Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática

Franciele do Carmo Silva

Construção de Reticulados via Corpos de Funções

Juiz de Fora
2019

Franciele do Carmo Silva

Construção de Reticulados via Corpos de Funções

Dissertação apresentada ao Programa de Pós-Graduação em Matemáticada Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2019

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF com os dados fornecidos pelo(a) autor(a)

Silva, Franciele do Carmo.
Construção de Reticulados via Corpos de Funções / Franciele do Carmo Silva. – 2019.
130 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2019.

1. Corpo de Funções Elípticas. 2. Corpo de Funções Hermitiano. 3. Reticulados Bem Arredondados. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

FRANCIELE DO CARMO SILVA

CONSTRUÇÃO DE RETICULADOS VIA CORPOS DE FUNÇÕES

Dissertação aprovada pela Comissão Examinadora abaixo elencada como requisito para a obtenção do título de Mestre em Matemática pelo Mestrado Acadêmico em Matemática do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora.

Beatriz L. R.

Profª. Drª. Beatriz Casulari da Motta Ribeiro
(Orientadora)
Mestrado Acadêmico em Matemática
Instituto de Ciências Exatas - UFJF

Flaviana Andrea Ribeiro

Profª. Drª. Flaviana Andrea Ribeiro
UFJF

p/ Beatriz L. R.

Profª. Drª. Grasiele Cristiane Jorge
UNIFESP

Juiz de Fora, 28 de junho de 2019.

AGRADECIMENTOS

Primeiramente a Deus, por me conceder força para progredir nessa caminhada.

Aos meus pais, Iza e Joel, e ao meu irmão, Lucas, por estarem sempre presentes em minha vida e por me apoiarem e me incentivarem de modo incessante em todas as minhas decisões. A vocês, minha eterna gratidão.

Ao meu companheiro de curso e amigo de toda a vida, Caio, por todos os momentos compartilhados ao longo desse tempo, pelo apoio incondicional e, sobretudo, pela amizade desmedida.

Aos meus amigos, especialmente à Elisa, Dabson, Davi e Daniel, pelo suporte e incentivo constantes e, principalmente, por trazerem mais leveza aos meus dias.

À professora e orientadora Beatriz Casulari da Motta Ribeiro pela generosidade, confiança e paciência com que me orientou em todo esse período, as quais se tornaram grande motivação em meu interesse pela Teoria dos Números.

A cada um dos professores da graduação pelos ensinamentos e pela contribuição em meu crescimento acadêmico e pessoal. Em especial, às professoras Flaviana Andrea Ribeiro e Grasiele Cristiane Jorge pela participação na banca examinadora.

Aos meus professores do ensino básico por terem despertado meu amor pela Matemática.

À Universidade Federal de Juiz de Fora e ao Departamento de Matemática pelas diversas oportunidades ofertadas.

Ao Conselho Nacional de Pesquisa e Desencolvimento (CNPq) pelo apoio financeiro no Programa de Iniciação Científica e Mestrado (PICME).

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-Brasil (CAPES) pelo fundamental apoio no mestrado (Código de Financiamento 001).

"It is impossible to be a mathematician without being a poet in soul."
(Sofia Kovalevskaya)

RESUMO

O objetivo principal deste trabalho é apresentar construções de reticulados utilizando certos corpos de funções elípticas e Hermitiano. Tais reticulados são gerados por seus vetores minimais, isto é, fazem parte da classe dos reticulados bem arredondados. Para tais reticulados, estabelecemos correspondências entre o conjunto de lugares racionais e o conjunto de pontos do reticulado, que nos levam a estimativas quanto ao número total de vetores minimais e a densidade de empacotamento dos mesmos.

Palavras-chave: Corpo de Funções Elípticas, Corpo de Funções Hermitiano, Reticulados Bem Arredondados.

ABSTRACT

The main purpose of this work is to present constructions of lattices using certain elliptic and Hermitian function fields. These lattices are generated by their minimal vectors, that is, form the well-rounded lattices class. For these lattices, we stabilize correspondences between the set of rational places and the set of lattice vectors, which lead us to estimates on the total number of minimal vectors and the packing density of the same.

Key-words: Elliptic Function Field. Hermitian Function Field. Well Rounded Lattices.

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{F}_p$	Corpo de Galois de ordem p (primo)
$\mathbb{F}_q$	Corpo finito com q elementos
F/K	Corpo de funções
$\tilde{K}$	Corpo de constantes de F/K
$\mathcal{O}$	Anel de valorização de F/K
P	Lugar de F/K
$\mathbb{P}_F$	Conjunto dos lugares de F/K
F_P	Corpo das classes residuais de P
$\deg P$	Grau do lugar P
$Div(F)$	Grupo de divisores de F
$Princ(F)$	Grupo dos divisores principais de F
$Cl(F)$	Grupo das classes dos divisores de F
$Div^0(F)$	Grupo de divisores de grau zero de $F/\mathbb{F}_q$
$Cl^0(F)$	Grupo das classes dos divisores de grau zero de $F/\mathbb{F}_q$
h_F	Número de classes de divisores (de grau zero) de F
$\mathcal{L}(D)$	Espaço de Riemann-Roch associado ao divisor D
$\ell(D)$	Dimensão do espaço $\mathcal{L}(D)$
g	Gênero de um corpo de funções
N	Número de lugares racionais de um corpo de funções
$Z_F(t)$	Função Zeta de $F/\mathbb{F}_q$

$L_F(t)$	L-polinômio de $F/\mathbb{F}_q$
$A = (a_{ij})$	Matriz A
A^T	Transposta da matriz A
$\det A$	Determinante da matriz A
I_d	Matriz Identidade
Λ	Reticulado em $\mathbb{R}^n$, sendo $n \in \mathbb{N}$
$\Lambda^\star$	Sub-reticulado de Λ
M	Matriz geradora para o reticulado Λ
$\mathcal{G}$	Matriz de Gram para o reticulado Λ
$\mathcal{P}_B$	Paralelotopo fundamental de Λ segundo uma base B
vol (X)	Volume de uma região X em $\mathbb{R}^n$
σ_d	Isometria segundo uma métrica d em $\mathbb{R}^n$
κ	Fator de dilatação
$\mu(\Lambda)$	Distância mínima de um reticulado
$\tau(\Lambda)$	*Kissing number* de um reticulado Λ
$\rho(\Lambda)$	Raio de empacotamento de um reticulado Λ
$\Delta(\Lambda)$	Densidade de um reticulado Λ
$\delta(\Lambda)$	Densidade de centro de um reticulado Λ
$\gamma(\Lambda)$	Raio de cobertura de um reticulado Λ
$K(E)$	Corpo de Funções Elípticas (sobre $\mathbb{F}_q$)
$\mathcal{P}$	Conjunto de lugares racionais
$\mathbf{P}$	Ponto sobre a curva elíptica E
$x(\mathbf{P})$	Abscissa do ponto $\mathbf{P}$
H	Corpo de Funções Hermitiano (sobre $\mathbb{F}_{q^2}$)

SUMÁRIO

1 INTRODUÇÃO

Um reticulado $\Lambda \subseteq \mathbb{R}^n$ se caracteriza como um conjunto discreto de pontos em $\mathbb{R}^n$ gerado por combinações lineares inteiras de $m \leq n$ vetores linearmente independentes em $\mathbb{R}^n$. Dado um reticulado, podemos considerar o *empacotamento esférico* a ele associado, ou seja, o conjunto de esferas de mesmo raio, centradas em todos os pontos do reticulado e que se intersectam, no máximo, em seus bordos. Tendo como motivação tais tipos de empacotamentos, pode-se aprofundar no estudo daqueles em que o raio das esferas é máximo. Nessa análise, surge um importante parâmetro: a *densidade de empacotamento*, a qual mede a proporção do espaço n-dimensional coberto pelo conjunto de esferas considerado. Esses empacotamentos esféricos, denominados *empacotamentos reticulados*, tornaram-se importantes ferramentas na busca por métodos criptográficos com baixa probabilidade de erro na transmissão de informações.

Em geral, sabe-se que reticulados com alta densidade de empacotamento produzem bons códigos nesse sentido. Dessa forma, um dos principais problemas envolvendo Teoria dos Códigos e Teoria dos Números consiste em, fixado um espaço n-dimensional e uma métrica em $\mathbb{R}^n$, obter reticulados com alta densidade de empacotamento. Mais geralmente, almeja-se exibir o reticulado cuja densidade de empacotamento seja máxima. No entanto, mesmo considerando a métrica euclidiana, normalmente é difícil calcular a densidade de empacotamento, uma vez que, para esse cálculo, torna-se necessário determinar a norma mínima do reticulado, o que é um problema complexo para reticulados gerais.

Motivado por tal problema, em meados do século XX, Hlawka demonstrou um importante resultado referente aos reticulados e à densidade de empacotamento que fora conjecturado e estudado por Minkowski [4]. Tal resultado, conhecido como Teorema de Minkowski-Hlawka, estabelece que para todo espaço n-dimensional existe um reticulado cuja densidade de empacotamento é maior ou igual a $\zeta(n)/2^{n-1}$, sendo ζ associada à função Zeta de Riemann. Apesar das demonstrações já obtidas para esse teorema não serem construtivas, principalmente ao considerarmos dimensões arbitrárias, em certo sentido o teorema possibilita uma nova abordagem para o problema inicial. Com efeito, neste momento, pode-se restringir o estudo às famílias assintóticas de reticulados cuja densidade de empacotamento seja tão próximo quanto possível da limitação de Minkowski e Hlawka.

Sob essa perspectiva, no início do século XXI, Tsfasman e Vladut [30] mostraram que reticulados construídos por meio de corpos de funções específicos produzem bons resultados nessa abordagem. Para tanto, eles estudaram essencialmente reticulados via corpos de funções em que o quociente n/g, sendo n o número de lugares racionais e g o gênero do corpo de funções considerado, fosse suficientemente grande. Nesse

mesmo período, Martinet [20] mostrou ainda que reticulados com alta densidade de empacotamento em geral constituem a classe dos *reticulados bem arredondados*. Trata-se de reticulados de posto $m \leq n$ que contém m vetores de norma mínima que são lineramente independentes. Em particular, tomando-se um reticulado gerado apenas por vetores minimais, tem-se que o mesmo é bem arredondado.

Nessas circunstâncias, este trabalho se propõe a unir as abordagens de tais matemáticos e, assim, apresentar algumas construções de reticulados, obtidos a partir de certos corpos de funções, que sejam gerados por seus vetores minimais. Além de apresentar estimativas para o número de vetores minimais de cada um dos reticulados, bem como suas densidades de empacotamento.

Para essas construções, seguindo a abordagem adotada por Bötcher, Fukshansky, Garcia e Maharaj em [4] e [13], utilizaremos o corpo de funções Hermitiano e corpos de funções elípticas, ambos sobre corpos de constantes completos e finitos. Com este intuito, destacaremos os principais resultados sobre tais corpos de funções, principalmente sobre seus conjuntos de lugares racionais $\mathcal{P}$. Além disso, estabeleceremos uma correspondência biunívoca entre cada um dos reticulados construídos e o conjunto de divisores principais do corpo de funções considerado com suporte em $\mathcal{P}$. Nesse cenário, apresentaremos a demonstração de que os vetores minimais dos reticulados obtidos são, precisamente, os divisores de funções relacionadas a determinadas retas do corpo de funções analisado.

Tendo em vista tais objetivos, dividiremos este trabalho da seguinte forma:

No capítulo 2, apresentaremos as noções fundamentais da Teoria dos Corpos de Funções Algébricas, tais como anéis de valorização, lugares, divisores e gênero. Caracterizaremos ainda tais conceitos ao analisarmos extensões de corpos. Além disso, estudaremos os espaços de Riemann-Roch e suas principais propriedades. Ao final, aprofundaremos essas análises ao considerarmos corpos de funções com corpos de constantes finitos e corpos de funções obtidos por meio de curvas algébricas planas.

No capítulo 3, introduziremos os conceitos básicos no estudo de reticulados, estabelecendo uma visão geométrica e topológica dos mesmos. Nas últimas seções, apresentaremos ainda os principais problemas nesse sentido, abordando a análise da distância mínima de um reticulado e enfatizando sua densidade de empacotamento e seu número de vizinhos.

No capítulo 4, detalharemos um dos problemas centrais no estudo de reticulados: a busca por reticulados com alta densidade de empacotamento. Sob essa perspectiva, apresentaremos a construção de reticulados por meio de corpos de funções gerais sobre corpos de constantes finitos e analisaremos suas principais propriedades, que serão mais exploradas nos capítulos seguintes, usando corpos de funções específicos

No capítulo 5, seguindo a abordagem feita para corpos de funções gerais,

aprofundaremo-nos na análise dos reticulados obtidos a partir de corpos de funções elípticas sobre corpos finitos. Para essa construção, utilizaremos a estrutura de grupo presente no conjunto dos pontos racionais de uma curva elíptica e analisaremos os divisores de determinadas retas pertencentes a tal corpo de funções. Assim, provaremos que sob certa condição quanto ao número de lugares racionais o reticulado construído torna-se gerado por seus vetores minimais e, consequentemente, bem arredondado. Ao final, apresentaremos ainda estimativas para o número de vizinhos e o raio de cobertura desse reticulado.

Por fim, no capítulo 6, apresentaremos a construção ao considerarmos o corpo de funções Hermitiano sobre um corpo finito. Utilizando novamente o estudo de divisores, demonstraremos que o reticulado obtido é gerado por seus vetores minimais e, portanto, bem arredondado. No final do capítulo, apresentaremos uma estimativa do número de vizinhos e da densidade de empacotamento para esse reticulado.

Destacamos que as figuras em que não é apresentada referência são de autoria própria, sendo confeccionadas com escala 1 : 1 e utilizando o programa *Geogebra*.

2 CORPOS DE FUNÇÕES ALGÉBRICAS

Extensões algébricas finitas de corpos estão presentes em diversas áreas, das quais podemos destacar a Geometria Algébrica, a Teoria dos Números e a Teoria das Superfícies Compactas de Riemann. Este capítulo se propõe a estudar extensões finitas específicas, a saber, os corpos de funções algébricas em uma variável.

No que se segue, apresentaremos os principais conceitos referentes à Teoria de Corpos de Funções Algébricas, tais como *lugares, anéis de valorização, valorização*, assim como a relação entre eles, *divisores* e *gênero* de uma função. Esses conceitos, juntamente com algumas de suas propriedades, serão essenciais nas construções de reticulados feitas nos Capítulos 4, 5 e 6.

Primeiramente, abordaremos tais noções ao considerarmos uma extensão algébrica arbitrária, apresentando exemplos quando tal extensão é um *corpo de funções racionais*. A seguir, apresentaremos corpos de funções obtidos por meio de curvas algébricas planas. Por fim, analisaremos suas propriedades ao considerarmos corpos de funções cujo *corpo de constantes* é finito.

2.1 DEFINIÇÕES INICIAIS

Com o intuito de definirmos *corpo de funções algébricas*, relembramos notações convenientes.

Dado um corpo K, representamos por $K[x]$ o conjunto de polinômios na variável x com coeficientes em K e por $K(x)$ o corpo constituído pelos quocientes de elementos em $K[x]$. Formalmente, temos:

$$\begin{aligned} K[x] &:= \left\{ f(x) = a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{N} \text{ e } a_i \in K \text{ para todo } i = 0, \ldots, n \right\} \\ K(x) &:= \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \right\} \end{aligned}$$

sendo que $K(x)$ é denominado **corpo de frações de** $K[x]$.

De modo análogo, fixado $n \in \mathbb{N}$, definimos $K[x_1, \ldots, x_n]$ como sendo o conjunto de polinômios nas variáveis $x_1, \ldots, x_n$ com coeficientes em K, e $K(x_1, \ldots, x_m)$ como o corpo de frações de $K[x_1, \ldots, x_n]$.

Definição 2.1.1. *Dizemos que F/K é um* ***corpo de funções algébricas em uma variável*** *sobre K se F/K é uma extensão de corpos tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.*

Nessas circunstâncias, denominamos ainda o conjunto:

$$\tilde{K} := \left\{ z \in F : z \text{ é algébrico sobre } K \right\}$$

como ***corpo de constantes*** *de F/K e, no caso em que $K = \tilde{K}$, dizemos que K é* ***algebricamente fechado em*** *F (ou ainda que K é o* ***corpo completo de constantes de*** *F).*

Observação 2.1.2. Para efeito de simplificação, iremos nos referir a F/K definido acima como sendo simplesmente um *corpo de funções*.

Utilizando o conceito de corpo de funções, obtemos uma caracterização para elementos transcendentes.

Definição 2.1.3. *Dado um corpo de funções F/K, dizemos que um elemento $z \in F$ é um elemento* ***transcendente*** *sobre K se a extensão $F/K(z)$ possui grau finito.*

Um dos principais exemplos de corpos de funções é obtido pela seguinte definição:

Definição 2.1.4. *Dizemos que F/K é um* ***corpo de funções racionais*** *se F/K é uma extensão de corpos e $F = K(x)$, para algum $x \in F$ transcendente sobre K.*

Claramente, temos que todo corpo de funções racionais é, em particular, um corpo de funções, o que torna a terminologia utilizada acima consistente.

Contudo, o conceito de corpos de funções racionais é ainda mais relevante, na medida em que nos permite caracterizar os corpos de funções. Com este intuito, relembramos o conceito de *extensão simples*.

Definição 2.1.5. *Uma extensão F/K é dita* ***simples*** *se existe $u \in F$ tal que $F = K[u]$.*

Utilizando a Definição 2.1.5, dado um corpo de funções arbitrário, podemos considerá-lo como sendo uma extensão algébrica simples de um corpo de funções racionais. Mais precisamente, podemos considerar $F = K(x, y)$ em que $\varphi(y) = 0$ para algum polinômio irredutível $\varphi(T) \in K(x)[T]$. Aprofundaremos nessa abordagem na próxima seção, em que apresentaremos um método para a construção de corpos de funções. Além disso, retomaremos esse resultado na Seção 2.4, onde descreveremos essencialmente corpos de funções com corpo de constantes finitos.

2.2 CORPO DE FUNÇÕES DE UMA CURVA

Conforme mostrado inicialmente, todo corpo de funções pode ser visto como uma extensão simples finita de um corpo de funções racionais. Esse fato nos motiva a estudar corpos de funções da forma F/K, em que $F = K(x, y)$, sendo x um elemento transcendente sobre K. Sob essa perspectiva, podemos considerar ainda que x e y satisfazem a equação de uma curva. Nesse contexto, esta última seção tem o intuito de exibir o corpo de funções associado a uma curva algébrica plana.

Para tanto, relembramos o conceito de *polinômio irredutível* em duas variáveis.

Definição 2.2.1. *Dado um polinômio $g \in K[X, Y]$ de grau d, dizemos que g é um* ***polinômio irredutível*** *se g não pode ser fatorado como o produto de polinômios em $K[X, Y]$ cujos graus sejam menores que d.*

Agora, consideremos C uma curva plana irredutível sobre o corpo K, ou seja,

$$C := V(f) = \Big\{(a, b) \in K^2 : \ f(a, b) = 0\Big\},$$

em que $f \in K[X, Y]$ é um polinômio irredutível.

Além disso, sejam x e y as funções coordenadas de C, as quais são dadas por:

$$\begin{array}{lll} x : C \to K & & y : C \to K \\ (a, b) \mapsto a & \text{e} & (a, b) \mapsto b \end{array}$$

Lembramos que uma função φ de C em K é dita regular se existe um polinômio $g \in K[X, Y]$ tal que $\varphi(a, b) = g(a, b)$ para cada $(a, b) \in C$. Nessas condições, definimos a *K-álgebra das funções regulares de C* como:

$$K[C] := K[x, y] = \frac{K[X, Y]}{\langle f \rangle}.$$

Assim, podemos definir o seu corpo de frações, a saber:

$$K(C) := K(x, y) = \left\{ \frac{g(x, y)}{h(x, y)} : \ g, h \in K[X, Y] \text{ e } f \nmid h \right\}.$$

Suponhamos agora que C não é a reta vertical $x = 0$. Dessa forma, como x não divide f, temos que $x \notin K$ e, então, x é transcendente sobre K. Consequentemente, garantimos que $K(C)/K$ é um corpo de funções, denominado *corpo das funções racionais de C*.

Exemplo 2.2.2. Consideremos a curva de equação $f : y^2 - x^3 = 0$ sobre $\mathbb{R}^2$. Pela construção feita acima, temos que x é transcendente sobre $\mathbb{R}$, visto que x não divide f. Desse modo, $\mathbb{R}(x, y)/\mathbb{R}$ é um corpo de funções. Mais precisamente, obtemos:

$$\mathbb{R}[x, y] = \frac{\mathbb{R}[X, Y]}{\langle y^2 - x^3 \rangle}.$$

E, portanto, tal corpo de funções é dado por:

$$\mathbb{R}(x, y) = \left\{ \frac{g(x, y)}{h(x, y)} : \ g, h \in K[X, Y] \text{ e } y^2 - x^3 \nmid h \right\}.$$

Aprofundaremo-nos no estudo de corpos de funções obtidos por meio de curvas algébricas planas no próximo capítulo, em que analisaremos os corpos de funções obtidos a partir da *curva hermitiana* e de *curvas elípticas*, considerando K como sendo um corpo finito.

2.3 PRINCIPAIS CONCEITOS

Nesta seção, inicialmente, estudaremos os *anéis de valorização* de um corpo de funções e seus respectivos ideais maximais (*lugares*). A seguir, obteremos uma caracterização para os mesmos por meio da análise de determinadas aplicações, chamadas *valorizações*. Em um segundo momento, estenderemos a noção de *lugar* ao considerarmos suas somas formais: os *divisores*. Nesse sentido, obteremos importantes resultados, destacando-se o famoso Teorema de Riemann-Roch. Por fim, analisaremos como tais conceitos se comportam em extensões de corpos de funções.

2.3.1 **Lugares e Valorizações**

Definição 2.3.1. *Um* ***anel de valorização*** *de um corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ satisfazendo as seguintes propriedades:*

(*i*) $K \subsetneq \mathcal{O} \subsetneq F$;

(*ii*) *Para todo $z \in F$ tem-se que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.*

Exemplo 2.3.2. Consideremos o corpo de funções racionais dado por $K(x)/K$, em que x é um elemento transcendente sobre K. Dado um polinômio mônico irredutível $p(x) \in K[x]$, definimos:

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], mdc(f(x), g(x)) = 1, p(x) \nmid g(x) \right\}.$$

Temos que $\mathcal{O}_{p(X)}$ é um anel de valorização do corpo de funções racionais $K(x)/K$. De fato, é imediato que $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$. Por outro lado, dado $\varphi \in K(x)$, sabemos que:

$$\varphi = \frac{f(x)}{g(x)} \text{ , sendo } f(x), g(x) \in K[x], mdc(f(x), g(x)) = 1 \text{ e } g(x) \neq 0.$$

Se $p(x) \nmid g(x)$, segue que $\varphi \in \mathcal{O}_{p(x)}$ e não há nada a fazer.

Por outro lado, se $p(x) \mid g(x)$, como $f(x)$ e $g(x)$ são primos entre si, segue que $p(x) \nmid f(x)$. Consequentemente, temos:

$$\varphi^{-1} = \frac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}.$$

Destacamos que a condição de $p(x)$ ser irredutível é crucial para que $\mathcal{O}_{p(x)}$ seja um anel. Com efeito, consideremos $f(x)/g(x)$ e $h(x)/s(x)$ elementos em $\mathcal{O}_{p(x)}$. Temos:

$$\frac{f(x)}{g(x)} + \frac{h(x)}{s(x)} = \frac{f(x)s(x) + h(x)g(x)}{g(x)s(x)}.$$

Sabemos que $p(x) \nmid g(x)$ e $p(x) \nmid s(x)$. No entanto, no caso em que $p(x)$ é redutível, não garantimos que $p(x) \nmid g(x)s(x)$.

Com efeito, consideremos $p(x) = a(x)b(x)$, com $mdc(a(x), b(x)) = 1$. Tomando $g(x)$ tal que $a(x) \mid g(x)$ e $b(x) \nmid g(x)$ e $s(x)$ tal que $b(x) \mid g(x)$ e $a(x) \nmid g(x)$), temos que $p(x) \mid g(x)s(x)$.

É possível também definir um outro anel de valorização em $K(x)/K$, sem a utilização de um polinômio mônico e irredutível fixado, a saber:

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

Notemos que, pelo Exemplo 2.3.2, todo corpo de funções racionais admite um anel de valorização, bastando considerar um polinômio mônico irredutível sobre tal corpo. Entretanto, em princípio, considerando um corpo de funções arbitrário F/K não garantimos, ainda, que o mesmo admite ao menos um anel de valorização. Para a demonstração dessa existência, que será feita ao final dessa subseção, optaremos pela abordagem a partir de *lugares*.

Proposição 2.3.3. *Seja O um anel de valorização do corpo de funções F/K. Então O é um anel local, i.e., O possui um único ideal maximal, a saber:*

$$P = O \setminus O^\times,$$

em que $O^\times$ corresponde ao grupo das unidades de O, ou seja,

$$O^\times := \left\{ z \in O : \text{ existe } w \in O \text{ tal que } zw = 1 \right\}.$$

Demonstração. Primeiramente, notemos que P é um ideal de O:

i) Dados $z \in O$ e $x \in P$, sabemos que $zx \in O$, visto que O é um anel.

Afirmamos que $zx \notin O^\times$. Com efeito, caso contrário, teríamos que $(zx)^{-1} \in O^\times$, donde resultaria que $z(zx)^{-1} = x \in O^\times$, uma contradição.

Logo, segue que $zx \in P$.

ii) Sejam $x, y \in P$. Novamente, como O é um anel, temos que $x + y \in O$.

Por outro lado, como $x, y \in F$ e F é corpo, temos que $x/y \in F$. Como O é anel de valorização, temos que $x/y \in O$ ou $y/x \in O$. Assim, a menos de troca de variáveis, podemos supor, sem perda de generalidade, que $x/y \in O$.

Dessa forma, $x/y + 1 \in O$ e, consequentemente:

$$x + y = \left(\frac{x}{y} + 1 \right) y \notin O^\times.$$

Portanto, $x + y \in P$.

Resta mostrar que P é o único ideal maximal de $\mathcal{O}$.

Com efeito, seja I um ideal próprio de $\mathcal{O}$ tal que $P \subseteq I \subsetneq \mathcal{O}$. Como $I \subsetneq \mathcal{O}$, segue que I não contém nenhuma unidade (caso contrário, $1 \in I$ e teríamos $I = \mathcal{O}$) e, então, $I \subseteq \mathcal{O} \setminus \mathcal{O}^\times = P$. Portanto, $I = P$, como queríamos.

A unicidade decorre do fato de que todo ideal propriamente contido em $\mathcal{O}$ está contido em P, o qual é maximal. □

O resultado apresentado nos motiva à definição de *lugar* de um corpo de funções.

Definição 2.3.4. *Dizemos que P é um **lugar** de um corpo de funções F/K se P é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K, ou seja, $P = \mathcal{O} \setminus \mathcal{O}^\times$.*

O conjunto de lugares de um corpo de funções F/K será denotado por $\mathbb{P}_F$, ou seja,

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

Observação 2.3.5. Dado um anel de valorização $\mathcal{O}$ em F/K e seu respectivo lugar $P = \mathcal{O}\setminus\mathcal{O}^\times$, segue diretamente da definição que, para cada $z \in F$, com $z \neq 0$, tem-se:

$$z \in P \Leftrightarrow z^{-1} \notin \mathcal{O}.$$

Desse modo, $\mathcal{O}$ é unicamente determinado por P, podendo ser escrito como:

$$\mathcal{O} = \Big\{z \in F : z^{-1} \notin P\Big\}.$$

Nessas circunstâncias, por vezes denotaremos o anel de valorização de F/K associado ao lugar $P \in \mathbb{P}_F$ como sendo $\mathcal{O}_P$.

Exemplo 2.3.6. Consideremos o corpo de funções racionais $K(x)$. Fixemos um polinômio mônico irredutível $p(x) \in K(x)$ e consideremos $\mathcal{O}_{p(x)}$ definido como no Exemplo 2.3.2:

$$\mathcal{O}_{p(x)} := \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x)\right\}.$$

Por definição, seu ideal maximal é dado por:

$$P_{p(x)} := \mathcal{O}_{p(x)}\setminus\mathcal{O}_{p(x)}^\times.$$

Assim, $P_{p(x)}$ (denominado *lugar finito*) é constituído pelos elementos $f(x)/g(x) \in \mathcal{O}_{p(x)}$ tais que $g(x)/f(x) \notin \mathcal{O}_{p(x)}$. Consequentemente,

$$P_{p(x)} := \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x), p(x) \mid f(x)\right\}. \tag{2.1}$$

A efeito de notação, quando $p(x) = x - \alpha$ para algum $\alpha \in K$, denotamos o lugar correspondente simplesmente por P_α.

Por outro lado, considerando o anel de valorização denotado por $\mathcal{O}_\infty$, ou seja:

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\},$$

temos que seu respectivo ideal maximal (denominado *lugar infinito de* $K(x)$) é dado por:

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\}. \tag{2.2}$$

Cabe destacar que a nomenclatura desses lugares depende da escolha para o elemento transcendente. Com efeito, sabemos que $K(x) = K(1/x)$; donde resulta que o lugar infinito com respeito a $1/x$ corresponde exatamente ao lugar P_0.

Pode-se mostrar ainda que esses dois exemplos descrevem todos os lugares para o corpo de funções racionais $K(x)/K$. Em outras palavras, qualquer lugar de $K(x)/K$ pode ser descrito por uma das equações: (2.1) ou (2.2) (ver [28], Proposição 1.2.1).

Um fato interessante a respeito de um lugar do corpo de funções F/K é o de que todos seus elementos não nulos são transcendentes sobre K. Mais geralmente, temos:

Proposição 2.3.7. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K com ideal maximal P e $\tilde{K}$ o corpo de constantes de F/K. Então $\tilde{K} \subseteq \mathcal{O}$ e, em particular, $\tilde{K} \cap P = \{0\}$.*

Demonstração. Seja $z \in \tilde{K}$. Suponhamos, por absurdo, que $z \notin \mathcal{O}$. Então, como $\mathcal{O}$ é anel de valorização, temos que $z^{-1} \in \mathcal{O}$. Agora, como $z^{-1} \in \tilde{K}$, uma vez que $\tilde{K}$ é corpo, existem $a_1, \ldots, a_n \in K$ tais que:

$$a_n(z^{-1})^n + \cdots + a_1 z^{-1} + 1 = 0$$

e, consequentemente,

$$z^{-1}(a_n(z^{-1})^{n-1} + \cdots + a_1) = -1.$$

Assim, $z = -(a_n(z^{-1})^{n-1} + \cdots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, uma contradição.

Portanto, $\tilde{K} \subseteq \mathcal{O}$ e, pela Observação 2.3.5, segue que $\tilde{K} \cap P = \{0\}$. □

Com o intuito de obter um estudo mais detalhado dos conceitos apresentados, utilizaremos uma segunda descrição por meio de *valorizações*.

Definição 2.3.8. *Seja F/K um corpo de funções. Uma* ***valorização discreta*** *de F/K é uma aplicação sobrejetiva $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfazendo:*

(*i*) $v(a) = 0$ *para todo* $0 \neq a \in K$;

(*ii*) $v(x) := \infty \Leftrightarrow x = 0$;

(*iii*) $v(xy) = v(x) + v(y)$ *para todo* $x, y \in F$;

(*iv*) $v(x+y) \geq \min\{v(x), v(y)\}$ *para todo* $x, y \in F$.

Observação 2.3.9. O símbolo ∞ denota um elemento que não pertence a $\mathbb{Z}$ e que, para quaisquer $m, n \in \mathbb{N}$, satisfaz:

$$\infty > n \quad \text{e} \quad \infty + \infty = \infty + n = n + \infty = \infty.$$

Além disso, destacamos que a noção de valorização é mais abrangente. Em geral, dado um grupo abeliano totalmente ordenado Γ, podemos definir uma valorização de F/K com grupo de valores Γ como sendo uma aplicação sobrejetiva $v : F \to \Gamma \cup \{\infty\}$ com as mesmas propriedades exigidas acima. Neste caso, se $\Gamma = \mathbb{Z}$, dizemos que tal valorização é discreta.

Para efeito de simplificação, iremos nos referir a v como na Definição 2.3.8 simplesmente como uma valorização. Entretanto, ressaltamos que todas as valorizações abordadas neste trabalho são necessariamente discretas.

Utilizando a propriedade (*iv*) da Definição 2.3.8, obtemos o seguinte resultado:

Proposição 2.3.10 (**Desigualdade Triangular Estrita**)**.** *Seja* v *uma valorização discreta de* F/K *e sejam* $x, y \in F$ *tais que* $v(x) \neq v(y)$*. Então,* $v(x+y) = \min\{v(x), v(y)\}$.

Demonstração. Como $v(x) \neq v(y)$, podemos considerar, sem perda de generalidade, que $v(x) < v(y)$. Suponhamos, por absurdo, que $v(x+y) > \min\{v(x), v(y)\}$, i.e., $v(x+y) > v(x)$. Assim, temos:

$$v(x) = v(x+y-y) \geq \min\{v(x+y), v(-y)\}.$$

Por outro lado, notemos que, dado $a \in K$, com $a \neq 0$, pelas propriedades (*i*) e (*iii*) temos que $v(ay) = v(y)$. Em particular, $v(-y) = v(y)$, donde resulta:

$$v(x) \geq \min\{v(x+y), v(y)\} = v(y),$$

uma contradição. Logo, segue que $v(x+y) = \min\{v(x), v(y)\}$. □

Mostraremos agora que, fixada uma valorização discreta v de F/K, podemos construir conjuntos P_v e $\mathcal{O}_v$ que sejam um lugar e seu respectivo anel de valorização de F/K. Reciprocamente, fixado um lugar P de um corpo de funções F/K, é possível definir uma aplicação v_P de modo que a mesma seja uma valorização discreta de F/K.

Para a primeira afirmação, temos:

Teorema 2.3.11. *Seja* v *uma valorização discreta do corpo de funções* F/K*. Definimos:*

$$\mathcal{O}_v := \Big\{z \in F : v(z) \geq 0\Big\};$$
$$P_v := \Big\{z \in F : v(z) > 0\Big\}.$$

Então, P_v *e* $\mathcal{O}_v$ *são um lugar e seu respectivo anel de valorização de* F/K.

Demonstração. Primeiramente, notemos que, como v é uma valorização, então $v(z) = 0$ para todo $z \in K$, com $z \neq 0$. Mais ainda, utilizando que v é sobrejetiva, temos $\mathcal{O}_v \subsetneq F$. Assim, segue que $K \subseteq \mathcal{O}_v \subsetneq F$.

Por outro lado, dado $z \in F$, caso $z \notin \mathcal{O}_v$, ou seja, $v(z) < 0$, notemos que:

$$0 = v(1) = v\left(z \cdot z^{-1}\right) = v(z) + v(z^{-1}),$$

donde resulta que $v(z^{-1}) > 0$ e, portanto, $z^{-1} \in \mathcal{O}_v$. Desse modo, $\mathcal{O}_v$ é de fato um anel de valorização.

Além disso, notemos que, nessas circunstâncias, o grupo das unidades de $\mathcal{O}_v$ é dado por:

$$\mathcal{O}_v^{\times} = \left\{z \in F : v(z) = 0\right\} \subseteq \mathcal{O}_v.$$

Com efeito, seja z unidade de $\mathcal{O}_v$. Então $z^{-1} \in \mathcal{O}_v$ e, procedendo como anteriormente, devemos ter necessariamente $v(z) = v(z^{-1}) = 0$. Reciprocamente, se $z \in F$ é tal que $v(z) = 0$, então segue que $v(z^{-1}) = 0$ e, portanto, $z \in \mathcal{O}_v$.

Logo, usando que $P_v = \mathcal{O}_v \setminus \mathcal{O}_v^{\times}$, obtemos a igualdade enunciada para P_v. Em outras palavras, concluímos que P é o ideal maximal de $\mathcal{O}_v$, como queríamos. □

Para a segunda afirmação, segundo a qual um lugar em F/K nos permite definir uma valorização neste corpo de funções, necessitaremos de alguns resultados auxiliares, os quais dependem principalmente do lema seguinte, cuja demonstração é feita em [28] (Lema 1.1.7).

Lema 2.3.12. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K e seja P seu ideal maximal. Consideremos $0 \neq x \in P$. Sejam $x_1, \ldots, x_n$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para todo $i = 2, \ldots, n$. Então:*

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

Observação 2.3.13. Destacamos que a desigualdade $[F : K(x)]$ é válida para todo elemento de F transcentdente sobre K (veja Definição 2.1.3). Além disso, pela Proposição 2.3.7, como $x \in P$, temos que x é necessariamente transcendente sobre K.

Proposição 2.3.14. *Seja F/K um corpo de funções e P um lugar de F/K, cujo anel de valorização associado é dado por $\mathcal{O}_P$. Consideremos que $P = t\mathcal{O}_P$ para algum $t \in P$.*

Então, dado $z \in F$, com $z \neq 0$, temos que ele possui uma única representação sob a forma:

$$z = t^n u, \text{ em que } n \in \mathbb{Z} \text{ e } u \in \mathcal{O}_P^{\times}.$$

Demonstração. Para a unicidade da representação, consideremos $z = t^n u = t^m r$, em que $u, r \in \mathcal{O}_P^{\times}$ e $m, n \in \mathbb{Z}$. Suponhamos, sem perda de generalidade, que $n \geq m$. Então $t^{n-m} = ru^{-1} \in \mathcal{O}_P$, donde temos $m = n$ e, consequentemente, $r = u$.

Para verificarmos a existência de tal representação, seja $z \in F$, com $z \neq 0$. Como $\mathcal{O}_P$ é um anel de valorização, temos que z ou z^{-1} pertence a $\mathcal{O}_P$. Dessa forma, podemos supor, sem perda de generalidade, que $z \in \mathcal{O}_P$. Caso $z \in \mathcal{O}_P^\times$, basta escrevermos $z = t^0 z$. Então, podemos nos limitar ao caso em que $z \notin \mathcal{O}_P^\times$, ou seja, em que $z \in P$.

Neste caso, consideremos o maior valor de m natural de modo que $x_i \in x_{i+1}P$ para todo $i = 2, \ldots, m$, sendo:

$$x_1 = z,\ x_2 = t^{m-1},\ x_3 = t^{m-2},\ \ldots,\ x_m = t.$$

Notemos que, de fato, existe ao menos um valor de m satisfazendo a condição acima, a saber, $m = 1$. Além disso, $x_i \in P$ para todo $i = 1, \ldots, m$.

Por outro lado, garantimos a existência de um valor máximo para m em função do Lema 2.3.12, pelo qual a sequência tomada é limitada.

Dessa forma, temos que $z = t^m u$, em que $u \in \mathcal{O}_P$. Afirmamos que u deve ser uma unidade de $\mathcal{O}_P$. Com efeito, caso contrário, teríamos que $u \in P = t\mathcal{O}_P$, ou seja, $u = tw$, sendo $w \in \mathcal{O}_P$. Como consequência teríamos $z = t^{m+1}w$, contrariando a maximalidade de m. Portanto, existe $n \in \mathbb{Z}$ tal que $z = t^n u$, sendo $u \in \mathcal{O}_P^\times$. □

Observação 2.3.15. Notemos que pela construção feita na proposição anterior, no caso geral em que $z \in F$, garantimos apenas que o expoente n em $z = t^n u$, com $u \in \mathcal{O}_P^\times$, é inteiro. Por outro lado, caso $z \in P$, tal expoente é necessariamente natural.

Proposição 2.3.16. *Seja F/K um corpo de funções e $P \in \mathbb{P}_F$. Então, P é um ideal principal. Mais ainda, $\mathcal{O}_P$ é um domínio de ideais principais.*

Demonstração. Primeiramente, mostraremos que P é um ideal principal de $\mathcal{O}_P$.

Para tanto, suponhamos, por absurdo, que P não é principal. Tomemos $x_1 \in P$ com $x_1 \neq 0$. Como $x_1\mathcal{O}_P \subsetneq P$, existe $x_2 \in P \setminus x_1\mathcal{O}_P$. Além disso, como $x_1\mathcal{O}_P \neq x_2\mathcal{O}_P$, segue que $x_2 {x_1}^{-1} \notin \mathcal{O}_P$ e, pela Observação 2.3.5, temos que ${x_2}^{-1}x_1 \in P$, donde $x_1 \in x_2 P$.

Por indução, podemos repetir esse processo sucessivamente. Assim, obtemos uma sequência infinita $x_1, x_2, \ldots$ em P tal que $x_i \in x_{i+1}P$ para todo $i \geq 1$. No entanto, isso contradiz o Lema 2.3.12. Logo, concluímos que P é um ideal principal. Em particular, $P = t\mathcal{O}_P$ para algum elemento primo $t \in P$.

Agora, resta-nos mostrar que os demais ideais de $\mathcal{O}_P$ também são principais. Seja $I \neq \{0\}$ ideal de $\mathcal{O}_P$. Definimos o conjunto:

$$C := \left\{ r \in \mathbb{N} \cup \{0\} : t^r \in I \right\}.$$

Notemos que C é não vazio, uma vez que dado $0 \neq x \in I \subseteq \mathcal{O}_P$, tem-se $x = t^r u$ com $u \in \mathcal{O}_P^\times$ e $r \in \mathbb{N} \cup \{0\}$. Então, como I é ideal, segue que $t^r = xu^{-1} \in I$. Tomemos $n := \min(C)$. Mostraremos que $I = t^n\mathcal{O}$.

Como $t^n \in I$ e I é um ideal, a inclusão $t^n\mathcal{O}_P \subseteq I$ é trivial. Para a outra inclusão, consideremos $0 \neq y \in I$. Sabemos pela Proposição 2.3.14 que $y = t^s w$, com $w \in \mathcal{O}_P^\times$ e $s \geq 0$. Assim, $t^s \in I$ e $s \geq n$, resultando que $y = t^n t^{s-n} w \in t^n\mathcal{O}_P$.

