathbb{Z}_p$ é finito, precisamos apenas mostrar que $\mathbb{Z}_p$ é um domínio de integridade. Note que $\bar{1}$ é identidade de $\mathbb{Z}_p$ e $\bar{a}\bar{b} = \overline{ab} = \bar{0}$ se, e somente se, $ab = kp$ para algum inteiro k. Mas, uma vez que p é primo, p divide ab se, e somente se, p divide a ou p divide b. Portanto, devemos ter $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Logo, $\mathbb{Z}_p$ é um domínio de integridade. □

Esses corpos $\mathbb{Z}_p$ são muito importantes pois, veremos mais adiante, todo corpo finito contém um subcorpo isomorfo a algum $\mathbb{Z}_p$. Precisamos, então, definir isomorfismo entre corpos.

Definição A.10. Uma aplicação bijetora $\varphi : R \to S$ de um corpo R em um corpo S é chamada um **isomorfismo** se, para todos $a, b \in R$, tivermos

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ e } \varphi(ab) = \varphi(a)\varphi(b).$$

De certa forma, podemos dizer que um isomorfismo φ de R em S induz uma estrutura de corpo em S, pois, tomando $s_1, s_2 \in S$, encontramos únicos $r_1, r_2 \in R$ tais que $\varphi(r_1) = s_1$ e $\varphi(r_2) = s_2$. Definimos, então $s_1 + s_2$ como sendo $\varphi(r_1 + r_2)$ e $s_1 s_2$ como sendo $\varphi(r_1 r_2)$. Esta estrutura em S é chamada **induzida por** φ e isso nos ajudará a representar melhor os corpos $\mathbb{Z}_p$.

Definição A.11. Para um primo p, seja $\mathbb{F}_p = \{0, 1, ..., p - 1\}$ o conjunto formado por inteiros e considere a aplicação $\varphi : \mathbb{Z}_p \to \mathbb{F}_p$ dada por $\varphi(\bar{a}) = a$. Então, $\mathbb{F}_p$ com a estrutura induzida por φ é um corpo finito, chamado **corpo de Galois de ordem** p.

Note que, em $\mathbb{F}_p$, $pb = 0$ para todo $b \in \mathbb{F}_p$ e p é o menor inteiro positivo para o qual isso é válido. De forma geral, todo corpo finito terá essa propriedade para algum inteiro q.

Definição A.12. Se R for um anel arbitrário e existe um inteiro positivo n tal que $nr = 0$ para todo $r \in R$, então o menor tal inteiro positivo é chamado de **característica** de R e R é dito ter característica (positiva) n. Se tal inteiro positivo n não existir, dizemos que R tem característica 0.

Teorema A.13. *Um anel $R \neq \{0\}$ de característica positiva, com unidade e sem divisores de zero deve ter característica prima.*

Demonstração. Uma vez que R contém elementos não-nulos, R tem característica $n \geq 2$. Se n não fosse primo, poderíamos escrever $n = km$ com $k, m \in \mathbb{Z}$, $1 < k$, $m < n$. Então, $0 = ne = (km)e = (ke)(ne)$, e isso implica $ke = 0$ ou $me = 0$, já que R não tem divisores de zero. Segue, então que ou $kr = (ke)r = 0$ para todo $r \in R$ ou $mr = (me) = 0$ para todo $r \in R$, contradizendo com a definição da característica n. □

Corolário A.14. *Todo corpo finito tem característica prima.*

Demonstração. Pelo teorema anterior, é suficiente mostrar que a característica de um corpo finito F é positiva. Considere os múltiplos $e, 2e, 3e, ...$ da unidade. Uma vez que F contém apenas uma quantidade finita de tais elementos que sejam distintos, existe inteiros k e m com $1 \leq k < m$ tal que $ke = me$ ou, $(m - k)e = 0$, e então F tem característica positiva. □

Um fato interessante sobre corpos de característica 2 é que, como $0 = 2a = a + a$ para todos os elementos a do corpo, $a = -a$ para todo a. Uma propriedade muito útil envolvendo a característica p de um corpo F é a seguinte.