Logo, $\mathcal{O}_P$ é um domínio de ideais principais. □

Corolário 2.3.17. *Sejam F/K um corpo de funções e $t \in P$ um elemento primo de $P \in \mathbb{P}_F$. Então, $P = t\mathcal{O}_P$.*

Demonstração. Como P é um ideal de $\mathcal{O}_P$, para todo $t \in P$ segue que $t\mathcal{O}_P \subseteq P$. Agora, como $\mathcal{O}_P$ é um domínio de ideais principais e $t\mathcal{O}_P$ é um ideal primo de $\mathcal{O}_P$ (visto que t é primo), segue que $t\mathcal{O}_P$ é um ideal maximal de $\mathcal{O}_P$. Pela unicidade de P como ideal maximal, concluímos que $P = t\mathcal{O}_P$. □

Observação 2.3.18. Destacamos que a existência de um elemento primo em P decorre do fato de $\mathcal{O}_P$ ser um domínio de ideais principais; mais precisamente, do fato de que, em particular, P é um ideal principal. Soma-se a isso a condição de que P é um ideal maximal e, consequentemente, um ideal primo.

Sejam F/K um corpo de funções e P um lugar de F/K. Definimos uma aplicação $v_P : F \to \mathbb{Z} \cup \{\infty\}$ do seguinte modo: dado um elemento primo t de P, para cada $z \in F$, com $z \neq 0$, sabemos que z pode ser representado unicamente como $z = t^n u$, em que $n \in \mathbb{Z}$ e $u \in \mathcal{O}_P^\times$. Assim, definimos:

$$v_P(z) := n \quad \text{e} \quad v_P(0) = \infty.$$

Teorema 2.3.19. *Sejam F/K um corpo de funções, P um lugar de F/K e $v_P : F \to \mathbb{Z} \cup \{\infty\}$ a aplicação como definida acima. Então:*

(1) *v_P está bem definida, ou seja, independe da escolha do primo $t \in P$.*

(2) *v_P é uma valorização discreta de F.*

(3) *$\mathcal{O}_P, \mathcal{O}_P^\times$ e P podem ser expressos a partir de v_P como:*

$$\mathcal{O}_P = \Big\{z \in F : v_P(z) \geq 0\Big\};$$
$$\mathcal{O}_P^\times = \Big\{z \in F : v_P(z) = 0\Big\};$$
$$P = \Big\{z \in F : v_P(z) > 0\Big\}.$$

Demonstração. **(1)** Consideremos outro elemento primo de P, digamos t'. Sabemos, pelo Corolário 2.3.17, que $P = t\mathcal{O}_P = t'\mathcal{O}_P$, donde resulta que $t = t'w$ para algum $w \in \mathcal{O}_P^\times$. Consequentemente, dado $z = t^n u \in P$, segue que:

$$z = t^n u = (t'w)^n u = t'^n(w^n u),$$

sendo que $w^n u \in \mathcal{O}_P^\times$.

(2) Devemos mostrar que são válidas as propriedades (i), (iii) e (iv) da Definição 2.3.8 (visto que (ii) e a sobrejetividade seguem diretamente da definição apresentada).

Para (i), basta notar que, dado $0 \neq a \in K$, como K é corpo e $\mathcal{O}_P$ é anel de valorização, então $a \in \mathcal{O}_P^\times$. Assim, $a = t^0 a$, ou seja, $v(a) = 0$.

Para (ii), sejam $x, y \in F$. Suponhamos, sem perda de generalidade, que $x, y \neq 0$. Assim, $x = t^n u$ e $y = t^m r$, sendo $m, n \in \mathbb{Z}$ e $u, r \in \mathcal{O}_P^\times$. Como $ur \in \mathcal{O}_P^\times$, temos:

$$v_P(xy) = v\left(t^{m+n} ur\right) = m + n = v_P(x) + v_P(y).$$

Por fim, para (iv), consideremos $x, y \in F$, sem perda de generalidade, $x, y \neq 0$. Novamente, escrevemos $x = t^n u$ e $y = t^m r$, como acima. Suponhamos, sem perda de generalidade, que $n \leq m < \infty$, ou seja, $\min\{v_P(x), v_P(y)\} = n$. Sabemos que:

$$x + y = t^n u + t^m r = t^n \left(u + t^{m-n} r\right) =: t^n z,$$

em que $z \in \mathcal{O}_P$.

Caso $z = 0$, temos $v_P(x + y) = \infty > n$. Caso contrário, como $z \in \mathcal{O}_P$, podemos escrever $z = t^k s$, sendo $k \geq 0$ e $s \in \mathcal{O}_P^\times$. Desse modo,

$$x + y = t^n (t^k s) = t^{n+k} s$$

e, como consequência,

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

Destacamos que, caso tenhamos pelo menos uma das variáveis x ou y tomadas acima igual a zero, as propriedades (ii) e (iv) seguem diretamente da definição da valorização v_P em 0, juntamente às propriedades de ∞.

(3) A igualdade referente a $\mathcal{O}_P^\times$ segue do fato de v_P satisfazer (i). Por outro lado, como $P = t\mathcal{O}_P$, temos da Proposição 2.3.14 que todo elemento $z \in P$ se expressa como $z = t^m u$, em que $u \in \mathcal{O}_P^\times$ e $m \geq 1$. Então, $v(z) = m > 0$, garantindo a igualdade referente a P. Por fim, para $\mathcal{O}_P$ basta utilizar que $\mathcal{O}_P = \mathcal{O}_P^\times \cup P$. □

Corolário 2.3.20. *Um elemento $x \in F$ é um elemento primo de P se, e somente se, $v(x) = 1$.*

Demonstração. A demonstração segue da afirmação **(1)** do Teorema 2.3.19, ou seja, do fato de que v_P pode ser definida considerando-se qualquer elemento primo de P. □

Corolário 2.3.21. *Todo anel de valorização $\mathcal{O}$ de F/K é um subanel próprio maximal de F.*

Demonstração. Consideremos $\mathcal{O}$ um anel de valorização de F/K, cujo ideal maximal é P e cuja valorização correspondente é dada por v_P. Mostraremos que, dado $z \in F \setminus \mathcal{O}$, temos $F = \mathcal{O}[z]$. É imediato que $\mathcal{O}[z] \subset F$. Por outro lado, seja $y \in F$. Como $z \notin \mathcal{O}$, temos que $v_P(z^{-1}) > 0$. Assim, existe $k \in \mathbb{Z}$, com $k \geq 0$, tal que $v_P(yz^{-k}) \geq 0$. Portanto, segue que $w := yz^{-k} \in \mathcal{O}$ e, por consequência, $y = wz^k \in \mathcal{O}[z]$. Logo, $\mathcal{O}[z] = F$, resultando que $\mathcal{O}$ é um subanel próprio de F. □

Os Teoremas 2.3.11 e 2.3.19 são de grande importância na Teoria de Corpos de Funções, na medida em que demonstram a existência de uma correspondência biunívoca entre lugares e valorizações. Mais ainda, pela Observação 2.3.5 e pelo Corolário 2.3.21 essa correspondência também é válida considerando-se anéis de valorização e lugares.

Nessas circunstâncias, ao estudar determinado problema, podemos, muitas vezes, optar por qual abordagem será feita, ou seja, com base em anéis de valorização, valorizações ou lugares. Neste trabalho, trabalharemos essencialmente com valorizações e lugares. Assim, encerramos essa subseção exibindo conceitos mais específicos, relativos aos lugares, além do teorema que demonstra a existência dos mesmos.

Definição 2.3.22. *Sejam F/K corpo de funções e $P \in \mathbb{P}_F$ lugar associado ao anel de valorização $\mathcal{O}_P$. Dizemos que $F_P := \mathcal{O}_P/P$ é o* ***corpo de classes residuais de P*** *ou simplesmente o* ***corpo residual de*** *P.*

As classes residuais de P permitem a construção do mapa:

$$\begin{aligned} \phi : F &\to F_P \cup \{\infty\} \\ x &\mapsto x(P) \end{aligned}$$

em que $x(P) := x + P$ para todo $x \in \mathcal{O}_P$ e $x(P) := \infty$ se $x \in F \setminus \mathcal{O}_P$ (aqui, o símbolo ∞ não apresenta o mesmo significado do que nas valorizações).

Observação 2.3.23. Destacamos que a terminologia utilizada deve-se ao fato de que P é um ideal maximal e, portanto, F_P é, de fato, um corpo.

Além disso, destacamos que o mapa definido acima nos permite considerar K (ou mesmo $\tilde{K}$) como imerso em $\mathcal{O}_P/P$. Com efeito, analisando a restrição:

$$\phi\big|_{\mathcal{O}_P} : \mathcal{O}_P \to \mathcal{O}_P/P,$$

notamos que ela induz uma imersão canônica de K (analogamente de $\tilde{K}$) em $\mathcal{O}_P/P$.

Exemplo 2.3.24. Consideremos o anel de valorização $\mathcal{O}_{p(x)}$ e seu respectivo lugar $P = P_{p(x)}$, sendo $p(x)$ um polinômio mônico irredutível em $K[x]$, definidos como no Exemplo 2.3.6. Notemos que P é gerado por $p(x)$ e, consequentemente, $p(x)$ é um elemento primo de P.

Assim, dado um elemento $z \in K(x) \setminus \{0\}$, podemos escrevê-lo como:

$$z = p(x)^n \left(\frac{f(x)}{g(x)} \right),$$

em que $n \in \mathbb{Z}$ e $f(x), g(x) \in K[x]$, sendo que $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$.

Dessa forma, definimos a valorização v_P como $v_P(z) = n$.

Agora, para a determinação do corpo das classes residuais de P, a qual denotaremos por $K(x)_P$, definimos o homomorfismo:

$$\begin{aligned} \phi : K[x] &\rightarrow K(x)_P \\ f(x) &\mapsto f(x)(P) \end{aligned}$$

Claramente temos que ϕ é sobrejetivo e que $Ker(\phi) = \langle p(x) \rangle$. Logo, pelo Teorema dos Isomorfismos, ϕ induz um isomorfismo entre o corpo residual e $K(x)/\langle p(x) \rangle$, donde resulta:

$$K(x)_P \cong \frac{K[x]}{\langle p(x) \rangle}.$$

Definição 2.3.25. *Sejam F/K corpo de funções e $P \in \mathbb{P}_F$. Definimos o **grau de** P como sendo:*

$$\deg P := [F_P : K].$$

*No caso em que o grau de P é igual a 1, dizemos que P é um **lugar racional** de F/K.*

Observação 2.3.26. Os lugares racionais são uma ferramenta eficaz no estudo de diversos problemas, não somente relativos à Teoria de Corpos de Funções, como também na Geometria Algébrica. Nessas circunstâncias, considerando o corpo de funções racionais $K(x)/K$, sendo K algebricamente fechado, é possível demonstrar a existência de uma correspondência biunívoca entre o conjunto de lugares racionais e $\mathbb{P}^1 := K \cup \{\infty\}$ (*linha projetiva*). Para um estudo detalhado das relações entre lugares e os *espaços projetivos*, sugerimos consultar [14].

Exemplo 2.3.27. Destacamos que, ao considerarmos o corpo de funções racionais $K(x)/K$, os lugares $P_{p(x)}$ em que $p(x)$ é um polinômio mônico irredutível de grau 1 são exemplos de lugares racionais. Mais geralmente, temos pelo Exemplo 2.3.24 que $\deg P_{p(x)} = \deg p(x)$.

Pode-se demonstrar que o grau de um lugar é sempre finito. Em geral, temos:

Proposição 2.3.28. *Sejam P um lugar do corpo de funções F/K e $0 \neq x \in P$. Então:*

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

Demonstração. Sabemos que todo elemento não nulo em P é transcendente sobre K e, consequentemente, temos que $F/K(x)$ é uma extensão finita. Assim, precisamos

apenas mostrar que quaisquer n elementos $z_1, \ldots, z_n \in \mathcal{O}_P$, cujas classes residuais $z_1(P), \ldots, z_n(P) \in F_P$ são linearmente independentes sobre K, são linearmente independentes sobre $K(x)$.

Suponhamos, por absurdo, que exista uma combinação linear não trivial

$$\sum_{i=1}^{n} \varphi_i(x) z_i = 0,$$

em que $\varphi_i(x) \in K(x)$ para todo $i = 1, \ldots, n$.

Podemos supor que $\varphi_i(x)$ são polinômios em x (bastando multiplicar pelo mdc dos eventuais denominadores de $\varphi_i(x)$) e que x não divide todos eles. Denotemos $a_i := \varphi_i(0)$ (termo constante de $\varphi_i(x)$). Então, podemos escrever $\varphi_i(x) = a_i + x g_i(x)$, em que $g_i(x) \in K[x]$ e nem todos a_i são iguais a zero.

Agora, como $x \in P$ e $g_i(x) \in \mathcal{O}_P$, temos que $\varphi_i(x)(P) = a_i(P) = a_i$ para todo $i = 1, \ldots, n$. Aplicando o mapa de classes de resíduos na combinação linear, obtemos:

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

No entanto, isso contradiz o fato de que $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K. □

Corolário 2.3.29. *O corpo $\tilde{K}$ de constantes de F/K é uma extensão finita de K.*

Demonstração. Seja $P \in \mathbb{P}_F$. O mapa de classes residuais nos permite considerar $\tilde{K}$ imerso em F_P, consequentemente, $[\tilde{K} : K] \leq [F_P : K] < \infty$. □

Corolário 2.3.30. *Se K é algebricamente fechado em F, então todos os lugares de F/K são racionais.*

Demonstração. Consideremos P um lugar racional do corpo de funções F/K. Temos que $\deg P = 1$, donde $[F_P : K] = 1$ e, consequentemente, $F_P = K$. Assim, o mapa de classes residuais de P leva F em $K \cup \{\infty\}$.

Agora, seja $Q \in \mathbb{P}_F$ um lugar arbitrário. Pelo Corolário anterior, sabemos que $[\tilde{K} : K] \leq [F_Q : K]$ e, sendo K algebricamente fechado, temos que $K = \tilde{K}$, donde $\deg Q \geq 1$.

Por outro lado, seja L/K uma extensão algébrica de K. Como K é algebricamente fechado, temos que todo elemento de L satisfaz um polinômio linear e, logo, pertence a K. Assim, dada qualquer extensão algébrica de K, segue que $L = K$. Em outras palavras, como K é algebricamente fechado, não existe nenhuma extensão algébrica própria de K. Em particular, como F_Q/K é uma extensão algébrica, concluímos que $F_Q = K$.

Logo, temos $[F_Q : K] = 1$, ou seja, Q tem grau 1. Por fim, como Q foi tomado de forma arbitrária em $\mathbb{P}_F$, concluímos que todos lugares de F são racionais. □

Observação 2.3.31. Dado um corpo de funções F/K, como pelo Corolário 2.3.29, $\tilde{K}$ é uma extensão finita de K, segue que F pode ser tratado como um corpo de funções sobre $\tilde{K}$. De fato, seja $x \in F$ um elemento transcendente sobre K. Pelo Teorema de Lagrange para extensão de corpos, sabemos que:

$$[F : K(x)] = [F : \tilde{K}(x)][\tilde{K}(x) : K(x)].$$

Agora, como $F/K(x)$ e $\tilde{K}/K$ são extensões finitas, segue que $F/\tilde{K}(x)$ também o é. Logo, $F/\tilde{K}$ é um corpo de funções.

Desse modo, a menos da eventual substituição de $\tilde{K}$ por K, podemos considerar F/K um corpo de funções cujo corpo de constantes é completo, ou seja, em que K é algebricamente fechado em F. Nesse contexto, a partir deste momento, salvo em menção contrária, sempre que nos referirmos ao corpo de funções F/K iremos considerar K como sendo o corpo completo de constantes de F.

Definição 2.3.32. *Sejam $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um* ***zero de*** *z se $v_P(z) > 0$; por outro lado, dizemos que P é um* ***polo de*** *z se $v_P(z) < 0$, sendo v_P a valorização induzida por P.*

Mais geralmente, se $v_P(z) = m > 0$, dizemos que P é um ***zero de*** *z* ***de ordem*** *m, enquanto se $v_P(z) = -m < 0$, dizemos que P é um* ***polo de*** *z* ***de ordem*** *m.*

Finalmente, apresentamos o teorema segundo o qual todo corpo de funções admite um anel de valorização. Assim, por meio da correpondência biunívoca descrita anteriormente, garantimos a existência de um lugar e de uma valorização em qualquer corpo de funções. Mais precisamente, provaremos que todo elemento transcendente sobre K possui pelo menos um polo e um zero.

Teorema 2.3.33 (Existência de Anéis de Valorização). *Seja F/K um corpo de funções e seja R um subanel de F tal que $K \subseteq R \subseteq F$. Suponhamos que I é um ideal primo não nulo de R. Então, existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Demonstração. Consideremos o conjunto:

$$\mathcal{F} := \Big\{S : \ S \text{ é subanel de } F \text{ com } R \subseteq S \text{ e } IS \neq S\Big\}.$$

em que IS é calculado da mesma forma que o produto usual de ideais.

Mostraremos que, pelo Lema de Zorn, o conjunto $\mathcal{F}$ admite elemento maximal e que este elemento se caracteriza como um anel de valorização de F/K.

Primeiramente, notemos que $\mathcal{F}$ é não vazio, uma vez que o fato de I ser ideal primo de R nos garante que $IR \neq R$; consequentemente, $R \in \mathcal{F}$. Por outro lado, podemos estabelecer uma ordem parcial em $\mathcal{F}$ por meio de inclução.

Com efeito, seja $\mathcal{H} \subseteq \mathcal{F}$ um subconjunto totalmente ordenado de $\mathcal{F}$. Definimos:

$$T := \bigcup \{S : S \in \mathcal{H}\}.$$

Provaremos que $T \in \mathcal{F}$. Para tanto, observemos que, por definição, T é um subanel de $\mathcal{F}$ tal que $R \subseteq T$. Agora, suponhamos, por absurdo, que $IT = T$. Em particular, temos que a identidade de T se escreve como:

$$1 = \sum_{r=1}^{n} a_r t_r \ \text{, em que } a_r \in I \text{ e } t_r \in T \text{ para todo } r = 1, \ldots, n.$$

Como $\mathcal{H}$ é totalmente ordenado, existe $S_0 \in \mathcal{H}$ tal que $t_1, \ldots, t_n \in S_0$. Assim, segue que $1 \in IS_0$, contradizendo o fato de que $S_0 \in \mathcal{F}$.

Nessas condições, podemos aplicar o Lema de Zorn, resultando que $\mathcal{F}$ possui um elemento maximal, o qual denotaremos por $\mathcal{O}$. Como $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$, temos que $\mathcal{O}$ não apenas é um subanel de F contendo K, como também estas inclusões são estritas, i.e., $K \subsetneq \mathcal{O} \subsetneq F$.

Para demonstrarmos a segunda condição inerente aos anéis de valorização, procederemos por indução ao absurdo. Suponhamos que exista $z \in F$ tal que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Como $I \subseteq \mathcal{O} \setminus \mathcal{O}^{\times}$, temos que $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Em particular, como $1 \in \mathcal{O}[z] \cap \mathcal{O}[z^{-1}]$, podemos escrever:

$$\begin{aligned} 1 &= a_0 + a_1 z + \cdots + a_n z^n; \\ 1 &= b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}, \end{aligned}$$

em que $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ e $n, m \geq 1$.

Consideremos, sem perda de generalidade, que n, m são os menores naturais que verificam tais igualdades, ou seja, tais que os coeficientes em $I\mathcal{O}$ são todos não nulos. Suponhamos ainda, que $m \leq n$. Multiplicando as equações anteriores por $1 - b_0$ e $a_n z^n$ respectivamente, obtemos:

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}. \end{aligned}$$

Somando tais equações, obtemos uma equação da forma:

$$1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1},$$

em que $c_0, \ldots, c_{n-1} \in I\mathcal{O}$.

Entretanto, isso contradiz a minimalidade de n.

Portanto, segue que pelo menos uma das condições seguintes é satisfeita: ou $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Por consequência, $\mathcal{O}$ é um anel de valorização de F/K, de modo que $P = \mathcal{O} \setminus \mathcal{O}^{\times}$ é seu lugar correspondente. □

Corolário 2.3.34. *Seja F/K um corpo de funções e $z \in F$ um elemento transcendente sobre K. Então, z admite pelo menos um polo e um zero. Em particular, temos que $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Consideremos no teorema 2.3.33, $R = K[z]$ e o ideal $I = zK[z]$. Como vimos na demonstração de tal resultado, existe $P \in \mathbb{P}_F$ tal que $z \in P$. Consequentemente, pela caracterização de lugar via valorização, segue que P é um zero de z.

Esse argumento pode ser aplicado igualmente ao elemento z^{-1}, de modo que obtemos $Q \in \mathbb{P}_F$ tal que Q é zero de z^{-1}. Pelas propriedades de uma valorização, concluímos que Q é um polo de z. □

Observação 2.3.35. Destacamos que, apesar do chamado *Teorema da Aproximação Fraca* garantir ainda a existência de infinitos lugares para um corpo de funções arbitrário F/K, fixado um elemento $0 \neq x \in F$, há somente uma quantidade finita de polos e zeros a ele associados (consultar [28], Teorema 1.3.3).

2.3.2 Divisores e Gênero

Como descrito anteriormente, consideramos, nesta e nas próximas seções, F/K um corpo de funções cujo corpo de constantes K é completo em F.

Definição 2.3.36. *Dado um corpo de funções F/K, definimos o **grupo dos divisores de** F/K, denotado por $Div(F)$, como sendo o grupo abeliano livre gerado pelos lugares de F/K. Mais precisamente, temos que um **divisor**, i.e., um elemento do grupo $Div(F)$, é uma soma formal, a saber:*

$$D := \sum_{P \in \mathbb{P}_F} n_P P \ \text{, em que } n_P \in \mathbb{Z} \text{ e } n_P = 0 \text{ para quase todo } P.$$

*No caso em que $D = P$ para algum $P \in \mathbb{P}_F$, dizemos ainda que D é um **divisor primo**.*

Como $Div(F)$ é um grupo abeliano livre, podemos definir a soma de divisores de um corpo de funções e exibir seu elemento neutro. Formalmente, dados $D, D' \in Div(F)$, com $D = \sum n_P P$ e $D' = \sum n'_P P$, temos:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

Além disso, o elemento neutro de $Div(F)$ é dado por:

$$0 := \sum_{P \in \mathbb{P}_F} r_P P \text{ , em que } r_P = 0 \text{ para todo } P.$$

Na definição acima, ao estabelecermos que $n_P = 0$ para quase todo P, consideramos que $n_P \neq 0$ apenas para um número finito de lugares $P \in \mathbb{P}_F$. Este fato nos motiva à definição de *suporte de* $Div(F)$ e à observação de que o mesmo é finito.

Definição 2.3.37. *Definimos o* ***suporte*** *de Div(F) como sendo o conjunto:*

$$supp(D) := \Big\{P \in \mathbb{P}_F : n_P \neq 0\Big\}.$$

Consequentemente, podemos reescrever qualquer divisor de F/K como a soma finita:

$$D = \sum_{P \in\, supp(D)} n_P P.$$

A análise dos inteiros n_P presentes na escrita de um divisor fixado permite-nos ainda caracterizar um divisor como sendo *positivo* ou *negativo*. Mais geralmente, temos que $Div(F)$ é um grupo parcialmente ordenado.

Definição 2.3.38. *Dados os divisores $D = \sum n_P P$ e $D' = \sum n'_P P$, definimos uma* ***ordem parcial****, denotada por $\leq$, em $Div(F)$ como:*

$$D \leq D' \Leftrightarrow n_p \leq n'_p \ \text{ para todo } \ P \in \mathbb{P}_F.$$

Caso $n_P \geq 0$ (respectivamente $n_P \leq 0$) para todo $P \in \mathbb{P}_F$, dizemos que D é um divisor ***positivo*** *ou, ainda,* ***efetivo*** *(resp.* ***negativo****) e representamos por $D \geq 0$ (resp. $D \leq 0$).*

Definição 2.3.39. *Definimos o* ***grau*** *de um divisor $D \in Div(F)$ como:*

$$\deg(D) := \sum_{P \in \mathbb{P}_F} n_P \deg P.$$

A fim de exemplificarmos o conceito de divisor, podemos definir o divisor de um elemento não nulo $z \in F$. Mais geralmente, podemos definir divisor principal, dos zeros e dos polos de z.

Definição 2.3.40. *Dado $0 \neq z \in F$, denotemos por Z (respectivamente, N) o conjunto dos zeros (respectivamente, polos) de z. Consideremos ainda que, para cada $P \in \mathbb{P}_F$, v_P é a valorização correspondente. Então, definimos:*

$$\begin{aligned}
(z)_0 &:= \sum_{P \in Z} v_P(z) P \text{ , o } \textbf{\textit{divisor dos zeros de z}};\\
(z)_\infty &:= \sum_{P \in N} (-v_P(z))\, P \text{ , o } \textbf{\textit{divisor dos polos de z}};\\
(z) &:= (z)_0 - (z)_\infty \text{ , o } \textbf{\textit{divisor principal de z}}.
\end{aligned}$$

Resulta da definição acima que o divisor principal de z pode ser expresso como:

$$(z) = \sum_{P \in \mathbb{P}_F} v_P(z) P. \tag{2.3}$$

Observação 2.3.41. Sabemos que, fixado um elemento não nulo $z \in F$, existe apenas um número finito de polos e zeros com relação a z. Assim, garantimos que as noções de divisores de um polo e de zeros de um elemento não nulo $z \in F$ estão bem definidas.

Por outro lado, pela definição de zero e de polo de um elemento $0 \neq z \in F$, notamos que tanto o divisor dos zeros quanto o divisor dos polos de z é positivo, ou seja, $(z)_0 \geq 0$ e $(z)_\infty \geq 0$. Em particular, para os elementos constantes $x \in F \setminus \{0\}$, obtemos a seguinte caracterização:

$$x \in K \Leftrightarrow (x) = 0.$$

A partir da noção de divisor principal de um elemento $z \in F$, com $z \neq 0$, podemos definir alguns subgrupos relevantes no estudo de divisores.

Definição 2.3.42. *O **grupo de divisores principais** de F/K é definido como:*

$$Princ(F) := \Big\{(z) : z \in F \setminus \{0\}\Big\}.$$

Este é um subgrupo de $Div(F)$, bastando observar que, pela equação (2.3), para $x, y \in F$ com $x, y \neq 0$, tem-se:

$$(xy) = (x) + (y).$$

*Definimos ainda o **grupo das classes dos divisores** como o grupo quociente:*

$$Cl(F) := \frac{Div(F)}{Princ(F)}.$$

*Neste caso, para um divisor $D \in Div(F)$, sua classe correspondente é denotada por $[D]$. Ainda, dois divisores $D, D' \in Div(F)$ determinam a mesma classe, i.e., são **equivalentes**, se $D = D' + (x)$ para algum $x \in F \setminus \{0\}$.*

O estudo de divisores principais nos permite estabelecer resultados mais fortes, sobretudo com relação ao grau de um divisor. Nesse contexto, tem-se:

Teorema 2.3.43. *Todos os divisores principais possuem grau zero. Mais precisamente, temos que, para todo $z \in F \setminus \{0\}$,*

$$\deg (z)_0 = \deg (z)_\infty = [F : K(z)].$$

Demonstração. Para a demonstração da segunda igualdade, são necessárias propriedades dos *espaços de Riemann-Roch* que não detalharemos. A demonstração completa desse resultado pode ser encontrada em [28] (Teorema 1.4.11).

Agora, consideremos a validade de tal igualdade, ou seja, que $\deg(z)_\infty = [F : K(z)]$ para todo $z \in F \setminus \{0\}$. Notemos que $(z)_0 = (z^{-1})_\infty$ para todo $z \in F \setminus \{0\}$. Assim, temos:

$$\deg(z)_0 = \deg(z^{-1})_\infty = [F : K(z^{-1})] = [F : K(z)].$$

□

Corolário 2.3.44. *Se D e D' são divisores equivalentes, então D e D' possuem o mesmo grau.*

Demonstração. Com efeito, nessas condições sabemos que existe $x \in F \setminus \{0\}$ tal que $D = D' + (x)$. Agora, utilizando a definição de grau, temos:

$$\deg(D) = \deg(D' + (x)) = \deg(D') + \deg(x) = \deg(D'),$$

em que a última igualdade resulta diretamente do teorema, uma vez que:

$$\deg(x) = \deg(x)_0 - \deg(x)_\infty = 0.$$

□

Definição 2.3.45. *Dado $D \in Div(F)$, cuja classe correspondente é $[D]$, definimos o* ***grau da classe de equivalência*** $[D]$ *como* $\deg[D] := \deg(D)$.

Com o intuito de definirmos o *gênero* de um corpo de funções arbitrário, necessitaremos do estudo dos chamados *espaços de Riemmann-Roch* associados a um divisor, cujas propriedades serão apresentadas de modo sucinto. Posteriormente, quando nos aprofundarmos na análise de corpos de funções de uma curva, obteremos uma caracterização equivalente para o gênero, a qual se mostrará mais prática e intuitiva.

Definição 2.3.46. *Dado um divisor $D \in Div(F)$, definimos o* ***espaço de Riemann-Roch*** *associado a D como sendo:*

$$\mathcal{L}(D) := \Big\{x \in F : (x) \geq -D\Big\} \cup \Big\{0\Big\}.$$

Observação 2.3.47. Uma interpretação da definição acima pode ser obtida por meio da análise dos polos e zeros de x. Para tanto, representamos D como uma soma finita e separamos as parcelas positivas e as negativas, ou seja, consideramos:

$$D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j = \sum_{P \in \mathcal{P}_F} m_P P,$$

em que $r, s, n_i, m_j \in \mathbb{N}$ e $P_i, Q_j \in \mathbb{P}_F$ para todo $i = 1, \ldots, r$ e $j = 1, \ldots, s$.

Nessas condições, $\mathcal{L}(D)$ é constituído pelos elementos $(x) \in Div(F)$ dados por:

$$(x) := \sum_{P \in \mathbb{P}_F} v_P(x) P$$

tais que $v_P(x) \geq m_i - n_i$ para todo $P \in \mathbb{P}_F$.

Em outras palavras, $x \in \mathcal{L}(D)$ é tal que:

- x tem zeros de ordem $\geq m_j$ em Q_j para $j = 1, \ldots, s$.

- x tem polo no máximo em $P_1, \ldots, P_r$, sendo a ordem de cada possível polo em P_i limitada por n_i $(i = 1, \ldots, r)$.

Pode-se demonstrar que, para todo $D \in Div(F)$, o espaço de Riemann-Roch $\mathcal{L}(D)$ é um espaço vetorial sobre K (corpo completo de constantes de F) com dimensão finita. Além disso, segue diretamente do Teorema 2.3.43 que divisores equivalentes determinam espaços de Riemann-Roch isomorfos.

Sabendo que $\mathcal{L}(D)$ é um espaço vetorial sobre K, podemos obter condições para os casos em que tal espaço é trivial ou ainda igual a K. Nesse sentido, temos:

Proposição 2.3.48. *O espaço de Riemann-Roch de um divisor satisfaz as seguintes propriedades:*

(*i*) $\mathcal{L}(0) = K$;

(*ii*) *Se* $D \in Div(F)$ *é tal que* $D < 0$, *então* $\mathcal{L}(D) = \{0\}$.

Demonstração. (*i*) Sabemos que, dado $x \in K$, temos $(x) = 0$, ou seja, $K \subset \mathcal{L}(D)$. Por outro lado, seja $x \in \mathcal{L}(D)$, com $x \neq 0$, i.e., $x \in F$ e $(x) \geq 0$. Pela Observação 2.3.47, segue que x não possui polo. Consequentemente, x não pode ser um elemento transcendente sobre K, ou seja, $x \in K$ (Corolário 2.3.34).

(*ii*) Suponhamos, por absurdo, que exista um elemento $x \in \mathcal{L}(D)$ tal que $x \neq 0$. Então, $(x) \geq -D > 0$, ou seja, x admite um zero mas não admite um polo, uma contradição. Logo, $\mathcal{L}(D) = \{0\}$.

□

Definição 2.3.49. *Dado um divisor* $D \in Div(F)$, *o inteiro* $\ell(D) := \dim \mathcal{L}(D)$ *é denominado* ***dimensão de*** D.

O estudo da dimensão de $\mathcal{L}(D)$, em que $D \in Div(F)$, fornece importantes resultados, dos quais destacamos a caracterização de um divisor principal de grau zero.

Proposição 2.3.50. *Seja* D *um divisor de grau zero. As seguintes condições são equivalentes:*

(*i*) D *é um divisor principal;*

(*ii*) $\ell(D) \geq 1$;

(*iii*) $\ell(D) = 1$.

Demonstração. (*i*) $\Rightarrow$ (*ii*) Se D é um divisor principal, então $D = (x)$ para algum $x \in F$, donde resulta que $x^{-1} \in \mathcal{L}(D)$. Consequentemente, $\ell(D) \geq 1$.

(ii) $\Rightarrow$ (iii) Consideremos $\ell(D) \geq 1$, sendo $\deg(D) = 0$. Por definição, deve existir um divisor $D' \sim D$ tal que $D' \geq 0$. Por outro lado, como D' possui também grau zero, da condição $D' \geq 0$ resulta que $D' = 0$. Finalmente, pela Proposição 2.3.48, temos $\ell(D) = \ell(D') = \ell(0) = 1$.

(iii) $\Rightarrow$ (i) Consideremos que $\ell(D) = 1$, com $\deg(D) = 0$. Seja $z \in \mathcal{L}(D)$, com $z \neq 0$. Então, $(z) + D \geq 0$ e, como $\deg((z) + D) = 0$, segue que $(z) + D = 0$. Assim, $D = -(z) = (z^{-1})$, concluindo que D é principal. □

Definição 2.3.51. *Definimos o* ***gênero*** *de F/K como:*

$$g := \max\Big\{ \deg(D) - \ell(D) + 1 : \ D \in Div(F)\Big\}.$$

Observação 2.3.52. Para verificar que essa definição é consistente, torna-se necessário mostrar que o conjunto acima é limitado. De fato, existe uma constante $\gamma \in \mathbb{Z}$ tal que $\deg(D) - \ell(D) \leq \gamma$ para todo divisor $D \in Div(F)$. Além disso, pode-se mostrar que o gênero de um corpo de funções é necessariamente um inteiro não negativo, ou seja, $g \geq 0$. Demonstrações para esses resultados podem ser encontradas em [28] (Teorema 1.4 e Corolário 1.4.16).

Encerramos essa subseção enunciando um dos mais importantes resultados na Teoria de Corpos de Funções Algébricas, que é um caso particular do Teorema de Riemann-Roch (veja [28], Teorema 1.5.15).

Teorema 2.3.53 (**Teorema de Riemann**)**.** *Seja D um divisor de F/K tal que* $\deg(D) \geq 2g - 1$. *Então,*

$$\ell(D) = \deg(D) + 1 - g.$$

Para a demonstração, sugerimos consultar [28] (Teorema 1.5.17).

2.3.3 Extensões de Corpos de Funções

Conforme mostrado ao final da seção 2.1, sabemos que todo corpo de funções pode ser visto como uma extensão simples dos corpos de funções racionais, cujas principais características foram expostas por meio de exemplos ao longo das subseções anteriores. Nesse contexto, torna-se necessário estudarmos extensões de corpos de funções, assim como os principais conceitos resultantes dessa análise, como o de lugar *ramificado* ou *totalmente ramificado*.

Definição 2.3.54. *Um corpo de funções F'/K' é chamado uma* ***extensão algébrica do corpo de funções*** *F/K se $F' \supseteq F$ é uma extensão algébrica de corpos e $K' \supseteq K$. Se $[F' : F] < \infty$, dizemos ainda que F'/K' é uma* ***extensão finita*** *de F/K.*

Observação 2.3.55. Notemos que, em particular, se F'/K' é uma extensão algébrica do corpo de funções F/K, então K'/K é uma extensão algébrica e $F \cap K' = K$.

Para efeito de notação, sempre que nos referirmos ao corpo de funções F'/K', estaremos considerando-o uma extensão algébrica de F/K.

Ressaltamos que, como F'/K' é também um corpo de funções, no caso, sobre K', podemos estudar as relações entre os lugares de F e de F' e seus grupos de divisores.

Definição 2.3.56. *Consideremos uma extensão F'/K' do corpo de funções F/K. Dizemos que um lugar $P' \in \mathbb{P}_{F'}$ **está sobre** $P \in \mathbb{P}_F$ se $P \subset P'$. Pode-se ainda dizer que P' é uma **extensão** de P, que P **repousa** sobre P' ou que P é a restrição de P' em F. Nesse caso, escrevemos $P' \big| P$.*

Podemos obter uma equivalência de tal relação envolvendo os anéis de valorização e as valorizações asssociadas aos respectivos lugares de cada corpo de funções, conforme é demonstrado em [28] (Proposição 3.1.4).

Proposição 2.3.57. *Seja F'/K' uma extensão algébrica do corpo de funções F/K. Consideremos P (resp. P') um lugar de F/K (resp. F'/K') e sejam $\mathcal{O}_P$ (resp. $\mathcal{O}'_P$) e v_P (resp. v'_P) o anel de valorização e a valorização correspondentes. Então, as seguintes condições são equivalentes:*

(1) $P' \big| P$;

(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$;

(3) *Existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = e \cdot v_P(x)$.*

Mais precisamente, se $P' \big| P$, então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.

Observação 2.3.58. Essa equivalência nos permite estabelecer as condições necessárias a fim de que, dada uma extensão algébrica F'/K' de F/K e fixado um lugar $P \in \mathbb{P}_F$, exista um lugar P' que está sobre P. Mais geralmente, mostra-se que, fixado um lugar P de F/K, existe, no mínimo, um lugar $P' \in \mathbb{P}_{F'}$ tal que $P' \big| P$ (e, em geral, existe um número finito de lugares em F'/K' com essa propriedade). Reciprocamente, fixado $P' \in \mathbb{P}_{F'}$, existe um único lugar em F/K tal que $P' \big| P$, a saber $P = P' \cap F$. Para uma demonstração completa de ambos os resultados, sugerimos consultar [28] (Proposição 3.1.7).

Destacamos que, pela Proposição 2.3.57, garantimos a existência de uma imersão canônica do corpo residual $F_P = \mathcal{O}_P/P$ no corpo residual $F'_{P'} = \mathcal{O}_{P'}/P'$, a qual é dada por:

$$\begin{aligned} i : F_P &\hookrightarrow F'_{P'} \\ x(P) &\mapsto x(P') \end{aligned}$$

Assim, podemos considerar F_P como um subcorpo de $F'_{P'}$. Desse modo, torna-se possível fazer as seguintes definições:

Definição 2.3.59. *Seja F'/K' uma extensão algébrica de F/K e sejam $P' \in \mathbb{P}'_F$ um lugar que está sobre $P \in \mathbb{P}_F$.*

(*i*) $f\left(P'\middle|P\right) := [F'_{P'} : F_P]$ *é denominado* ***grau relativo de*** P' ***sobre*** P.

(*ii*) *O inteiro positivo* $e\left(P'\middle|P\right) :=$ *e tal que*

$$v_{P'}(x) = e \cdot v_P(x) \text{ para todo } x \in F$$

é denominado ***índice de ramificação de*** P' ***sobre*** P.

Sob essas circunstâncias, dizemos que $P'\middle|P$ *é* ***ramificado*** *se* $e > 1$ *e, caso contrário, ou seja, se* $e = 1$, *dizemos que* $P'\middle|P$ *é* ***não ramificado***.

Além disso, dizemos que P *é* ***ramificado*** *(recip.* ***não ramificado****) em* F'/F *se existe pelo menos um lugar* $P' \in \mathbb{P}_{F'}$ *tal que* $P'\middle|P$ *é ramificado (recip. não ramificado).*

Definição 2.3.60. *Seja F'/K' uma extensão algébrica de F/K e seja $P \in \mathbb{P}_F$.*

(*i*) *Caso exista apenas um lugar* $P' \in \mathbb{P}_{F'}$ *tal que* P' *é uma extensão de* P *e se* $e\left(P'\middle|P\right) = [F' : F]$, *dizemos que* P *é* ***totalmente ramificado*** *em* F'/F.

(*ii*) *Caso existam exatamente* $n = [F' : F]$ *lugares* $P' \in \mathbb{P}_{F'}$ *que sejam extensões de* P, *dizemos que* P ***se decompõe completamente*** *em* F'/F.

Com o intuito de estabelecermos um homomorfismo entre os grupos de divisores de F'/K' e F/K, apresentamos o conceito de *conorma*.

Definição 2.3.61. *Seja F'/K' uma extensão algébrica de F/K. Dado um lugar $P \in \mathbb{P}_F$, definimos a* ***conorma em*** P ***com respeito a*** F'/F *como sendo a soma formal:*

$$Con_{F'/F}(P) := \sum_{P'|P} e\left(P'\middle|P\right) P,$$

em que essa soma percorre todos os lugares $P' \in \mathbb{P}_{F'}$ *que estão sobre* P.

Dessa forma, podemos definir o ***mapa da conorma com respeito a*** F'/F, *o qual se estende a um homomorfismo de* $Div(F)$ *em* $Div(F')$ *fazendo:*

$$Con_{F'/F}\left(\sum n_P P\right) := \sum n_p \cdot Con_{F'/F}(P).$$

Observação 2.3.62. Pode-se demonstrar que a conorma leva divisores principais de F em divisores principais de F'. Além disso, o mapa definido acima induz um homomorfismo entre os grupos das classes de divisores $Cl(F)$ e $Cl(F')$, o qual é denotado por $Con_{F'/F}$ também.

2.4 CORPOS DE FUNÇÕES SOBRE CORPOS FINITOS

Nessa seção, estudaremos corpos de funções da forma F/K, em que K é um corpo de constantes finito, isto é, $F/\mathbb{F}_q$ em que q é uma potência de um número primo.

Primeiramente, estudaremos o grupo de divisores de tais corpos, com ênfase nos positivos, e, a seguir, analisaremos outros subgrupos de $Div(F)$.

Proposição 2.4.1. *Seja $F/\mathbb{F}_q$ um corpo de funções. Para todo inteiro $n \geq 0$, existe apenas um número finito de divisores positivos de grau n.*

Demonstração. Sabemos que um divisor positivo pode ser visto como a soma de divisores primos. Desse modo, temos que mostrar que, fixado $n \geq 0$, o seguinte conjunto é finito:

$$S := \left\{ P \in \mathbb{P}_F : \deg P \leq n \right\}.$$

Fixemos um elemento $x \in F \setminus \mathbb{F}_q$ (note que x é transcendente sobre $\mathbb{F}_q$) e consideremos o conjunto:

$$S_0 := \left\{ P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} : \deg P_0 \leq n \right\}.$$

Observemos que, para todo $P \in S$, temos $P \cap \mathbb{F}_q(x) \in S_0$. Com efeito, dado $P \in S$, associamos P à sua (única) valorização correspondente $v_P : F \to \mathbb{Z} \cup \{\infty\}$. Por outro lado, $P \cap \mathbb{F}_q(x)$ está associado a uma valorização $v : \mathbb{F}_q(x) \to \mathbb{Z} \cup \{\infty\}$, a qual, pela unicidade, deve ser igual à restrição de v_P em $\mathbb{F}_q(x)$. Assim, tal valorização está associada unicamente a um lugar de $\mathbb{F}_q(x)$, confirmando a afirmação anterior.

Além disso, sabemos que cada $P_0 \in S_0$ possui apenas um número finito de extensões em F. Então, basta mostrarmos que S_0 é finito. Como o conjunto de lugares de $\mathbb{F}_q(x)$ corresponde ao conjunto de polinômios mônicos irredutíveis $p(x) \in \mathbb{F}_q[x]$ de mesmo grau (visto que o grau do lugar corresponde ao grau do polinômio pelo Exemplo 2.3.27). Agora, como estamos considerando o corpo de constantes finito, o número de tais polinômios é finito, concluindo a demonstração. □

A partir desse resultado, temos que, em particular, se definirmos um subgrupo de $Div(F)$ constituído apenas por divisores positivos de grau não negativo previamente fixado, então tal subgrupo é finito, possibilitando a seguinte definição:

Definição 2.4.2. *Para cada n inteiro não negativo, definimos o número A_n como:*

$$A_n := \left| \left\{ D \in Div(F) : D \geq 0 \; e \; \deg(D) = n \right\} \right|.$$

Podemos nos perguntar se ao considerarmos o conjunto de divisores não necessariamente positivos com grau fixo, continuamos tendo um conjunto de cardinalidade finita. Pode-se demonstrar que isso ocorre, veja [28] (Proposição 5.1.3).

Quanto aos conjuntos de divisores mencionados acima, utilizaremos posteriormente aquele cujo grau dos divisores é exatamente igual a zero, além, evidentemente, dos lugares racionais. Assim, necessitamos das seguintes definições:

Definição 2.4.3. *Definimos o* ***grupo de divisores de grau zero*** *como sendo o subgrupo:*

$$Div^0(F) := \Big\{D \in Div(F) : \ \deg(D) = 0\Big\}$$

e o ***grupo das classes de divisores de grau zero*** *como:*

$$Cl^0(F) := \Big\{[D] \in Cl(F) : \ \deg[D] = 0\Big\}$$

Observação 2.4.4. Destacamos que $Cl^0(F)$ está bem definido, pois, conforme já demonstrado, temos que $\deg[D] = \deg(D)$. Dessa maneira, $Cl^0(F)$ é constituído pelas classes de divisores cujo grau é zero. Mais ainda, temos que ambos os subgrupos definidos acima são não vazios, bastando considerar os divisores principais e suas respectivas classes de elementos $x \in F \setminus \{0\}$. É interessante destacar que no caso em que o gênero é igual a zero, pelo Teorema de Riemann, os divisores principais são os únicos divisores cujo grau é zero.

Definição 2.4.5. *Definimos h_F o* ***número de classe de divisores*** *de F como a ordem do grupo $Cl^0(F)$, ou seja, $h_F := \left|Cl^0(F)\right|$.*

Retornando à definição dos números A_n, um segundo questionamento se refere a como estimá-los. Esse questionamento torna-se ainda mais relevante ao estudarmos o conjunto de lugares racionais de um corpo de funções F/F_q e se configura como um dos estudos centrais na Teoria de Corpos de Funções e na Teoria de Corpos Finitos. Nesse contexto, estamos interessados em estimar ou mesmo estabelecer o valor exato, quando possível, do número de lugares racionais de $F/\mathbb{F}_q$. Em função da relevância desse tópico, designamos a próxima notação.

Definição 2.4.6. *Definimos o* ***número de lugares racionais*** *de $F/\mathbb{F}_q$ por:*

$$N := N(F) = \Big|\Big\{P \in \mathbb{P}_F : \deg P = 1\Big\}\Big|.$$

Proposição 2.4.7. *Temos que $N = N(F) = A_1$.*

Demonstração. Para efeito de notação, consideremos $A_1 = |C|$, em que C denota o conjunto de divisores positivos cujo grau é igual a 1.

Primeiramente, temos que o conjunto dos lugares racionais de $F/\mathbb{F}_q$ é um subconjunto de C, pois cada lugar pode ser visto como a soma finita de lugares, no caso, a soma de apenas um elemento. Dessa maneira, resta-nos mostrar que todo divisor positivo é necessariamente um lugar.

Notemos que, dados $P, P_1, P_2 \in \mathbb{P}_F$, os conjuntos nP, sendo n natural, e $P_1 + P_2$ são lugares de $\mathbb{P}_F$. Para tanto, basta utilizarmos a correspondência entre lugares e valorizações. Mais precisamente, se v_P, v_{P_1}, v_{P_2} representam as respectivas valorizações de P, P_1, P_2, temos que nP e $P_1 + P_2$ podem ser expressos como os lugares associados às valorizações nv_P e $v_{P_1} + v_{P_2}$.

Portanto, combinando esses dois resultados e utilizando indução, temos que C está contido no conjunto de lugares racionais, concluindo a prova. □

Nessas circunstâncias, podemos nos aprofundar no estudo dos números A_n, os quais nos fornecem a *função Zeta de* $F/\mathbb{F}_q$ e seu respectivo *L-polinômio*.

Definição 2.4.8. *A* ***função Zeta de*** $F/\mathbb{F}_q$ *é definida como a seguinte série de potências:*

$$Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]].$$

No caso em que o corpo de funções $F/\mathbb{F}_q$ *tem gênero* g*, a função Zeta é racional e satisfaz*

$$Z_F(t) = \frac{L_F(t)}{(1-t)(1-qt)},$$

sendo $L_F(t)$ *é um polinômio em* t*. Neste caso, denominamos* $L_F(t)$ *de* $L-$***polinômio de*** F*.*

Pode-se demonstrar que a função Zeta converge quando a variável complexa t é tal que $|t| < q^{-1}$, em que q é a cardinalidade do corpo de constantes. Mais precisamente, temos que, sob tal condição, $Z_F(t)$ pode ser expressa como um produto absolutamente convergente, a saber:

$$Z_F(t) = \prod_{P \in \mathbb{P}_F} (1 - t^{\deg P})^{-1}.$$

Tal representação é conhecida como Produto de Euler e sua demonstração se encontra em [28] (Proposição 5.1.8).

Apesar dessa representação apresentar uma visão mais detalhada quanto à função Zeta, sua aplicabilidade pode se mostrar complexa em determinados problemas. Neste cenário, surge uma nova representação da função $Z_F(t)$ por meio da *equação funcional* a seguir:

$$Z_F(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right).$$

Por outro lado, o estudo aprofundado da convergência de $Z(t)$ nos permite demonstrar que $L_F(t)$ é um polinômio em $\mathbb{Z}[t]$ cujo grau é igual a $2g$ ([28], Corolário 5.1.12), resultando que ele pode ser escrito como:

$$L_F(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g},$$

em que cada $a_i \in \mathbb{Z}$, sendo $i = 0, \ldots, 2g$.

A importância do L-polinômio, especialmente visto sob tal representação reside no fato de que o mesmo contém informações sobre os números A_n. Formalmente, utilizando a equação funcional de $Z(t)$, juntamente ao fato de $L_F(t) \in \mathbb{Z}[t]$ ser um polinômio de grau $2g$, é possível mostrar ([28], Teorema 5.1.15) que:

$$A_1 = N = a_1 + (q + 1).$$

Portanto, obtemos um método para o cálculo do número de lugares racionais de $F/\mathbb{F}_q$ por meio do L-polinômio. Entretanto, sem o cálculo explícito do polinômio, ainda não somos capazes de estimar o valor de N. Nesse contexto, uma das primeiras e principais estimativas para N foi fornecida por Hasse e Weil no início do século XX.

Antes porém, destacamos que, conforme demonstrado em [28] (Teorema 5.1.15), o polinômio $L_F(t)$ pode ser fatorado em $\mathbb{C}[t]$ a partir de inteiros algébricos da seguinte forma:

$$L_F(t) = \prod_{i=1}^{2g} (1 - \alpha_i t), \tag{2.4}$$

em que os complexos α_i são inteiros algébricos, inversos das raízes de $L_F(t)$ de forma que $\alpha_{g+i} = \overline{\alpha_i}$.

Por meio de uma série de resultados auxiliares, Hasse e Weil demonstraram o seguinte teorema, cuja prova é apresentada em [28] (Teorema 5.2.1), o qual é considerado como a Hipótese de Riemann para Corpos de Funções.

Teorema 2.4.9 (**Teorema de Hasse-Weil**). *Os inteiros algébricos α_i presentes na fatoração de $L_F(t)$ satisfazem a igualdade:*

$$|\alpha_i| = q^{1/2} \ \textit{para todo} \ \ i = 1, \ldots, 2g\,.$$

Uma das conclusões cruciais desse teorema é exatamente uma condição de limitação para N (consultar [28], Teorema 5.2.3):

Teorema 2.4.10 (**Cota de Hasse-Weil**). *O número N de lugares racionais de $F/\mathbb{F}_q$ satisfaz a inequação:*

$$|N - (q + 1)| \leq 2gq^{1/2}\,.$$

É interessante destacar que há exemplos de corpos $F/\mathbb{F}_q$ cujo número de lugares racionais atinge a cota superior apresentada:

Definição 2.4.11. *Um corpo de funções $F/\mathbb{F}_q$ de gênero g é denominado* ***maximal*** *se*

$$N = q + 1 + 2gq^{1/2}\,.$$

Ressaltamos que, a fim de N ser finito como esperado, devemos ter q sendo um quadrado perfeito; ou seja, apenas sob essa condição existem corpos maximais. Tendo em vista tal exigência, na construção de reticulados via corpos de funções, utilizaremos por vezes corpos de funções da forma $F/\mathbb{F}_{q^2}$.

3 RETICULADOS

O estudo de reticulados tem se mostrado uma importante ferramenta na Teoria de Códigos e de Telecomunicações, além de despertar grande interesse do ponto de vista teórico. Sob essa perspectiva, um dos principais problemas consiste em, fixada a dimensão, obter um reticulado que satisfaça determinada propriedade ou, mais precisamente, classes de reticulados que cumpram a mesma para diversas dimensões.

Com o objetivo de explorar tais problemas em contextos específicos, este capítulo estabelecerá os conceitos básicos no estudo de reticulados. Dessa forma, inicialmente apresentaremos as principais definições e, a seguir, nos aprofundaremos no estudo dos chamados *sub-reticulados* e das *regiões fundamentais*, as quais permitem associar a visão algébrica à visão geométrica de reticulados. Posteriormente, estabeleceremos uma correspondência entre quocientes de espaços euclideanos n-dimensionais por reticulados e toros n-dimensionais. Essa abordagem possibilitará estender a visão topológica a respeito dos reticulados, além de simplificar o cálculo de seu volume sob determinadas circunstâncias. Ao fim do capítulo, apresentaremos problemas relevantes envolvendo reticulados, tais como a densidade de empacotamento, o número de vizinhos e o raio de cobertura.

Ao longo desse capítulo, os parâmetros relacionados aos reticulados serão estudados essencialmente considerando a métrica euclidiana. Para o estudo dos mesmos sob a métrica da soma, sugerimos consultar [17].

3.1 NOÇÕES GERAIS

Nesta seção, apresentaremos conceitos básicos sobre *reticulados*. Para efeito de notação, sempre que nos referirmos ao espaço $\mathbb{R}^n$, estaremos considerando $n \in \mathbb{N}$ fixado.

Definição 3.1.1. *Seja $\{v_1, \ldots, v_m\}$ um conjunto arbitrário de vetores linearmente independentes em $\mathbb{R}^n$ tal que $m \leq n$. Definimos o **reticulado** com relação a este conjunto como sendo:*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i : \ \lambda_i \in \mathbb{Z} \ \text{ para todo } i = 1, \ldots, m \right\}.$$

*Neste caso, dizemos ainda que $\{v_1, \ldots, v_m\}$ é **uma base** do reticulado.*

Notemos que, pela definição apresentada, um reticulado é um subgrupo de $(\mathbb{R}^n, +)$, visto que Λ é fechado para a soma de vetores. Mostra-se ainda que trata-se de um subgrupo aditivo discreto de $\mathbb{R}^n$. Tal descrição é mais abrangente e nos fornece uma caracterização equivalente para reticulado, a qual será apresentada ao final desta seção.

Observação 3.1.2. É importante ressaltar que o conjunto $\{v_1, \ldots, v_m\}$ é, de fato, apenas uma base para o reticulado, ou seja, não é a única base possível. Mais ainda, fixado um reticulado Λ, afirmamos que o mesmo admite diversas bases.

Aprofundaremos nessa análise ao apresentarmos o conceito de *matriz geradora*, quando estabeleceremos condições a fim de que dois conjuntos distintos linearmente independentes gerem o mesmo reticulado (Proposição 3.1.7).

Neste momento, destacamos apenas que todas as bases de um mesmo reticulado possuem o mesmo número de vetores, o que motiva a próxima definição.

Definição 3.1.3. *Denominamos* ***posto*** *de um reticulado Λ o número de vetores de uma base de Λ (representado por m), ou seja, a dimensão do subespaço gerado por Λ em $\mathbb{R}^n$. No caso em que $m = n$, diremos ainda que o reticulado tem* ***posto máximo*** *(ou* ***completo****).*

Exemplo 3.1.4. Consideremos em $\mathbb{R}^2$ o conjunto $\{(1,3),(1,0)\}$. Como tais vetores são linearmente independentes, constituem uma base para um reticulado de posto 2:

$$\begin{aligned} \Lambda_0 &= \Big\{\lambda_1(1,3) + \lambda_2(1,0) : \lambda_1, \lambda_2 \in \mathbb{Z}\Big\} \\ &= \Big\{(\lambda_1 + \lambda_2, 3\lambda_1) : \lambda_1, \lambda_2 \in \mathbb{Z}\Big\} \\ &= \Big\{(m, 3n) : m, n \in \mathbb{Z}\Big\}. \end{aligned}$$

A figura a seguir mostra a disposição de alguns dos pontos deste reticulado:

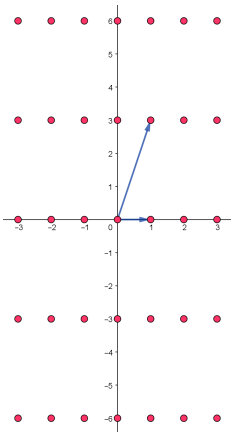


Figura 1 – Reticulado Λ_0

Destacamos que, de modo semelhante, poderíamos adotar o conjunto $\{(0,3),(1,0)\}$ como uma outra base para o reticulado representado acima.

Definição 3.1.5. *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\{v_1, \ldots, v_m\}$ uma base para Λ. Para cada $i = 1, \ldots, m$, consideremos $v_i = (v_{i1}, \ldots, v_{in})$. Denominamos de* ***matriz geradora*** *do reticulado*

Λ *uma matriz* M *formada pelos vetores de uma base de* Λ *dispostos em suas linhas, ou seja,*

$$M = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}.$$

Nessas circunstâncias, a matriz $\mathcal{G} = MM^T$*, cujas entradas são dadas por* $g_{ij} = \left\langle v_i, v_j \right\rangle$ *para* $1 \leq i, j \leq m$*, é denominada uma* ***matriz de Gram*** *para o reticulado* Λ*.*

Observação 3.1.6. Notemos que o conceito de matriz geradora deve-se ao fato de que um reticulado Λ de posto m pode ser reescrito como:

$$\Lambda = \left\{(\lambda_{1i})_{1\times m} M : \ \lambda_{1i} \in \mathbb{Z} \text{ para todo } i = 1, \dots, m\right\},$$

em que $(\lambda_{1i})_{1\times m}$ denota uma matriz de tamanho $1 \times m$ cujas entradas são dadas por $\lambda_{1i} := \lambda_i \in \mathbb{Z}$ para todo $i \in \{1, \dots, m\}$.

Com efeito, se $\{v_1, \dots, v_m\}$ constitui uma base para o reticulado Λ, e cada vetor v_i, com $i = 1, \dots, m$, pode ser visto como $v_i = (v_{i1}, \dots, v_{in})$, temos, por definição, que um ponto $p \in \Lambda$ é da forma:

$$\begin{aligned} p &= \lambda_1(v_{11}, \dots, v_{1n}) + \cdots + \lambda_m(v_{m1}, \dots, v_{mn}) \\ &= \left(\sum_{i=1}^{m} \lambda_i v_{i1}, \dots, \sum_{i=1}^{m} \lambda_i v_{in}\right) \end{aligned}$$

em que $\lambda_i \in \mathbb{Z}$ para todo $i = 1, \dots, m$.

Logo, segue que Λ é o conjunto de pontos obtidos a partir da multiplicação:

$$(\lambda_{1i})M = \begin{pmatrix} \lambda_1 & \cdots & \lambda_m \end{pmatrix} \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}.$$

Portanto, sendo M uma matriz geradora para o reticulado Λ, podemos representá-lo como:

$$\Lambda = \left\{\lambda M : \ \lambda \in \mathbb{Z}^m\right\}. \tag{3.1}$$

Conforme visto anteriormente, existem infinitas bases para um reticulado Λ; consequentemente, existem infinitas matrizes geradoras para tal reticulado. Então, podemos nos perguntar quando matrizes distintas geram o mesmo reticulado. Nesse contexto, temos:

Proposição 3.1.7. *Duas matrizes* M_1 *e* M_2 *geram o mesmo reticulado se, e somente se, existe uma matriz unimodular* U *(i.e., com entradas inteiras e tal que* $\det U = \pm 1$*) satisfazendo* $M_2 = UM_1$*.*

Demonstração. ($\Rightarrow$) Seja Λ um reticulado de $\mathbb{R}^n$ de posto $m \leq n$.

Sejam M_1 e M_2 matrizes geradoras de Λ com relação às bases $\{a_1, \ldots, a_m\}$ e $\{b_1, \ldots, b_m\}$, respectivamente.

Como M_1 gera o reticulado Λ, sabemos que todo ponto de Λ se expressa como combinação linear inteira dos vetores $a_1, \ldots, a_m$. Em particular, para cada vetor b_{i_0}, com $i_0 \in \{1, \ldots, m\}$ fixado, é possível obter escalares inteiros u_{i_0} tais que:

$$b_{i_0} = \sum_{i=1}^{m} u_{i_0} a_i.$$

Nesse caso, cada j-ésima coordenada fixada de b_{i_0}, sendo $j = 1, \ldots, m$, será determinada por:

$$b_{i_0 j} = \sum_{i=1}^{m} u_{i_0} a_{ij}.$$

Desse modo, existe uma matriz U com entradas inteiras satisfazendo $M_2 = UM_1$.

Reciprocamente, existe uma matriz V de entradas inteiras tais que $M_1 = VM_2$.

Segue dessas igualdades que:

$$M_2 = UM_1 = UVM_2.$$

Assim, $UV = I_d$ e, consequentemente, $\det U = \pm 1$, como queríamos mostrar.

($\Leftarrow$) Sejam M_1 e M_2 matrizes satisfazendo $M_2 = UM_1$ para alguma matriz unimodular U.

Sejam Λ e Λ' os reticulados gerados por M_1 e M_2 respectivamente. Mostraremos que $\Lambda = \Lambda'$.

Tomemos $p \in \Lambda'$. Conforme mostrado na observação anterior, temos que existe $c \in \mathbb{Z}^m$ tal que $p = cM_2$. Agora, utilizando que $M_2 = UM_1$, segue:

$$p = cM_2 = (cU)M_1 = c'M_1.$$

Como $c' \in \mathbb{Z}^m$, resulta que $p \in \Lambda$ e, consequentemente, $\Lambda' \subseteq \Lambda$.

A demonstração de que $\Lambda \subseteq \Lambda'$ é inteiramente análoga, bastando observar que, como U é unimodular, em particular, uma matriz invertível, temos $M_1 = U^{-1}M_2$.

Portanto, M_1 e M_2 são matrizes geradoras para um mesmo reticulado. □

Corolário 3.1.8. *No caso em que as matrizes M_1 e M_2 são matrizes geradoras de Λ, as respectivas matrizes de Gram, denotadas por $\mathcal{G}_1$ e $\mathcal{G}_2$ estão relacionadas da seguinte forma:*

$$\mathcal{G}_2 = U\mathcal{G}_1U^T.$$

Em particular, o determinante de qualquer matriz de Gram para o reticulado Λ não varia.

Demonstração. Como M_1 e M_2 são matrizes geradoras de Λ, sabemos que existe uma matriz unimodular U tal que $M_2 = UM_1$. Assim, utilizando a definição de matriz de Gram, obtemos:

$$\mathcal{G}_2 = M_2\left(M_2^T\right) = UM_1(UM_1)^T = U\left(M_1M_1^T\right)U^T = U\mathcal{G}_1U^T.$$

Por outro lado, como $\det U^T = \det U = \pm 1$, segue que $\det(UU^T) = 1$, donde, sendo o determinante uma função multiplicativa, resulta $\det \mathcal{G}_2 = \det \mathcal{G}_1$. □

Definição 3.1.9. *Definimos o* ***determinante*** *de um reticulado Λ e denotamos por* $\det(\Lambda)$ *o determinante de uma matriz de Gram de Λ.*

Exemplo 3.1.10. Consideremos o reticulado ilustrado abaixo, chamado *reticulado hexagonal*, com duas bases distintas $\{(1,0),(1/2,\sqrt{3}/2)\}$ e $\{(3/2,\sqrt{3}/2),(7/2,3\sqrt{3}/2)\}$.

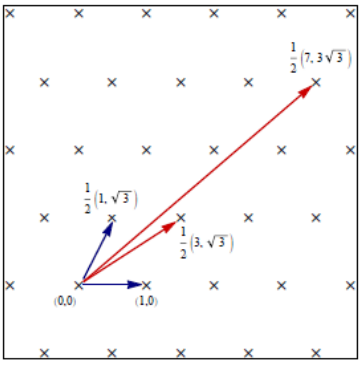


Figura 2 – Reticulado Hexagonal [5]

As matrizes associadas a essas bases são:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} \text{ e } M_2 = \begin{pmatrix} 3/2 & \sqrt{3}/2 \\ 7/2 & 3\sqrt{3}/2 \end{pmatrix},$$

cujas matrizes de Gram são, respectivamente,

$$\mathcal{G}_1 = \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} \qquad \text{e} \qquad \mathcal{G}_2 = \frac{1}{4}\begin{pmatrix} 12 & 30 \\ 30 & 76 \end{pmatrix}.$$

Utilizando uma dessas matrizes de Gram, concluímos que o determinante do reticulado hexagonal é 3/4.

Observação 3.1.11. Destacamos que, no caso em que o reticulado Λ tem posto completo, suas matrizes geradoras são todas quadradas e, consequentemente, o determinante do reticulado é dado por $\det(\Lambda) = \det^2(M)$, em que M é uma matriz geradora de Λ.

Por fim, mostraremos que é possível definir um reticulado como sendo um subgrupo aditivo discreto de $\mathbb{R}^n$. Antes, porém, relembramos o conceito de *conjunto discreto* e definimos o *subespaço coberto por* Λ.

Definição 3.1.12. *Seja d uma métrica em $\mathbb{R}^n$. Dado $r \in \mathbb{R}$ com $r > 0$, definimos a* ***bola fechada (em $\mathbb{R}^n$) centrada em*** $0 = (0, \ldots, 0) \in \mathbb{R}^n$ ***e de raio*** *r como:*

$$B_d[0, r] := \left\{ z \in \mathbb{R}^n : \ d(z, 0) \leq r \right\}.$$

No caso em que d é a métrica euclidiana, definimos ainda $d(x, y) = ||x - y||$ para quaisquer $x, y \in \mathbb{R}^n$. Neste caso, lembramos que dado $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, temos:

$$||x|| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}.$$

Nessas condições, no caso em que d é a métrica eucliana denotaremos a bola fechada de raio r centrada na origem simplesmente por $B[0, r]$, sendo:

$$B[0, r] := \left\{ z \in \mathbb{R}^n : \ ||z|| \leq r \right\}.$$

Definição 3.1.13. *Dizemos que um conjunto $X \subset \mathbb{R}^n$ é* ***discreto*** *se, para qualquer $r \in \mathbb{R}$ sendo $r > 0$, a bola fechada $B[0, r]$ intersecta X em um número finito de pontos.*

Observação 3.1.14. Destacamos que a definição de conjunto discreto poderia ser feita a partir de uma métrica arbitrária, tendo em vista a equivalência das normas em $\mathbb{R}^n$. A escolha pela métrica euclidiana foi somente para simplificar as notações.

Definição 3.1.15. *Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, de posto $m \leq n$ e com uma matriz geradora M, definimos o subespaço m-dimensional de $\mathbb{R}^n$ coberto por Λ, denotado por* ***span (Λ)****, como sendo o conjunto:*

$$span\ (\Lambda) = \left\{ uM : \ u \in \mathbb{R}^m \right\}.$$

Ou equivalentemente, se $\{v_1, \ldots, v_m\}$ é a base de Λ associada à matriz geradora M, temos:

$$span\ (\Lambda) = \left\{ \sum_{i=1}^{m} u_i v_i : \ u_i \in \mathbb{R} \ \ para\ todo\ i = 1, \ldots, m \right\}.$$

Observação 3.1.16. Primeiramente, observemos que a definição acima é consistente, na medida em que independe da matriz geradora escolhida para Λ. De fato, dadas matrizes geradoras distintas M_1 e M_2 para Λ, sabemos que $M_2 = UM_1$ ou, equivalentemente, $M_1 = U^{-1}M_2$, sendo U uma matriz $m \times m$ unimodular de entradas inteiras.

De forma semelhante à argumentação feita na Proposição 3.1.7, usamos que $u' = uU \in \mathbb{R}^m$ (ou reciprocamente, $u' = uU^{-1}$) sempre que $u \in \mathbb{R}^m$. Assim, segue diretamente que:

$$\left\{ u'M_1 : \ u' \in \mathbb{R}^m \right\} = \left\{ uM_2 : \ u \in \mathbb{R}^m \right\}.$$

Além disso, destacamos que ao definir span (Λ) como um subespaço de $\mathbb{R}^n$ de dimensão $m \leq n$, estamos considerando o espaço $\mathbb{R}^m$ imerso em $\mathbb{R}^n$ (via imersão canônica).

Por fim, cabe ressaltar que a equivalência entre as definições é provada de modo completamente análogo às equivalências apresentadas para a definição do reticulado Λ (conforme feito na Observação 3.1.6).

Finalmente, temos a seguinte equivalência:

Teorema 3.1.17. *Um conjunto $\Lambda \subset \mathbb{R}^n$ é um reticulado se, e somente se, é um subgrupo aditivo discreto de $\mathbb{R}^n$.*

Demonstração. ($\Rightarrow$) Conforme argumentamos anteriormente, é imediato que, se Λ é um reticulado, então, Λ é um subgrupo aditivo de $\mathbb{R}^n$. Resta, portanto, mostrar que Λ é discreto.

Consideremos $\{v_1, \ldots, v_m\}$, com $m \leq n$, uma base de Λ.

Queremos mostrar que $\Lambda \cap B[0, r]$ é um conjunto finito.

Para tanto, seja $x \in \Lambda \cap B[0, r]$, sendo

$$x = \sum_{i=1}^{m} \lambda_i v_i \ \text{, em que } \lambda_i \in \mathbb{Z}.$$

Afirmamos que $\|(\lambda_1, \ldots, \lambda_n)\| \leq k$ para algum $k \in \mathbb{R}$.

Com efeito, consideremos a aplicação:

$$\begin{aligned} f : span(\Lambda) &\rightarrow \mathbb{R}^n \\ \sum_{i=1}^{n} a_i v_i &\mapsto (a_1, \ldots, a_n) \end{aligned}$$

em que $a_i \in \mathbb{R}$ para todo $i = 1, \ldots, n$.

Como f é contínua, temos que $f(B[0, r])$ é limitado, ou seja, existe $k \in \mathbb{R}$ tal que $\|f(v)\| \leq k$, para todo $v \in B[0, r]$. Dessa forma, segue que:

$$|\lambda_i| \leq \|(\lambda_1, \ldots, \lambda_n)\| \leq k.$$

Agora, notemos que o número de soluções inteiras para esta desigualdade é finito. Em outras palavras, existe apenas um número finito de elementos pertencentes à interseção $\Lambda \cap B[0, r]$, como queríamos.

($\Leftarrow$) Seja $G \subset \mathbb{R}^n$ um subgrupo aditivo discreto de $\mathbb{R}^n$.

Consideremos $\{g_1, \ldots, g_m\}$ um subconjunto maximal em G de elementos linearmente independentes. De modo análogo ao span de um reticulado, definimos:

$$V := \left\{ \sum_{i=1}^{m-1} u_i g_i : \ u_i \in \mathbb{R} \ \text{ para todo } i = 1, \ldots, m \right\}.$$

Façamos ainda $G_0 := G \cap V$. Como $G_0 \subseteq G$, temos que G_0 é um conjunto discreto.

Por hipótese de indução em m, podemos considerar que G_0 é um reticulado. Nesse contexto, devemos provar que G também o é.

Visto que G_0 é um reticulado, o mesmo admite uma base, digamos $B = \{v_1, \ldots, v_{m-1}\}$. Por outro lado, como $\{g_1, \ldots, g_{m-1}\}$ constitui um conjunto de vetores linearmente independentes de G_0 com mesma cardinalidade que B, temos que esse é também uma base para G_0. Dessa forma, todo elemento de G_0 se expressa como uma combinação linear inteira de $g_1, \ldots, g_{m-1}$.

Consideremos, agora, T como sendo o conjunto dos elementos $x \in G$ tais que

$$x = \sum_{i=1}^{m} a_i g_i,$$

em que $a_i \in \mathbb{R}$ é tal que $0 \leq a_i < 1$ para $i = 1, \ldots, m-1$ e $0 \leq a_m \leq 1$.

Notemos que T é limitado e, como G é discreto, é ainda finito. Nessas circunstâncias, podemos escolher $y \in T$, digamos

$$y = b_1 g_1 + \cdots + b_m g_m,$$

tal que b_m é o menor valor não nulo possível para o coeficiente de g_m.

Temos que $\{g_1, \ldots, g_{m-1}, y\}$ é um conjunto de vetores linearmente independentes, por hipótese. Mostraremos que todo elemento de G é uma combinação linear inteira destes elementos.

Seja $g \in G$. Podemos escolher coeficientes $c_i \in \mathbb{Z}$ de modo que

$$g' = g - c_1 g_1 - \cdots - c_{m-1} g_{m-1} - c_m y$$

pertença a T.

Mais ainda, tal escolha pode ser feita de modo que o coeficiente de g_m em g' seja um inteiro não negativo menor que b_m. Pela minimalidade de b_m, devemos ter que tal coeficiente se anula.

Assim, pela igualdade anterior, verificamos que g pode ser escrito como uma combinação linear inteira de $g_1, \ldots, g_{m-1}, y$ (visto que $g' \in T$).

Logo, o conjunto $\{g_1, \ldots, g_{m-1}, y\}$ gera G como um $\mathbb{Z}$ - módulo. Em outras palavras, este conjunto constitui uma base para G e, consequentemente, G é um reticulado. □

Observação 3.1.18. Ao longo dessa seção, definimos reticulado sobre o espaço $\mathbb{R}^n$. Contudo, cabe destacar que, ao estabeler um isomorfismo entre o corpo complexo $\mathbb{C}$ e $\mathbb{R}^2$, podemos estender naturalmente tal conceito, obtendo, assim, um *reticulado complexo*. Desse modo, todos os conceitos e propriedades dos reticulados apresentados permanecem válidos.

3.2 SUB-RETICULADOS E GRUPO QUOCIENTE

Considerando os reticulados como subgrupos aditivos discretos de $\mathbb{R}^n$, podemos analisar subconjuntos dos mesmos que também se caracterizem como reticulados, os quais denominaremos *sub-reticulados*. Tal objeto matemático, sob certas circunstâncias, possibilitará a análise do grupo quociente obtido através dessa estrutura e de suas principais características.

Definição 3.2.1. *Dizemos que $\Lambda^\star \subset \Lambda$ é um **sub-reticulado** de Λ se $\Lambda^\star$ é um reticulado.*

Observação 3.2.2. Notemos que, se M é uma matriz geradora do reticulado Λ e $\Lambda^\star$ é um sub-reticulado de Λ, podemos escrever:

$$\Lambda^\star = \left\{\lambda AM : \ \lambda \in \mathbb{Z}^m\right\},$$

em que A é uma matriz $m \times m$ com entradas inteiras.

De fato, consideremos N uma matriz geradora para $\Lambda^\star$. Dado um ponto $p \in \Lambda^\star$, sabemos que o mesmo também pertence a Λ. Então, existem $\lambda \in \mathbb{Z}^m$ e $\nu \in \mathbb{Z}^m$ tais que:

$$p = \lambda M = \nu N\,.$$

De modo semelhante ao feito na Proposição 3.1.7, temos que existe uma matriz A com entradas inteiras tais que $N = AM$, demonstrando a igualdade fornecida para $\Lambda^\star$.

Destacamos que, nesse caso, como a inclusão $\Lambda \subset \Lambda^\star$ não é, em geral, verdadeira (a menos do sub-reticulado trivial $\Lambda^\star = \Lambda$), tal matriz A não será unimodular.

Ressaltamos ainda que essa caracterização fornece-nos um método prático para a construção de sub-reticulados conhecendo uma de suas bases.

Com o intuito de sintetizar algumas propriedades de um reticulado em uma única terminologia, definimos *grupo abeliano livre de posto r*.

Definição 3.2.3. *Dizemos que um $\mathbb{Z}$-módulo M é **livre de posto r** se existem r vetores $v_1, \ldots, v_r \in M$ linearmente independentes em $\mathbb{Z}$ tais que, para todo $m \in M$, tem-se que*

$$m = \sum_{i=1}^{r} a_i v_i \ \text{, com } a_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, r.$$

Definição 3.2.4. *Dizemos que um grupo abeliano G é **livre de posto r** se G é um $\mathbb{Z}$-módulo livre de posto r.*

É imediato das definições acima e do Teorema 3.1.17 que todo reticulado Λ é um grupo abeliano livre; mais ainda, um sub-reticulado $\Lambda^\star$ é um subgrupo de Λ. Dessa forma, podemos considerar o grupo quociente $\Lambda/\Lambda^\star$.

Definição 3.2.5. *O **grupo quociente** $\Lambda/\Lambda^\star$ é definido como:*

$$\frac{\Lambda}{\Lambda^\star} = \left\{x + \Lambda^\star : \ x \in \Lambda\right\}.$$

*Dizemos que $x, y \in \Lambda$ estão na mesma **classe de equivalência** se $x + \Lambda^\star = y + \Lambda^\star$, ou seja, se $x - y \in \Lambda^\star$.*

*A cardinalidade do grupo quociente $\Lambda/\Lambda^\star$, ou seja, o número de classe de equivalência distintas em Λ com respeito a $\Lambda^\star$, é denominada **índice** de $\Lambda/\Lambda^\star$.*

Antes de apresentarmos alguns exemplos, vejamos como melhor caracterizar o índice do grupo quociente $\Lambda/\Lambda^\star$, quando o mesmo é finito (para a demonstração, consultar [27], Teorema 1.17).

Proposição 3.2.6. *Sejam G um grupo abeliano livre de posto r e H um subgrupo de G. Temos que G/H é finito se, e somente se, posto(G) = posto(H).*

Neste caso, se $\{x_1, \ldots, x_r\}$ constitui uma $\mathbb{Z}$-base para G e $\{y_1, \ldots, y_r\}$ é uma $\mathbb{Z}$-base para H tal que

$$y_i = \sum_{j=1}^{n} a_{ij}x_j \ \text{, com } a_{ij} \in \mathbb{Z} \text{ para todo } i = 1, \ldots, r,$$

então a cardinalidade de G/H é dada por:

$$\left|\frac{G}{H}\right| = \left|\det\left(a_{ij}\right)\right|.$$

Corolário 3.2.7. *Seja Λ um reticulado com sub-reticulado $\Lambda^\star$. Então o grupo quociente $\Lambda/\Lambda^\star$ é um grupo finito se, e somente se, posto(Λ) = posto$(\Lambda^\star)$.*

Neste caso, segue que:

$$\left|\frac{\Lambda}{\Lambda^\star}\right| = \sqrt{\frac{\det\left(\Lambda^\star\right)}{\det\left(\Lambda\right)}}.$$

Demonstração. A primeira afirmação segue diretamente da Proposição 3.2.6, bastando tomar $G = \Lambda$ e $H = \Lambda^\star$.

Para o cálculo do índice de $\Lambda/\Lambda^\star$ no caso finito, utilizaremos a caracterização do sub-reticulado $\Lambda^\star$ fornecida pela Observação 3.2.2. Conforme tal observação, sabemos que, se M é uma matriz geradora de Λ e N uma matriz geradora para $\Lambda^\star$, então existe uma matriz A com entradas inteiras tal que $N = AM$.

Agora, consideremos, sem perda de generalidade, que Λ e $\Lambda^\star$ têm posto completo, ou seja, as matrizes M e N são quadradas. Desse modo, garantimos a existência de $\det(M)$ e $\det(N)$. Mais precisamente, temos que $\det(N) = \det(A)\det(M)$.

Assim, utilizando a Proposição acima, juntamente à definição de determinante de um reticulado, obtemos:

$$\left|\frac{\Lambda}{\Lambda^\star}\right| = |\det(A)| = \left|\frac{\det(N)}{\det(M)}\right| = \sqrt{\frac{\det(\Lambda^\star)}{\det(\Lambda)}}.$$

□

Exemplo 3.2.8. Consideremos o reticulado $\Lambda = \mathbb{Z}^3 = \{(a,b,c) : a,b,c \in \mathbb{Z}\}$ e seus sub-reticulados $\Lambda^* = \{(a(0,1,0) + b(0,0,1) : a,b \in \mathbb{Z}\}$ e $\Lambda^\star = \{a(1,3,0) + b(0,0,1) + c(2,0,5) : a,b,c \in \mathbb{Z}\}$.

Notemos que $\Lambda^\star$ e Λ possuem ambos posto 3, ao passo que Λ^* possui posto 2. Dessa forma, o grupo quociente $\Lambda/\Lambda^\star$ é finito, a saber, seu índice é dado por:

$$\left|\frac{\Lambda}{\Lambda^\star}\right| = \sqrt{\frac{\det(\Lambda^\star)}{\det(\Lambda)}} = \sqrt{\frac{36}{1}} = 6.$$

Para o cálculo de $\det\Lambda$, basta utilizar a base formada pelos vetores canônicos. Além disso, lembramos que, como a matriz de Gram é da forma $\mathcal{G} = MM^T$, sendo M uma matriz geradora do reticulado (ou do sub-reticulado) em questão, tem-se que $\det(\mathcal{G}) = \det(M)^2$.

Por outro lado, pelo corolário anterior, tendo em vista a diferença entre os postos de Λ e Λ^*, temos que o quociente Λ/Λ^* é um grupo infinito.

Utilizando a noção de equivalência de classes em Λ/Λ^*, a igualdade acima é facilmente verificada. Com efeito, dados, por exemplo, $c_1, c_2 \in \mathbb{Z}$, com $c_1 \neq c_2$, temos que $(c_1,0,0) - (c_2,0,0) = (c_1 - c_2, 0, 0) \notin \Lambda^*$, donde resulta que esses vetores pertencem a classes distintas no quociente Λ/Λ^*. Assim, o grupo quociente Λ/Λ^* admite infinitas classes laterais.

3.3 REGIÃO FUNDAMENTAL

Nessa seção, apresentaremos o conceito de *região fundamental*, o qual nos permitirá fornecer um significado geométrico para o determinante de um reticulado além de ser uma das principais ferramentas para a abordagem de problemas envolvendo reticulados. Enfatizaremos ainda o estudo de um tipo específico de região fundamental, denominada *paralelotopo fundamental*.

Definição 3.3.1. *Uma **região fundamental** de um reticulado Λ é um subconjunto F de $\mathbb{R}^n$ que satisfaz as seguintes propriedades:*

(*i*) $\bigcup_{v\in\Lambda} v + F = span(\Lambda)$

(*ii*) *Se $x, y \in \Lambda$, sendo $x \neq y$, então $(x + F) \cap (y + F) = \emptyset$*

Assim, uma região fundamental consiste de um subconjunto de $\mathbb{R}^n$ que ladrilha span (Λ) por translações de vetores do reticulado de modo que dois ladrilhos ou são disjuntos ou se interceptam somente nos bordos.

Observação 3.3.2. Notemos que, se o reticulado $\Lambda \subseteq \mathbb{R}^n$ em questão possui posto máximo, então, temos que span (Λ) corresponde ao próprio espaço $\mathbb{R}^n$. Nestas circunstâncias, a região fundamental constitui um ladrilhamento de $\mathbb{R}^n$ satisfazendo as mesmas características anteriores. Dessa forma, alguns textos optam por definir a região fundamental sob a exigência de que o reticulado Λ possua posto máximo. No caso das definições envolvendo span (Λ), como a apresentada acima, utilizamos a abordagem adotada em [5] e [10].

Destacamos que existem diferentes configurações geométricas para regiões fundamentais de um mesmo reticulado, por exemplo, por meio da utilização de poliedros distintos. Mais ainda, existem infinitas regiões fundamentais utilizando um mesmo poliedro. Neste trabalho, abordaremos duas regiões fundamentais específicas, a saber os *politopos fundamentais* e a *região de Veronoi*, a qual será estudada na próxima seção. Por ora, apresentamos o exemplo seguinte apenas como uma motivação geométrica proporcionada pela Definição 3.3.1.

Exemplo 3.3.3. Consideremos o reticulado $\Lambda \subset \mathbb{R}^2$ com base $\{(1,2),(2,-1)\}$. As configurações a seguir apresentam regiões fundamentais para tal reticulado.