Teorema A.15. *Seja F um corpo de característica prima p. Então,*

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

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

Demonstração. Usamos o fato de que

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \equiv 0 (\text{mod } p)$$

para todo $i \in \mathbb{Z}$ com $0 < i < p$, o que segue do fato de que $\begin{pmatrix} p \\ i \end{pmatrix}$ ser um inteiro e da observação de que o fator p do numerador não poder ser cancelado. Então, pelo Teorema do Binômio de Newton,

$$(a + b)^p = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1}b + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} ab^{p-1} + b^p = a^p + b^p,$$

e usando indução sobre n, completamos a prova da primeira identidade. Pelo que já mostramos, obtemos

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

e a segunda identidade é válida. □

Com isso, temos definidas a principal estrutura com a qual trabalharemos na demonstração do Teorema de Wedderburn: os corpos finitos. Também, provamos que todos eles têm característica prima p. Podemos, agora definir polinômios e corpos de decomposição, que nos serão muito úteis.

A.2 Polinômios

Agora, vale destacar alguns resultados importantes sobre polinômios e seus corpos de decomposição, que serão essenciais para a construção de uma classe especial deles: os polinômios ciclotômicos e para a caracterização dos corpos finitos.

Definição A.16. Um **polinômio** sobre um anel R é uma expressão da forma

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

onde n é um inteiro não-negativo e os **coeficientes** a_i, $0 \leq i \leq n$ são elementos de R. Se f for um polinômio com, pelo menos, um coeficiente não-nulo, seja n o maior índice tal que $a_n \neq 0$. Então, a_n é chamado de **coeficiente líder** e a_0 é chamado **termo constante**, enquanto n é chamado **grau** e denotado por $n = \deg(f)$. Polinômios com grau 0 são chamados de **polinômios constantes**. Se o anel R tiver unidade 1 e o coeficiente líder de f for 1, chamaremos f de **polinômio mônico**.

Podemos, ainda, escrever os polinômios numa forma "estendida", observando que $f(x) = a_0 + a_1 x + \cdots + a_n x^n = a_0 + a_1 x + \cdots + a_n x^n + 0a_{n+1}x^{n+1} + \cdots$. Assim, a soma e o produto de dois polinômios $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} x^j$ como sendo

$$f(x) + g(x) = \sum_{k=0}^{max(i,j)} (a_k + b_k)x^k$$

e

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ onde } c_k = \sum_{i+j=k} a_i b_j.$$

Com essas operações, é fácil ver que os polinômios formam um anel, chamado de **anel de polinômios**. e denotado por $R[x]$. O elemento nulo de $R[x]$ é o polinômio $f(x) = 0$, onde 0 é o elemento nulo de R e, se o anel tiver unidade 1, então a unidade de $R[x]$ será $f(x) = 1$.

Assim como no caso dos elementos nulo e identidade, o anel $R[x]$ "herda" certas características de R, por exemplo $R[x]$ é comutativo se, e só se, R for comutativo e $R[x]$ é um domínio de integridade se, e só se, R for um domínio de integridade. No que se segue, usaremos polinômios sobre um corpo F. Com isso, $F[x]$ é um domínio de integridade comutativo e com unidade $f(x) = 1$. Vale a pena destacar um resultado bem conhecido: o algoritmo da divisão.

Teorema A.17 (Algoritmo da divisão)**.** *Seja $g \neq 0$ um polinômio em $F[x]$. Então, para todo $f \in F[x]$, existem polinômios $q, r \in F[x]$ tais que*

$$f = qg + r, \text{ onde } r = 0 \text{ ou } deg(r) < deg(g).$$

Agora que definimos uma forma para dividir polinômios, podemos pensar em divisores e múltiplos e, como no caso dos inteiros, procurar o máximo divisor comum e o mínimo múltiplo comum entre dois polinômios não-nulos. Isso é sempre possível, como afirma o próximo teorema (que será aceito sem demonstração).

Teorema A.18. *Sejam $f_1, ..., f_m \in F[x]$. Então existe um polinômio mônico unicamente determinado $d = mdc(f_1, ..., f_m) \in F[x]$ (que chamaremos **máximo divisor comum entre** $f_1, ..., f_m$) com as seguintes propriedades: (i) d divide cada f_j, $1 \leq j \leq m$; (ii) qualquer polinômio $c \in F[x]$ que divide todos os f_j, $1 \leq j \leq m$ também divide d. Por fim, existem polinômios $b_1, ..., b_m \in F[x]$ tais que*

$$d = b_1 f_1 + \cdots + b_m f_m.$$

*Além disso, existe um polinômio mônico unicamente determinado $e = mmc(f_1, ..., f_m) \in F[x]$ (que chamaremos **mínimo múltiplo comum entre** $f_1, ..., f_m$) com as seguintes propriedades: (i) e é um múltiplo de cada f_j, $1 \leq j \leq m$; (ii) qualquer polinômio $b \in F[x]$ que seja um múltiplo de todos os f_j, $1 \leq j \leq m$ também é múltiplo de e.*

Assim como fomos capazes de "estender" o conceito de mdc e mmc dos números inteiros para os polinômios, podemos pensar em estender o conceito de números primos, para isso precisamos da definição de um elemento irredutível pois, em certas estruturas algébricas, elementos irredutíveis nem sempre são elementos primos.