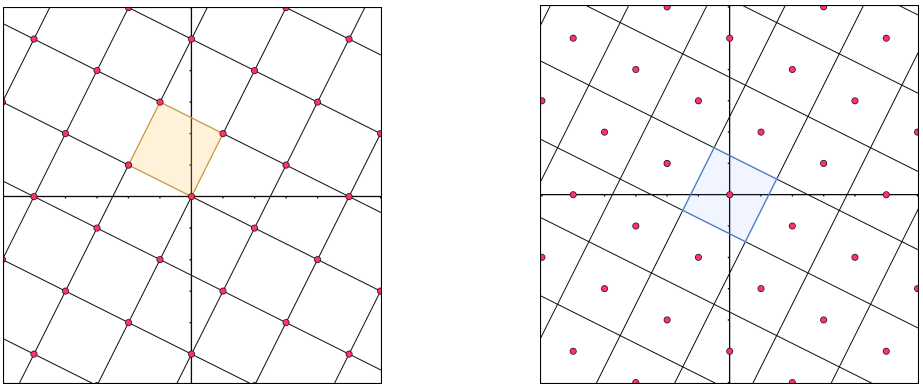


Figura 3 – Regiões fundamentais para o reticulado de base $\{(1,2),(2,-1)\}$

Notemos que uma região fundamental é, em particular um subconjunto não vazio de $\mathbb{R}^n$ e, como tal, possui volume. A Proposição 3.3.4, cuja demonstração pode ser encontrada em [3] (Teorema 9.1.3), motiva a definição de volume de um reticulado.

Proposição 3.3.4. *Toda região fundamental de um reticulado $\Lambda \subseteq \mathbb{R}^n$ tem o mesmo volume.*

Definição 3.3.5. *Denominamos o* ***volume*** *de um reticulado Λ, denotado por vol (Λ), como sendo o volume de uma de suas regiões fundamentais.*

Para o cálculo do volume de um reticulado, nos aprofundaremos no estudo dos chamados *politopos fundamentais*, os quais se caracterizam não apenas como um tipo de região fundamental, mas, também, como um subconjunto próprio de span (Λ).

A partir deste momento, para as próximas definições e resultados, consideraremos, apenas os reticulados $\Lambda \subseteq \mathbb{R}^n$ de posto n, ou seja, de posto completo.

Definição 3.3.6. *Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$ com base $B = \{b_1, \ldots, b_n\}$, chamamos de **politopo (ou paralelotopo) fundamental** a região do $\mathbb{R}^n$ definida como:*

$$\mathcal{P}_B = \left\{ \sum_{i=1}^{n} a_i b_i : \ 0 \leq a_i < 1 \text{ para todo } i = 1, \ldots, n \right\}.$$

Observação 3.3.7. Cabe destacar que, em algumas literaturas, como [6] e [2], a região fundamental de um reticulado é definida como sendo a generalização da noção de politopo fundamental, apresentada acima, para o caso em que Λ possui posto $m \leq n$. E assim, é imediato que o politopo fundamental é, em particular, uma região fundamental.

Exemplo 3.3.8. Considerando o reticulado hexagonal, com base $\{(1,0), (1/2, \sqrt{3}/2)\}$, temos, por exemplo, os seguintes politopos fundamentais e seus ladrilhamentos:

$$\begin{aligned} \mathcal{P}_1 &= \left\{ a_1(1,0) + a_2(1/2, \sqrt{3}/2) : 0 \leq a_1, a_2 < 1 \right\}; \\ \mathcal{P}_2 &= \left\{ a_1(3/2, \sqrt{3}) + a_2(1/2, \sqrt{3}/2) : 0 \leq a_1, a_2 < 1 \right\}. \end{aligned}$$

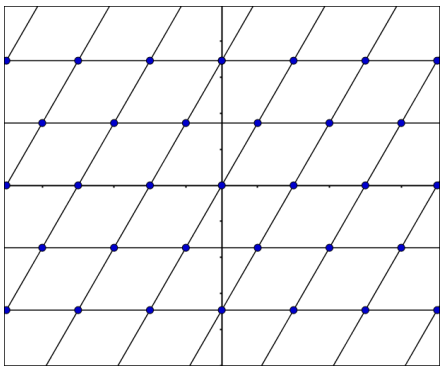


Figura 4 – Ladrilhamentos segundo $\mathcal{P}_1$

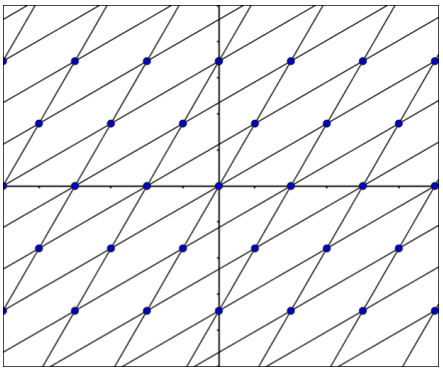


Figura 5 – Ladrilhamentos segundo $\mathcal{P}_2$

Proposição 3.3.9. *O politopo fundamental de um reticulado $\Lambda \subseteq \mathbb{R}^n$ de posto n é uma região fundamental e seu volume é dado por $\sqrt{\det(\Lambda)}$. Portanto, o volume de Λ é dado por:*

$$vol\ (\Lambda) = \sqrt{\det(\Lambda)}.$$

Demonstração. Sejam Λ um reticulado com base $B = \{b_1, \ldots, b_n\}$ e $\mathcal{P}_B$ o politopo fundamental de Λ com relação a B. Mostraremos que $\mathcal{P}_B$ satisfaz as propriedades (i) e (ii) da Definição 3.3.1. De fato, temos:

(*i*) Seja $r \in \text{span}\,(\Lambda)$. Então, sabemos que r é da forma:

$$r = \sum_{i=0}^{n} u_i b_i \text{ , em que } u_i \in \mathbb{R} \text{ para todo } i = 1, \ldots, n.$$

Sabemos que para cada i fixado, $u_i = \lfloor u_i \rfloor + a_i$, em que $\lfloor u_i \rfloor$ denota a parte inteira de u_i e a_i é um número real satisfazendo $0 \leq a_i < 1$. Assim, utilizando a primeira equação, obtemos:

$$r = \sum_{i=0}^{n} \lfloor u_i \rfloor b_i + \sum_{i=0}^{n} a_i b_i =: v + \sum_{i=0}^{n} a_i b_i,$$

donde resulta que $r \in v + \mathcal{P}_B$, com $v \in \Lambda$ definido como acima.

Portanto, segue que:

$$\bigcup_{v \in \Lambda} v + \mathcal{P}_B = \text{span}\,(\Lambda).$$

Lembrando que a inclusão contrária é imediata, tendo em vista a definição de Λ e o fato, já mencionado, de que $\mathcal{P}_B \subset \text{span}\,(\Lambda)$.

(*ii*) Sejam $x, y \in \Lambda$, com $x \neq y$.

Suponhamos, por contradição, que exista $c \in (x + \mathcal{P}_B) \cap (y + \mathcal{P}_B)$. Nesse caso, temos que $c = x + p = y + q$, sendo $p, q \in \mathcal{P}_B$. Utilizando a última igualdade, juntamente ao fato de que Λ é um subgrupo aditivo, tem-se:

$$x - y = (q - p) \in \Lambda.$$

Por outro lado, como $q, p \in \mathcal{P}_B$, podemos reescrever essa igualdade como:

$$x - y = \sum_{i=0}^{n} a_i b_i - \sum_{i=0}^{n} \tilde{a}_i b_i = \sum_{i=0}^{n} (a_i - \tilde{a}_i) b_i,$$

em que $0 \leq a_i, \tilde{a}_i < 1$ para todo $i = 1, \ldots, n$.

Como tal elemento pertence ao reticulado Λ, para cada i fixado devemos ter $a_i - \tilde{a}_i \in \mathbb{Z}$. Notemos que, aqui, utilizamos que todo elemento de Λ se expressa de modo único como combinação linear inteira dos vetores da base (tal resultado decorre do fato de os vetores da base serem linearmente independentes). Logo, pelo intervalo de definição de a_i e $\tilde{a}_i$, concluímos que a única possibilidade é que $a_i - \tilde{a}_i = 0$ para todo $i = 1, \ldots, n$. Consequentemente, $x = y$, gerando uma contradição.

Portanto, para quaisquer $x, y \in \Lambda$, com $x \neq y$, temos $(x + \mathcal{P}_B) \cap (y + \mathcal{P}_B) = \emptyset$.

Agora, utilizando o processo de ortogonalização de Gram Smith para uma base do span(Λ) e o cálculo do volume via integral, pode-se demonstrar que o volume do paralelotopo fundamental de Λ corresponde a $\sqrt{\det(\Lambda)}$ (consultar [11], Lema 4). □

3.4 GRUPO QUOCIENTE DE UM RETICULADO

Nesta última seção, aprofundaremo-nos na visão topológica de reticulados, os quais, como caracterizados anteriormente, são subgrupos discretos de $\mathbb{R}^n$. Sob essa óptica, dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, podemos estudar o grupo quociente $\mathbb{R}^n/\Lambda$. Mostraremos que existe uma correspondência entre esse grupo e o toro n-dimensional quando Λ tem posto completo e apresentaremos uma correspondência semelhante no caso em que o reticulado Λ não tem posto completo. Por meio dessa correspondência, obteremos uma nova descrição para o volume de um reticulado, a qual será retomada nas construções de reticulados do último capítulo.

Definição 3.4.1. *Seja S o conjunto de todos números complexos cujo módulo é igual a 1, o qual denominamos S **círculo**. Definimos o **toro n-dimensional**, denotado por T^n, como o produto direto cartesiano de n cópias de S.*

Observação 3.4.2. Notemos que S é um grupo sob a multiplicação usual e, consequentemente, essa estrutura de grupo é estendida ao toro n-dimensional.

Exemplo 3.4.3. O toro bidimensional, denominado muitas vezes como simplesmente toro, expressa-se como $T^2 = S \times S$. Geometricamente, temos:

Lema 3.4.4. *O grupo quociente $\mathbb{R}/\mathbb{Z}$ é isomorfo ao círculo S.*

Demonstração. Consideremos o homomorfismo dado por:

$$\begin{aligned} \varphi : \mathbb{R} &\to S \\ a &\mapsto e^{2\pi i a} \end{aligned}$$

onde $e^{2\pi i a} = \cos(2\pi a) + i\,\mathrm{sen}(2\pi a)$. Notemos que tal mapa é claramente sobrejetor. Além disso, $Ker(\varphi) = \mathbb{Z}$, resultando pelo Teorema dos Isomorfismos que $\mathbb{R}/\mathbb{Z} \cong S$. □

Teorema 3.4.5. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto completo, ou seja, o posto de Λ é igual a n. Então o grupo quociente $\mathbb{R}^n/\Lambda$ é isomorfo ao toro n-dimensional T^n.*

Demonstração. Consideremos $\{v_1, \ldots, v_n\}$ uma base para Λ. Sabemos que tais vetores geram o espaço $span(\Lambda)$, o qual corresponde exatamente a $\mathbb{R}^n$, visto que o posto é completo. Desse modo, essa é uma base para $\mathbb{R}^n$.

Estendemos o homomorfismo definido anteriormente para $\mathbb{R}^n$:

$$\begin{aligned} \varphi : \mathbb{R}^n &\to T^n \\ a_1 v_1 + \cdots + a_n v_n &\mapsto (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n}) \end{aligned}$$

Claramente, temos que φ é sobrejetivo. Além disso, pelo lema anterior, o núcleo de φ é igual ao reticulado Λ, donde obtemos $\mathbb{R}^n/\Lambda \cong T^n$. □

Corolário 3.4.6. *Consideremos Λ com uma base $B = \{v_1, \ldots, v_n\}$ com seu respectivo politopo fundamental $\mathcal{P}_B$. Então, o mapa φ definido no teorema estabelece uma bijeção entre $\mathcal{P}_B$ e T^n.*

Demonstração. Basta notarmos que, ao considerarmos $\mathcal{P}_B$, temos $0 \leq a_i < 1$ para cada $i = 1, \ldots, n$ fixado. Assim, a injetividade do mapa $\varphi\big|_{\mathcal{P}_B}$ segue das propriedades das funções *seno* e *cosseno*. □

Corolário 3.4.7. *O volume de uma região fundamental de Λ de posto n corresponde ao volume de T^n. Mais precisamente, temos:*

$$vol\,(\mathbb{R}^n/\Lambda) = vol(T^n) = vol(\mathcal{P}_B) = vol(\Lambda).$$

Geometricamente, o toro n-dimensional pode ser obtido por meio de identificações dos lados opostos do fecho do politopo $\mathcal{P}_B$, denotado por $\overline{\mathcal{P}_B}$, quando o reticulado em questão tem posto n.

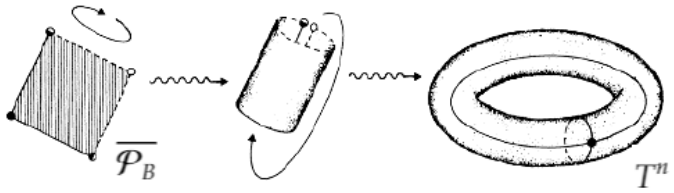


Figura 6 – Toro n-dimensional [27]

Já no caso dos reticulados sem posto completo, temos a próxima correspondência:

Teorema 3.4.8. *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado de posto $m < n$. Então, $\mathbb{R}^n/\Lambda$ é isomorfo a $T^m \times \mathbb{R}^{n-m}$.*

Demonstração. Consideremos o espaço coberto por Λ dado por $V := span(\Lambda)$. Sabemos que o mesmo possui dimensão m, sendo isomorfo a $\mathbb{R}^m$. Podemos descrever $\mathbb{R}^n$ como a soma direta $\mathbb{R}^n = V \oplus W$, em que W é um complementar de V. Como $\Lambda \subseteq V$, pelo Teorema 3.4.5, temos que $V/\Lambda \cong T^m$, donde $W \cong \mathbb{R}^{n-m}$. Portanto, segue que $\mathbb{R}^n/\Lambda \cong T^m \times \mathbb{R}^{n-m}$. □

Destacamos que essa visão geométrica permite demonstrar importantes resultados presentes na Teoria dos Números. Nesse contexto, um dos resultados mais conhecidos é o Teorema de Minkovsky, o qual fornece condições a fim de que um determinado conjunto de $\mathbb{R}^n$ (limitado, convexo e simétrico) possua pontos de um reticulado de posto completo. Esse teorema se mostra uma das principais ferramentas utilizadas na demonstração via reticulados do Teorema de Dois Quadrados e no Teorema dos Quatro Quadrados, os quais afirmam que todo número inteiro se escreve como a

soma de dois e de quatro quadrados, respectivamente. Tal abordagem é apresentada em [27] (Capítulo 7).

3.5 RETICULADOS EQUIVALENTES

Algumas propriedades de um reticulado são preservadas via determinadas transformações. Assim, torna-se natural estabelecermos as noções de *reticulados equivalentes* e de *invariante geométrico*.

Definição 3.5.1. *Dada uma métrica d em $\mathbb{R}^n$, dizemos que σ_d é uma* ***isometria*** *se $\sigma_d : \mathbb{R}^n \to \mathbb{R}^n$ é uma aplicação satisfazendo $d(x, y) = d(\sigma_d(x), \sigma_d(y))$ para todo $x, y \in \mathbb{R}^n$.*

Definição 3.5.2. *Fixemos uma métrica d em $\mathbb{R}^n$. Dizemos que dois reticulados Λ_1 e Λ_2 são* ***d-equivalentes*** *se existirem uma isometria $\sigma_d : \mathbb{R}^n \to \mathbb{R}^n$ e um número real positivo κ tais que $(\kappa\sigma_d)(\Lambda_1) = \Lambda_2$. Nesse caso, a constante κ é denominada* ***fator de dilatação****. Além disso, quando $\kappa = 1$, dizemos ainda que os reticulados Λ_1 e Λ_2 são* ***congruentes****.*

Definição 3.5.3. *Dizemos que um parâmetro de um reticulado Λ é um* ***invariante geométrico*** *se ele permanece constante na classe de reticulados equivalentes.*

A noção de equivalência entre reticulados está diretamente relacionada à métrica adotada. Neste trabalho, abordaremos apenas os reticulados equivalentes sob a métrica euclidiana. É comum estudarmos ainda tal equivalência considerando-se a métrica da soma (consultar [17], Seção 1.2.2). Sob tal circunstância, pode-se mostrar que toda isometria com a métrica da soma é uma isometria com a métrica euclidiana. Desse modo, reticulados equivalentes segundo a métrica da soma são também equivalentes segundo a métrica euclidiana (no entanto, a recíproca não é válida).

3.5.1 Reticulados equivalentes pela métrica euclidiana

Ao fixarmos a métrica euclidiana, podemos reformular o conceito de reticulados equivalentes, conforme [5] (Seção 1.1).

Definição 3.5.4. *Dizemos que dois reticulados Λ_1 e Λ_2 são* ***equivalentes*** *segundo a métrica euclidiana se, fixadas matrizes geradoras, digamos M_1 e M_2 respectivamente, existem uma matriz unimodular U, uma matriz ortogonal Q e um número real positivo κ tais que:*

$$\kappa U M_1 Q = M_2.$$

Ou, equivalentemente,

$$(\kappa Q)(\Lambda_1) = \Lambda_2.$$

Observação 3.5.5. Intuitivamente, dois reticulados Λ_1 e Λ_2 são equivalentes segundo a métrica euclidiana se podemos obter Λ_2 a partir de Λ_1 por meio de uma composição de rotações, reflexões e translações por vetores do reticulado Λ_1.

A equivalência entre essa definição e a definição apresentada acima decorre da Proposição 3.1.7 juntamente à caracterização das isometrias de $\mathbb{R}^n$ via a métrica euclidiana. Mais precisamente, é possível demonstrar que uma aplicação $\sigma_d : \mathbb{R}^n \to \mathbb{R}^n$, sendo d a métrica euclidiana, é uma isometria se, e somente se,

$$\sigma_d(x) = T(x) + x_0,$$

em que T é um operador linear de $\mathbb{R}^n$ ortogonal (e, portanto está associado a uma matriz ortogonal Q) e $x_0 \in \mathbb{R}^n$. Este resultado é conhecido da Análise no $\mathbb{R}^n$ e sua prova pode ser encontrada em [19] (Teorema 2.3).

Destacamos que, em consequência direta da definição anterior, se Λ_1 e Λ_2 são reticulados equivalentes na métrica euclidiana, com matrizes de Gram G_1 e G_2, respectivamente, então tais matrizes estão associadas da seguinte forma:

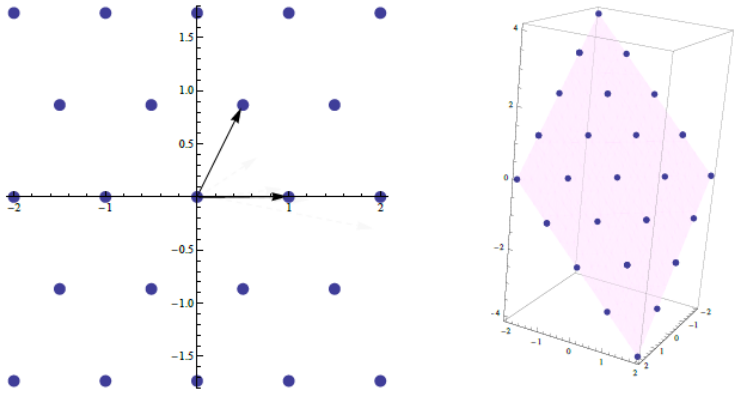
$$G_2 = M_2 M_2^T = \kappa^2 U M_1 M_1^T U^T = \kappa^2 U G_1 U^T,$$

sendo que a última igualdade decorre do Corolário 3.1.8.

Outras propriedades dos reticulados equivalentes na métrica euclidiana serão apresentadas quando abordarmos a noção de *densidade de um empacotamento reticulado*.

Vejamos agora um exemplo de reticulados equivalentes.

Exemplo 3.5.6. Consideremos o reticulado hexagonal com base $\{(1,0),(1/2,\ \sqrt{3}/2)\}$ e o reticulado A_2 com base $\{(-1,1,0),(0,-1,1)\}$ definidos em $\mathbb{R}^3$.



(a) Reticulado hexagonal (b) Reticulado A_2

Figura 7 – Reticulados Equivalentes na Métrica Euclidiana [17]

Conforme indica a Figura 7, o reticulado A_2 é obtido por meio de uma dilatação do reticulado hexagonal (a saber, uma dilatação de $\sqrt{2}$) seguida de rotações; consequentemente, tais reticulados são equivalentes pela métrica euclidiana.

Formalmente, esse resultado pode ser notado por meio das matrizes geradoras de cada reticulado. Consideremos o reticulado hexagonal imerso em $\mathbb{R}^3$; para tanto, basta considerarmos a base anterior como $\{(1,0,0),(1/2,\ \sqrt{3}/2,0)\}$. Assim, aplicamos uma contração de $\sqrt{2}$ no reticulado A_2 e, a seguir, utilizamos a transformação ortogonal dada por:

$$R = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{3} \\ -1/\sqrt{2} & 1/\sqrt{6} & 1/\sqrt{3} \\ 0 & 2\sqrt{2}/\sqrt{3} & 1/\sqrt{3} \end{pmatrix}.$$

Nessas condições, temos:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \cdot R = \begin{pmatrix} 1 & 0 & 0 \\ 1/2 & \sqrt{3}/2 & 0 \end{pmatrix},$$

sendo a matriz à esquerda uma matriz geradora para A_2 e a matriz à direita uma matriz geradora do reticulado hexagonal.

Logo, segue pela Definição 3.5.4 que os reticulados em questão são, de fato, equivalentes pela métrica euclidiana.

Observação 3.5.7. Destacamos que o reticulado A_2 apresentado no exemplo anterior compõe uma importante classe de reticulados, denominados *reticulados raízes*. Retomaremos o estudo de reticulados como esse no Capítulo 4.

3.6 PROBLEMAS RELEVANTES

Nesta seção, apresentaremos alguns dos principais problemas envolvendo reticulados, dada sua aplicabilidade na Teoria de Códigos e na Teoria dos Números. Alguns desses problemas serão retomados no Capítulo 4.

Com o intuito de simplificar os cálculos, consideramos, a partir deste momento o reticulado $\Lambda \subseteq \mathbb{R}^n$ de posto completo. Notemos que tal consideração não diminui a generalidade dos conceitos e resultados apresentados.

Com efeito, podemos analisar cada reticulado com relação ao espaço coberto por Λ, cuja dimensão, visto como subespaço vetorial, corresponde ao posto de Λ.

3.6.1 **Número de Vizinhos**

Definição 3.6.1. *Seja d uma métrica em $\mathbb{R}^n$. Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$, denominamos* ***vetor de distância mínima*** *os vetores não nulos $x \in \Lambda$ que minimizam o valor de*

$$d(\Lambda) := \min\left\{d(y,0) : y \in \Lambda \ e\ y \neq 0\right\}.$$

*Denominamos ainda **distância mínima** o valor de $\mu := d(\Lambda)$ sendo x vetor de distância mínima.*

Definição 3.6.2. *Dado um reticulado $\Lambda \subseteq \mathbb{R}^n$ e uma métrica d em $\mathbb{R}^n$, denominamos de **kissing number** (ou **número de vizinhos**) o número de vetores de distância mínima do reticulado, o qual denotaremos por $\tau(\Lambda)$.*

Observação 3.6.3. É possível obter uma interpretação geométrica interessante para o *kissing number*. Para tanto, fixados um reticulado Λ e uma métrica d em $\mathbb{R}^n$, tracemos esferas de raio $\mu/2$ ao redor de cada ponto do reticulado. Como μ é a distância mínima a partir da métrica d, segue que tais esferas no máximo tangenciam umas às outras. Assim, o *kissing number* calcula o número de esferas que tocam a esfera de raio $\mu/2$ centrada na origem (denominada *esfera central*).

Exemplo 3.6.4. Cabe destacar que o *kissing number* depende da métrica considerada. Como exemplo, podemos considerar o reticulado de base $\{(-3,0),(-2,0)\}$. No caso da métrica euclidiana, temos que os vetores de distância mínima são dados por $\{(1,2),(-1,-2)\}$ (figura à esquerda); enquanto na métrica da soma, temos $\{(1,2),(-1,-2),(3,0),(-3,0)\}$ (figura à direita).

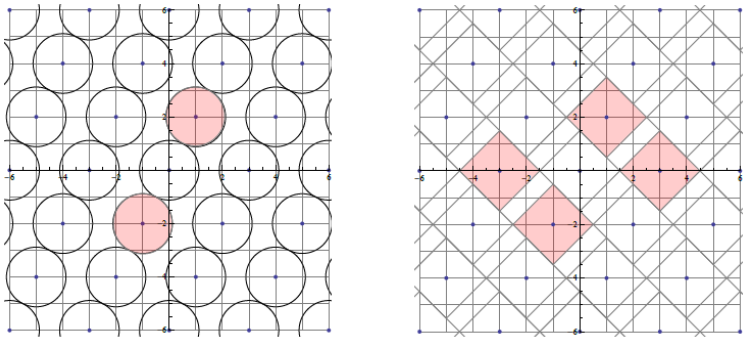


Figura 8 – Kissing Number [17]

3.6.2 Densidade de Empacotamento

Explorando uma noção geométrica semelhante à proporcionada pelo *kissing number*, surge uma interessante questão, a qual se caracteriza como um dos principais tópicos de estudo envolvendo reticulados. Dado um reticulado Λ e uma métrica d em $\mathbb{R}^n$ nos perguntamos o quanto do espaço pode ser coberto por esferas de mesmo raio na métrica d de modo que as mesmas não se intersectam ou sejam apenas tangentes. Essa medida é fornecida pela *densidade de empacotamento*.

Esse problema é mais geral e não envolve apenas o uso de reticulados. Dessa forma, definimos primeiramente *empacotamento de esferas* e, a seguir, *empacotamento reticulado*.

Definição 3.6.5. *Seja d uma métrica em $\mathbb{R}^n$. Um **empacotamento de esferas** (ou, simplesmente, um **empacotamento no** $\mathbb{R}^n$) é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que quaisquer duas esferas não se intersectam ou se intersectam apenas no bordo.*

*Um **empacotamento reticulado** é um empacotamento no $\mathbb{R}^n$ em que o conjunto dos centros das esferas forma um reticulado em $\mathbb{R}^n$.*

Observação 3.6.6. Notemos que um empacotamento de esferas pode ser descrito a partir dos centros e do raio das esferas. Além disso, destacamos que, apesar do conjunto dos centros das esferas constituir um conjunto discreto de $\mathbb{R}^n$, o mesmo nem sempre é um subgrupo aditivo de $\mathbb{R}^n$.

Exemplo 3.6.7. A figura 8 apresenta dois empacotamentos reticulados, na métrica euclidiana e na métrica da soma, respectivamente.

Notemos que nesse exemplo, caso o raio das esferas em cada situação fossem maiores que o apresentado, teríamos as esferas se intersectando em mais de um ponto. Dessa forma, as esferas em questão possuem o maior raio para o qual duas esferas se intersectam no máximo no bordo. Este fato motiva a próxima definição.

Definição 3.6.8. *Dado um reticulado Λ, denominamos **raio de empacotamento** com relação à métrica d (fixada) o valor:*

$$\rho := \rho(\Lambda) = \max\left\{r \in \mathbb{R} : \Lambda + B_d[0,r] \text{ é um empacotamento reticulado}\right\},$$

sendo $B_d[0,r]$ a bola fechada de centro 0 e raio r na métrica d em $\mathbb{R}^n$.

Observação 3.6.9. É imediato que $\rho = \mu/2$, sendo μ a distância mínima. Entretanto, calcular a distância mínima de um reticulado é um problema difícil de ser resolvido, mesmo computacionalmente. Mais precisamente, utilizando a distância euclidiana, foi conjecturado em [15] que não existe algoritmo capaz de calcular tal distância em tempo polinomial.

Definição 3.6.10. *Dado um empacotamento reticulado, denominamos a proporção do espaço coberta pela união das esferas de raio ρ centradas nos pontos do reticulado Λ de **densidade de empacotamento**, a qual será denotada por $\Delta(\Lambda)$.*

Em outras palavras, temos que, fixada uma métrica d em $\mathbb{R}^n$,

$$\Delta(\Lambda) = \frac{\textit{Volume de uma esfera de raio } \rho}{\textit{Volume de uma região fundamental de } \Lambda} = \frac{vol\left(B_d[0,\rho]\right)}{\det(\Lambda)^{\frac{1}{2}}} = \frac{vol\left(B_d[0,1]\right)\rho^n}{\det(\Lambda)^{\frac{1}{2}}}.$$

Para o cálculo do volume de uma bola unitária n-dimensional, são utilizados métodos que não detalharemos.

No caso da métrica euclidiana, em [9] (Cap. 21, §2C), é provado que:

$$vol\,(B_d[0,1]) = \begin{cases} \dfrac{\pi^{n/2}}{\left(\frac{n}{2}\right)!}, \text{ se } n \text{ é par;} \\ \\ \dfrac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!}, \text{ se } n \text{ é ímpar.} \end{cases}$$

Uma formulação equivalente, contemplando ambas as paridades de n, utiliza a *função Gamma* Γ (veja [9]), estudada por matemáticos como Euler e Legendre, estabelece que:

$$vol\,(B_d[0,1]) = \frac{\pi^{n/2}}{\Gamma\left(\dfrac{n}{2}+1\right)}.$$

Tal função (consultar [23], §14) estende a noção da função fatorial, a qual, fixado $n \in \mathbb{N}$ é dada por $\Gamma(n) := (n-1)!$. Neste caso, ao considerarmos um número complexo z, exceto inteiros não positivos, define-se:

$$\Gamma(z) := \int_0^\infty x^{z-1} e^{-x} dx.$$

Fixada a dimensão, o problema do empacotamento máximo se restringe ao estudo de um parâmetro relativamente mais simples.

Definição 3.6.11. *A **densidade de centro** de um reticulado Λ, denotada por $\delta(\Lambda)$, é*

$$\delta(\Lambda) = \frac{\rho^n}{\det(\Lambda)}.$$

Observação 3.6.12. Decorre diretamente das definições acima que tanto a densidade de um reticulado quanto sua densidade de centro dependem da métrica considerada.

Exemplo 3.6.13. Consideremos o reticulado hexagonal Λ com base $\{(1,0), (1/2, \sqrt{3}/2)\}$. A figura a seguir mostra um dos empacotamentos de esfera associada a este reticulado.

Utilizando a fórmula para a bola bidimensional, juntamente à fórmula da densidade de empacotamento, obtemos:

$$vol\ B_d[0,1] = \pi \text{ , donde } \Delta(\Lambda) = \frac{(1/2)^2\pi}{\sqrt{3}/2} = \frac{\pi}{2\sqrt{3}}.$$

Além disso, temos que a densidade de centro é dada por:

$$\delta(\Lambda) = \frac{(1/2)^2}{\sqrt{3}/2} = \frac{1}{2\sqrt{3}}.$$

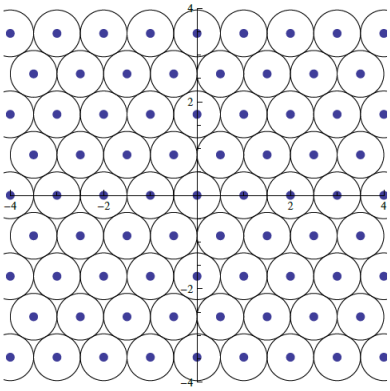


Figura 9 – Empacotamento Reticulado [17]

O exemplo anterior é interessante porque a Figura 9 exibe o empacotamento mais denso em $\mathbb{R}^2$, inclusive se comparado aos empacotamentos não reticulados. Este fato não é de verificação imediata e compõe um dos principais estudos a respeito da Teoria de Reticulados.

Nessas circunstâncias, nos perguntamos qual o empacotamento de esferas mais denso para determinada métrica em um espaço cuja dimensão esteja previamente fixada. Além disso, podemos nos perguntar se o empacotamento encontrado é também um empacotamento reticulado. No caso da métrica euclidiana, já se conhecem tais empacotamentos nas dimensões de 1 a 8 e na dimensão 24, sendo que foi demonstrado que nesses casos tais empacotamentos são reticulados. Para as dimensões de 1 a 3, sugerimos consultar [9] (Cap.1 e 2), para as dimensões 8 e 24, sugerimos [29] e [8], respectivamente.

A importância de tais conceitos se estende pois, na métrica euclidiana em $\mathbb{R}^n$, mostra-se que a densidade é um invariante geométrico.

Proposição 3.6.14. *Se Λ_1 e Λ_2 são reticulados equivalentes na métrica euclidiana, então $\Delta(\Lambda_1) = \Delta(\Lambda_2)$.*

Demonstração. Como o volume de uma bola n dimensional segundo a métrica d depende apenas do valor de n e da métrica d considerada, devemos mostrar que:

$$\frac{\rho_1^n}{\det(\Lambda_1)^{\frac{1}{2}}} = \frac{\rho_2^n}{\det(\Lambda_2)^{\frac{1}{2}}},$$

sendo ρ_1 e ρ_2 os raios de empacotamento de Λ_1 e Λ_2, respectivamente.

Como Λ_1 e Λ_2 são d-equivalentes, sendo d a métrica euclidiana, existem Q uma matriz ortogonal e κ real positivo satisfazendo:

$$(\kappa Q)(\Lambda_1) = \Lambda_2,$$

ou seja, dado $y \in \Lambda_2$, existe $x \in \Lambda_1$ tal que $y = (\kappa Q)(x)$.

Assim, resulta que:

$$\langle (\kappa Q)(u), (\kappa Q)(v) \rangle = \kappa^2 \langle u, v \rangle .$$

Consequentemente,

$$||(\kappa Q)(v)|| = \kappa ||v||,$$

sendo $\|\cdot\|$ a norma proveniente do produto interno.

Por outro lado, notemos que $\rho_1 = \mu_1/2$ e $\rho_2 = \mu_2/2$, sendo μ_1 e μ_2 as distâncias mínimas de Λ_1 e Λ_2. Além disso, podemos considerar a norma acima como a norma euclidiana (isto é, associada com a métrica d).

Desse modo, utilizando as relações anteriores, obtemos:

$$\begin{aligned}
\mu_2 &= \min\left\{d(y,0) : y \in \Lambda_2 \text{ e } y \neq 0\right\} \\
&= \min\left\{\|y\| : y \in \Lambda_2 \text{ e } y \neq 0\right\} \\
&= \min\left\{\kappa\|x\| : x \in \Lambda_1 \text{ e } x \neq 0\right\} \\
&= \kappa\left\{\|x\| : x \in \Lambda_1 \text{ e } x \neq 0\right\} \\
&= \kappa\mu_1.
\end{aligned}$$

Assim, segue que $\rho_2 = \kappa\rho_1$.

Agora, para a relação entre os determinantes dos reticulados em questão, utilizaremos o fato já mostrado que, se G_1 e G_2 são matrizes de Gram para os reticulados Λ_1 e Λ_2, então $G_2 = \kappa^2 U G_1 U^T$. Dessa forma,

$$\det(\Lambda_2) = \det(G_2) = \det \kappa^2 U G_1 U^T = \det \kappa^2 I \det(G_1) = \kappa^{2n} \det \Lambda_1.$$

Finalmente, temos:

$$\frac{\rho_2^n}{\det \Lambda_2{}^{\frac{1}{2}}} = \frac{(\kappa\rho_1)^n}{\kappa^n \det(\Lambda_1)} = \frac{\rho_1^n}{\det(\Lambda_1)},$$

donde resulta que $\Delta(\Lambda_1) = \Delta(\Lambda_2)$. □

Observação 3.6.15. As noções de raio e densidade de empacotamento podem ser estendidas e definidas para um empacotamento qualquer de esferas (não necessariamente um empacotamento reticulado). Esse estudo não será abordado neste trabalho, no entanto, destacamos que uma das abordagens utiliza uma aproximação por reticulados, juntamente com o conceito dos chamados *empacotamentos periódicos* (ver [22]).

3.6.3 Raio de Cobertura

Um problema em certo sentido dual ao problema do raio de empacotamento consiste em, dado um reticulado Λ, obter o menor raio tal que a reunião de esferas de mesmo raio cobrem o espaço $span(\Lambda)$.

Definição 3.6.16. *Dado um reticulado Λ, denominamos **raio de cobertura** de Λ com relação à métrica d (fixada) o valor:*

$$\gamma := \gamma(\Lambda) = \inf\left\{r \in \mathbb{R}_+ : \ B_{d,V}[0,r] + \Lambda = V\right\},$$

em que $V := span(\Lambda)$ e $B_{d,V}[0,r]$ é a bola fechada de raio r centrada na origem de V e sob a métrica d.

*Neste caso, dizemos ainda que $B_{d,V}[0,r] + \Lambda$ é uma **cobertura** para $V = span(\Lambda)$.*

Exemplo 3.6.17. Consideremos o reticulado hexagonal como no exemplo do raio de empactotamento. O seu raio de cobertura com relação à métrica euclidiana é ilustrado na figura seguinte.

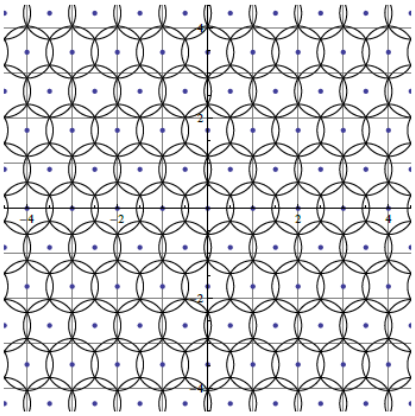


Figura 10 – Raio de Cobertura [17]

3.6.4 Região de Voronoi

A *região de Voronoi* de um ponto $x \in \Lambda$ segundo uma métrica fixada d se caracteriza como o conjunto dos pontos de $\mathbb{R}^n$ (mais precisamente, em span (Λ)) que estão mais próximos de x do que de qualquer outro ponto de Λ. Formalmente, definimos:

Definição 3.6.18. *Seja $v \in \Lambda$ e d uma métrica em $\mathbb{R}^n$. A **região de Voronoi do ponto** v é*

$$R(v) = \left\{x \in \mathbb{R}^n : d(v,x) \leq d(u,x), u \in \Lambda\right\}.$$

Observação 3.6.19. Notemos que, como translações a partir de um vetor do reticulado constituem uma isometria (tanto na métrica euclideana quanto na métrica da soma), a

região de Voronoi de qualquer ponto $v \in \Lambda$ pode ser obtida a partir de uma translação da região de Voronoi no ponto zero, ou seja, $R(v) = v + R(0)$ para todo $v \in \Lambda$.

Exemplo 3.6.20. *A figura a seguir exibe a região de Voronoi do reticulado $\mathbb{Z}^2$ para a origem segundo a métrica euclidiana.*

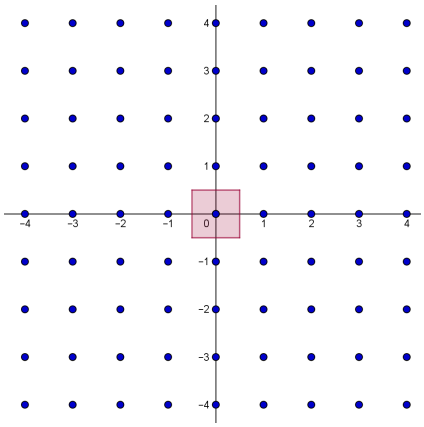


Figura 11 – Região de Voronoi do reticulado $\mathbb{Z}^2$

Conforme já mencionado, fixado um reticulado Λ, é possível ladrilhar o espaço span (Λ) a partir da região de Voronoi. Em outras palavras, pode-se demonstrar que a mesma é uma região fundamental. Consequentemente, o volume de uma região de Voronoi é igual ao volume de um paralelotopo fundamental, isto é, equivale a $\det(\Lambda)$.

O estudo das regiões de Voronoi é interessante especialmente por uma propriedade comum aos seus vértices: trata-se dos pontos de $\mathbb{R}^n$ cuja distância ao reticulado é um máximo absoluto (consultar [9], Seção 1.2).

4 RETICULADOS VIA CORPOS DE FUNÇÕES

Conforme apresentado na seção 3.6, um dos principais problemas envolvendo reticulados consiste em, dado um subespaço m-dimensional V de $\mathbb{R}^n$, obter um reticulado $\Lambda \subset V$ tal que $V = \text{span}(\Lambda)$. Queremos garantir, inclusive, que este é o reticulado com maior densidade de empacotamento dentre os demais reticulados contidos em V.

Nesse estudo, destaca-se o Teorema de Minkowsky-Hlawka, segundo o qual, para todo espaço n-dimensional, existe um reticulado cuja densidade de empacotamento é maior ou igual a $\zeta(n)/2^{n-1}$, sendo que $\zeta(n)$ está associada à função Zeta de Riemann. No entanto, as demonstrações conhecidas para este teorema não são construtivas e, no caso em que as dimensões são arbitrárias, construções de reticulados satisfazendo a limitação acima são, em geral, desconhecidas. Tal circunstância motivou, como ainda motiva, a busca de famílias assintóticas [1] de reticulados cuja densidade de empacotamento seja tão próximo quanto possível do valor estabelecido por Minkowsky e Hlawka.

Tendo em vista essa motivação, lembramos que, como apresentado na Definição 3.6.10, a densidade de um reticulado Λ de posto m na métrica euclidiana é dada por:

$$\Delta(\Lambda) = \frac{\rho^m \pi^{m/2}}{\Gamma\left(\frac{m}{2}+1\right)\det(\Lambda)^{1/2}},$$

em que ρ é o raio de empacotamento de Λ e Γ denota a função Gamma.

Equivalentemente, utilizando que $\rho = d(\Lambda)/2$, sendo $d(\Lambda)$ a distância mínima do reticulado, podemos representar:

$$\Delta(\Lambda) = \frac{d(\Lambda)^m \omega_m}{2^m \det(\Lambda)^{1/2}},$$

sendo ω_m o volume da bola unitária m-dimensional na métrica euclidiana.

Assim, a fim de maximizar a densidade de um reticulado, podemos tomar um reticulado cujo quociente entre sua distância mínima e seu determinante sejam tão grandes quanto possível. De acordo com a construção feita por Tsfasman e Vladut em [30], os reticulados obtidos por meio de corpos de funções específicos fornecem bons resultados nesse sentido, bastando garantir que o quociente n/g seja suficientemente grande. Por outro lado, resultados apresentados em [20] mostraram que reticulados com alta densidade em geral constituem um importante grupo de reticulados, os quais são denominados *reticulados bem arredondados*.

Nessas condições, nosso principal objetivo é construir reticulados, a partir de corpos de funções específicos, que possuam características relevantes no estudo da densidade de empacotamento. Para tanto, seguiremos a abordagem feita em [13] e [4].

[1] Reticulados que produzem bons resultados em altas dimensões, ou seja, quando $n \to \infty$.

4.1 PROPRIEDADES GERAIS

Nas próximas construções, consideraremos corpos de funções da forma $F/\mathbb{F}_q$, em que q é a potência de um número primo, cujo gênero é igual a g. Denotaremos ainda o conjunto dos lugares racionais de $F/\mathbb{F}_q$, o qual sabemos ser finito, por:

$$\mathcal{P} := \left\{P_0, P_1, \ldots, P_{n-1}\right\} \subseteq \mathbb{P}_F,$$

em que n corresponde à cardinalidade de tal conjunto. Além disso, para cada lugar P_i, representaremos sua respectiva valorização (discreta) por v_i, sendo $i = 0, \ldots, n-1$.

Definição 4.1.1. *Definimos $\mathcal{O}^*_{\mathcal{P}}$ como o conjunto das funções não nulas $f \in F/\mathbb{F}_q$ cujo divisor tem suporte contido em $\mathcal{P}$, ou seja,*

$$\mathcal{O}^*_{\mathcal{P}} := \left\{f \in F/\mathbb{F}_q : \ f \neq 0 \text{ e } supp(f) \subseteq \mathcal{P}\right\}.$$

Observação 4.1.2. Destacamos que ao nos referirmos a um divisor do elemento $f \in F$, estamos considerando seu divisor principal, ou seja,

$$(f) = (f)_0 - (f)_\infty = \sum_{P \in \mathbb{P}_F} v_P(f)P,$$

em que P percorre todos os lugares de $F/\mathbb{F}_q$ (não somente os racionais) e v_P é sua valorização correspondente. Nesse caso, temos ainda que:

$$supp(f) = \{P \in \mathbb{P}_F : v_P(f) \neq 0\}.$$

Assim, no contexto da definição anterior, $\mathcal{O}^*_{\mathcal{P}}$ se constitui das funções não nulas em $F/\mathbb{F}_q$ tais que as únicas valorizações que não se anulam nas mesmas são aquelas associadas a lugares racionais. Por consequência, dada $f \in \mathcal{O}^*_{\mathcal{P}}$, segue que:

$$(f) = \sum_{i=0}^{n-1} v_i(f)P_i.$$

Por outro lado, como (f) é um divisor principal, sabemos que seu grau é igual a zero (Teorema 2.3.43), resultando que:

$$\deg(f) = \sum_{i=0}^{n-1} v_i(f) = 0.$$

Observação 4.1.3. Observamos que $\mathcal{O}^*_{\mathcal{P}}$ é um grupo abeliano sob a multiplicação formal, no qual consideramos:

$$\begin{aligned} (f)\cdot(g) &:= \sum_{i=0}^{n-1} \left(v_i(f) + v_i(g)\right) P_i; \\ (1) &:= \sum_{i=0}^{n-1} P_i. \end{aligned}$$

Definição 4.1.4. *Dada uma função $f \in O_{\mathcal{P}}^*$, definimos o* ***grau de*** *f por:*

$$\deg f := \sum_{v_i(f)>0} v_i(f) = \frac{1}{2}\sum_{i=0}^{n-1} \left|v_i(f)\right|.$$

Definimos o homomorfismo $\phi_{\mathcal{P}}$ por:

$$\begin{aligned} \phi_{\mathcal{P}} : O_{\mathcal{P}}^* &\to \mathbb{Z}^n \\ f &\mapsto (v_0(f), v_1(f), \ldots, v_{n-1}(f)) \end{aligned}$$

Consideremos $L_{\mathcal{P}} := \mathrm{Im}(\phi_{\mathcal{P}})$ ou seja,

$$L_{\mathcal{P}} := \left\{(v_0(f), \ldots, v_{n-1}(f)) \in \mathbb{Z}^n : \ f \in O_{\mathcal{P}}^*\right\}. \tag{4.1}$$

Mostraremos ao longo deste capítulo que $L_{\mathcal{P}}$ não somente é um reticulado de $\mathbb{R}^n$ como também, ao impor certas condições sobre o corpo de funções $F/\mathbb{F}_q$, ele se torna *gerado por seus vetores minimais* e, consequentemente, *bem arredondado*. Antes de estabelecermos estas noções, relembramos alguns dos conceitos que foram apresentados na Seção 3.6.1, utilizando especificamente a métrica euclidiana de $\mathbb{R}^n$.

Definição 4.1.5. *Definimos a* ***distância mínima*** *(na métrica euclidiana) de um reticulado Λ como:*

$$d(\Lambda) := \min\left\{\|y\| : y \in \Lambda \setminus \{0\}\right\}.$$

Nesse caso, denominamos os vetores $x \in \Lambda$ para os quais $\|x\| = d(\Lambda)$ de ***vetores de distância mínima*** *ou, equivalentemente,* ***vetores minimais****.*

Denotaremos o ***conjunto de vetores minimais*** *de Λ por $S(\Lambda)$. Formalmente,*

$$S(\Lambda) := \left\{x \in \Lambda : \ \|x\| = d(\Lambda)\right\}.$$

Observação 4.1.6. Ressaltamos que, conforme já apresentado, o *kissing number* de um reticulado, denotado por $\tau(\Lambda)$, corresponde ao número de seus vetores minimais. Nesse sentido, temos que $\tau(\Lambda)$ é igual à cardinalidade de $S(\Lambda)$.

Analisando o conjunto de vetores minimais $S(\Lambda)$, podemos considerar os subespaços cobertos por seus vetores tanto sobre $\mathbb{Z}$ quanto sobre $\mathbb{R}$. Nessas circunstâncias, de modo semelhante ao $span(\Lambda)$, definimos:

Definição 4.1.7. *Consideremos $S(\Lambda) = \{v_1, \ldots, v_t\}$. Definimos o subespaço coberto por $S(\Lambda)$ com relação a $\mathbb{Z}$, o qual denotamos $span_{\mathbb{Z}}(S(\Lambda))$, como:*

$$span_{\mathbb{Z}}(S(\Lambda)) = \left\{\sum_{i=1}^{t} \lambda_i v_i : \ \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, t\right\}.$$

Definimos ainda o subespaço coberto por $S(\Lambda)$ com relação a $\mathbb{R}$, denotado por $span_{\mathbb{R}}(S(\Lambda))$, como:

$$span_{\mathbb{R}}(S(\Lambda)) = \left\{ \sum_{i=1}^{t} u_i v_i : \ u_i \in \mathbb{R} \text{ para todo } i = 1, \ldots, t \right\}.$$

Assim, sob a métrica euclidiana, definimos:

Definição 4.1.8. *Dizemos que um reticulado $\Lambda \subseteq \mathbb{R}^m$ é **gerado por seus vetores minimais** se o reticulado Λ corresponde ao subespaço coberto pelo conjunto de seus vetores minimais, ou seja, se $\Lambda = span_{\mathbb{Z}}(S(\Lambda))$.*

Definição 4.1.9. *Dizemos que um reticulado Λ de posto m é **bem arredondado** se ele contém m vetores minimais linearmente independentes. Equivalentemente, se $S(\Lambda)$ gera $\mathbb{R}^m$, ou seja, se $span_{\mathbb{R}}(S(\Lambda)) = \mathbb{R}^m$.*

A importância dos reticulados bem arredondados reside no fato de os mesmos fornecerem bons métodos de otimização, principalmente relativos à Criptografia e à Teoria de Códigos (veja [12]). Além disso, eles podem ser utilizados na investigação dos principais problemas envolvendo reticulados, como o empacotamento esférico, o número de vizinhos e a conexão de suas propriedades com a chamada Conjectura de Minkowsky (consultar [21]). Algumas destas propriedades serão detalhadas ao longo deste capítulo.

Nesse contexto, uma das formas de se verificar que um reticulado é bem arredondado consiste em provar que ele é gerado por seus vetores minimais. Com efeito, segue diretamente das Definições 4.1.8 e 4.1.9 a validade desta implicação. Por outro lado, contudo, esta não é uma equivalência: existem reticulados bem arredondados que não são gerados por seus vetores minimais. Mais geralmente, sabe-se que se $m \leq 4$, a equivalência vale; caso contrário, ou seja, se $m \geq 5$, existem reticulados bem arredondados, mas cujos vetores minimais geram apenas subreticulados de índice maior que 1, conforme demonstrado em [20].

Sob essa perpectiva, um questionamento natural é saber para quais corpos de funções $F/\mathbb{F}_q$ o reticulado $L_{\mathcal{P}}$ correspondente é bem arredondado. Neste trabalho, apresentaremos uma resposta parcial a esta questão. Mais precisamente, mostraremos que, utilizando o *corpo de funções Hermitiano* (sobre $\mathbb{F}_{q^2}$) ou o *corpo de funções elípticas* (sobre $\mathbb{F}_q$), o reticulado $L_{\mathcal{P}}$ associado é, não somente um reticulado bem arredondado, como, também, gerado por seus vetores minimais. Porém, cabe destacar, que a construção que faremos, seguindo a abordagem utilizada por Böttcher, Fukshansky, Garcia e Maharaj, em princípio não se generaliza para quaisquer corpos de funções. Com efeito, as características estudadas para o reticulado, como volume, densidade de empacotamento, juntamente às condições de ser bem arredondao ou, inclusive, gerado

por vetores minimais, dependem do corpo de funções considerado. Assim, generalizar o resultado é, normalmente, uma tarefa complexa.

Em vista disso, nesta seção, apresentaremos as propriedades do reticulado $L_{\mathcal{P}}$ que são válidas sob qualquer corpo de funções $F/\mathbb{F}_q$. Nos capítulos posteriores, aprofundaremo-nos nas propriedades obtidas através do corpo de funções considerado e de suas respectivas particularidades.

Teorema 4.1.10. *O conjunto $L_{\mathcal{P}} := Im(\phi_{\mathcal{P}})$ é um sub-reticulado do reticulado $\mathcal{A}_{n-1}$ dado por:*

$$\mathcal{A}_{n-1} := \left\{ x = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n : \sum_{i=0}^{n-1} x_i = 0 \right\}.$$

Além disso, a distância mínima do reticulado $L_{\mathcal{P}}$, denotada por $d(L_{\mathcal{P}})$, satisfaz:

$$d(L_{\mathcal{P}}) \geq min \left\{ \sqrt{2 \deg f} : f \in O^*_{\mathcal{P}} \setminus \mathbb{F}_q \right\}. \tag{4.2}$$

Demonstração. Primeiramente, notemos que $L_{\mathcal{P}}$ é um subconjunto de $\mathcal{A}_{n-1}$, uma vez que $\deg(f) = 0$ para todo $f \in O^*_{\mathcal{P}}$. Por outro lado, é imediato que tanto $L_{\mathcal{P}}$ quanto $\mathcal{A}_{n-1}$ são reticulados, pois trata-se de subgrupos aditivos discretos de $\mathbb{R}^n$.

Agora, sabemos, por definição, que:

$$d(L_{\mathcal{P}}) = min \left\{ \sqrt{\sum_{i=0}^{n-1} v_i(f)^2} : f \in O^*_{\mathcal{P}} \setminus \{0\} \right\},$$

sendo que para todo $f \in O^*_{\mathcal{P}} \setminus \mathbb{F}_q$, temos

$$\sqrt{\sum_{i=0}^{n-1} v_i(f)^2} \geq \sqrt{\sum_{i=0}^{n-1} |v_i(f)|} = \sqrt{2 \deg f}.$$

Logo, vale a desigualdade representada em (4.2). □

Agora, com o intuito de obtermos uma limitação para o volume do reticulado $L_{\mathcal{P}}$ e, consequentemente, para seu determinante, iremos nos restringir inicialmente ao estudo do determinante de $\mathcal{A}_{n-1}$, o qual é calculado por meio de sua matriz de Gram.

Proposição 4.1.11. *O determinante de $\mathcal{A}_{n-1}$ é igual a* $\det(\mathcal{A}_{n-1}) = n$. *Em outras palavras, temos que $vol(\mathcal{A}_{n-1}) = \sqrt{n}$.*

Demonstração. Notemos que a definição apresentada para $\mathcal{A}_{n-1}$ é equivalente a:

$$\mathcal{A}_{n-1} = \left\{ \sum_{i=0}^{n} x_i e_i : x_i \in \mathbb{Z} \text{ para todo } i = 0, 1, \ldots, n \text{ e } \sum_{i=0}^{n} x_i = 0 \right\},$$

sendo $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{R}^n$, ou seja, cada e_i corresponde ao vetor em $\mathbb{R}^n$ cuja i-ésima coordenada é igual a 1 e as demais são nulas.

Afirmação 1: *O reticulado $\mathcal{A}_{n-1}$ é gerado pelos vetores:*

$$b_1 = e_1 - e_2,\ b_2 = e_2 - e_3,\ \ldots,\ b_{n-1} = e_{n-1} - e_n,\ b_n = e_1 - e_n.$$

Prova. Devemos mostrar que o reticulado gerado por tais vetores, o qual denotaremos por Λ, é igual a $\mathcal{A}_{n-1}$. Assim, seja:

$$\Lambda := \left\{ \sum_{i=1}^{n} \lambda_i (e_i - e_{i+1}) : \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, n \text{ e } \lambda_n = 0 \right\}.$$

Destacamos que, na definição acima, colocamos $\lambda_n = 0$ a fim de que Λ possa ser visto como um reticulado em $\mathbb{R}^n$; nesse caso, temos claramente que o posto de Λ é igual a $n-1$. Temos ainda que, dado $y \in \Lambda$, podemos escrever:

$$\begin{aligned} y &= \lambda_1(e_1 - e_2) + \lambda_2(e_2 - e_3) + \cdots + \lambda_{n-1}(e_{n-1} - e_n) + \lambda_n(e_1 - e_n) \\ &= (\lambda_1 + \lambda_n, -\lambda_1 + \lambda_2, \ldots, -\lambda_i + \lambda_{i+1}, \ldots, -\lambda_{n-2} + \lambda_{n-1}, -\lambda_{n-1} + \lambda_n) \\ &= (\lambda_1, -\lambda_1 + \lambda_2, \ldots, -\lambda_i + \lambda_{i+1}, \ldots, -\lambda_{n-2} + \lambda_{n-1}, -\lambda_{n-1}). \end{aligned}$$

Segue, portanto, que a soma das coordenadas de y é igual a zero, ou seja, $y \in \mathcal{A}_{n-1}$, donde $\Lambda \subseteq \mathcal{A}_{n-1}$.

Por outro lado, ao tomarmos $x \in \mathcal{A}_{n-1}$, sabemos que $x = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n$, em que as somas dos elementos x_i, com $i = 0, \ldots, n$, é nula. É imediato que existem $\lambda_1, \ldots, \lambda_{n-1} \in \mathbb{Z}$ satisfazendo:

$$(x_0, x_1, \ldots, x_{n-2}, x_{n-1}) = (\lambda_1, -\lambda_1 + \lambda_2, \ldots, -\lambda_{n-2} + \lambda_{n-1}, -\lambda_{n-1}).$$

pois, comparando tais elementos termo a termo e considerando em princípio λ_1, λ_{n-1} incógnitas, obtemos um sistema com n equações e $n-1$ incónitas, o qual possui solução. Além disso, cada λ_i se expressa a partir de combinações lineares das coordenadas de x, consequentemente, cada λ_i é inteiro.

Logo, temos que $\mathcal{A}_{n-1} = \Lambda$, resultando que $\mathcal{A}_{n-1}$ é gerado pelos vetores $b_1, \ldots, b_n$. Mais precisamente, uma base para $\mathcal{A}_{n-1}$ consiste em tomar o conjunto $\{b_1, \ldots, b_{n-1}\}$, uma vez que b_n corresponde à soma de todos os b_i's, com $i = 1, \ldots, n-1$. Em particular, o reticulado $\mathcal{A}_{n-1}$ possui posto $n-1$.

Afirmação 2: *O determinante de $\mathcal{A}_{n-1}$ é dado por* $\det(\mathcal{A}_{n-1}) = n$ *ou, equivalentemente,* $vol(\mathcal{A}_{n-1}) = \sqrt{n}$.

Prova. Escrevendo a matriz geradora de $\mathcal{A}_{n-1}$, digamos M, cujas linhas são os vetores

$b_1, \ldots, b_{n-1}$ e fazendo a multiplicação por sua transposta, obtemos uma matriz de Gram para $\mathcal{A}_{n-1}$. No caso $n = 3$, ou seja, usando o reticulado $\mathcal{A}_2$, obtemos $\det(\mathcal{G}_{\mathcal{A}}) = 3$, pois

$$\mathcal{G}_{\mathcal{A}} = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}.$$

Para $n \geq 4$, temos que uma matriz de Gram associada a $\mathcal{A}_{n-1}$ é dada por:

$$\mathcal{G}_{\mathcal{A}} = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2 \end{bmatrix}_{(n-1)\times(n-1)} . \tag{4.3}$$

Para o cálculo do determinante dessa matriz, utilizaremos indução em n.

Primeiramente, notemos que se $n = 4$, a matriz $\mathcal{G}_{\mathcal{A}}$ acima, de dimensão 3×3, possui determinante igual a 4. Agora, utilizando o cálculo do determinante via cofatores para a matriz $\mathcal{G}_{\mathcal{A}}$ de dimensão $(n-1) \times (n-1)$ apresentada acima, obtemos:

$$\det(\mathcal{G}_{\mathcal{A}}) = 2\det(A) + \det(B) \tag{4.4}$$

em que A é uma matriz $(n-2) \times (n-2)$ com o mesmo formato que (4.3) e a matriz B é dada por:

$$B = \begin{bmatrix} -1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 2 & -1 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & -1 & 0 \\ 0 & 0 & 0 & \cdots & -1 & 2 & -1 \\ 0 & 0 & 0 & \cdots & 0 & -1 & 2 \end{bmatrix}_{(n-2)\times(n-2)} .$$

Observemos que, pela definição da matriz A, temos que a mesma é uma matriz de Gram associada ao reticulado $\mathcal{A}_{n-2}$. Assim, por hipótese de indução, temos que $\det(A) = n - 1$. Resta, então, calcularmos o determinante da matriz B. Novamente, utilizando o cálculo por cofatores, obtemos:

$$\det(B) = -\det(C) + \det(D).$$

em que C corresponde à matriz de formato (4.3), porém com dimensão $(n-3) \times (n-3)$ e D é uma matriz cuja primeira coluna é toda nula.

Desse modo, utilizando a hipótese de indução, sabemos que C corresponde a uma matriz de Gram para $\mathcal{A}_{n-3}$ e, logo, tem determinante $n-2$. Por outro lado, como D tem uma coluna nula, segue que $\det(D) = 0$. Consequentemente, $\det(B) = -(n-2)$.

Portanto, como $\det(A) = n-1$ e $\det(B) = 2-n$, segue pela equação (4.4) que:

$$\det(\mathcal{G}_{\mathcal{A}}) = 2(n-1) + 2 - n = n.$$

Dessa forma, fica provado que, para todo $n \in \mathbb{N}$ o determinante de $\mathcal{A}_{n-1}$, o qual corresponde ao determinante de $\mathcal{G}_{\mathcal{A}}$, é igual a n. □

Com esse resultado, para a limitação do volume de $L_{\mathcal{P}}$, precisamos apenas estabelecer uma relação entre seu volume e o volume de $\mathcal{A}_{n-1}$. Para isto, estabeleceremos uma correspondência entre os reticulados $\mathcal{A}_{n-1}$ e $L_{\mathcal{P}}$ e determinados subgrupos de divisores de F.

Definição 4.1.12. *Consideremos $Div(\mathcal{P})$ o subgrupo de $Div(F)$ cujos divisores têm suporte contido em $\mathcal{P}$:*

$$Div(\mathcal{P}) := \Big\{D \in Div(F) : \ supp(D) \subseteq \mathcal{P}\Big\}.$$

No caso em que todos os divisores em $Div(\mathcal{P})$ têm grau zero, definimos:

$$Div^0(\mathcal{P}) := \Big\{D \in Div(F) : \ supp(D) \subseteq \mathcal{P} \ e \ \deg D = 0\Big\}.$$

O subgrupo de $Div(\mathcal{P})$ formado pelos divisores principais com suporte em $\mathcal{P}$ é

$$Princ(\mathcal{P}) := \Big\{(f) \in Div(F) : \ supp(f) \subseteq \mathcal{P}\Big\}.$$

Observação 4.1.13. Como nas definições dos grupos de divisores de F, segue diretamente da definição que: $Princ(\mathcal{P}) \leq Div^0(\mathcal{P}) \leq Div(\mathcal{P})$.

Proposição 4.1.14. *Existe um isomorfismo entre o subgrupo de divisores $Div^0(\mathcal{P})$ e o reticulado $\mathcal{A}_{n-1}$. Mais precisamente,*

$$Div(\mathcal{P}) \cong \mathbb{Z}^n \ \ e \ \ Div^0(\mathcal{P}) \cong \mathcal{A}_{n-1}.$$

Demonstração. Para a primeira correspondência biunívoca notemos que, dado um divisor $D \in Div(\mathcal{P})$, podemos escrevê-lo como:

$$D = \sum_{P \in \mathcal{P}} n_P P = \sum_{i=1}^{n} n_i P_i,$$

em que $n_i = n_{P_i} \in \mathbb{Z}$.

Assim, a cada divisor $D \in Div(\mathcal{P})$ corresponde um único ponto $(n_1, \ldots, n_n) \in \mathbb{Z}^n$. Reciprocamente, dado um ponto em $\mathbb{Z}^n$, é possível associá-lo a um único divisor com suporte em $\mathcal{P}$ como acima.

Por outro lado, analisando o grupo $Div^0(\mathcal{P})$, notamos que todos os seus divisores possuem grau zero, uma vez que são principais. Desse modo, utilizando o argumento anterior, obemos uma correspondência biunívoca entre $Div^0(\mathcal{P})$ e o reticulado $\mathcal{A}_{n-1}$. □

Corolário 4.1.15. *O reticulado $L_{\mathcal{P}}$ é isomorfo ao grupo de divisores das funções pertencentes a $O^*_{\mathcal{P}}$. Formalmente, temos:*

$$L_{\mathcal{P}} \cong \left\{(f) \in Div(F) : f \in O^*_{\mathcal{P}}\right\} = Princ(\mathcal{P}).$$

Observação 4.1.16. Ressaltamos que, apesar de as funções pertencentes a $O^*_{\mathcal{P}}$ serem todas não nulas, em geral, o divisor nulo pertence a $L_{\mathcal{P}}$. De fato, basta tomar uma função $f \in K$, por exemplo. Como o suporte de tais funções é vazio, está contido em $\mathcal{P}$.

Teorema 4.1.17. *O volume de $L_{\mathcal{P}}$ é tal que:*

$$vol(L_{\mathcal{P}}) \leq \sqrt{n}h_F \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g. \tag{4.5}$$

em que h_F é o número de classes de divisores de F, ou seja, a cardinalidade do grupo $Cl^0(F)$.

Demonstração. Primeiramente, demonstraremos a segunda igualdade, a qual depende apenas do estudo do número de classe h_F.

Para tanto, necessitaremos de alguns fatos conhecidos sobre a função Zeta de Riemman para um corpo de funções, os quais foram expostos ao final da seção 2.3.3. Relembramos que o polinômio $L_F(t)$ (L-polinômio) satisfaz:

$$L_F(t) = \prod_{i=1}^{2g}(1 - \alpha_i t),$$

em que os complexos α_i são inteiros algébricos, inversos das raízes de $L(F,t)$ de forma que $\alpha_{g+i} = \overline{\alpha_i}$. Temos ainda pelo Corolário 5.1.16 de [28] que o número de pontos racionais de F satisfaz:

$$n = q + 1 - \sum_{i=1}^{2g}\alpha_i.$$

Agora, como $h_F = L_F(1)$ (veja [28], Teorema 5.1.15), segue da desigualdade da média geométrica que

$$h_F = \prod_{i=1}^{2g}(1-\alpha_i) = \prod_{i=1}^{g}(q+1-\alpha_i-\overline{\alpha_i}) \leq \left(\frac{\sum_{i=1}^{g}(q+1-\alpha_i-\overline{\alpha_i})}{g}\right)^g = \left(q+1+\frac{n-q-1}{g}\right)^g.$$

Dessa forma, provamos a segunda desigualdade do teorema.

Para a primeira desigualdade, utilizaremos o cálculo do volume de um reticulado a partir do grupo quociente por um reticulado, conforme demonstrado no Corolário 3.4.7, juntamente às correspondências descritas acima.

Observemos que:

$$\frac{\mathbb{R}^{n-1}}{L_{\mathcal{P}}} \cong \frac{\mathbb{R}^{n-1}}{\mathcal{A}_{n-1}} \cdot \frac{\mathcal{A}_{n-1}}{L_{\mathcal{P}}}.$$

Neste momento, destacamos que o grupo quociente $\mathcal{A}_{n-1}/L_{\mathcal{P}}$ está bem definido tendo em vista que ambos os reticulados possuem o mesmo posto $n-1$.

Por outro lado, pela Proposição 4.1.14 e pelo seu respectivo corolário, podemos reescrever o isomorfismo acima como:

$$\frac{\mathbb{R}^{n-1}}{L_{\mathcal{P}}} \cong \frac{\mathbb{R}^{n-1}}{\mathcal{A}_{n-1}} \cdot \frac{Div^0(\mathcal{P})}{Princ(\mathcal{P})}.$$

Consequentemente, utilizando que $\mathcal{A}_{n-1}/L_{\mathcal{P}}$ é um grupo quociente e que o volume de $\mathcal{A}_{n-1}$ é igual a $\sqrt{n}$ (Proposição 4.1.11), segue:

$$vol(L_{\mathcal{P}}) = vol(\mathbb{R}^{n-1}/L_{\mathcal{P}}) = vol(\mathbb{R}^{n-1}/\mathcal{A}^{n-1})[\mathcal{A}_{n-1} : L_{\mathcal{P}}] = \sqrt{n}\left[Div^0(\mathcal{P}) : Princ(\mathcal{P})\right].$$

Por fim, como $Div^0(\mathcal{P})/Princ(\mathcal{P})$ é um subgrupo do grupo das classes de divisores de grau zero de F, cuja ordem é denotada por h_F, concluímos que $vol(L_{\mathcal{P}}) \leq \sqrt{n}h_F$, como queríamos. □

Observação 4.1.18. Os reticulados da forma $\mathcal{A}_{n-1}$ constituem um dos principais exemplos para os chamados *reticulados raízes*, ou seja, reticulados gerados por vetores de norma 2 e cujo produto interno de quaisquer dois de seus vetores é integral ou reticulados iguais a $\mathbb{Z}$ (veja [9] e [20]). Sabe-se ainda que tais reticulados apresentam as melhores densidades euclidianas possíveis nas dimensões 2 e 3, inclusive se comparada à densidade de empacotamentos não-reticulados (consultar Capítulo 1 de [17]). Um estudo mais detalhado sobre tais reticulados pode ser encontrado no Capítulo 4 de [20].

5 RETICULADOS VIA CORPOS DE FUNÇÕES ELÍPTICAS

Neste capítulo, estudaremos os reticulados da forma $L_{\mathcal{P}}$, definidos no Capítulo 4, obtidos a partir do corpo de funções elípticas. Para tanto, em princípio, estabeleceremos as principais definições quanto ao corpo de funções elípticas e suas propriedades ao considerarmos um corpo de constantes arbitrário K. Aprofundaremo-nos, ainda, no estudo da estrutura de grupo presente no conjunto de pontos de uma curva elíptica, a qual pode ser estendida ao grupo de lugares racionais do corpo de funções elípticas. Por fim, utilizaremos a construção de determinadas retas neste corpo de funções quando o corpo de constantes a ele associado é finito, juntamente ao estudo de certos espaços de Riemann-Roch a fim de obter os vetores geradores do reticulado $L_{\mathcal{P}}$. Finalmente, provaremos que, ao considerarmos tal corpo de funções com pelo menos 5 lugares racionais, o reticulado em questão é gerado por seus vetores minimais e, consequentemente, bem arredondado. Ao final do capítulo, apresentaremos também alguns resultados relativos ao *kissing number* e ao raio de cobertura do reticulado $L_{\mathcal{P}}$.

Para esta abordagem, utilizaremos principalmente as referências [13] e [26].

5.1 CORPO DE FUNÇÕES ELÍPTICAS

Definição 5.1.1. *Um corpo de funções F/K, sendo K corpo de constantes completo, é denominado um* ***corpo de funções elípticas*** *se as seguintes condições são satisfeitas;*

(i) *o gênero de F/K é igual a* 1*;*

(ii) *existe um divisor $D \in Div(F)$ tal que* $\deg D = 1$.

Outra forma de definir um corpo de funções elípticas, equivalente à apresentada, consiste em considerá-lo como sendo um corpo de funções da forma $K(x, y)/K$ em que x e y são as funções coordenadas associadas à chamada *curva elíptica*.

Definição 5.1.2. *Denominamos de* ***curva elíptica*** *o par $(E, \mathbf{O})$, em que $\mathbf{O} \in E$ e E é uma curva não singular de gênero* 1.

Observação 5.1.3. Ressaltamos que, ao dizermos que o gênero da curva (E, O) é igual a 1, estamos nos referindo ao gênero do corpo de funções a ela associado. Lembramos ainda que uma curva é dita não singular se as derivadas parciais não são todas nulas em cada ponto da curva.

Além disso, consideraremos o ponto fixo $\mathbf{O}$ representado acima como o único ponto no infinito com relação ao eixo z. Em outras palavras, podemos, a menos de homogeneização da equação definidora da curva elíptica, considerar que tal curva pertence ao espaço projetivo $K\mathbb{P}^2$. Neste caso, o ponto $\mathbf{O}$ em questão corresponde a

$\mathbf{O} = (0 : 1 : 0)$. Uma abordagem mais aprofundada de curvas elípticas no plano projetivo é feita em [25].

A efeito de simplificação, representaremos uma curva elíptica apenas por E, sendo o ponto $\mathbf{O}$ subentendido. De modo semelhante, denotaremos o corpo de funções elípticas por $K(E)/K$.

Vejamos um exemplo de corpo de funções elíptico.

Exemplo 5.1.4. Consideremos a curva E de equação $y^2 = x^3 - 3x + 3$ sobre $\mathbb{R}^2$, sendo x um elemento transcendente sobre $\mathbb{R}$.

Notemos que, de fato tal curva é não singular, visto que suas derivadas parciais são todas nulas apenas nos pontos $(1, 0)$ e $(-1, 0)$ de $\mathbb{R}^2$, os quais não pertencem à curva E. Por outro lado, pode-se demonstrar (veja [28], Proposição 6.1.3), que o gênero associado a esta curva é igual a 1.

Homogeneizando essa equação, obtemos $y^2z = x^3 - 3xz^2 + 3z^3$ e, dessa forma, o ponto $\mathbf{O}$ corresponde ao ponto $(0 : 1 : 0)$ no espaço projetivo $\mathbb{RP}^2$.

Assim, temos que $(E, \mathbf{O})$ é uma curva elíptica. Além disso, o corpo de funções associado a $(E, \mathbf{O})$, dado por $\mathbb{R}(E)/\mathbb{R}$, corresponde a $\mathbb{R}(x, y)/\mathbb{R}$ em que x e y satisfazem $y^2 = x^3 - 3x + 3$. Mais precisamente, temos:

$$\mathbb{R}[x, y] = \frac{\mathbb{R}[X, Y]}{\langle y^2 - x^3 + 3x - 3 \rangle}$$

e, consequentemente,

$$\mathbb{R}(x, y) = \left\{ \frac{g(x, y)}{h(x, y)} : \ g, h \in \mathbb{R}[X, Y] \text{ e } y^2 - x^3 + 3x - 3 \nmid h \right\}.$$

Motivados pelo Exemplo 5.1.4, podemos obter uma descrição mais detalhada para o corpo de funções elípticas, dada a partir da característica do corpo K (veja [28], Proposição 6.1.2).

Teorema 5.1.5. *Seja $K(E)/K$ um corpo de funções elípticas.*

(**1**) *Se $\mathrm{char}(K) \neq 2$, então existem $x, y \in K(E)$ tais que $K(E) = K(x, y)$ e y satisfaz:*

$$y^2 = f(x) \in K[x],$$

em que $f(x)$ é um polinômio livre de quadrados de grau 3.

(**2**) *Se $\mathrm{char}(K) = 2$, então existem $x, y \in K(E)$ tais que $K(E) = K(x, y)$, em que:*

$$y^2 + y = f(x) \in K[x] \ \textit{com} \ \deg f(x) = 3$$

ou

$$y^2 + y = x + \frac{1}{ax + b} \ \textit{com } a, b \in K \textit{ e } a \neq 0.$$

Nesse contexto, é possível estudarmos os lugares do corpo de funções elípticas e suas propriedades analisando cada um dos casos descritos anteriormente (veja [28] - Proposição 6.1.3). Neste trabalho, utilizaremos apenas que $K(E)$ admite um único polo, o lugar infinito Q_∞, e que os demais lugares racionais estão associados a pontos da curva elíptica. Além disso, destacamos que, independentemente da característica do corpo K, o mesmo constitui o corpo de constantes completo de $K(E)$.

5.2 ESTRUTURA DE GRUPO EM CURVAS ELÍPTICAS

As curvas elípticas são amplamente estudadas, tanto teoricamente quanto de forma aplicada, com grande importância na Criptografia. Uma das principais motivações para esse estudo deve-se ao fato de que os pontos das curvas elípticas possuem a estrutura de um grupo abeliano.

Para a obtenção de tal estrutura, utilizaremos que uma curva elíptica é, necessariamente, uma curva de grau 3. Mais precisamente, é possível mostrar que toda curva elíptica $(E, \mathbf{O})$ é isomorfa a uma curva dada por uma equação de Weiestrass de grau 3 (veja Proposição 3.1 em [26]). Assim, resulta pelo Teorema de Bézout que toda reta L intersecta a curva E em três pontos (não necessariamente distintos).

Nesse contexto, a estrutura de grupo em curvas elípticas é obtida a partir de uma operação entre dois pontos, denominada *soma*, a qual é definida do seguinte modo:

Definição 5.2.1. *Dados pontos* $\mathbf{P}, \mathbf{Q} \in E$, *consideremos L a reta passando por* $\mathbf{P}$ *e* $\mathbf{Q}$ *(no caso em que* $\mathbf{P} = \mathbf{Q}$, *consideramos L a reta tangente a E no ponto* $\mathbf{P}$*). Seja* $\mathbf{R}$ *o terceiro ponto de interseção da reta L com a curva E. Consideremos L' a reta passando por* $\mathbf{R}$ *e* $\mathbf{O}$ *(ponto no infinito). A reta L' intersecta a curva E em* $\mathbf{R}$, $\mathbf{O}$ *e em um terceiro ponto. Denotamos este terceiro ponto por* $\mathbf{P} + \mathbf{Q}$ *e dizemos que o mesmo representa a* ***soma dos pontos*** $\mathbf{P}$ ***e*** $\mathbf{Q}$.

Observação 5.2.2. Lembramos que o ponto $\mathbf{O}$ corresponde ao ponto no infinito de $K\mathbb{P}^2$ dado por $\mathbf{O} = (0 : 1 : 0)$. Utilizando este fato, pode-se demonstrar (consultar [26]) que, sob a notação da Definição 5.2.1, o ponto $\mathbf{P} + \mathbf{Q}$ corresponde ao simétrico do ponto $\mathbf{R}$ com relação ao eixo x. Assim, $x(\mathbf{R}) = x(\mathbf{P} + \mathbf{Q})$ e $y(\mathbf{P} + \mathbf{Q}) = -y(\mathbf{R})$.

Ressaltamos, ainda, que o cálculo do terceiro ponto de interseção $\mathbf{R}$ pode ser feito utilizando a *multiplicidade de interseção* através da *curva hessiana* (para uma descrição mais detalhada, sugerimos consultar [14]), além do uso de ferramentas computacionais.

A operação de soma apresentada é ilustrada na Figura 12.

Observação 5.2.3. Destacamos que a figura apresentada é puramente uma representação, na medida em que esboça somente o caso em que a curva elíptica se encontra sobre $\mathbb{R}^2$. Apesar disso, a definição algébrica de reta sobre um corpo arbitrário K é feita de

forma semelhante à estabelecida em corpos euclidianos. De fato, dizemos que L é uma linha sobre K se L é um polinômio da forma $L = ax + by + c$, em que $a, b, c \in K$ e $a \neq 0$ ou $b \neq 0$. Consequentemente, dizemos que um ponto P pertence à reta L se P é uma raiz do polinômio L.

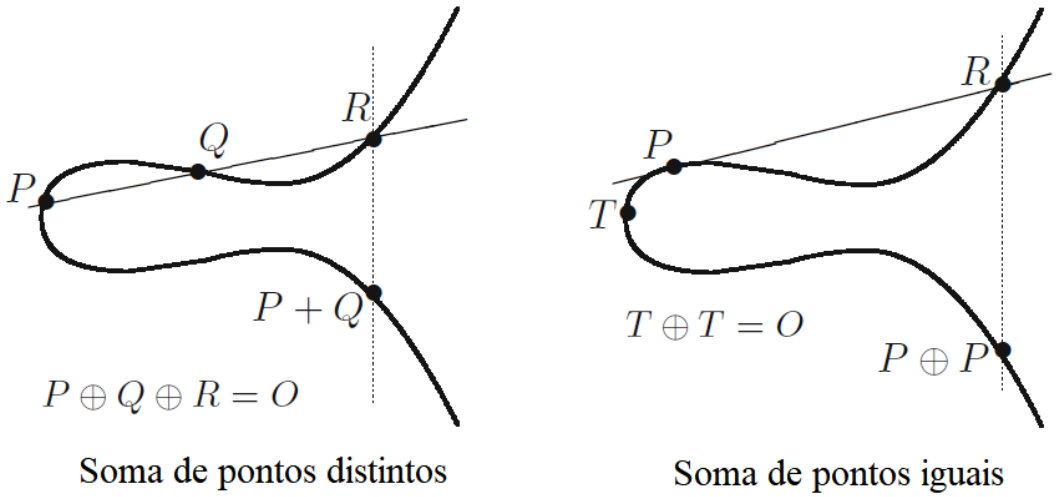


Figura 12 – Lei de Grupo em Curvas Elípticas [26]

Exemplo 5.2.4. Consideremos a curva elíptica de equação $E : y^2 = x^3 - 3x + 3$ em $\mathbb{R}^2$ e os pontos $\mathbf{P} = (1, -1)$ e $\mathbf{Q} = (-2, 1)$.

A reta secante de $\mathbf{P}$ e $\mathbf{Q}$ é dada por $L : 2x + 3y + 1 = 0$. Além disso, o terceiro ponto de interseção entre a reta L e a curva E é $\mathbf{R} = (13/9, -35/27)$. Para o cálculo da soma $\mathbf{P} + \mathbf{Q}$, utilizamos a Observação 5.2.2. Assim, $\mathbf{P} + \mathbf{Q}$ corresponde ao simétrico de $\mathbf{R}$ em relação ao eixo x, ou seja, $\mathbf{P} + \mathbf{Q} = (13/9, 35/27)$. Por outro lado, notemos que a reta tangente a E em $\mathbf{P}$ é dada por $-2y - 2 = 0$. Calculando o terceiro ponto de interseção entre essa reta e a curva E, obtemos $\mathbf{S} = (-2, -1)$. Desse modo, temos $\mathbf{P} + \mathbf{P} = (-2, 1) = \mathbf{Q}$.

Por fim, pode-se demonstrar que o conjunto de pontos da curva elíptica E com essa operação torna-se, de fato, um grupo abeliano.

Teorema 5.2.5 (Lei de Grupo em Curvas Elípticas). *A operação de soma de pontos da curva elíptica E satisfaz as seguintes propriedades:*

(**1**) $\mathbf{O}$ *é o elemento neutro de E, ou seja,* $\mathbf{P} + \mathbf{O} = \mathbf{P}$ *para todo* $\mathbf{P} \in E$;

(**2**) *Para todo* $\mathbf{P} \in E$ *existe um ponto em E, denotado por* $\mathbf{P}'$, *tal que* $\mathbf{P} + \mathbf{P}' = \mathbf{O}$. *A saber,* $\mathbf{P}'$ *corresponde ao terceiro ponto de interseção da reta que liga* $\mathbf{P}$ *e* $\mathbf{O}$ *com a curva E;*

(**3**) *Temos que* $\mathbf{P} + \mathbf{Q} = \mathbf{Q} + \mathbf{P}$ *para todos pontos* $\mathbf{P}, \mathbf{Q} \in E$;

(**4**) *Vale a associatividade, ou seja,* $\mathbf{P} + (\mathbf{Q} + \mathbf{R}) = (\mathbf{P} + \mathbf{Q}) + \mathbf{R}$ *para todos pontos* $\mathbf{P}, \mathbf{Q}, \mathbf{R} \in E$.

As propriedades listadas acima seguem diretamente da definição, exceto pela associatividade. Uma demonstração geométrica da mesma utiliza o Teorema dos 9 Pontos Associados e pode ser encontrada em [25] (Lema 2.6). Outra abordagem possível utiliza o Teorema de Riemann-Roch, o qual permite definir uma estrutura de grupo no conjunto de pontos racionais de $K(E)$.

A fim de apresentarmos a construção desta estrutura de grupo, denotemos como anteriormente $\mathcal{P}$ o conjunto de lugares racionais de $K(E)$. Sabemos que, independentemente da característica de $\mathbb{F}_q$, o corpo de funções $K(E)/K$ possui um único polo comum de x e y, digamos Q_∞, o qual tem grau 1. Assim, temos que $Q_\infty \in \mathcal{P}$.

Nessas circunstâncias, podemos escrever $\mathcal{P}$ como:

$$\mathcal{P} := \left\{P_0, P_1, \ldots, P_{n-1}\right\},$$

em que $P_0 := Q_\infty$.

Consideremos a aplicação:

$$\begin{aligned} \Phi : \mathcal{P} &\rightarrow Cl^0(E) \\ P &\mapsto [P - Q_\infty] \end{aligned} \tag{5.1}$$

em que $Cl^0(E)$ é o grupo das classes de divisores de $K(E)$.

Mostraremos que Φ é uma bijeção, a qual induz uma estrutura de grupo em $\mathcal{P}$.