Definição A.19. Um polinômio $p \in F[x]$ será dito **irredutível sobre** F se p tiver grau positivo e $p = bc$ com $b, c \in F[x]$ implica que b ou c é um polinômio constante. Se $p \in F[x]$ não for irredutível, chamaremos p de **redutível**.

Note que a irredutibilidade de um polinômio depende do corpo sob o qual estamos trabalhando. Por exemplo, $x^2-2 \in \mathbb{Q}[x]$ é irredutível, mas $x^2-2 = (x+\sqrt{2})(x-\sqrt{2}) \in \mathbb{R}[x]$. Os polinômios irredutíveis desempenham um papel importante no estudo dos anéis $F[x]$,

uma vez que, nessas estruturas, todo elemento irredutível é primo (isto é, se $p \in F[x]$ for irredutível e p dividir o produto $f_1 \cdots f_m$, então p dividirá pelo menos um dos fatores f_i).

Além disso, vale a fatoração única em $F[x]$, ou seja, todo $f \in F[x]$ pode ser escrito de forma única (a menos de reordenação dos fatores) da forma $f = ap_1^{e_1} \cdots p_m^{e_m}$, onde $a \in F$, $p_1, ..., p_m$ são polinômios mônicos irredutíveis distintos e $e_1, ..., e_m$ são inteiros não-negativos.

Assim como fizemos para construir os corpos $\mathbb{F}_p$, podemos construir um anel $F[x]/(f)$ a partir de um polinômio f. Usaremos a mesma relação de equivalência que nos fornece as classes de restos na divisão por f e a soma e produto de duas classes será feito de modo similar aos elementos de $\mathbb{F}_p$. Dessa forma, $F[x]/(f)$ será o conjunto formado pela união dessas classes. Como os elementos irredutíveis e primos em $F[x]$ são os mesmos, segue que $F[x]/(f)$ é um corpo se, e somente se, f for irredutível. Além disso, se $F = \mathbb{F}_p$ e $\deg(f) = n \geq 0$, então $F[x]/(f)$ terá p^n elementos.

Em breve, definiremos outro corpo que se relaciona com um polinômio irredutível $f \in F[x]$: o corpo de decomposição de f. Antes disso, porém, precisamos definir o que são as raízes de um polinômio e como elas se relacionam com a redutibilidade de f.

Definição A.20. Um elemento $b \in F$ é chamado uma **raiz** do polinômio $f \in F[x]$ se $f(b) = 0$.

Teorema A.21. *Um elemento $b \in F$ é uma raiz do polinômio $f \in F[x]$ se, e somente se, $x - b$ dividir f.*

Demonstração. Usamos o algoritmo da divisão para expressar $f(x) = q(x)(x - b) + c$, com $q \in F[x]$ e $c \in F$. Substituindo b por x, obtemos $c = f(b)$. Logo, $f(x) = q(x)(x - b) + f(b)$ e o resultado segue dessa identidade. □

Definição A.22. Seja $b \in F$ uma raiz de um polinômio $f \in F[x]$. Se k for um inteiro positivo tal que $f(x)$ é divisível por $(x - b)^k$, mas não por $(x - b)^{k+1}$, então k é chamado de **multiplicidade** de b. Se $k = 1$, então b é chamado **raiz simples** de f e, se $k \geq 2$, b é chamado de **raiz múltipla** de f.

Teorema A.23. *Seja $f \in F[x]$ com $\deg(f) = n \geq 0$. Se $b_1, ..., b_m \in F$ forem raízes distintas de f com multiplicidades $k_1, ..., k_m$ respectivamente, então $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ divide $f(x)$. Consequentemente, $k_1 + \cdots + k_m \leq n$ e f pode ter no máximo n raízes distintas em F.*

Demonstração. Note que cada polinômio $x - b_j$, $1 \leq j \leq m$ é irredutível sobre F, e então $(x - b_j)^{k_j}$ aparece na fatoração de f. Além disso, o fator $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ aparece na fatoração de f e é, portanto, um divisor de f. Comparando graus, encontramos $k_1 + \cdots + k_m \leq n$ e $m \leq k_1 + \cdots + k_m \leq n$ mostra a última afirmação. □

Definição A.24. Se $f(x) = a_0 + a_1x + a_2x^2 \cdots + a_nx^n \in F[x]$, então a **derivada** f' de f é definida como sendo $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$.