Lema 5.2.6. *Para cada $A \in Div(E)$ de grau 1 fixado, existe um único lugar $P \in \mathbb{P}_E$ tal que $A \sim P$. Em particular, $\mathbb{P}_{K(E)} \neq \emptyset$.*

Demonstração. Pelo Teorema de Riemann, o qual garante a existência do gênero como previamente definido, sabemos que $g \geq \deg A - \ell(A) + 1$ e, como $g = 1$ e $\deg(A) = 1$, segue que $\ell(A) \geq 1$. Assim, temos que o espaço de Riemann associado ao divisor A, denotado por $\mathcal{L}(A)$, é não vazio, resultando que existe um divisor $P \sim A$, com $P > 0$ (lembrando que a desigualdade é estrita tendo em vista que o grau de A é 1). Agora, como P é um divisor positivo de grau 1, P deve ser um lugar racional, comprovando a existência.

Para a unicidade, suponhamos, por absurdo, que $A \sim P$ e $A \sim Q$, sendo $P, Q \in \mathcal{P}$ e $P \neq Q$. Como essa é uma relação de equivalência, resulta que $P \sim Q$, ou seja, existe $x \in K(E)$ tal que $P = Q + (x)$. Por outro lado, sabemos (pelo Teorema 2.3.43) que:

$$[K(E) : K(x)] = \deg(x)_\infty = \deg(Q) = 1,$$

donde $K(E) = F(x)$, uma contradição com o fato de $K(E)$ ser o corpo de funções elípticas. □

Proposição 5.2.7. *A aplicação Φ definida na equação (5.1) é uma bijeção.*

Demonstração. Primeiramente, notemos que Φ está bem definida, uma vez que $\mathcal{P}$ se constitui dos divisores racionais de $K(E)$ e que $Q_\infty \in \mathcal{P}$; consequentemente, fixado $P \in \mathcal{P}$, a classe do divisor $P - Q_\infty$ possui grau zero.

Para a prova de que Φ é sobrejetivo, consideremos $[D] \in Cl^0(E)$. Então, $\deg[D] = 0$, donde $Q_\infty + D$ é um divisor de grau 1. Pelo Lema 5.2.6, existe um único lugar $P \in \mathcal{P}$ tal que $P \sim D + Q_\infty$, ou seja, tal que o lugar P pertence à mesma classe de equivalência de $D + Q_\infty$. Logo, $[P] = [Q_\infty + D]$, implicando que $[P - Q_\infty] = [D]$ e, por consequência, $\Phi(P) = [D]$.

Para a prova da injetividade, tomemos $P, Q \in \mathcal{P}$ tais que $\Phi(P) = \Phi(Q)$. Dessa forma, temos que $[P - Q_\infty] = [Q - Q_\infty]$, implicando que $P \sim Q$. Como, em particular, $P, Q \in \mathbb{P}_{K(E)}$, utilizando a unicidade do Lema 5.2.6, concluímos que $P = Q$. □

Como Φ é bijeção, podemos transferir a estrutura de grupo presente em $Cl^0(E)$ para o conjunto dos lugares racionais de $K(E)$. Para tanto, dados $P, Q \in \mathcal{P}$, definimos a operação:

$$P \oplus Q := \Phi^{-1}(\Phi(P) + \Phi(Q)). \tag{5.2}$$

Observação 5.2.8. O símbolo $\oplus$ utilizado acima denota uma operação de soma não usual; seu significado, neste capítulo, difere de soma direta, como utilizado na seção 3.4.

A seguir, apresentamos as principais propriedades dessa operação.

Proposição 5.2.9. *Consideremos $K(E)/K$ um corpo de funções elípticas. Então:*

(1) *O mapa Φ definido em (5.1) é um isomorfismo de grupos;*

(2) *O conjunto de lugares racionais $\mathcal{P}$ é um grupo abeliano sob a operação definida em (5.2);*

(3) *O lugar Q_∞ é o elemento neutro (ou identidade) de $\mathcal{P}$;*

(4) *Dados $P, Q, R \in \mathcal{P}$, vale a equivalência:*

$$P \oplus Q = R \Leftrightarrow P + Q \sim R + Q_\infty.$$

Demonstração. As afirmações (1), (2) e (3) são diretamente verificadas.

Para a afirmação (4), temos:

$$\begin{aligned} P \oplus Q = R &\Leftrightarrow \Phi^{-1}(\Phi(P) + \Phi(Q)) = R \\ &\Leftrightarrow \Phi(P) + \Phi(Q) = \Phi(R) \\ &\Leftrightarrow R - Q_\infty \sim (P - Q_\infty) + (Q - Q_\infty) \\ &\Leftrightarrow R + Q_\infty \sim P + Q. \end{aligned}$$

□

Observação 5.2.10. É interessante destacar que, para a garantia de que Φ é uma bijeção, não utilizamos o fato de Q_∞ ser um polo. Com efeito, o mapa Φ pode ser definido de modo inteiramente análogo, trocando-se Q_∞ por um lugar racional arbitrário $P_0 \in \mathcal{P}$. Ainda sob tais circunstâncias, provaríamos a existência de uma bijeção entre $Cl^0(E)$ e $\mathcal{P}$ e, consequentemente, da estrutura de grupo induzida pelo novo mapa. A escolha por Q_∞ deve-se, portanto, aos resultados que serão exibidos posteriormente, os quais envolvem a propriedade de Q_∞ ser polo de x e y.

Pode-se demonstrar que a estrutura geométrica de grupo apresentada no início da subseção e esta estrutura algébrica no conjunto dos pontos racionais de $K(E)$ são essencialmente a mesma (veja [26], Proposição 3.4-*e*). Consequentemente, obtemos uma correspondência biunívoca entre o conjunto de pontos da curva elíptica E sobre o corpo K (ditos *pontos racionais*) e o conjunto de lugares racionais de $K(E)/K$. Assim, a partir desse momento, denotaremos o ponto no infinito como $\mathbf{Q}_\infty := \mathbf{O}$, ou seja, como o ponto correspondente ao lugar infinito Q_∞.

5.3 RESULTADOS PRELIMINARES

Apesar da generalidade da definição e das propriedades anteriormente apresentadas para corpos de funções elípticas, a qual se aplica para corpos da forma F/K, neste trabalho consideraremos apenas corpos de funções elípticas definidos sobre um corpo finito $K := \mathbb{F}_q$, em que q é a potência de um primo. Assim, para efeito de notação, representaremos tal corpo por $K(E)/\mathbb{F}_q$.

Além disso, considerando a correspondência biunívoca entre valorizações e lugares, sabemos que a cada lugar P de $K(E)$ corresponde um único ponto sobre a curva elíptica em questão. Nessas circunstâncias, denotaremos o ponto correspondente ao lugar P como sendo $\mathbf{P}$. Consequentemente, ao escrevermos $P + Q$ estaremos nos referindo à soma de P e Q vistos como divisores; enquanto $\mathbf{P} + \mathbf{Q}$ denotará a soma dos pontos $\mathbf{P}$ e $\mathbf{Q}$ associados a tais lugares. Representaremos ainda por P' o lugar correspondente ao inverso aditivo do ponto $\mathbf{P}$, ou seja, $\mathbf{P} + \mathbf{P}' = \mathbf{Q}_\infty$. Destacamos que, sendo a abscissa do ponto $\mathbf{P}$ denotada por $x(\mathbf{P})$, sabemos que $x(\mathbf{P}) = x(\mathbf{P}')$.

Dados pontos $\mathbf{P}$ e $\mathbf{Q}$ pertencentes à curva elíptica E, definimos:

$$m(\mathbf{P},\mathbf{Q}) := \begin{cases} \text{reta passando por } \mathbf{P} \text{ e } \mathbf{Q}, \text{ se } P, Q \neq Q_\infty \text{ e } P \neq Q; \\ \text{reta tangente a } E \text{ em } \mathbf{P}\text{ , se } P = Q\ (\neq Q_\infty); \\ 1 \in \mathbb{F}_q, \text{ se } P = Q_\infty \text{ ou } Q = Q_\infty. \end{cases}$$

Notemos que, assim, considerando $P, Q \neq Q_\infty$ e $P \neq Q$, podemos representar $m(\mathbf{P},\mathbf{Q}) = ax + by + c$, em que $a, b, c \in \mathbb{F}_q$ de modo que os pontos $\mathbf{P}$ e $\mathbf{Q}$ pertencem a tal

reta, ou seja, são raízes da equação $m(\mathbf{P},\mathbf{Q}) = 0$. Além disso, caso tenhamos $Q = P'$ ($\neq Q_\infty$), sabemos que $x(\mathbf{P}) = x(\mathbf{Q})$, donde resulta que $m(\mathbf{P},\mathbf{Q}) = x - x(\mathbf{P}) = x - x(\mathbf{Q})$.

Queremos avaliar o divisor de $m(\mathbf{P},\mathbf{Q})$, visto como função em $K(E)/\mathbb{F}_q$. Para tanto, temos os seguintes resultados:

Proposição 5.3.1. *Sejam $P \neq Q_\infty$ e $Q \neq Q_\infty$ e consideremos $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. Então, o divisor de $m(\mathbf{P},\mathbf{Q})$ é dado por:*

$$(m(\mathbf{P},\mathbf{Q})) = P + Q + R' - 3Q_\infty.$$

Em particular, caso tenhamos $Q = P'$, segue que:

$$(m(\mathbf{P},\mathbf{Q})) = (x - x(\mathbf{P})) = P + P' - 2Q_\infty.$$

Demonstração. Analisemos cada uma das possibilidades para a reta $m(\mathbf{P},\mathbf{Q})$.

Sabemos que, se $\mathbf{P}$ e $\mathbf{Q}$ são pontos finitos distintos em E, digamos $\mathbf{P} = (a_1, b_1)$ e $\mathbf{Q} = (a_2, b_2)$, então a reta passando por $\mathbf{P}$ e $\mathbf{Q}$ é dada por:

$$m(\mathbf{P},\mathbf{Q}) := \begin{cases} \dfrac{b_2 - b_1}{a_2 - a_1}(x - a_1) - (y - b_1), \text{ se } a_1 \neq a_2; \\ \\ x - a_1 = x - x(\mathbf{P}), \text{ se } a_1 = a_2. \end{cases}$$

Consideremos, primeiramente, o caso mais geral, i.e., em que $Q \neq Q_\infty$ (e consequentemente, $a_1 \neq a_2$). Para qualquer lugar racional $S \in \mathcal{P}$, temos, pelas propriedades de valorização, que:

$$\begin{aligned} v_S(m(\mathbf{P},\mathbf{Q})) &= \min\left\{ v_S\left(\frac{b_2 - b_1}{a_2 - a_1}(x - a_1)\right), v_S(y - b_1)\right\} \\ &= \min\left\{v_S(x - a_1), v_S(y - b_1)\right\}. \end{aligned}$$

Assim, no caso em que $S = P$, é imediato que $v_P(m(\mathbf{P},\mathbf{Q})) = 1$; para notarmos que o mesmo vale para o lugar Q, basta fazermos uma mudança de variáveis. Ainda, temos que $v_{R'}(m(\mathbf{P},\mathbf{Q})) = 1$, visto que podemos reescrever a reta $m(\mathbf{P},\mathbf{Q})$ em função das coordenadas de $\mathbf{R}'$. Lembramos que aqui estamos utilizando fortemente que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, ou seja, $\mathbf{P}, \mathbf{Q}, \mathbf{R}'$ pertencem à reta $m(\mathbf{P},\mathbf{Q})$.

Por outro lado, sabemos que esses são os únicos pontos de E que pertencem à reta $m(\mathbf{P},\mathbf{Q})$. Desse modo, dado um ponto $\mathbf{S}$ finito de E distinto desses três, tem-se $v_S(m(\mathbf{P},\mathbf{Q})) = 0$.

Por fim, para o ponto infinito $\mathbf{Q}_\infty$, utilizaremos o fato já observado de que o grau do divisor $(m(\mathbf{P},\mathbf{Q}))$ é igual a zero, visto que o mesmo é um divisor principal. Em outras palavras, temos:

$$\deg\left(m(\mathbf{P},\mathbf{Q})\right) = \sum_{i=0}^{n-1} v_i(m(\mathbf{P},\mathbf{Q})) = 0.$$

Agora, utilizando o cálculo feito para $v_S(m(\mathbf{P},\mathbf{Q}))$ quando S é um ponto finito, segue que:

$$\deg\left(m(\mathbf{P},\mathbf{Q})\right) = v_P(m(\mathbf{P},\mathbf{Q})) + v_Q(m(\mathbf{P},\mathbf{Q})) + v_{R'}(m(\mathbf{P},\mathbf{Q})) + v_\infty(m(\mathbf{P},\mathbf{Q})) = 0,$$

donde resulta:

$$v_\infty(m(\mathbf{P},\mathbf{Q})) = -3.$$

Logo, no caso em que $Q' \neq P$, o divisor da reta em questão é dado por:

$$(m(\mathbf{P},\mathbf{Q})) = P + Q + R' - 3Q_\infty.$$

Para o caso particular, procedemos exatamente como enunciado para os pontos finitos de E. Nesse caso, concluímos, de modo análogo, que $v_S(x - x(\mathbf{P})) = 1$ quando $S = P$ ou $S = Q$ e $v_S(x - x(\mathbf{P})) = 0$ para pontos finitos S distintos desses. Ressaltamos aqui que, como $\mathbf{P} + \mathbf{Q} = \mathbf{Q}_\infty$, temos a garantia de que $\mathbf{P}$ e $\mathbf{Q}$ são, de fato, os únicos pontos finitos de E que interceptam a reta $x - x(\mathbf{P})$. Assim, resta calcularmos o valor da valorização associada ao lugar Q_∞ para essa reta. Utilizando a análise do grau do divisor de $(m(\mathbf{P},\mathbf{Q}))$ como anteriormente, temos $v_\infty(m(\mathbf{P},\mathbf{Q})) = -2$, concluindo a demonstração. □

Corolário 5.3.2. *Consideremos* $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, *sendo* $R \neq Q_\infty$. *Então, segue que:*

$$\left(\frac{m(\mathbf{P},\mathbf{Q})}{x - x(\mathbf{R})}\right) = P + Q - R - Q_\infty.$$

Demonstração. Como $m(\mathbf{P},\mathbf{Q})$ e $x - x(\mathbf{R})$ podem ser vistos como funções em $K(E)$, obtemos:

$$\begin{aligned} v\left(\frac{m(\mathbf{P},\mathbf{Q})}{x - x(\mathbf{R})}\right) &= v(m(\mathbf{P},\mathbf{Q})) + v\left((x - x(\mathbf{R}))^{-1}\right) \\ &= v(m(\mathbf{P},\mathbf{Q})) - v(x - x(\mathbf{R})), \end{aligned}$$

para toda valorização v associada a um lugar de $K(E)/\mathbb{F}_q$.

Por outro lado, R e R' possuem a mesma abscissa, donde $x - x(R) = m(\mathbf{R},\mathbf{R}')$. Assim, segue que:

$$\begin{aligned} \left(\frac{m(\mathbf{P},\mathbf{Q})}{m(\mathbf{R},\mathbf{R}')}\right) &= (m(\mathbf{P},\mathbf{Q})) - (m(\mathbf{R},\mathbf{R}')) \\ &= (P + Q + R' - 3Q_\infty) - (R + R' - 2Q_\infty) \\ &= P + Q - R - Q_\infty. \end{aligned}$$

□

Observação 5.3.3. É possível definir grau de um polinômio no corpo de funções elípticas utilizando o conceito de grau de um polinômio em uma variável (veja a seção §3 de

[31]). Então, pode-se demonstrar que x/y é um elemento primo de Q_∞ e o cálculo de $v_\infty(m(\mathbf{P},\mathbf{Q}))$ pode ser feito escrevendo a reta $m(\mathbf{P},\mathbf{Q})$ como o produto de uma potência de x/y por uma função de $K(E)$. Nesse caso, prova-se que, quando $Q \neq P'$, tal expoente é igual a -3 e, em caso contrário, igual a -2. Desse modo, obtemos uma prova alternativa para a proposição anterior.

Consideremos $\mathbf{P},\mathbf{Q} \in E$ tais que $\mathbf{P}+\mathbf{Q}=\mathbf{R}$. Definimos, agora, uma função que será fundamental para determinar os vetores que geram o reticulado $L_{\mathcal{P}}$.

$$F(\mathbf{P},\mathbf{Q}) := \begin{cases} \dfrac{x - x(R)}{m(\mathbf{P},\mathbf{Q})}, \text{ se } \mathbf{P},\mathbf{Q},\mathbf{R} \neq \mathbf{Q}_\infty; \\ \dfrac{1}{m(\mathbf{P},\mathbf{Q})}, \text{ se } \mathbf{P},\mathbf{Q} \neq \mathbf{Q}_\infty \text{ e } \mathbf{R} = \mathbf{Q}_\infty; \\ 1, \text{ se } \mathbf{P} = \mathbf{Q}_\infty \text{ ou } \mathbf{Q} = \mathbf{Q}_\infty. \end{cases} \tag{5.3}$$

Proposição 5.3.4. *O divisor de $F(\mathbf{P},\mathbf{Q})$ é dado nos três casos por:*

$$(F(\mathbf{P},\mathbf{Q})) = -P - Q + R + Q_\infty.$$

Demonstração. Procederemos como no Corolário 5.3.2. O primeiro caso é imediato. Para os demais, notemos que:

- Se $\mathbf{P},\mathbf{Q} \neq \mathbf{Q}_\infty$ e $R = Q_\infty$, então $\mathbf{R}' = \mathbf{Q}_\infty$, donde obtemos:

$$(F(\mathbf{P},\mathbf{Q})) = -(P + Q + R' - 3Q_\infty) = -P - Q + 2Q_\infty = -P - Q + R + Q_\infty.$$

- Se $\mathbf{P} = \mathbf{Q}_\infty$ (ou $\mathbf{Q} = \mathbf{Q}_\infty$), temos que $R = Q$ (resp. $R = P$), resultando em:

$$(F(\mathbf{P},\mathbf{Q})) = 0 = -P - Q + R + Q_\infty.$$

□

Neste momento, visamos mostrar que o grupo $\mathcal{O}^*_{\mathcal{P}}$ é gerado por funções $F(\mathbf{P},\mathbf{Q})$, em que $P,Q \in \mathcal{P}$. A partir de tal resultado, obteremos os vetores geradores para o reticulado $L_{\mathcal{P}}$. Com este intuito, apresentaremos uma série de resultados referentes a determinados espaços de Riemann-Roch obtidos pela soma de lugares racionais. Antes, porém, generalizamos a ideia de subespaço m-dimensional de $\mathbb{R}^n$ coberto por um reticulado para o span do produto de um número finito de funções em F.

Definição 5.3.5. *Seja $m \in \mathbb{N}$ fixado e sejam $f_1,\ldots,f_m \in F$. Definimos:*

$$span_K\{f_1,\ldots,f_m\} := \left\{ \sum_{i=1}^{m} a_i f_i : \ a_i \in K \text{ para todo } i = 1,\ldots,m \right\}.$$

Em particular, para cada $j \in \{1, \ldots, m\}$, temos:

$$span_K\{f_j\} := \left\{a_j f_j : \ a_j \in K\right\}.$$

Além disso, definimos o span do produto como:

$$span_K\{f_1 \cdots f_m\} := \prod_{j=1}^{m} span_K\{f_j\}.$$

Calcularemos, agora, o $\text{span}_K\{F(\mathbf{P}, \mathbf{Q})\}$.

Lema 5.3.6. *Dada uma função f de um corpo de funções F, tem-se que $f\mathcal{L}(D) = \mathcal{L}(D - (f))$ para todo divisor $D \in Div(F)$. Mais geralmente, $f^m\mathcal{L}(D) = \mathcal{L}(D - m(f))$ para todo $m \in \mathbb{N}$.*

Demonstração. Sabemos que o espaço de Riemann-Roch de um divisor D é dado por:

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

Denotemos $D = \sum n_P P$. Seja $x \in \mathcal{L}(D)$. Temos:

$$(fx) = \sum_{P \in \mathbb{P}_F} (v_P(f) + v_P(x))\, P \geq \sum_{P \in \mathbb{P}_F} (v_P(f) - n_P)\, P.$$

Assim, segue que $fx \in \mathcal{L}(D - (f))$ e, portanto, $f\mathcal{L}(D) \subset \mathcal{L}(D - (f))$.

Reciprocamente, consideremos $y \in \mathcal{L}(D - (f))$. Podemos escrever $y = fx$ para algum $x \in F$. Além disso, sabemos que para todo $P \in \mathbb{P}_F$ vale:

$$v_P(fx) = v_P(f) + v_P(x) \geq -n_P + v_P(f),$$

resultando que $x \in \mathcal{L}(D)$.

Logo, $f\mathcal{L}(D) = \mathcal{L}(D-(f))$. A última afirmação é obtida por indução em $m \in \mathbb{N}$. □

Observação 5.3.7. Destacamos que, conforme indica a nomenclatura adotada para o corpo de funções, o resultado apresentado no lema anterior se verifica para qualquer corpo de funções algébricas F; ou seja, não apenas para o corpo de funções elípticas.

Proposição 5.3.8. *Sejam P, Q lugares racionais do corpo elíptico $K(E)$. Então, dado um lugar racional R de $K(E)$, temos que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ se, e somente se, $\mathcal{L}(P + Q - R - Q_\infty) \neq \{0\}$.*

Neste caso,

$$\mathcal{L}(P + Q - R - Q_\infty) = span_K\{F(\mathbf{P}, \mathbf{Q})\}.$$

Demonstração. ($\Rightarrow$) Seja R um lugar racional de $K(E)$ tal que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. Suponhamos que $R \neq Q_\infty$. Pelo Corolário 5.3.2, sabemos que:

$$\left(\frac{m(\mathbf{P}, \mathbf{Q})}{x - x(R)}\right) = P + Q - R - Q_\infty,$$

resultando, por definição, em:

$$\frac{m(\mathbf{P},\mathbf{Q})}{x-x(R)} \in \mathcal{L}(P+Q-R-Q_\infty).$$

Por outro lado, se $R = Q_\infty$, ou seja, $Q = P'$, temos pela Proposição 5.3.1 que $m(\mathbf{P},\mathbf{P'}) \in \mathcal{L}(P+P'-2Q_\infty)$. Por fim, basta notar que $\mathcal{L}(P+Q-R-Q_\infty) = \mathcal{L}(P+P'-2Q_\infty)$.

Consequentemente, em ambos os casos, concluímos que $\mathcal{L}(P+Q-R-Q_\infty) \neq \{0\}$.

($\Leftarrow$) Seja R um lugar racional de $K(E)$ e consideremos que:

$$\mathcal{L}(P+Q-R-Q_\infty) \neq \{0\}.$$

Queremos mostrar que $\mathbf{P}+\mathbf{Q}=\mathbf{R}$.

Suponhamos, primeiramente, que $P, Q \neq Q_\infty$. Neste caso, utilizando o lema anterior, temos:

$$\begin{aligned} \frac{1}{F(\mathbf{P},\mathbf{Q})}\mathcal{L}(P+Q-R-Q_\infty) &= \mathcal{L}\left(P+Q-R-Q_\infty-\left(\frac{1}{F(\mathbf{P},\mathbf{Q})}\right)\right) \\ &=: \mathcal{L}(S-R), \end{aligned} \tag{5.4}$$

em que

$$S := P+Q-Q_\infty-\left(\frac{1}{F(\mathbf{P},\mathbf{Q})}\right).$$

Denotemos o terceiro ponto de interseção da reta $m(\mathbf{P},\mathbf{Q})$ com a curva elíptica E por $\mathbf{T}'$. Ou seja, consideremos que $\mathbf{P}+\mathbf{Q}=\mathbf{T}$. Mostraremos que $\mathbf{T}=\mathbf{S}$. Com efeito, vejamos cada um dos casos:

- Se $\mathbf{T}=\mathbf{Q}_\infty$, temos:

$$\begin{aligned} S &= P+Q-Q_\infty-(m(\mathbf{P},\mathbf{Q})) \\ &= P+Q-Q_\infty-(P+Q+T'-3Q_\infty) \\ &= -T'+2Q_\infty \end{aligned}$$

  e, assim, $\mathbf{S} = -\mathbf{T}'+2\mathbf{Q}_\infty = \mathbf{T}+\mathbf{Q}_\infty = \mathbf{T}$.

- Se $\mathbf{T} \neq \mathbf{Q}_\infty$, utilizando as propriedades das valorizações, temos:

$$\begin{aligned} S &= P+Q-Q_\infty-\left(\frac{m(\mathbf{P},\mathbf{Q})}{x-x(\mathbf{T})}\right) \\ &= P+Q-Q_\infty-[(m(\mathbf{P},\mathbf{Q}))-(x-x(\mathbf{T}))] \\ &= T+(x-x(\mathbf{T})) \\ &= T+(m(\mathbf{T},\mathbf{T}')) \end{aligned}$$

  e, então, $\mathbf{S} = 2\mathbf{T}+\mathbf{T}'-2\mathbf{Q}_\infty = \mathbf{T}-\mathbf{Q}_\infty = \mathbf{T}$

Consequentemente, temos que $\mathbf{P} + \mathbf{Q} = \mathbf{S}$.

Agora, como por hipótese $\mathcal{L}(P + Q - R - Q_\infty)$ tem dimensão positiva, então o mesmo é válido para $\mathcal{L}(S - R)$. Além disso, como S e R são lugares racionais, temos que $\deg(S - R) = 0$, donde, pelo resultado anterior, segue que $\ell(S - R) = 1$. Assim, $\mathcal{L}(S - R) = K = \mathbb{F}_q$, garantindo que $S - R = 0$, ou seja, $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, como queríamos.

E, pela equação (5.4), obtemos:

$$\mathcal{L}(P + Q - R - Q_\infty) = span_K\{F(\mathbf{P}, \mathbf{Q})\}.$$

Suponhamos, por outro lado, que $P = Q_\infty$. Então, $\mathbf{P} + \mathbf{Q} = \mathbf{Q}$ e, conforme enunciado,

$$\mathcal{L}(P + Q - R - Q_\infty) = \mathcal{L}(Q - R) \neq \{0\}.$$

Procedendo como anteriormente, resulta que $\mathcal{L}(Q - R) = \mathbb{F}_q$ e $Q = R$. Consequentemente, $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ e $\mathcal{L}(P + Q - R - Q_\infty) = span_K\{1\} = span_K\{F(\mathbf{P}, \mathbf{Q})\}$.

Para o caso em que $Q = Q_\infty$ a implicação segue de modo completamente análogo ao anterior. □

Tal resultado pode ser generalizado, estabelecendo as condições para que, fixado o número de lugares racionais n de $K(E)$, tenhamos $n\mathbf{P} = \mathbf{Q}_\infty$.

Teorema 5.3.9. *Consideremos $n \geq 1$ o número de lugares racionais de $K(E)$. Temos que $n\mathbf{P} = \mathbf{Q}_\infty$ se, e somente se,*

$$\mathcal{L}(nP - nQ_\infty) = span_K\Big\{F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, 2\mathbf{P}) \cdots F\left(\mathbf{P}, (n-1)\mathbf{P}\right)\Big\}.$$

Demonstração. O caso $n = 1$ é imediato, visto que:

$$\mathbf{P} = \mathbf{Q}_\infty \Leftrightarrow \mathcal{L}(P - Q_\infty) = K = span_K\{F(\mathbf{P}, \mathbf{Q}_\infty)\}.$$

Para $s \geq 1$, denotemos $\mathbf{P_s} := s\mathbf{P}$. Consideremos agora $s \geq 2$. Notemos que $\mathbf{P} + \mathbf{P}_{s-1} = \mathbf{P}_s$ e, pela Proposição 5.3.8,

$$\mathcal{L}(P + P_{s-1} - P_s - Q_\infty) = span_K\{F(\mathbf{P}, \mathbf{P_{s-1}})\}.$$

Aplicaremos esse procedimento sucessivamente.

Suponhamos que $n\mathbf{P} = \mathbf{Q}_\infty$. Assim, temos que $\mathbf{P} + \mathbf{P}_{n-1} = \mathbf{P}_n$ e, consequentemente,

$$\mathcal{L}(P + P_{n-1} - P_s - Q_\infty) = span_K\{F(\mathbf{P}, \mathbf{P}_{n-1})\}. \tag{5.5}$$

De modo geral, fazendo $\mathbf{P} + \mathbf{P}_{n-i-1} = \mathbf{P}_{n-i}$, em que $i = 1, 2, \ldots, n-2$, temos que as seguintes identidades são verdadeiras:

$$\begin{aligned} \mathcal{L}(P + P_{n-2} - P_{n-1} - Q_\infty) &= span_K\{F(\mathbf{P}, \mathbf{P}_{n-2})\}; \\ \mathcal{L}(P + P_{n-3} - P_{n-2} - Q_\infty) &= span_K\{F(\mathbf{P}, \mathbf{P}_{n-3})\}; \\ &\vdots \\ \mathcal{L}(P + P - P_2 - Q_\infty) &= span_K\{F(\mathbf{P}, \mathbf{P})\}. \end{aligned} \tag{5.6}$$

Observemos que, se $\mathcal{L}(D_1) = span_K\{f_1\}$ e $\mathcal{L}(D_2) = span_K\{f_2\}$, sendo f_1 e f_2 funções, então $\mathcal{L}(D_1 + D_2) = span_K\{f_1 f_2\}$. De fato, como $span_K\{f_1\} \cdot span_K\{f_2\} = span_K\{f_1 f_2\}$, basta mostrarmos que $\mathcal{L}(D_1 + D_2) = \mathcal{L}(D_1) \cdot \mathcal{L}(D_2)$. Tal resultado utiliza apenas que K é corpo, juntamente às definições dos espaços em questão, e pode ser verificado facilmente.

Desse modo, combinando todas as $(n-1)$ identidades apresentadas em (5.5) e (5.6) e utilizando o resultado descrito no parágrafo anterior, obtemos:

$$\mathcal{L}(n\mathbf{P} - n\mathbf{Q}_\infty) = span_K\Big\{F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \cdots F(\mathbf{P}, \mathbf{P}_{n-1})\Big\}, \tag{5.7}$$

como queríamos.

Para a outra implicação, consideremos que a identidade (5.7) seja válida. Devemos mostrar que $n\mathbf{P} = \mathbf{Q}_\infty$.

Notemos que, utilizando as propriedades das valorizações, o divisor do produto

$$T_{n-2}(\mathbf{P}) := F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \cdots F(\mathbf{P}, \mathbf{P}_{n-2})$$

pode ser escrito como a soma dos divisores de cada parcela, ou seja, corresponde a:

$$\begin{aligned} &(-P - P + P_2 + Q_\infty) + (-P - P_2 + P_3 + Q_\infty) + \cdots + (-P - P_{n-2} + P_{n-1} + Q_\infty) \\ &= -(n-1)P + P_{n-1} + (n-2)Q_\infty. \end{aligned}$$

Por outro lado, aplicando o Lema 5.3.6 ao produto em questão, temos:

$$\begin{aligned} \frac{1}{T_{n-2}(\mathbf{P})}\mathcal{L}(nP - nQ_\infty) &= \mathcal{L}\left(nP - nQ_\infty - \left(\frac{1}{T_{n-2}(\mathbf{P})}\right)\right) \\ &= \mathcal{L}\Big(nP - nQ_\infty + (T_{n-2}(\mathbf{P}))\Big). \end{aligned}$$

Logo, utilizando o cálculo feito para tal divisor, concluímos que:

$$\frac{1}{F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, \mathbf{P}_2) \cdots F(\mathbf{P}, \mathbf{P}_{n-2})}\mathcal{L}(nP - nQ_\infty) = \mathcal{L}(P + P_{n-1} - 2Q_\infty).$$

Por fim, como o espaço de Riemann-Roch $\mathcal{L}(nP - nQ_\infty)$ é não trivial, segue que $\mathcal{L}(P + P_{n-1} - 2Q_\infty)$ também não é. Assim, podemos aplicar a Proposição 5.3.8, a qual nos garante que $\mathbf{P} + \mathbf{P}_{n-1} = \mathbf{Q}_\infty$, ou seja, $n\mathbf{P} = \mathbf{Q}_\infty$, como queríamos provar. □

Finalmente, somos capazes de provar que $O^*_{\mathcal{P}}$ é gerado pelas funções da forma $F(\mathbf{P}, \mathbf{Q})$, em que $P, Q \in \mathcal{P}$ e obtermos a caracterização dos vetores geradores para o reticulado $L_{\mathcal{P}}$.

Teorema 5.3.10 (Caracterização dos vetores geradores de $L_{\mathcal{P}}$). *Seja D um divisor de grau zero de $K(E)$ dado por:*

$$D := rQ_\infty + \sum_{i=1}^{n-1} a_i P_i.$$

Então, D é principal se, e somente se

$$\sum_{i=1}^{n-1} a_i \mathbf{P}_i = \mathbf{Q}_\infty. \tag{5.8}$$

Neste caso, temos que $D = (f)$, em que f é o produto de funções da forma $F(\mathbf{P}, \mathbf{Q})$ sendo $P, Q \in \mathcal{P}$. Além disso, o grupo $O^*_{\mathcal{P}}$ é gerado por tais funções. E, consequentemente, o reticulado $L_{\mathcal{P}}$ é gerado pelos vetores da forma $P + Q - R - Q_\infty$, em que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$.

Demonstração. Notemos primeiramente que é possível assumir, sem perda de generalidade, que $a_i \geq 0$ para todo $1 \leq i \leq n-1$.

Com efeito, suponhamos que exista um índice j com $1 \leq j \leq n-1$ tal que $a_j < 0$. Consideremos a ordem do ponto $\mathbf{P}_j$ denotada por s_j, ou seja, s_j é o menor inteiro tal que $s_j \mathbf{P}_j = \mathbf{Q}_\infty$. Como no teorema anterior, denotemos ainda $\mathbf{P}_i := i\mathbf{P}$ e, para todo $s \geq 2$, façamos:

$$T_s(\mathbf{P}) := F(\mathbf{P}, \mathbf{P})F(\mathbf{P}, 2\mathbf{P}) \cdots F(\mathbf{P}, (s-1)\mathbf{P}).$$

Agora, calculando o divisor de $T_{s_j}(\mathbf{P}_j)$ como no Teorema 5.3.9, obtemos:

$$\Big(T_{s_j}(\mathbf{P}_j)\Big) = -s_j P_j + s_j Q_\infty.$$

Consequentemente, segue que, para todo natural t,

$$\begin{aligned}\left(\frac{1}{T_{s_j}(\mathbf{P}_j)}\right)^t \mathcal{L}(D) &= \mathcal{L}\Big(D + t(T_{s_j}(\mathbf{P}_j))\Big) \\ &= \mathcal{L}(D - ts_j P_j + ts_j Q_\infty) \\ &=: \mathcal{L}(D'),\end{aligned}$$

em que

$$D' := (r - ts_j)Q_\infty + \sum_{i=1,\, i\neq j}^{n-1} a_i P_i + (a_j + ts_j)P_j.$$

Em particular, tomemos $t \in \mathbb{N}$ suficientemente grande de modo que $a_j + ts_j \geq 0$. Nesse caso, temos então:

$$\sum_{i=1,\, i\neq j}^{n-1} a_i P_i + (a_j + ts_j)P_j = \sum_{i=1}^{n-1} a_i P_i,$$

com $a_i \geq 0$ para todo $i = 1, \ldots, n-1$ na escrita de D'.

Notemos que, pela relação estabelecida entre $\mathcal{L}(D)$ e $\mathcal{L}(D')$ e como D' tem grau zero tal como D, segue, utilizando a Proposição 2.3.50, que D é um divisor principal se, e somente se, D' é principal.

Logo, a suposição de que $a_i \geq 0$ na escrita de D pode ser, de fato, assumida.

Dessa forma, podemos escrever:

$$D = rQ_\infty + Q_1 + Q_2 + \cdots + Q_k,$$

em que $k = -r$ e repetições de Q_i's são permitidas, ou seja, é possível que $Q_i = Q_j$ para $i \neq j$ com $i, j = 1, \ldots, k$.

Definimos:

$$S_i := Q_{k-i} + Q_{k-i+1} + \cdots + Q_k. \qquad \text{e} \qquad \mathbf{T_i} := \mathbf{Q}_{k-i} + \mathbf{Q}_{k-i+1} + \cdots + \mathbf{Q}_k.$$

E, conforme convencionado previamente, denotaremos T_i como sendo o lugar racional associado ao ponto $\mathbf{T}_i$.

Façamos ainda:

$$f := F(\mathbf{Q}_{k-1}, \mathbf{Q}_k)F(\mathbf{Q}_{k-2}, \mathbf{T}_1)F(\mathbf{Q}_{k-3}, \mathbf{T}_2)\cdots F(\mathbf{Q}_1, \mathbf{T}_{k-2}).$$

Afirmamos que

$$\frac{1}{f}\mathcal{L}(D) = \mathcal{L}(-Q_\infty + T_{k-1}).$$

De fato, calculando o divisor de f obtemos:

$$\begin{aligned}&(-Q_{k-1} - Q_k + T_1 + Q_\infty) + (-Q_{k-2} - T_1 + T_2 + Q_\infty) + \cdots + (-Q_1 - T_{k-2} + T_{n-1} + Q_\infty)\\ &= -(Q_1 + Q_2 + \cdots + Q_k) + T_{k-1} + (k-1)Q_\infty.\end{aligned}$$

Assim, segue que:

$$D - \left(\frac{1}{f}\right) = D + (f) = T_{k-1} + (r + k - 1)Q_\infty = -Q_\infty + T_{k-1},$$

como queríamos.

Utilizando essa afirmação, temos que D é um divisor principal se, e somente se, $-Q_\infty + T_{k-1}$ é principal. Por outro lado, como tais divisores possuem grau zero, $-Q_\infty + T_{k-1}$

é principal se, e somente se, $T_{k-1} = Q_\infty$, ou seja, se, e somente se, $\mathbf{Q}_1 + \cdots + \mathbf{Q}_k = \mathbf{Q}_\infty$. Pela definição de D como enunciado, temos então que D é principal se, e somente se, a igualdade em (5.8) se verifica.

Consideremos agora que D é principal. Então, $\mathcal{L}(-Q_\infty + T_{k-1}) = \mathcal{L}(0) = \mathbb{F}_q$ e, consequentemente, $\mathcal{L}(D) = span_K\{f\}$. Logo, $D = (f)$.

Para as últimas afirmações, observemos primeiramente que toda função do tipo $F(\mathbf{P}, \mathbf{Q})$, com $P, Q \in \mathcal{P}$, é não nula e tem suporte em $\mathcal{P}$, donde $F(\mathbf{P}, \mathbf{Q}) \in \mathcal{O}^*_{\mathcal{P}}$. Por outro lado, o grupo $\mathcal{O}^*_{\mathcal{P}}$ pode ser visto como:

$$\mathcal{O}^*_{\mathcal{P}} = \bigcup \mathcal{L}(D) \setminus \{0\},$$

em que D percorre todos os divisores principais com suporte em $\mathcal{P}$.

Com efeito, temos que $z \in \mathcal{L}(z^{-1})$ para todo $z \in \mathcal{O}^*_{\mathcal{P}}$ fixado; para a recíproca, utilizamos que todo lugar de $K(E)/\mathbb{F}_q$ é racional.

Dessa forma, usando que $\mathcal{L}(D) = span_K\{f\}$ e a igualdade acima, concluímos que $\mathcal{O}^*_{\mathcal{P}}$ é igual ao span do produto de todas as funções da forma $F(\mathbf{P}, \mathbf{Q})$ em que $P, Q \in \mathcal{P}$. Como consequência, resulta que $\mathcal{O}^*_{\mathcal{P}}$ é gerado por funções $F(\mathbf{P}, \mathbf{Q})$ em que $P, Q \in \mathcal{P}$, como queríamos.

Por fim, sabemos pelo Corolário 4.1.15, que o reticulado $L_{\mathcal{P}}$ é isomorfo a $Princ(\mathcal{P})$, ou seja, é isomorfo ao grupo de divisores das funções pertencentes a $\mathcal{O}^*_{\mathcal{P}}$. Como $\mathcal{O}^*_{\mathcal{P}}$ é grupo, sabemos ainda que o mesmo contém funções da forma $F(\mathbf{P}, \mathbf{Q})^{-1}$, sendo $P, Q \in \mathcal{P}$, cujo divisor é dado por $P + Q - R - Q_\infty$ com $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. Tais argumentos garantem a prova de que $L_{\mathcal{P}}$ é gerado por vetores da forma $P + Q - R - Q_\infty$, em que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. □

Observação 5.3.11. Destacamos que a condição $\mathbf{P} + \mathbf{Q} = \mathbf{R}$ para os vetores geradores de $L_{\mathcal{P}}$ é crucial, tanto para a definição da função $F(\mathbf{P}, \mathbf{Q})$ quanto para a garantia de que $\mathcal{L}(P + Q - R - Q_\infty) \neq \{0\}$ e sua caracterização como $span_K\{F(\mathbf{P}, \mathbf{Q})\}$ (Proposição 5.3.8).

5.4 PROPRIEDADES DO RETICULADO

Nesta seção demonstraremos os principais resultados que almejamos. Para tanto, descreveremos os vetores minimais de $L_{\mathcal{P}}$, conforme o número de lugares racionais e sua respectiva distância mínima. A seguir, demonstraremos que, sob a condição de que E possua no mínimo 5 lugares racionais, $L_{\mathcal{P}}$ é gerado por seus vetores minimais sendo, portanto, um reticulado bem arredondado.

O Teorema 4.1.10 nos fornece um limite superior para a distância mínima do reticulado $L_{\mathcal{P}}$ considerando um corpo de funções arbitrário da forma $F/\mathbb{F}_q$. No entanto, ao considerarmos o corpo de funções elípticas, podemos efetuar tal cálculo. Mais precisamente, somos capazes de exibir os vetores minimais para tal reticulado, como mostra o próximo teorema.

Teorema 5.4.1 (**Distância Mínima de** $L_{\mathcal{P}}$)**.** *Consideremos que o número de pontos (resp. lugares) racionais n é tal que* $n \geq 4$*. Então, a distância mínima do reticulado* $L_{\mathcal{P}}$ *é igual a* 2 *e os vetores minimais de* $L_{\mathcal{P}}$ *são da forma* $P + Q + R - S$*, em que* $P, Q, R, S \in \mathcal{P}$ *são distintos e* $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.

Por outro lado, se $n = 3$*, então a distância mínima de* $L_{\mathcal{P}}$ *é igual a* $\sqrt{6}$ *e os vetores minimais são da forma* $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q_\infty)$ *e* $\pm(-2P + Q + Q_\infty)$*, em que* $\mathcal{P} = \{P, Q, Q_\infty\}$.

Demonstração. Sabemos pelo Teorema 4.1.10 que a distância mínima de $L_{\mathcal{P}}$ satisfaz:

$$d(L_{\mathcal{P}}) \geq \min\left\{ \sqrt{2 \deg f} : \ f \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q \right\}.$$

Como $P - Q$ é principal se, e somente se, $P = Q$, temos que $\deg f \neq 1$ para qualquer $f \in K(E)$. De fato, suponhamos, por absurdo, que exista $f \in K(E)$ tal que $\deg f = 1$. Nessas condições, utilizando a Definição 4.1.4, temos:

$$\frac{1}{2} \sum_{i=0}^{n-1} |v_i(f)| = 1 \text{ , i.e., } \sum_{i=0}^{n-1} |v_i(f)| = 2.$$

No entanto, caso isso ocorresse, aplicando o argumento estabelecido na Proposição 4.1.14, teríamos $(v_0(f), \ldots, v_{n-1}(f))$ sendo isomorfo a um divisor da forma $P + Q$ (ou, de modo semelhante, a $-P - Q$). Mas, utilizando a estrutura de grupo existente em $\mathcal{P}$, tal soma corresponde a um único lugar racional, digamos $R \in \mathcal{P}$. Resulta, então, que $\sum |v_i(f)| = 1$, uma contradição.

Assim, como $\deg f \neq 1$ para todo $f \in K(E)$, concluímos que o valor mínimo de $\deg f$ quando $f \in \mathcal{O}_{\mathcal{P}}^* \setminus \mathbb{F}_q$ é maior ou igual a 2, donde $d(L_{\mathcal{P}}) \geq 2$.

Por outro lado, consideremos que $n \geq 4$. Neste caso, garantimos a existência de ao menos dois pontos distintos, digamos $\mathbf{P}$ e $\mathbf{Q}$, ambos distintos de $\mathbf{Q}_\infty$, tais que $\mathbf{P} \neq \mathbf{Q}'$. Consequentemente, temos que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$, em que $\mathbf{R} \neq \mathbf{Q}_\infty, \mathbf{P}, \mathbf{Q}$. Sabemos que o divisor de $F(\mathbf{P}, \mathbf{Q})$ é dado por $-P - Q + R + Q_\infty$. Desse modo,

$$\sqrt{\sum_{i=0}^{n-1} v_i(F(\mathbf{P}, \mathbf{Q}))^2} = 2.$$

Agora, utilizando a definição da distância mínima de $L_{\mathcal{P}}$, a qual é dada por:

$$d(L_{\mathcal{P}}) = \min\left\{ \sqrt{\sum_{i=0}^{n-1} v_i(f)^2} : f \in \mathcal{O}_{\mathcal{P}}^* \setminus \{0\} \right\},$$

concluímos que $d(L_{\mathcal{P}}) \leq 2$.

Dessas desigualdades, obtemos que, quando $n \geq 4$, a distância mínima de $L_{\mathcal{P}}$ é igual a $d(L_{\mathcal{P}}) = 2$.

Para a descrição dos vetores minimais de $L_{\mathcal{P}}$ neste mesmo caso, consideremos v um tal vetor. Pela definição de vetor minimal, sabemos que $\|v\| = d(L_{\mathcal{P}}) = 2$, sendo $v = (v_0(f), \ldots, v_{n-1}(f))$ para algum $f \in \mathcal{O}_{\mathcal{P}}^*$. Desse modo, v é da forma $P + Q - R - S$, em que P, Q, R, S são lugares racionais distintos. Resta mostrarmos que $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.

Notemos que, como $L_{\mathcal{P}} \cong Princ(\mathcal{P})$, então $P + Q - R - S$ é um divisor principal. Consideremos que $\mathbf{P} + \mathbf{Q} = \mathbf{R}_1$. Assim, segue pelo Teorema 5.3.10 que $P + Q - R_1 + Q_\infty$ também é um divisor principal. Dessa forma, o seguinte divisor também é principal:

$$(P + Q - R_1 - Q_\infty) - (P + Q - R - S) = R + S - R_1 - Q_\infty.$$

Como consequência, segue que $\mathcal{L}(R + S - R_1 - Q_\infty) \neq \{0\}$ e, pela Proposição 5.3.8, temos que $\mathbf{R} + \mathbf{S} = \mathbf{R}_1$ e, logo, $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$, concluindo a primeira parte do teorema.

Agora, consideremos o caso em que $n = 3$. Então, decorre da estrutura de grupo em curvas elípticas, que $\mathcal{P} = \{P, Q, Q_\infty\}$, sendo ainda $\mathbf{Q} = 2\mathbf{P}$.

Seja $a_1P + b_1Q + c_1Q_\infty$ um vetor do reticulado $L_{\mathcal{P}}$. Afirmamos que $a_2P + b_2Q + c_2Q_\infty$, em que $a_1 \equiv a_2 \mod 3$, $b_1 \equiv b_2 \mod 3$ e $c_2 = -a_2 - b_2$, pertence também a $L_{\mathcal{P}}$.

Para tanto, primeiramente, notemos que $3P = 3Q = 2P - Q = P - 2Q = Q_\infty$. Desse modo, aplicando o Teorema 5.3.10, obtemos que os seguintes vetores são principais: $L_{\mathcal{P}}$: $3P - 3Q_\infty$, $3Q - 3Q_\infty$, $2P - Q - Q_\infty$ e $P - 2Q + Q_\infty$. Como os mesmos possuem suporte contido em $\mathcal{P}$, segue que pertencem a $L_{\mathcal{P}}$.

Tomemos então a_2, b_2 e c_2 como descrito. Sabemos que $a_2 = 3a + a_1$, $b_2 = 3b + b_1$ e $c_2 = -a_2 - b_2$, em que $a, b \in \mathbb{Z}$, Assim, podemos escrever:

$$a_2P + b_2Q + c_2Q_\infty = a(3P - 3Q_\infty) + b(3Q - 3Q_\infty) + (a_1P + b_1Q + c_1Q_\infty) - (a_1 + b_1 + c_1)Q_\infty,$$

resultando que $a_2P + b_2Q + c_2Q_\infty \in \mathcal{P}$.

Por fim, como queremos obter os vetores minimais de $L_{\mathcal{P}}$, devemos tomar $a_2 = b_2 = 1$ e $c_2 = -2$. Portanto, utilizando a definição da distância mínima de $L_{\mathcal{P}}$, obtemos:

$$d(L_{\mathcal{P}}) = \|P + Q - 2Q_\infty\| = \sqrt{1 + 1 + (-2)^2} = \sqrt{6}.$$

Logo, os vetores minimais de $L_{\mathcal{P}}$ são da forma $\pm(P + Q - 2Q_\infty)$, $\pm(P - 2Q + Q_\infty)$ e $\pm(-2P + Q_\infty + Q_\infty)$. □

Finalmente, mostraremos que, quando $n \geq 5$, o reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais e, portanto, trata-se de um reticulado bem arredondado.

Teorema 5.4.2 (Reticulado Bem Arredondado). *Suponhamos que E possua, no mínimo, 5 pontos. Então, o reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais. Em particular, $L_{\mathcal{P}}$ é bem arredondado.*

Demonstração. Sabemos pela caracterização dos vetores geradores de $L_{\mathcal{P}}$ (Teorema 5.3.10) que os mesmos são vetores não nulos da forma $v := -P - Q + R + Q_\infty$ em que $\mathbf{P} + \mathbf{Q} = \mathbf{R}$. Devemos mostrar que cada vetor de tal forma se expressa em termos dos vetores minimais de $L_{\mathcal{P}}$.

Podemos supor que v não é um vetor minimal de $L_{\mathcal{P}}$ (caso contrário, o resultado segue diretamente), ou seja, podemos supor, utilizando o Teorema 5.4.1, que P, Q, R, Q_∞ não são todos distintos. Como v é um vetor não nulo, não podemos ter P ou Q sendo igual a Q_∞; de modo semelhante, não pode ocorrer $P = R$ ou $Q = R$. Dessa maneira, as únicas possibilidades são: $P = Q$ ou $R = Q_\infty$. Analisaremos cada uma delas.

Suponhamos que $P = Q$. Assim, temos $v = -2P + R + Q_\infty$, em que $2\mathbf{P} = \mathbf{R}$. Agora, como E possui no mínimo 5 pontos, podemos escolher um lugar racional U tal que $\mathbf{U}$ é diferente de $\mathbf{Q}_\infty$, $\mathbf{P}$, $-\mathbf{P}$ e $2\mathbf{P}$. Façamos $\mathbf{S} := \mathbf{P} + \mathbf{U}$. Notemos ainda que:

$$v = -2P + R + Q_\infty = (-P - U + S + Q_\infty) - (P + S - R - U).$$

Afirmamos que $-P - U + S + Q_\infty$ e $P + S - R - U$ são vetores minimais.

Com efeito, pela escolha feita, $U \neq P, Q_\infty$. Por outro lado, $U \neq S$ (visto que $\mathbf{P} \neq \mathbf{Q}_\infty$), $S \neq P$ (pois $\mathbf{U} \neq \mathbf{Q}_\infty$) e $S \neq Q_\infty$ (pois $\mathbf{U} \neq -\mathbf{P}$). Além disso, claramente temos $\mathbf{P} + \mathbf{U} = \mathbf{S} + \mathbf{Q}_\infty$. Assim, pelo Teorema 5.3.10 resulta que $-P - U + S + Q_\infty$ é um vetor minimal.

Para o segundo vetor, notemos primeiramente que $\mathbf{P} + \mathbf{S} = 2\mathbf{P} + \mathbf{U} = \mathbf{R} + \mathbf{U}$, garantindo que $P + S - R - U$ é um ponto do reticulado $L_{\mathcal{P}}$. Como P, S, U são todos distintos, resta-nos mostrar que nenhum deles pode ser igual a R. O fato $P \neq R$ já foi observado, então devemos mostrar que $S \neq R$ e $U \neq R$. Caso $S = R$, teríamos $\mathbf{P} + \mathbf{U} = \mathbf{R} = 2\mathbf{P}$, implicando que $\mathbf{P} = \mathbf{U}$, uma contradição. Caso $U = R$, teríamos $\mathbf{P} + \mathbf{U} = \mathbf{P} + 2\mathbf{P}$, donde $\mathbf{U} = 2\mathbf{P}$, uma contradição. Logo, $P + Q - R - U$ é, também, um vetor minimal.

Portanto, se $P = Q$, provamos que v é igual à diferença de dois vetores minimais.

Suponhamos agora que $R = Q_\infty$. Então, segue que $v = -P - Q + 2Q_\infty$, sendo $\mathbf{P} + \mathbf{Q} = \mathbf{Q}_\infty$. Utilizando que E possui pelo menos 5 pontos, é possível escolher um ponto racional $\mathbf{U}$ distinto de $\mathbf{Q}_\infty$, $\mathbf{P}$, $\mathbf{Q}$ e $2\mathbf{P}$. Façamos $\mathbf{S} := \mathbf{Q} + \mathbf{U}$. Podemos escrever:

$$v = -P - Q - 2Q_\infty = (Q + U - S - Q_\infty) + (P + S - U - Q_\infty).$$

De modo semelhante ao feito no caso anterior, afirmamos que ambos os vetores $Q + U - S - Q_\infty$ e $P + S - U - Q_\infty$ são vetores minimais de $L_{\mathcal{P}}$.

Primeiramente, notemos que ambos pertencem ao reticulado $L_{\mathcal{P}}$, uma vez que $\mathbf{Q} + \mathbf{U} = \mathbf{S} + \mathbf{Q}_\infty$ e $\mathbf{P} + \mathbf{S} = \mathbf{P} + \mathbf{Q} + \mathbf{U} = \mathbf{U}$. Por outro lado, pela escolha de U, sabemos que $\mathbf{U} \neq \mathbf{Q}, \mathbf{Q}_\infty$, donde $S \neq Q$; ainda, $U \neq S$, caso contrário, teríamos $\mathbf{Q} = \mathbf{Q}_\infty$, e $S \neq Q_\infty$, caso contrário, teríamos $\mathbf{U} = -\mathbf{Q} = \mathbf{P}$. Assim, $Q + U - S - Q_\infty$ é um vetor minimal de $L_{\mathcal{P}}$.

Para o vetor $P + S - U - Q_\infty$, como já mostramos que S, U, Q_∞ são distintos e como $\mathbf{P} \neq \mathbf{U}, \mathbf{Q}_\infty$, basta mostrarmos que $P \neq S$. Se $P = S$, teríamos que $\mathbf{U} = \mathbf{P} + \mathbf{S} = 2\mathbf{P}$, uma contradição. Então, segue que $P + S - U - Q_\infty$ também é um vetor minimal de $L_{\mathcal{P}}$.

Portanto, no caso em que $R = Q_\infty$, concluímos que v é igual à soma de dois vetores minimais.

Consequentemente, $L_{\mathcal{P}}$ é gerado por seus vetores minimais. E, utilizando que todo reticulado gerado por seus vetores minimais é bem arredondado (resultado decorrente das definições), concluímos a demonstração do teorema. □

5.5 NÚMERO DE VIZINHOS E RAIO DE COBERTURA

Nesta última seção, calcularemos o número de vetores minimais em $L_{\mathcal{P}}$ (*kissing number* ou número de vizinhos) e estimaremos seu raio de cobertura.

Para tanto, notemos que a Proposição 5.4.1 exibe todos os vetores minimais de $L_{\mathcal{P}}$ no caso em que $n = 3$, os quais totalizam 6 vetores. Tal resultado nos motiva a obter o número de vetores minimais de $L_{\mathcal{P}}$ no caso geral, ou seja, quando $n \geq 4$. Para esse cálculo, o qual nos fornece exatamente o *kissing number* de $L_{\mathcal{P}}$, necessitaremos de um conceito específico relativo a curvas elípticas: os *pontos de torsão* de E.

Definição 5.5.1. *Dado um inteiro $m \geq 1$, dizemos que $\mathbf{P}$ é um m-**ponto de torsão** da curva elíptica E se a ordem de $\mathbf{P}$ em E é igual a m, ou seja, se*

$$m\mathbf{P} = \underbrace{\mathbf{P} + \cdots + \mathbf{P}}_{m \text{ termos}} = \mathbf{Q}_\infty.$$

*Nessas circunstâncias, definimos ainda o m-**subgrupo de torsão**, denotado por $E[m]$, como o conjunto de pontos de E de ordem m:*

$$E[m] := \left\{\mathbf{P} \in E : \ m\mathbf{P} = \mathbf{Q}_\infty\right\}.$$

*O **subgrupo de torsão** de E, denotado por E_{tors}, é o conjunto de pontos de ordem finita:*

$$E_{tors} := \bigcup_{m=1}^{\infty} E[m].$$

Teorema 5.5.2 (Número de Vetores Minimais de $L_{\mathcal{P}}$). *Consideremos que $n \geq 4$ e seja ϵ o número de 2-pontos de torsão de E. Então, o número de vetores minimais de $L_{\mathcal{P}}$ é igual a:*

$$\frac{n}{\epsilon} \cdot \frac{(n-\epsilon)(n-\epsilon-2)}{4} + \left(n - \frac{n}{\epsilon}\right) \cdot \frac{n(n-2)}{4}. \tag{5.9}$$

Demonstração. Consideremos o homomorfismo:

$$\begin{aligned} \tau_E : E &\to E \\ \mathbf{P} &\mapsto \tau_E(\mathbf{P}) := 2\mathbf{P} \end{aligned}$$

Notemos que o núcleo de τ_E é igual ao conjunto de 2-pontos de torsão de E, ou seja, corresponde ao conjunto $E[2]$. Assim, pelo Teorema dos Isomorfismos, obtemos:

$$\mathrm{Im}(\tau_E) \cong \frac{E}{E[2]},$$

donde resulta

$$|\mathrm{Im}(\tau_E)| = \frac{n}{\epsilon} \text{ em que } \epsilon := \left|E[2]\right|.$$

Utilizando a caracterização dos vetores minimais apresentada na Proposição 5.4.1, queremos obter o número de soluções $\{\mathbf{P}, \mathbf{Q}, \mathbf{R}, \mathbf{S}\}$, todos distintos, para a igualdade $\mathbf{P} + \mathbf{Q} = \mathbf{R} + \mathbf{S}$.

Para tanto, fixemos um ponto racional $\mathbf{A}$ em E. Primeiramente, calcularemos o número de soluções para a equação $\mathbf{P}+\mathbf{Q} = \mathbf{A}$, em que $\mathbf{P}, \mathbf{Q}$ são pontos de E. Observemos que $\mathbf{P} = \mathbf{Q}$ se, e somente se, $\mathbf{A} \in \mathrm{Im}(\tau_E)$.

Caso $\mathbf{A} \in \mathrm{Im}(\tau_E)$, temos que existem ϵ soluções $\mathbf{P} \in E$ para a equação $2\mathbf{P} = \mathbf{A}$. Consequentemente, existem $(n - \epsilon)$ pontos $\mathbf{P}$ satisfazendo $\mathbf{Q} := \mathbf{A} - \mathbf{P} \neq \mathbf{P}$ e, então, $(n - \epsilon)/2$ pares $\{\mathbf{P}, \mathbf{Q}\}$ tais que $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ e $\mathbf{P} \neq \mathbf{Q}$. Nessas condições, o número de pares $\{\mathbf{R}, \mathbf{S}\}$ distintos de $\{\mathbf{P}, \mathbf{Q}\}$ e tais que $\mathbf{R} + \mathbf{S} = \mathbf{A}$ corresponde a $(n - \epsilon - 2)/2$. Assim, segue que existem:

$$\frac{(n - \epsilon)(n - \epsilon - 2)}{4}$$

possibilidades para $P + Q - R - S$ satisfazendo $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$, sendo todos os pontos distintos. Mais ainda, como a imagem de τ_E tem cardinalidade n/ϵ, o número de vetores minimais $P + Q - R - S$ tais que $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$ com $\mathbf{A} \in Im(\tau_E)$ é dado por:

$$\frac{n}{\epsilon} \cdot \frac{(n - \epsilon)(n - \epsilon - 2)}{4}.$$

Consideremos agora o caso em que $\mathbf{A} \notin \mathrm{Im}(\tau_E)$. Então, não existe $\mathbf{P} \in E$ tal que $2\mathbf{P} = \mathbf{A}$. Resulta que existem n pontos $\mathbf{P}$ que satisfazem $\mathbf{Q} := \mathbf{A} - \mathbf{P} \neq \mathbf{P}$. Desse modo, obtemos $n/2$ pares $\{\mathbf{P}, \mathbf{Q}\}$ tais que $\mathbf{P} + \mathbf{Q} = \mathbf{A}$ e $\mathbf{P} \neq \mathbf{Q}$. Assim, há $(n - 2)/2$ pares $\{\mathbf{R}, \mathbf{S}\}$ distintos de $\{\mathbf{P}, \mathbf{Q}\}$ com $\mathbf{R} + \mathbf{S} = \mathbf{A}$. Logo, o número de vetores minimais $P + Q - R - S$ tais que $\mathbf{P} + \mathbf{Q} = \mathbf{A} = \mathbf{R} + \mathbf{S}$ com $\mathbf{A} \notin \mathrm{Im}(\tau_E)$ é dado por:

$$\left(n - \frac{n}{\epsilon}\right) \cdot \frac{n(n - 2)}{4}.$$

Portanto, o número de vetores minimais de $L_{\mathcal{P}}$ é dado por (5.9). □

Por fim, apresentaremos uma estimativa para o raio de cobertura de $L_{\mathcal{P}}$ com relação à métrica euclidiana. Relembramos que tal raio de cobertura de $L_{\mathcal{P}}$ é dado por:

$$\gamma(L_{\mathcal{P}}) = \inf\left\{r \in \mathbb{R}_+ : \ B_V[0,r] + L_{\mathcal{P}} = V\right\},$$

em que $V = span(L_{\mathcal{P}})$ e $B_V[0,r]$ é a bola fechada de raio r centrada na origem de V sob a métrica euclidiana.

Teorema 5.5.3 (**Raio de Cobertura de** $L_{\mathcal{P}}$)**.** *O raio de cobertura de $L_{\mathcal{P}}$ satisfaz a desigualdade:*

$$\gamma(L_{\mathcal{P}}) \leq \frac{1}{2}\left(\sqrt{n^2+4n+8} + \sqrt{n}\right).$$

Em outras palavras, se $V = span(\mathcal{A}_{n-1}) = span(L_{\mathcal{P}}) \subset \mathbb{R}^n$ e $v \in V$, então existe um ponto no reticulado $L_{\mathcal{P}}$ com distância a v dada por:

$$\frac{1}{2}\left(\sqrt{n^2+4n+8} + \sqrt{n}\right).$$

Além disso, se $v \in \mathcal{A}_{n-1}$, existe um ponto em $L_{\mathcal{P}}$ com distância a v dada por $\sqrt{2}$.

Demonstração. Façamos $V = span(\mathcal{A}_{n-1}) = span(L_{\mathcal{P}})$, como enunciado (destacamos que a última igualdade decorre do fato de $L_{\mathcal{P}}$ ser um sub-reticulado de $\mathcal{A}_{n-1}$ com mesmo posto que esse). Seja $v = (v_0, \ldots, v_{n-1}) \in V$; então, $v_0 + \cdots + v_{n-1} = 0$. Consideremos ainda $w_1 := (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$, em que a_i é o inteiro mais próximo a v_i (no caso em que v_i é exatamente a metade de um inteiro, consideramos a_i o inteiro abaixo de v_i).

Nessas condições, sabemos que $a_0\mathbf{P}_0 + a_1\mathbf{P}_1 + \cdots + a_{n-1}\mathbf{P}_{n-1}$ é igual a um ponto $\mathbf{P}_j$ para algum j com $0 \leq j \leq n-1$.

Primeiramente, suponhamos que $j \neq 0$. Seja $A_0 := -a_1 - a_2 - \cdots - a_{n-1} - 1$. Observemos que, pelo Teorema 5.3.10, temos que

$$w_2 := (A_0, a_1, \ldots, a_{j-1}, a_j - 1, a_{j+1}, \ldots, a_{n-1})$$

é um ponto do reticulado $L_{\mathcal{P}}$.

Com efeito, utilizando as definições acima, w_2 é isomorfo ao divisor:

$$\begin{aligned} w_2 &\cong A_0P_0 + a_1P_1 + \cdots + a_{j-1}P_{j-1} + a_jP_j - P_j + a_{j+1}P_{j+1} + \cdots + a_{n-1}P_{n-1} \\ &= A_0P_0 - a_0P_0 = (-a_0 - a_1 - \cdots - a_{n-1} - 1)P_0. \end{aligned}$$

Agora, calculando a distância entre w_2 e v, obtemos:

$$\begin{aligned} \|v - w_2\| &\leq \|v - w_1\| + \|w_1 - w_2\| \\ &\leq \sqrt{\left(\frac{a_0^2 + \cdots + a_{n-1}^2}{4}\right)} + \sqrt{(A_0 - a_0)^2 + 1} \\ &\leq \sqrt{\frac{n}{4}} + \sqrt{(a_0 + a_1 + \cdots + a_{n-1} - 1)^2 + 1} \\ &\leq \frac{\sqrt{n}}{2} + \sqrt{S^2 - 2S + 2}, \end{aligned}$$

em que $S = a_0 + a_1 + \cdots + a_{n-1}$.

Por outro lado,

$$\begin{aligned} |S| &= |a_0 + a_1 + \cdots + a_{n-1}| = |(a_0 - v_0) + \cdots (a_{n-1} - v_{n-1}| \\ &\leq |a_0 - v_0| + \cdots + |a_{n-1} - v_{n-1}| \\ &\leq \frac{n}{2}. \end{aligned}$$

E, assim, resulta:

$$\|v - w_2\| \leq \frac{\sqrt{n}}{2} + \sqrt{\frac{n^2}{4} + 2\left(\frac{n}{2}\right) + 2} = \frac{1}{2}\left(\sqrt{n} + \sqrt{n^2 + 4n + 8}\right).$$

Suponhamos que $j = 0$. Definimos

$$A_0 := -a_1 - a_2 - \cdots - a_{n-1}$$

e

$$w_2 := (A_0, a_1, \ldots, a_{n-1}).$$

Temos:

$$\begin{aligned} \|v - w_2\| &\leq \|v - w_1\| + \|w_1 - w_2\| \\ &\leq \sqrt{\frac{n}{4}} + \sqrt{(A_0 - a_0)^2} \\ &\leq \frac{\sqrt{n}}{2} + |S| \\ &\leq \frac{\sqrt{n}}{2} + \frac{n}{2}. \end{aligned}$$

Então, conseguimos uma limitação menor do que a enunciada, concluindo a primeira parte da demonstração.

Para a última afirmação, basta notarmos que, se $v \in \mathcal{A}_{n-1}$, então, $S = 0$ e $v = w_1$. Logo, segue da limitação estabelecida que $\|v - w_2\| \leq \sqrt{2}$, como queríamos. □

6 RETICULADOS VIA CORPO DE FUNÇÕES HERMITIANO

Este capítulo se dedica ao estudo dos reticulados da forma $L_{\mathcal{P}}$ obtidos a partir do corpo de funções Hermitiano. Primeiramente, estabeleceremos algumas propriedades básicas do corpo de funções Hermitiano e, a seguir, descreveremos as principais características do reticulado $L_{\mathcal{P}}$, demonstrando, por fim, que se trata de um reticulado gerado por seus vetores minimais e, consequentemente, bem arredondado. Como última seção, apresentaremos uma estimativa do *kissing number* do reticulado obtido.

Para esta abordagem, utilizaremos principalmente as referências [4] e [28].

6.1 CORPO DE FUNÇÕES HERMITIANO

Definição 6.1.1. *Seja q uma potência de um número primo. Definimos o* ***corpo de funções Hermitiano*** *como $H := \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$, onde x, y satisfazem*

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

Observação 6.1.2. Ressaltamos que o corpo de funções Hermitiano é o corpo de funções associado à curva $y^q + y = x^{q+1}$ sobre $\mathbb{F}_{q^2}$, conhecida como *curva hermitiana*.

Com o intuito de obter as principais propriedades de tal corpo de funções, utilizaremos a noção de *extensão de Kummer*.

Definição 6.1.3. *Seja $n \in \mathbb{N}$. Dizemos que ζ_n é uma* ***n-ésima raiz da unidade*** *se $\zeta^n = 1$. No caso em que $\zeta_n^m \neq 1$ para todo $m \in \{1, \ldots, n-1\}$, dizemos ainda que ζ_n é uma* ***n-ésima raiz primitiva da unidade****.*

Definição 6.1.4. *Seja $n > 1$, Sejam F/K um corpo de funções tal que K contém uma n-ésima raiz primitiva da unidade com $mdc(n, char(K)) = 1$. Consideremos $u \in F$ tal que:*

$$u \neq w^d \text{ para todo } w \in F \text{ e } d \mid n, d > 1\,.$$

Se F' é tal que $F' = F(y)$ com $y^n = u$, dizemos que F'/F é uma ***extensão de Kummer*** *sobre F.*

Observação 6.1.5. O corpo de funções H pode ser visto como uma extensão de Kummer sobre $\mathbb{F}_{q^2}(y)$. Com efeito, observemos que $H = \mathbb{F}_{q^2}(y)(x)$ e façamos $x^{q+1} =: u$. Pela definição de H, temos ainda que $x^{q+1} = y^q + y = u \in \mathbb{F}_{q^2}(y)$. Assim, basta notarmos que, para todo $w \in \mathbb{F}_{q^2}(y)$ e todo divisor $d > 1$ de $q+1$, vale

$$u = y^q + y \neq w^d.$$

Ressaltamos que a existência de uma $(q+1)$-ésima raiz primitiva da unidade decorre do fato de que $\mathbb{F}_{q^2}$ é algebricamente fechado. Em particular, temos que o polinômio $p(x) = x^q + x^{q-1} + \cdots + x + 1$ possui ao menos uma raiz em H, digamos ζ. Logo, segue que $\zeta \neq 1$ é tal que $\zeta^{q+1} = 1$ e $\zeta^m \neq 1$ sempre que $m \in \{1, \ldots, q\}$.

Utilizando o fato de que o corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$ é uma extensão de Kummer sobre $\mathbb{F}_{q^2}(y)$, podemos obter todos os lugares racionais de tal corpo de funções, além de caracterizar seu gênero e seu corpo de constantes. Para a obtenção das propriedades de uma extensão de Kummer arbitrária, sugerimos consultar [28] (Proposição 3.7.10).

A seguir, destacamos as principais características do corpo de funções Hermitiano, cujas demonstrações são apresentadas na Proposição 6.4.1 e no Exemplo 6.4.2 de [28].

Teorema 6.1.6. *As seguintes afirmações se verificam no corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$:*

(**1**) *O corpo $\mathbb{F}_{q^2}$ é corpo completo de constantes de H.*

(**2**) *O gênero de H é dado por:*

$$g = \frac{q(q-1)}{2}.$$

(**3**) *O corpo de funções H possui $N = q^3 + 1$ lugares racionais, obtidos da seguinte forma:*

- *O polo comum Q_∞ de x e y;*
- *E, para cada $\alpha \in \mathbb{F}_{q^2}$, existem q elementos $\beta \in \mathbb{F}_{q^2}$ tais que $\beta^q + \beta = \alpha^{q+1}$ e para cada par (α, β), existe um único lugar racional $P_{\alpha,\beta}$ de H com $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.*

(**4**) *$H/\mathbb{F}_{q^2}$ é um corpo de funções maximal.*

Observação 6.1.7. Cabe destacar que, como $\mathbb{F}_{q^2}$ é corpo completo de constantes de H, pelo Corolário 2.3.30, temos que todos os lugares de $H/\mathbb{F}_{q^2}$ são necessariamente racionais e, consequentemente, caracterizados como no item (**3**) do Teorema 6.1.6.

Observação 6.1.8. No caso em que $q = 2$, pelo Teorema 6.1.6, o gênero do corpo de funções Hermitiano é igual a 1. Além disso, neste caso, a equação da curva hermitiana é dada por $y^2 + y = x^3$. Por um cálculo direto, podemos notar que tal curva não admite pontos cujas derivadas parciais são todas nulas, isto é, é não singular. Consequentemente, nesse caso, o corpo de funções Hermitiano é também um corpo de funções elípticas.

Encerramos esta seção apresentando propriedades específicas das aplicações norma e traço ao considerarmos o corpo de funções Hermitiano. Lembramos que as aplicações norma e traço de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$, denotadas por N e T respectivamente, são dadas por:

$$\begin{array}{rcl} N : \mathbb{F}_{q^2} & \to & \mathbb{F}_q \\ z & \mapsto & z^{q+1} \end{array} \quad \text{e} \quad \begin{array}{rcl} T : \mathbb{F}_{q^2} & \to & \mathbb{F}_q \\ z & \mapsto & z + z^q \end{array} \tag{6.1}$$

Assim, podemos ver o corpo de funções Hermitiano como $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ tal que $T(y) = N(x)$.

Proposição 6.1.9. *A aplicação N restrita a $\mathbb{F}_{q^2}^*$, ou seja, a aplicação N de $\mathbb{F}_{q^2}^*$ em $\mathbb{F}_q^*$ é sobrejetora.*

Demonstração. Sabemos que o núcleo de N se constitui dos elementos $z \in \mathbb{F}_{q^2}^*$ tais que $z^{q+1} = 1$. Assim, temos que $|\ker(N)| \leq q+1$ e, consequentemente, pelo Teorema dos Isomorfismos, segue:

$$|\mathrm{Im}(N)| = \frac{\left|\mathbb{F}_{q^2}^*\right|}{|\ker(N)|} = \frac{q^2-1}{|\ker(N)|} \geq \frac{q^2-1}{q+1} = q-1.$$

Como $\mathrm{Im}(N) \subseteq \mathbb{F}_q^*$ e $\left|\mathbb{F}_q^*\right| = q-1$, concluímos que $\mathrm{Im}(N) = \mathbb{F}_q^*$, ou seja, a restrição de N considerada é sobrejetora. □

Ressaltamos que essas aplicações podem ser estendidas à qualquer corpo $\mathbb{F}_{q^m}$, sendo $m \in \mathbb{N}$ (consultar Seção §2.3 de [18]). Além disso, pode-se demonstrar que a aplicação norma torna-se sobrejetora ao considerarmos sua restrição a $F_{q^m}^*$.

6.2 RESULTADOS PRELIMINARES

Nesta seção, estudaremos as principais propriedades das retas no corpo de funções Hermitiano com o objetivo de, posteriormente, obter os vetores geradores de $L_{\mathcal{P}}$. Nessas condições, lembramos que uma reta em $H = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ é uma função da forma $ax + by + c$, em que $a, b, c \in \mathbb{F}_{q^2}$ e a, b não são ambos nulos.

Antes de estudarmos retas arbitrárias em H, analisaremos especificamente as retas tangentes à curva hermitiana em um ponto fixado. Para tanto, motivados pela caracterização apresentada aos lugares racionais de H, definimos o conjunto:

$$\mathcal{K} := \left\{(\alpha,\beta) \in \mathbb{F}_{q^2}^2 : \ \beta^q + \beta = \alpha^{q+1}\right\}.$$

Dessa forma, temos que $\mathcal{P}$ se constitui do polo infinito Q_∞ e de lugares da forma $P_{\alpha,\beta}$ em que $(\alpha,\beta) \in \mathcal{K}$.

Para cada par $(\alpha,\beta) \in \mathcal{K}$, definimos ainda:

$$\tau_{\alpha,\beta} := y - \beta - \alpha^q(x-\alpha). \tag{6.2}$$

Proposição 6.2.1. *A função $\tau_{\alpha,\beta}$ definida como acima satisfaz:*

$$\tau_{\alpha,\beta} = y - \alpha^q x + \beta^q \qquad e \qquad \tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} = (x-\alpha)^{q+1}.$$

Da primeira igualdade, segue que $\tau_{\alpha,\beta} = 0$ corresponde à reta tangente à curva Hermitiana no ponto (α,β).

Demonstração. De fato, utilizando a definição do conjunto $\mathcal{K}$, temos:

$$\tau_{\alpha,\beta} = y - \alpha^q x - (\alpha^{q+1} - \beta) = y - \alpha^q x + \beta^q.$$

Por outro lado, utilizando que $y^q + y = x^{q+1}$ e que q é um múltiplo da característica de $\mathbb{F}_{q^2}$, temos:

$$\begin{aligned}
\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} &= (y - \alpha^q x + \beta^q)^q + (y - \alpha^q x + \beta^q) \\
&= (y^q + y) + (\beta^{q^2} + \beta^q) - \alpha^{q^2} x^q - \alpha^q x \\
&= x^{q+1} + (\beta^q + \beta) - \alpha x^q - \alpha^q x \\
&= x^{q+1} - \alpha x^q - \alpha^q x + \alpha^{q+1} \\
&= (x - \alpha)^{q+1}.
\end{aligned}$$

Por fim, lembramos que, dada uma curva com equação $f := f(x, y) = 0$, sua reta tangente no ponto (x_0, y_0) é dada por:

$$\frac{\partial f(x_0, y_0)}{\partial x}(x - x_0) + \frac{\partial f(x_0, y_0)}{\partial y}(y - y_0) = 0.$$

Assim, utilizando a curva hermitiana, cuja equação pode ser escrita como $y^q + y - x^{q+1} = 0$, sua reta tangente em (α, β) corresponde a:

$$\begin{aligned}
-(q+1)\alpha^q(x - \alpha) + (q\beta^{q-1} + 1)(y - \beta) &= 0 \\
-\alpha^q(x - \alpha) + y - \beta &= 0,
\end{aligned}$$

ou seja, tal reta tangente é dada exatamente pela equação $\tau_{\alpha,\beta} = 0$. □

Por meio de tal resultado, somos capazes de calcular o divisor da reta $\tau_{\alpha,\beta} = 0$.

Proposição 6.2.2. *Fixemos $(\alpha, \beta) \in \mathcal{K}$. O divisor da reta $\tau_{\alpha,\beta} = 0$ é dado por:*

$$(\tau_{\alpha,\beta}) = (q+1)P_{\alpha,\beta} - (q+1)Q_\infty.$$

Demonstração. Seja S um lugar racional em H diferente do lugar infinito Q_∞. Pela Proposição 6.2.1, temos que:

$$v_S\left(\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta}\right) = (q+1) \cdot v_S(x - \alpha).$$

Por outro lado,

$$\begin{aligned}
v_S\left(\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta}\right) &= \min\left\{v_S(\tau_{\alpha,\beta}^q), v_S(\tau_{\alpha,\beta})\right\} \\
&= \min\left\{q \cdot v_S(\tau_{\alpha,\beta}), v_S(\tau_{\alpha,\beta})\right\}.
\end{aligned}$$

Como Q_∞ é o único polo de H, segue que $v_S(\tau_{\alpha,\beta}) > 0$ para todo lugar $S \in \mathcal{P} \setminus Q_\infty$, donde resulta:

$$(q+1) \cdot v_S(x-\alpha) = v_S(\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta}) = v_S(\tau_{\alpha,\beta}).$$

Agora, se S corresponde exatamente ao lugar $P_{\alpha,\beta}$, associado ao ponto (α,β) fixado, temos $v_{P_{\alpha,\beta}}(x-\alpha) = 1$ e, assim, $v_{P_{\alpha,\beta}}(\tau_{\alpha,\beta}) = q+1$.

Caso contrário, ou seja, caso S corresponda a um lugar $P_{\alpha',\beta'} \in \mathcal{P}$ sendo $(\alpha',\beta') \neq (\alpha,\beta)$, segue que $v_S(x-\alpha) = 0$, donde $v_S(\tau_{\alpha,\beta}) = 0$.

Por fim, para a análise do lugar infinito Q_∞, lembramos que o grau do divisor $(\tau_{\alpha,\beta})$ é igual a zero, visto tratar-se de um divisor principal. Dessa forma:

$$\deg(\tau_{\alpha,\beta}) = \sum_{i=0}^{n-1} v_i(\tau_{\alpha,\beta}) = 0.$$

Pelo cálculo já feito para os lugares racionais, podemos reescrever essa igualdade como:

$$(q+1) + v_\infty(\tau_{\alpha,\beta}) = 0 \Rightarrow v_\infty(\tau_{\alpha,\beta}) = -(q+1).$$

Portanto, concluímos que:

$$(\tau_{\alpha,\beta}) = (q+1)P_{\alpha,\beta} - (q+1)Q_\infty.$$

□

Ao estudarmos retas tangentes da forma $\tau_{\alpha,\beta} = 0$, com $(\alpha,\beta) \in \mathcal{K}$, visamos caracterizar os vetores minimais do reticulado $L_{\mathcal{P}}$ sobre o corpo de funções Hermitiano. Mais precisamente, nosso intuito é mostrar que os vetores minimais de $L_{\mathcal{P}}$ se originam a partir de divisores da forma (f_1/f_2), em que f_1 e f_2 são retas distintas em H satisfazendo determinadas condições.

Tendo em vista tal propósito, primeiramente destacamos que H pode ser visto como uma extensão de Kummer sobre $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. Com efeito, pela definição de $\tau_{\alpha,\beta}$, juntamente à Proposição 6.2.1, temos:

$$H = \mathbb{F}_{q^2}(x,y) = \mathbb{F}_{q^2}(\tau_{\alpha,\beta}, x).$$

Nesse caso, a condição de ser especificamente uma extensão de Kummer segue da Observação 6.1.5.

Seguindo a notação estabelecida, denotaremos os lugares racionais finitos de $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ a partir de seus respectivos polinômios mônicos irredutíveis e, no caso do lugar infinito, representaremos por $P_\infty(\tau_{\alpha,\beta})$.

Considerando que H é uma extensão de Kummer sobre $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, podemos estabelecer as principais propriedades de seus lugares racionais, conforme indica o lema a seguir (veja [28], Proposição 6.4.1).

Lema 6.2.3. *Consideremos H como uma extensão de Kummer sobre $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$. Então, os lugares racionais de $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ satisfazem as seguintes condições:*

(**i**) *Para cada $\gamma \in \mathbb{F}_{q^2}$ tal que $\gamma^q + \gamma = 0$, o lugar $\tau_{\alpha,\beta} - \gamma$ é totalmente ramificado em H, ou seja, existe apenas um lugar que é extensão desse e o índice de ramificação é igual a $[H : \mathbb{F}_{q^2}(\tau_{\alpha,\beta})] = q + 1$.*

Caso tenhamos $\gamma^q + \gamma \neq 0$, o lugar $\tau_{\alpha,\beta} - \gamma$ se decompõe completamente em H, ou seja, existem $q + 1$ lugares que são extensões de $\tau_{\alpha,\beta} - \gamma$.

(**ii**) *O polo de $\tau_{\alpha,\beta}$ é totalmente ramificado.*

Observação 6.2.4. A demonstração anterior não utiliza nenhuma propriedade intrínseca à função $\tau_{\alpha,\beta}$. Com efeito, considerando H uma extensão de Kummer sobre $\mathbb{F}_{q^2}(y)$, obtemos resultados inteiramente análogos aos apresentados. Em outras palavras, as condições enunciadas permanecem válidas trocando-se $\tau_{\alpha,\beta}$ por y.

Por meio dessa análise, determinamos os divisores de todas as retas no corpo de funções Hermitiano e obtemos os pontos de $\mathcal{K}$ pertencentes a uma tal reta fixada, conforme é apresentado nas proposições seguintes.

Proposição 6.2.5. *Consideremos $H/\mathbb{F}_{q^2}$ o corpo de funções Hermitiano e seja $\gamma \in \mathbb{F}_{q^2}$. Então, são satisfeitas as seguintes propriedades:*

(**1**) *Se $\gamma^q + \gamma = 0$, o divisor de $\tau_{\alpha,\beta} - \gamma$ é dado por:*

$$(\tau_{\alpha,\beta} - \gamma) = (q+1)P_{\alpha,\beta+\gamma} - (q+1)Q_\infty.$$

Além disso, a reta $\tau_{\alpha,\beta} - \gamma = 0$ é uma reta tangente.

(**2**) *Se $\gamma^q + \gamma \neq 0$, o divisor de $\tau_{\alpha,\beta} - \gamma$ é dado por:*

$$(\tau_{\alpha,\beta} - \gamma) = \sum_{i=0}^{q} P_{\alpha+\delta\zeta^i,\, \beta+\gamma+\alpha^q\delta\zeta^i} - (q+1)Q_\infty,$$

em que ζ é uma $(q+1)$-ésima raiz primitiva da unidade em $\mathbb{F}_{q^2}$ e $\delta \in \mathbb{F}_{q^2}^*$ é tal que $\gamma^q + \gamma = \delta^{q+1}$.