Teorema A.25. *O elemento $b \in F$ é uma raiz múltipla de $f \in F[x]$ se, e somente se, for uma raiz de f e f' simultaneamente.*

Agora, podemos estudar extensões de corpos e corpos de decomposição. Essas duas estruturas serão muito utilizadas na demonstração do Teorema de Wedderburn.

A.3 Extensões de corpos

Seja F um corpo. Um subconjunto $K \subseteq F$ que também é um corpo com as operações de F será chamado de **subcorpo** de F. Nesse contexto, F é chamado uma **extensão** de K. Se $K \neq F$, diremos que K é um **subcorpo próprio** de F.

Se K for um subcorpo do corpo finito $\mathbb{F}_p$, p primo, então K deve conter os elementos 0 e 1, e todos os outros elementos de $\mathbb{F}_p$ uma vez que K é fechado pela adição. Segue que $\mathbb{F}_p$ não tem nenhum subcorpo próprio. Um corpo com tal propriedade é chamado de **corpo primo**.

Pelo argumento acima, qualquer corpo finito de ordem p, p primo, é um corpo primo. Um outro exemplo de um corpo primo, embora seja infinito, é o corpo dos números racionais $\mathbb{Q}$. A interseção de de todos os subcorpos de F nos fornece o **subcorpo primo** de F, que é obviamente um corpo primo.

Teorema A.26. *O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou $\mathbb{Q}$, conforme a característica de F é um primo p ou 0.*

Definição A.27. Seja K um subcorpo de F e M qualquer subconjunto de F. O corpo $K(M)$ é obtido pela interseção de todos os subcorpos de F contendo K e M e é chamado de extensão de K obtida pela **adjunção** dos elementos de M. Para um conjunto $M = \{\theta_1, ..., \theta_n\}$ finito, escrevemos $K(M) = K(\theta_1, ..., \theta_n)$. Se M consistir de um único elemento $\theta \in F$, então $L = K(\theta)$ é dito uma **extensão simples** de K e θ é chamado um **elemento definidor** de L sobre K.

Definição A.28. Sejam K um subcorpo de F e $\theta \in F$. Se θ satisfizer uma equação polinomial não-trivial, isto é, se $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ com $a_i \in K$ não todos nulos, então θ é dito **algébrico** sobre K. Uma extensão L de K é dita **extensão algébrica** se todo elemento de L for algébrico sobre K.

Definição A.29. Seja $\theta \in K$ algébrico e tome todos os polinômios $f \in K[x]$ tais que $f(\theta) = 0$. É possível provar que existe um único polinômio mônico irredutível $g(x) \in K[x]$ de menor grau tal que $g(\theta) = 0$, que será chamado de **polinômio minimal de θ sobre** K e o **grau** de θ é definido como sendo o grau de $g(x)$.

Uma propriedade interessante do polinômio minimal $g(x)$ de $\theta \in K$ é que, para todo $f \in K[x]$, $f(\theta) = 0$ se, e somente se, g dividir f. Note que o polinômio minimal, bem como o grau de um elemento dependem do corpo sobre o qual estamos trabalhando. Por exemplo, $\sqrt{2}$ tem polinômio minimal $x^2 - 2$ e grau 2 em $\mathbb{Q}[x]$, mas tem polinômio minimal $x - \sqrt{2}$ e grau 1 em $\mathbb{R}[x]$.

Se L for uma extensão de K, então L pode ser visto como um espaço vetorial sobre K. Primeiro, note que os elementos de L formam um grupo abeliano com respeito à adição. Além disso, cada "vetor" $\theta \in L$ pode ser multiplicado por um "escalar" $r \in K$ de forma que $r\theta$ pertença a L (basta usar a multiplicação usual do corpo L), e, com isso, os axiomas de multiplicação por escalar serão satisfeitos.

Definição A.30. Seja L uma extensão de corpos de K. Se L, visto como espaço vetorial sobre K, for de dimensão finita, dizemos que L é uma **extensão finita** de K. A dimensão do espaço vetorial L sobre K é chamado **grau** de L sobre K e denotado por $[L : K]$.

Apresentaremos a seguir três resultados conhecidos que serão aceitos sem demonstração, eles nos serão bem úteis para provar a unicidade (a menos de isomorfismo) de um tipo especial de extensão de corpos: os corpos de decomposição.

Teorema A.31. *Se L for uma extensão finita de K e M é uma extensão finita de L, então M é uma extensão finita de K com*

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

Teorema A.32. *Toda extensão finita de K é algébrica sobre K.*

Teorema A.33. *Seja $\theta \in F$ algébrico de grau n sobre K e seja g o seu polinômio minimal sobre K. Então:*

1. *$K(\theta)$ é isomorfo a $K[x]/(g)$.*
2. *$[K(\theta) : K] = n$ e $\{1, \theta, ..., \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K.*
3. *Todo $\alpha \in K(\theta)$ é algébrico sobre K e seu grau sobre K é um divisor de n.*

Dessa forma, os elementos de uma extensão algébrica simples $K(\theta)$ sobre K podem ser representados de forma única como um polinômio em θ, ou seja, podem ser escritos de forma única como $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ com $a_i \in K$ para $0 \leq i \leq n - 1$.

Teorema A.34. *Seja $f \in K[x]$ irredutível sobre o corpo K. Então existe uma extensão algébrica simples de K com uma raiz de f como elemento definidor.*

Demonstração. Considere o anel de classes residuais $L = K[x]/(f)$, que é um corpo pois f é irredutível. Os elementos de L são as classes residuais denotadas por $[h] = h + (f)$

com $h \in K[x]$. Para todo $a \in K$, podemos formar a classe residual $[a]$ determinada pelo polinômio constante igual a a e, se $a, b \in K$ forem distintos, então $[a] \neq [b]$ uma vez que f tem grau positivo. O mapa $a \mapsto [a]$ nos fornece um isomorfismo de K em um subcorpo K' de L, de modo que K' pode ser identificado com K. Em outras palavras, podemos ver L como uma extensão de K. Para todo $h(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$ temos $[h] = [a_0 + a_1x + \cdots + a_mx^m] = [a_0] + [a_1][x] + \cdots + [a_m][x^m] = a_0 + a_1[x] + \cdots + a_m[x]^m$ pelas regras de operações com classes residuais e a identificação $[a_i] = a_i$. Então, todo elemento de L pode ser escrito como uma expressão polinomial em $[x]$ com coeficientes em K. Uma vez qualquer corpo contendo K e $[x]$ deve conter essas expressões polinomiais, L é uma extensão simples de K obtida pela adjunção de $[x]$. Se $f(x) = b_0 + b_1x + \cdots + b_nx^n$, então $f([x]) = b_0 + b_1[x] + \cdots + b_n[x]^n = [b_0 + b_1x + \cdots + b_nx^n] = [f] = [0]$, logo $[x]$ é uma raiz de f e L é uma extensão algébrica simples de K. □

Teorema A.35. *Sejam α e β raízes de $f \in K[x]$ que é irredutível sobre K. Então $K(\alpha)$ e $K(\beta)$ são isomorfos sob um isomorfismo que leva α em β e fixa os elementos de K.*

Agora podemos definir os corpos de decomposição, que são estruturas que contém todas as raízes de um dado polinômio.

Definição A.36. Seja $f \in K[x]$ de grau positivo e F uma extensão de K. Dizemos que f se **decompõe** em F se f puder ser escrito como produto de fatores lineares em $F[x]$, isto é, se existirem elementos $\alpha_1, \alpha_2, ..., \alpha_n \in F$ tais que

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

onde a é o coeficiente líder de f. O corpo F é um **corpo de decomposição** de f sobre K se f se decompuser em F e, além disso, $F = K(\alpha_1, \alpha_2, ..., \alpha_n)$.

É claro que um corpo de decomposição F de f sobre K é, de certa forma, o menor subcorpo contendo todas as raízes de f (nenhum subcorpo próprio de F que seja uma extensão de K contém todas as raízes de f). Aplicando repetidamente o processo usado no Teorema A.34, pode-se provar a primeira parte do seguinte resultado. A segunda parte é uma extensão do Teorema A.35.

Teorema A.37 (Existência e Unicidade de Corpos de Decomposição)**.** *Se K for um corpo e f é um polinômio de grau positivo em $K[x]$, então existe um corpo de decomposição de f sobre K. Além disso, dois corpos de decomposição de f sobre K são isomorfos segundo o isomorfismo que fixa os elementos de K e mapeia as raízes de f umas nas outras.*

Uma vez que corpos de decomposição podem ser identificados uns com os outros, podemos procurar *o* corpo de decomposição de f sobre K. Ele pode ser obtido adjuntando uma quantidade finita de elementos algébricos sobre K, e, portanto, pode-se provar, tendo

como base os Teoremas A.31 e A.33(2), que o corpo de decomposição de f sobre K é uma extensão finita sobre K.