Os pontos de $\mathcal{K}$ que pertencem à reta $\tau_{\alpha,\beta} - \gamma$ são precisamente:

$$(\alpha + \delta\zeta^i, \beta + \gamma + \alpha^q\delta\zeta^i) \text{ , em que } 0 \leq i \leq q.$$

Nesse caso, a reta $\tau_{\alpha,\beta} - \gamma = 0$ não é uma reta tangente.

Demonstração. Vejamos cada uma das afirmações.

(**1**) Observemos que, se $\gamma^q + \gamma = 0$, então $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$, pois:

$$\begin{aligned} \tau_{\alpha,\beta} - \gamma &= y - \alpha^q x + \beta^q - \gamma \\ &= y - \alpha^q x + (\beta + \gamma)^q \\ &= \tau_{\alpha,\beta+\gamma}. \end{aligned}$$

Assim, o cálculo do divisor de $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$ é análogo ao apresentado na Proposição 6.2.2. Ainda, o fato de $\tau_{\alpha,\beta}$ ser a reta tangente da curva hermitiana no ponto $(\alpha, \beta + \gamma)$ decorre da Proposição 6.2.1.

(**2**) Seja $\gamma + \gamma^q = c \in \mathbb{F}_{q^2}^*$.

Notemos que $c = T(\gamma)$, em que T é a aplicação traço tratada na seção 6.1. Agora, pela Proposição 6.1.9, temos que existe um elemento $\delta \in \mathbb{F}_{q^2}^*$ tal que $c = N(\delta)$. Desse modo, garantimos a existência de $\delta \in \mathbb{F}_{q^2}^*$ satisfazendo $\delta^{q+1} = \gamma + \gamma^q$.

Seja ζ uma $(q+1)$-ésima raiz primitiva da unidade em $\mathbb{F}_{q^2}$.

Para exibirmos os pontos de interseção entre a reta $\tau_{\alpha,\beta}$ e o conjunto $\mathcal{K}$, consideremos $(x, y) \in \mathbb{F}_{q^2}^2$ um tal ponto. Sabemos que $\tau_{\alpha,\beta}(x, y) - \gamma = 0$, donde decorre:

$$\begin{aligned} \gamma^q + \gamma &= \tau_{\alpha,\beta}^q(x, y) + \tau_{\alpha,\beta}(x, y) \\ &= (x - \alpha)^{q+1}. \end{aligned}$$

Assim, segue que x satisfaz a igualdade $\delta^{q+1} = \gamma^q + \gamma = (x - \alpha)^{q+1}$. Notemos agora que o conjunto de soluções para a mesma é consituído pelos pontos x tais que $x - \alpha = \delta\zeta^i$, ou seja, $x = \alpha + \delta\zeta^i$, em que $0 \leq i \leq q$.

Por outro lado, utilizando que $\tau_{\alpha,\beta}(x, y) = \gamma$, sendo x dado como anteriormente, temos:

$$\gamma = \tau_{\alpha,\beta}(x, y) = y - \beta - \alpha^q(x - \alpha) = y - \beta - \alpha^q\delta\zeta^i.$$

Ou seja, y é da forma $\gamma + \beta + \alpha^q\delta\zeta^i$, em que $0 \leq i \leq q$.

Por fim, um cálculo direto nos mostra que, para cada i fixado $(0 \leq i \leq q)$, o ponto $p_i := (x, y) = (\alpha + \delta\zeta^i, \gamma + \beta + \alpha^q\delta\zeta^i)$ pertence a $\mathcal{K}$. Com efeito:

$$\begin{aligned} (\beta + \gamma + \alpha^q\delta\zeta^i) + (\beta + \gamma + \alpha^q\delta\zeta^i)^q &= \alpha^{q+1} + \delta^{q+1} + \alpha^q\delta\zeta^i + \alpha^{q^2}\delta^q\zeta^{iq} \\ &= \alpha^{q+1} + \delta^{q+1} + \alpha^q(\delta\zeta^i + \delta^q\zeta^{iq}) \\ &= (\alpha + \delta\zeta^i)^{q+1}. \end{aligned}$$

Finalmente, podemos calcular o divisor de $\tau_{\alpha,\beta} - \gamma$.

Observemos pelo Lema 6.2.3 que o lugar $\tau_{\alpha,\beta}-\gamma$ possui $q+1$ zeros em H, digamos $Z_0, Z_1, \ldots, Z_q$. Além disso, como as funções $x-\alpha-\delta\zeta^i$ e $y-\beta-\alpha^q\delta\zeta^i$ possuem um único zero comum em H, a saber o lugar associado ao ponto $p_i=(x,y)$ definido como acima, temos que $Z_i = P_{\alpha+\delta\zeta^i,\beta+\gamma+\alpha^q\delta\zeta^i}$ para cada i fixado.

Agora, denotando a valorização associada ao lugar Z_i por v_i, temos:

$$v_i(\tau_{\alpha,\beta}-\gamma) = v_i(y-\beta-\alpha^q\delta\zeta^i-\gamma) = 1.$$

Ainda, sabemos pela escrita de $\tau_{\alpha,\beta}-\gamma$ que todo polo de $\tau_{\alpha,\beta}-\gamma$ deve ser um polo de x ou y. Pela definição do corpo de funções Hermitiano, temos também que os polos de x e y são os mesmos; mais precisamente, existe um único polo comum de x e y: o polo Q_∞. Nessas circunstâncias, Q_∞ é o único polo de $\tau_{\alpha,\beta}-\gamma$ e o cálculo de $v_\infty(\tau_{\alpha,\beta}-\gamma)$ é feito a partir do grau do divisor, como na Proposição 6.2.2. Dessa forma,

$$v_\infty(\tau_{\alpha,\beta}-\gamma) = -(q+1).$$

Portanto, o divisor de $\tau_{\alpha,\beta}-\gamma$ é dado por:

$$(\tau_{\alpha,\beta}-\gamma) = \sum_{i=0}^{q} P_{\alpha+\delta\zeta^i,\,\beta+\gamma+\alpha^q\delta\zeta^i} - (q+1)Q_\infty.$$

Destacamos que a condição de $\tau_{\alpha,\beta}-\gamma$ não ser reta tangente decorre da caracterização das retas tangentes à curva hermitiana (Proposição 6.2.1), juntamente ao fato de $\gamma^q+\gamma\neq 0$, donde $\tau_{\alpha,\beta}-\gamma \neq \tau_{\alpha',\beta'}$ para todo $(\alpha',\beta')\in\mathcal{K}$.

□

Observação 6.2.6. Uma demonstração alternativa para a caracterização dos pontos da interseção de $\mathcal{K}$ com $\tau_{\alpha,\beta}-\gamma$ feita em (**2**), consiste em mostrar, por meio de cálculo direto, que os pontos da forma p_i pertencem tanto a $\mathcal{K}$ quanto à reta $\tau_{\alpha,\beta}-\gamma$. Nesse contexto, o fato de esses serem os únicos pontos de interseção decorre do Teorema de Bézout, o qual garante a existência de $q+1$ pontos a menos de multiplicidade de interseção, juntamente ao fato de que $p_i\neq p_j$ para todo $j\neq i$.

Proposição 6.2.7. *Seja $H/\mathbb{F}_{q^2}$ o corpo de funções Hermitiano.*

(**1**) *Consideremos que $f=x-c$. Então, o divisor de f é igual a:*

$$(f) = \left(\sum_d P_{c,d}\right) - qQ_\infty,$$

em que a soma acima percorre as q soluções $d\in\mathbb{F}_{q^2}$ para $d^q+d=c^{q+1}$.

(**2**) *Consideremos que $f = y + bx + c$. Seja $\delta \in \mathbb{F}_{q^2}$ tal que $\delta^{q+1} = b^{q+1} - (c^q + c)$. Então, os pontos de $\mathcal{K}$ pertencentes à reta f são precisamente:*

$$(-b^q + \delta\zeta^i, b^{q+1} - c - b\delta\zeta^i) \text{ , em que } 0 \leq i \leq q.$$

Resulta, nessas condições, que f é uma reta tangente se, e somente se, $\delta = 0$, se, e somente se, $(-b^q, c^q) \in \mathcal{K}$ (se, e somente se, $(-b, c) \in \mathcal{K}$).

Assim, no caso em que f é uma reta tangente, temos $f = \tau_{-b^q, c^q}$.

Destacamos que, se $\delta \neq 0$, então f contém exatamente $q + 1$ pontos de $\mathcal{K}$.

Demonstração. Primeiramente, ressaltamos que os casos enunciados contemplam todas as retas no corpo Hermitiano H. Com efeito, seja $ax + by + c$ uma reta em H. Caso tenhamos $b = 0$, necessariamente $a \neq 0$, donde tal reta corresponde, a menos de mudança de variável, a uma reta do tipo (**1**). Em caso contrário, uma mudança de variáveis nos garante que a reta em questão equivale a uma reta no formato apresentado em (**2**).

(**1**) Consideremos $f = x - c$. Seja S um lugar racional finito de H; então, temos que S corresponde a um ponto da curva hermitiana, digamos $(\alpha, \beta) \in \mathcal{K}$. Nessas condições, podemos escrever $S = P_{\alpha,\beta}$ e, consequentemente:

$$v_{P_{\alpha,\beta}}(x - c) = \begin{cases} 1, \text{ se } \alpha = c \\ 0, \text{ se } \alpha \neq c. \end{cases}$$

No primeiro caso, ou seja, quando $\alpha = c$, temos que $\beta = d$ em que d satisfaz $d^q + d = c^{q+1}$. Assim, segue que os únicos zeros de $x - c$ são os q lugares finitos $P_{c,d}$, sendo $d \in \mathbb{F}_{q^2}$ com $d^q + d = c^{q+1}$; mais ainda, todos esses zeros têm ordem 1.

Como Q_∞ é o único polo de H e como existem q zeros de $x - c$, temos que $v_\infty(x - c) = 0$, concluindo que o divisor de $x - c$ é conforme enunciado.

(**2**) Consideremos $f = y + bx + c$. Primeiramente, notemos que $b^{q+1} - (c^q + c) \in \mathbb{F}_{q^2}$ e, assim, por meio de uma argumentação análoga à apresentada na prova do item (**2**) da Proposição 6.2.5, garantimos a existência de $\delta \in \mathbb{F}_{q^2}$ satisfazendo $\delta^{q+1} = b^{q+1} - (c^q + c)$.

Façamos $\alpha := -b^q$. Então, segue que $\alpha^{q^2} = -b^q$, implicando em $b = -\alpha^q$. Agora, seja $\beta \in \mathbb{F}_{q^2}$ tal que $\beta^q + \beta = \alpha^{q+1} = b^{q+1}$. Dessa maneira, podemos escrever $f = y + bx + c = y - \alpha^q x + c = \tau_{\alpha,\beta} - \gamma$, em que $\gamma = \beta^q - c$.

Por outro lado, observemos que

$$\gamma^q + \gamma = (\beta^q - c)^q + \beta^q - c = b^{q+1} - (c^q + c) = \delta^{q+1}.$$

Sob tais circunstâncias, podemos aplicar a Proposição 6.2.5(**2**), a qual nos garante que os pontos de $\mathcal{K}$ pertencentes à reta f são dados por:

$$(-b^q + \delta\zeta^i, b^{q+1} - c - b\delta\zeta^i) \text{ , em que } 0 \leq i \leq q.$$

Por consequência, temos, ainda, que o divisor de f é dado por:

$$(f) = \left(\sum_{i=0}^{q} P_{-b^q+\delta\zeta^i,\, b^{q+1}-c-b\delta\zeta^i} \right) - (q+1)Q_\infty. \tag{6.3}$$

Para o último resultado, notemos que f é uma reta tangente à curva hermitiana se, e somente se, $f = \tau_{B,C} = y - B^q x + C^q$ para algum $(B, C) \in \mathcal{K}$, i.e., se, e somente se, $(b, c) = (-B^q, C^q)$ para algum $(B, C) \in \mathcal{K}$. Agora, observemos que $b = -B^q$ (resp. $c = C^q$) se, e somente se, $B = -b^q$ (resp. $C = c^q$). Logo, temos que f é uma reta tangente se, e somente se, $(-b^q, c^q) \in \mathcal{K}$, o que ocorre se, e somente se, $\delta = 0$.

Por fim, quando $\delta \neq 0$, temos que os pontos de interseção entre $\mathcal{K}$ e a reta f são todos distintos, uma vez que ζ é uma $(q+1)$-ésima raiz primitiva da unidade.

□

6.3 DISTÂNCIA MÍNIMA

A fim de obtermos uma caracterização para os vetores minimais do reticulado $L_{\mathcal{P}}$, apresentamos nessa seção o cálculo de sua distância mínima.

Notemos que o Teorema 4.1.10 nos fornece, em certo sentido, uma limitação para a distância mínima do reticulado $L_{\mathcal{P}}$ considerando-se um corpo de funções arbitrário da forma $F/\mathbb{F}_q$. Entretanto, quando consideramos o corpo de funções Hermitiano, é possível obter o valor exato para a distância mínima, como mostra o teorema a seguir.

Teorema 6.3.1 (**Distância Mínima de** $L_{\mathcal{P}}$)**.** *A distância mínima do reticulado $L_{\mathcal{P}}$ sobre o corpo Hermitiano $H/\mathbb{F}_{q^2}$ é igual a $\sqrt{2q}$. Além disso, o menor grau possível para uma função não nula em $\mathcal{O}_{\mathcal{P}}^*$ é q.*

Demonstração. Tomemos um ponto $P = (\alpha, \beta)$ na curva hermitiana e escolhamos duas retas distintas e não tangentes, digamos f_1 e f_2, que passam por P e não são verticais, ou seja, nenhuma das retas é da forma $x - \alpha$, com $\alpha \in \mathbb{F}_{q^2}$.

Primeiramente, destacamos que tal escolha é possível. De fato, escolhemos dois valores distintos $M_1, M_2 \in \mathbb{F}_{q^2}$, ambos diferentes de $-\alpha^q$. Então, pela sobrejetividade do mapa de Frobenius, dado por:

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

garantimos a existência de $m_1, m_2 \in \mathbb{F}_{q^2}$ satisfazendo $M_1 = m_1^q$ e $M_2 = m_2^q$.

Assim, definimos $f_1 = y - \beta - m_1^q(x - \alpha)$ e $f_2 = y - \beta - m_2^q(x - \alpha)$. Claramente, ambas as retas são distintas e passam por P. Por outro lado, pela Proposição 6.2.7 (**2**), sabemos que f_1 e f_2 não são retas tangentes à curva hermitiana no ponto P, pois, em caso contrário, teríamos m_1^q ou m_2^q sendo igual a $-\alpha^q$. Além disso, tais retas não podem ser tangentes a nenhum outro ponto da curva hermitiana, visto que toda reta tangente passa por apenas um ponto da curva hermitiana e já sabemos que ambas as retas passam por P.

Notemos, agora, que ambas as retas f_1 e f_2 definidas como acima são da forma $f_i = \tau_{m_i,n_i} - \gamma_i$, com $i = 1, 2$ para algum $n_i, \gamma_i \in \mathbb{F}_{q^2}$. Mais precisamente, basta tomarmos n_i e γ_i satisfazendo $n_i^q - \gamma_i = m_i^q\alpha - \beta$ para cada $i = 1, 2$ fixado. De fato:

$$\begin{aligned} \tau_{m_i,n_i} - \gamma_i &= y - m_i^q x + (n_i^q - \gamma_i) \\ &= y - m_i^q x + (m_i^q\alpha - \beta) = f_i. \end{aligned}$$

Ainda, ressaltamos que $\gamma_i \neq 0$ para qualquer $i = 1, 2$, caso contrário, f_1 e f_2 seriam retas tangentes. Podemos, então, aplicar a Proposição 6.2.2 (item (**2**)), a qual nos garante que a interseção dos suportes de f_1 e f_2 é constituída apenas dos lugares $P_{\alpha,\beta}$ e Q_∞. Assim, utilizando a caracterização dos divisores das funções f_1 e f_2 (apresentadas na equação (6.3) da proposição citada), obtemos que o divisor de f_1/f_2 é da forma:

$$\left(\frac{f_1}{f_2}\right) = \sum_{i=1}^{q} P_{c_i,d_i} - \sum_{i=1}^{q} P_{s_i,t_i},$$

em que (c_i, d_i) (resp. (s_i, t_i)), com $1 \leq i \leq q$, percorre todos os pontos comuns à reta f_1 (resp. f_2) e à curva hermitiana, exceto o ponto P.

Cabe destacar que, como as retas f_1 e f_2 não são retas tangentes, temos $P_{c_i,d_i} \neq P_{c_j,d_j}$ e $P_{s_i,t_i} \neq P_{s_j,t_j}$ para todo $i \neq j$ (segue do item (**2**) da Proposição 6.2.7). Além disso, fixado qualquer i, temos que $P_{c_i,d_i} \neq P_{s_j,t_j}$ para todo $1 \leq j \leq q$, visto que o único lugar racional comum a f_1 e f_2 é $P_{\alpha,\beta}$.

Pela descrição do divisor de f_1/f_2 e pelo isomorfismo existente entre $L_{\mathcal{P}}$ e $Princ(\mathcal{P})$ (Corolário 4.1.15), temos então que f_1/f_2 corresponde a um ponto com q entradas iguais a 1 e q entradas iguais a -1, sendo o restante das entradas iguais a zero. Utilizando a norma euclidiana, vemos que tal vetor possui norma igual a $\sqrt{2q}$. Logo, a distância mínima de $L_{\mathcal{P}}$ é no máximo $\sqrt{2q}$.

Resta mostrarmos que é exatamente igual a $\sqrt{2q}$. Para tanto, tomemos uma função f correspondente a um vetor não nulo do reticulado $L_{\mathcal{P}}$. Como o grau do divisor f é igual a zero, temos que a soma das entradas positivas desse vetor é igual a menos a soma das entradas negativas, a qual equivale ao grau da função f, i.e., $[H : \mathbb{F}_{q^2}(f)]$.

Por outro lado, H pode ser visto como uma extensão de $\mathbb{F}_{q^2}(f)$. Dessa forma, o número de lugares racionais de H é limitado pelo número de lugares de $\mathbb{F}_{q^2}(f)$ contados como eles se estendem. Formalmente, temos:

$$q^3 + 1 \leq [H : \mathbb{F}_{q^2}(f)](q^2 + 1),$$

donde resulta:

$$[H : \mathbb{F}_{q^2}(f)] \geq \frac{q^3 + 1}{q^2 + 1} \geq q.$$

Consequentemente, concluímos que a norma euclidiana do vetor associado e f é maior ou igual a $\sqrt{2q}$. E, assim, pela argumentação feita anteriormente, obtemos que o reticulado $L_{\mathcal{P}}$ possui distância mínima igual a $\sqrt{2q}$.

Por fim, destacamos que se f é uma função correspondente a um vetor não nulo do reticulado, então sua norma euclidiana em geral é maior ou igual a $\sqrt{2q}$ e garantimos a igualdade no caso em que $f = f_1/f_2$, sendo f_1 e f_2 construídas como acima.

Finalmente, a afirmação quanto ao menor grau possível para uma função não nula em $O_{\mathcal{P}}$ segue da construção acima, juntamente à definição do grau de uma função como a soma de todas as entradas positivas do vetor associado à função. Neste caso, basta observarmos que uma função da forma f_1/f_2 possui norma igual a $\sqrt{2q}$ e, portanto, grau igual a q. □

6.4 PROPRIEDADES DO RETICULADO

Esta seção tem o intuito de apresentar as principais características do reticulado $L_{\mathcal{P}}$ sobre o corpo de funções Hermitiano, especialmente uma caracterização para os seus vetores minimais. Demonstraremos, então, que o reticulado é gerado por seus vetores minimais e, consequentemente, é bem arredondado.

Ao associarmos o cálculo da distância mínima do reticulado $L_{\mathcal{P}}$ com as propriedades das retas no corpo de funções Hermitiano (Proposições 6.2.5 e 6.2.7), podemos exibir quais os vetores minimais do reticulado $L_{\mathcal{P}}$ sob certas condições.

Teorema 6.4.1 (Vetores Minimais de $L_{\mathcal{P}}$). *Sejam f_1 e f_2 retas distintas. Então, o divisor (f_1/f_2) (ou (f_2/f_1)) é um vetor minimal de $L_{\mathcal{P}}$ se, e somente se, vale uma das seguintes condições:*

- *f_1 e f_2 são da forma $x - \alpha$;*
- *uma das funções f_1 ou f_2 é da forma $x - \alpha$ e a outra é uma reta não tangente (da forma $y - bx + c$) e as retas possuem exatamente um ponto de interseção;*
- *ambas as retas f_1 e f_2 são não tangentes (da forma $y - bx + c$) com um ponto de interseção pertencente a $\mathcal{K}$.*

Demonstração. Conforme calculado no Teorema 6.3.1, a distância mínima de $L_{\mathcal{P}}$ é $\sqrt{2q}$. Assim, temos que o divisor (f_1/f_2), sendo f_1 e f_2 retas distintas, é um vetor minimal se, e somente se, a norma do vetor associado a tal divisor é igual a $\sqrt{2q}$. Ressaltamos que aqui utilizamos o isomorfismo entre $L_{\mathcal{P}}$ e $Princ(\mathcal{P})$ (Corolário 4.1.15).

Assim, para a verificação de que nos três casos enunciados temos que (f_1/f_2) corresponde a um vetor de norma $\sqrt{2q}$, basta utilizarmos o cálculo dos divisores de uma reta apresentado na Proposição 6.2.7. Sob tais condições, mostra-se que tal divisor corresponde a um ponto com $2q$ entradas não nulas. Consequentemente, na norma euclidiana, temos que a norma do vetor associado a (f_1/f_2) é, de fato, igual a $\sqrt{2q}$.

- Se f_1 e f_2 são dadas por $x - \alpha$ e $x - \beta$, então:

$$\left(\frac{f_1}{f_2}\right) = \sum_{i=1}^{q} P_{c_i,d_i} - \sum_{i=1}^{q} P_{s_i,t_i}$$

  em que $(c_i, d_i) = (\alpha, d_i)$ e $(s_i, t_i) = (\beta, t_i)$. Neste caso, temos ainda que d_i (resp. s_i) percorre todas as q soluções em $\mathbb{F}_{q^2}$ da equação $d^q + d = \alpha^{q+1}$ (resp. $s^q + s = \beta^{q+1}$).

- Se f_1 é da forma $x - \alpha$ e f_2 é não tangente da forma $y - bx + c$, então:

$$\left(\frac{f_1}{f_2}\right) = \sum_{i=1}^{q-1} P_{c_i,d_i} - \sum_{i=0}^{q-1} P_{s_i,t_i} + q\mathrm{Q}_\infty$$

  em que (c_i, d_i) é como no item acima, com a ressalva de que todos diferem do ponto em comum entre as retas e (s_i, t_i) percorre todos os pontos de f_2 pertencentes a $\mathcal{K}$, exceto o ponto em comum.

- Se f_1 e f_2 são retas não tangentes da forma $y - bx + c$ com um ponto em comum pertencente a $\mathcal{K}$, conforme visto no Teorema 6.3.1, temos:

$$\left(\frac{f_1}{f_2}\right) = \sum_{i=1}^{q} P_{c_i,d_i} - \sum_{i=1}^{q} P_{s_i,t_i}$$

  em que (c_i, d_i) (resp. (s_i, t_i)), com $1 \leq i \leq q$, percorre todos os pontos comuns à reta f_1 (resp. f_2) e à curva hermitiana, exceto o ponto P.

Ressaltamos que os cálculos acima permanecem válidos trocando-se a ordem de f_1 e f_2 em cada item.

Por fim, devemos mostrar que, para quaisquer outras combinações de retas diferentes dos casos enunciados, o divisor (f_1/f_2) está associado a um vetor cuja norma é estritamente maior que $\sqrt{2q}$. De fato, os casos não considerados são aqueles em que ao menos uma das retas é tangente. No entanto, um cálculo direto utilizando o divisor de uma reta tangente (Proposição 6.2.2), mostra que se uma das retas f_1 ou f_2 é tangente, então o divisor de (f_1/f_2) é maior que $\sqrt{2q}$. □

Para a demonstração de que o reticulado $L_{\mathcal{P}}$ é bem arredondado, necessitaremos de uma série de resultados auxiliares.

Para efeito de simplificação, diremos que uma reta $f = ax+by+c$ é *boa* se o divisor de f é uma combinação inteira de vetores minimais. Nessas circunstâncias, os lemas seguintes apresentam retas pertencentes ao corpo de funções Hermitiano que são boas. Mais ainda, como mostraremos, esses lemas caracterizam todas as retas pertencentes a tal corpo de funções. Nesses lemas, denotaremos por $\zeta \in \mathbb{F}_{q^2}$ uma $(q+1)$-ésima raiz primitiva da unidade.

Lema 6.4.2 (**Caso 1**). *Consideremos $d, e \in \mathbb{F}_{q^2}$ satisfazendo $d^q + d = e^{q+1}$, com $e \neq 0$. Afirmamos que as retas $y - d$ e $x - e$ são boas.*

Demonstração. Sejam $d_1 = d, d_2, \ldots, d_q$ todas as soluções da equação $y^q + y = e^{q+1}$.

Então:

$$\prod_{i=1}^{q}(y - d_i) = y^q + y - e^{q+1} = x^{q+1} - e^{q+1} = \prod_{i=0}^{q}(x - \zeta^i e),$$

resultando que:

$$x - e = \prod_{i=1}^{q}\left(\frac{y - d_i}{x - \zeta^i e}\right).$$

Notemos que as retas $y - d_i$ e $x - e_i$ possuem um único ponto em comum e que a reta $y - d_i$ é não tangente, visto que $d^q + d \neq 0$. Assim, tais retas cumprem a segunda condição do Teorema 6.4.1, garantindo que o vetor associado à função $(y - d_i)/(x - \zeta^i e)$, para cada i fixado, é um vetor minimal de $L_{\mathcal{P}}$.

Agora, como o divisor de $x - e$ é a soma dos divisores dessas funções, variando i no intervalo $0 \leq i \leq q$, concluímos que a reta $x - e$ é boa.

Por outro lado, podemos escrever:

$$y - d = (x - e)(x - \zeta e)\prod_{i=2}^{q}\left(\frac{y - d_i}{x - \zeta^i e}\right).$$

Como no lado direito da equação cada um dos fatores corresponde a um vetor minimal ou a um vetor que se expressa como combinação linear de vetores minimais, concluímos que $y - d$ é, também, uma reta boa. □

Lema 6.4.3 (**Caso 2**). *Toda reta não tangente da forma $f = y + bx + c$ é boa.*

Demonstração. Pelo item (**2**) da Proposição 6.2.7, sabemos que, se f como acima é uma reta não tangente, então $(-b^q, c^q) \notin \mathcal{K}$, ou seja, $c^q + c \neq (-b)^{q+1} = b^{q+1}$.

Seguindo a abordagem feita em tal proposição, seja $\alpha = -b^q$; então, $b = -\alpha^q$. Notemos que $\alpha^{q+1} = b^{q+1}$. Consideremos agora $\beta \in \mathbb{F}_{q^2}$ satisfazendo $\beta^q + \beta = \alpha^{q+1} = b^{q+1}$. Assim, temos $f = y + bx + c = y - \alpha^q x + c = \tau_{\alpha,\beta} - d$, sendo $d = \beta^q - c$.

Destacamos ainda que

$$d^q + d = (\beta^q - c)^q + \beta^q - c = b^{q+1} - (c^q + c).$$

Escolhemos $e \in \mathbb{F}_{q^2}$ tal que $d^q + d = e^{q+1}$ (como consequência, $c^q + c = b^{q+1} - e^{q+1}$). Notemos que $e \neq 0$. De modo semelhante ao caso 1, sejam $d_1 = d, d_2, \ldots, d_q$ todas as soluções para $y^q + y = e^{q+1}$. Temos:

$$\prod_{i=1}^{q}(\tau_{\alpha,\beta} - d_i) = \tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} - e^{q+1} = (x-\alpha)^{q+1} - e^{q+1} = \prod_{i=0}^{q}(x - \alpha - \zeta^i e). \tag{6.4}$$

Segue assim que:

$$x - \alpha - e = \prod_{i=1}^{q}\left(\frac{\tau_{\alpha,\beta} - d_i}{x - \alpha - \zeta^i e}\right). \tag{6.5}$$

Notemos que tanto as retas da forma $\tau_{\alpha,\beta} - d_i$ quanto $x - \alpha - \zeta^i e$ são não tangentes, uma vez que $d_i^q + d_i = e^{q+1} = d^q + d \neq 0$. Além disso, temos que, para cada i fixado, tais retas se intersectam em um único ponto, a saber: $(\alpha + \zeta^i e, \beta + d_i + \alpha^q \zeta^i e)$. E, por meio de cálculo direto, vemos que tal ponto pertence a $\mathcal{K}$, pois:

$$\begin{aligned}(\beta + d_i + \alpha^q\zeta^i e)^q + \beta + d_i + \alpha^q\zeta^i e &= \alpha^{q+1} + e^{q+1} + \alpha\zeta^{iq}e^q + \alpha^q\zeta^i e \\ &= (\alpha + \zeta^i e)^{q+1}.\end{aligned}$$

Logo, temos que as retas satisfazem a terceira condição do Teorema 6.4.1, donde resulta que os vetores correspondentes às funções da forma $(\tau_{\alpha,\beta})/(x - \alpha - \zeta^i e)$, com $1 \leq i \leq q$, são vetores minimais. Pela equação (6.5), segue que $x - \alpha - e$ é uma reta boa.

Ainda, o argumento apresentado pode ser refeito para a reta $x - \alpha - \zeta e$ (apenas trocando-se e por ζe), resultando que $x - \alpha - \zeta e$ também é boa. Nesse contexto, reescrevemos a equação (6.4) do seguinte modo:

$$f = \tau_{\alpha,\beta} - d = (x - \alpha - e)(x - \alpha - \zeta e)\prod_{i=2}^{q}\left(\frac{x - \alpha - \zeta^i e}{\tau_{\alpha,\beta} - d_i}\right).$$

Como os fatores à direita estão associados a vetores minimais ou vetores que são combinações lineares de vetores minimais, decorre que f é uma reta boa, como queríamos. É interessante destacar que, demonstrado este caso, o Caso 1 (Lema 6.4.2) torna-se um caso especial deste, bastando tomar $b = 0$. □

Lema 6.4.4 (**Caso 3**). *A reta x é boa.*

Demonstração. Primeiramente, notemos que:

$$y^q + y - (x^q + x) = x^{q+1} - x^q - x = (x-1)^{q+1} - 1 = \prod_{i=0}^{q}(x - 1 - \zeta^i).$$

E, por outro lado,

$$y^q + y - (x^q + x) = (y-x)^q + (y-x) = \prod_{i=0}^{q}(y - x - \eta_i),$$

sendo $\eta_1, \ldots, \eta_p \in \mathbb{F}_{q^2}$ as soluções para $\eta^q + \eta = 0$.

Desse modo, obtemos:

$$\prod_{i=0}^{q}(x - 1 - \zeta^i) = \prod_{i=0}^{q}(y - x - \eta_i).$$

Utilizando que $\zeta^j = -1$, como anteriormente, temos então:

$$x = (y - x - \eta_j) \prod_{i=0,\, i\neq j}^{q} \left(\frac{y - x - \eta_i}{x - (1 + \zeta^i)}\right). \tag{6.6}$$

Notemos que as retas $y - x - \eta_i$ são não tangentes para todo i com $0 \leq i \leq q$, visto que $(1, \eta_i) \notin \mathcal{K}$ (pois $\eta_i^q + \eta = 0 \neq 1$). Além disso, as retas $y - x - \eta_i$ e $x - (1 + \zeta^i)$, com i fixado e $0 \leq i \neq j \leq q$, intersectam-se em um único ponto, a saber $(1 + \zeta^i, 1 + \zeta^i + \eta_i)$. Tal ponto pertence a $\mathcal{K}$, como mostra o cálculo a seguir:

$$(1 + \zeta^i + \eta_i)^q + 1 + \zeta^i + \eta_i = 1 + \zeta^{iq} + \zeta + 1 = (1 + \zeta)^{q+1}.$$

Logo, pela segunda condição do Teorema 6.4.1, concluímos que o quociente de tais funções, com $0 \leq i \neq j \leq q$, está associado a um vetor minimal. E, como $y - x - \eta_j$ é uma reta não tangente, sabemos do Caso 2 (Lema 6.4.3) que a mesma é boa. Consequentemente, temos pela equação (6.6) que a reta x é boa. □

Lema 6.4.5 (**Caso 4**). *A reta tangente em* $(0, 0)$*, isto é, a reta* $\tau_{0,0} = y$*, é boa.*

Demonstração. De modo semelhante ao caso anterior (Lema 6.4.4), observemos que:

$$y^{q+1} - x^{q+1} = y^{q+1} - y^q - y = (y-1)^{q+1} - 1 = \prod_{i=0}^{q}(y - 1 - \zeta^i).$$

Por outro lado, podemos escrever:

$$y^{q+1} - x^{q+1} = \prod_{i=0}^{q}(y - \zeta^i x)$$

e, assim,

$$\prod_{i=0}^{q}(y-1-\zeta^i)=\prod_{i=0}^{q}(y-\zeta^i x).$$

Agora, como -1 é uma $(q+1)$-ésima raiz da unidade, existe um único índice $j\in\{0,\ldots,q\}$ tal que $\zeta^j=-1$ (caso a característica seja 2, temos $j=0$ e, caso contrário, $j=(q+1)/2$). Dessa maneira, obtemos:

$$y=(y-\zeta^j x)\prod_{i=0,\,i\neq j}^{q}\left(\frac{y-\zeta^i x}{y-1-\zeta^i}\right). \tag{6.7}$$

Mostraremos que, fixado $i\neq j$, as retas $y-\zeta^i x$ e $y-1-\zeta^i=y-(1+\zeta^i)$ são não tangentes e se intesectam em um único ponto, o qual pertence a $\mathcal{K}$. Com efeito, como $(\zeta^i)^{q+1}=1\neq 0$, segue que $(\zeta^i,0)\notin\mathcal{K}$ e, pela Proposição 6.2.7, tais retas não podem ser tangentes. Além disso, temos que o único ponto de interseção entre $y-\zeta^i x$ e $y-(1+\zeta^i)$, para i fixado em $0\leq i\neq j\leq q$, é dado por $((1+\zeta^i)\zeta^{q+1-i},1+\zeta^i)$. De fato, tal ponto pertence ao conjunto $\mathcal{K}$, uma vez que:

$$\begin{aligned}((1+\zeta^i)\zeta^{q+1-i})^{q+1} &= (1+\zeta^i)^{q+1}=(1+\zeta^{iq})(1+\zeta)\\ &= 1+\zeta^{iq}+\zeta^i+1=(1+\zeta^i)^q+1+\zeta^i.\end{aligned}$$

Nessas circunstâncias, vemos, pelo Teorema 6.4.1, que o vetor correspondente ao quociente das funções $y-\zeta^i x$ e $y-1-\zeta^i$, para cada i fixado com $0\leq i\leq q$ e $i\neq j$, é um vetor minimal de $L_{\mathcal{P}}$. Agora, utilizando que a reta $y-\zeta^j x$ é também não tangente, concluímos da equação (6.7) que a reta y é boa. □

Para o último caso a ser considerado, em que provaremos que toda reta tangente é boa, será necessário destacar uma propriedade dos automorfismos do corpo hermitiano.

Para tanto, lembramos que o conjunto dos automorfismos de $H/\mathbb{F}_{q^2}$ é dado por:

$$Aut(H/\mathbb{F}_{q^2}):=\left\{\sigma:H\to H:\ \sigma\text{ é um automorfismo de }H/\mathbb{F}_{q^2}\right\}.$$

No próximo resultado, analisaremos um subgrupo específico de $Aut(H/\mathbb{F}_{q^2})$, a saber:

$$Aut(Q_\infty):=\left\{\sigma\in Aut(H/\mathbb{F}_{q^2}):\ \sigma(Q_\infty)=Q_\infty\right\}.$$

Lema 6.4.6. *Para cada $(d,e)\in\mathcal{K}$ (i.e., $e^q+e=d^{q+1}$), existe um automorfismo $\sigma\in Aut(H/\mathbb{F}_{q^2})$ tal que $\sigma(x)=x+d$ e $\sigma(y)=y+d^q x+e$. Mais precisamente, mostraremos que um tal automorfismo pertence a $Aut(Q_\infty)$.*

Demonstração. Consideremos $d\in\mathbb{F}_{q^2}$. Sabemos que a equação $e^q+e=d^{q+1}$ possui q soluções em $\mathbb{F}_{q^2}$. Para cada d satisfazendo tal equação, definimos:

$$\sigma(x):=x+d\qquad\text{e}\qquad\sigma(y):=y+d^q x+e.$$

Notemos que, pela definição acima, segue que σ é um automorfismo de $H/\mathbb{F}_{q^2}$. Além disso, afirmamos que σ fixa Q_∞.

Para tanto, lembramos que H é uma extensão de Kummer sobre $\mathbb{F}_{q^2}(y)$. Em particular, podemos considerar que $H/\mathbb{F}_{q^2}(y)$ é uma extensão de $H/\mathbb{F}_{q^2}$. Mais ainda, de modo semelhante ao Lema 6.2.3), pode-se demonstrar que Q_∞ é totalmente ramificado em H. Assim, o polo de x em $H/\mathbb{F}_{q^2}(y)$ é o único lugar que está sobre Q_∞ e seu índice de ramificação é igual a q. Denotemos o polo de x em $H/\mathbb{F}_{q^2}(y)$ por P_∞. Como esse é um corpo de funções racionais, sabemos qe P_∞ é dado por:

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : \ f, g \in H/\mathbb{F}_{q^2}(y) \text{ e } \deg f(x) < \deg g(x) \right\}.$$

Fixemos $(e, d) \in \mathcal{K}$ e consideremos σ o automorfismo associado a tal ponto, definido como em (6.4). Denotemos $f'(x) := f(x + d)$ e $g'(x) := g(x + d)$. Observemos então que $\sigma(f(x)) = f'(x)$ e $\sigma(g(x)) = g'(x)$. Além disso, temos que $\deg f'(x) = \deg f(x)$ e $\deg g'(x) = \deg g(x)$. Assim, para todos $f, g \in H/\mathbb{F}_{q^2}(y)$ com $\deg f(x) < \deg g(x)$ temos:

$$\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f'(x)}{g'(x)} \in P_\infty.$$

Por outro lado, dado $f(x)/g(x) \in P_\infty$, façamos $x' := x + c$ para algum $c \in \mathbb{F}_{q^2} \setminus \{0\}$ fixado. Então, de modo análogo ao feito anteriormente, temos:

$$\frac{f(x)}{g(x)} = \sigma\left(\frac{f(x' - c)}{g(x' - c)}\right) \in \sigma(P_\infty).$$

Assim, garantimos que $\sigma(P_\infty) = P_\infty$. Para a análise do lugar $Q_\infty \subset P_\infty$, utilizamos a caracterização de Q_∞ via valorização (Teorema 2.3.11):

$$Q_\infty = \left\{ z \in H : \ v_{Q_\infty}(z) > 0 \right\}.$$

E, pela definição do índice de ramificação (Definição 2.3.59), juntamente ao fato de que o mesmo é igual a q, temos ainda:

$$v_{P_\infty}(z) = q \cdot v_{Q_\infty}(z) \quad \forall z \in H. \tag{6.8}$$

em que v_{P_∞} e v_{Q_∞} denotam as valorizações associadas aos lugares P_∞ e Q_∞, respectivamente.

Tomemos $z \in Q_\infty$. Queremos mostrar que $\sigma(z) \in Q_\infty$. Como $Q_\infty \subset P_\infty$, segue que $v_{P_\infty}(z) > 0$. Agora, como $\sigma(P_\infty) = P_\infty$, temos que $\sigma(z) \in P_\infty$, ou seja, $v_{P_\infty}(\sigma(z)) > 0$. Desse modo, pela equação (6.8), resulta que $v_{Q_\infty}(\sigma(z)) > 0$ e, então, $\sigma(z) \in Q_\infty$. Como z foi tomado de modo arbitrário em Q_∞, concluímos que $\sigma(Q_\infty) \subset Q_\infty$.

Por outro lado, consideremos $z \in Q_\infty$. Queremos mostrar que $z \in \sigma(Q_\infty)$. Como $z \in P_\infty$, temos:

$$z = \frac{f(x)}{g(x)} = \sigma\left(\frac{f(x'-c)}{g(x'-c)}\right), \tag{6.9}$$

em que $f, g \in H/\mathbb{F}_{q^2}(y)$ e $x' = x + c$, sendo $c \in \mathbb{F}_{q^2} \setminus \{0\}$ fixado.

Notemos agora que, como $z \in Q_\infty$, temos $v_{Q_\infty}(z) > 0$ ou, equivalentemente, $v_{Q_\infty}(f(x)) - v_{Q_\infty}(g(x)) > 0$. Além disso, como $c \in \mathbb{F}_{q^2}$ e $c \neq 0$, segue das propriedades de valorização, segue que $v_{Q_\infty}(f(x'-c))$ e $v_{Q_\infty}(g(x)) = v_{Q_\infty}(g(x'-c))$. Consequentemente, temos que $v_{Q_\infty}(f(x'-c)) - v_{Q_\infty}(g(x'-c)) > 0$ e, então, pela equação (6.9), concluímos que $z \in \sigma(Q_\infty)$. Logo, mostramos que $Q_\infty \subset \sigma(Q_\infty)$.

Portanto, $\sigma \in Aut(Q_\infty)$, como queríamos. □

Observação 6.4.7. Cabe destacar que os automorfismos definidos na equação (6.4), em que $(d, e) \in \mathcal{K}$, não apenas são automorfismos que fixam Q_∞ como descrevem um importante subgrupo de $Aut(Q_\infty)$, a saber o único p-subgrupo de Sylow de $Aut(Q_\infty)$. Para uma descrição mais detalhada do grupo $Aut(Q_\infty)$ e de seus subgrupos, sugerimos consultar [1]. Além disso, ressaltamos que o resultado apresentado no Lema 6.4.6 pode ser estendido para os corpos de funções associados às chamadas *curvas hermitianas generalizadas*, conforme é apresentado em [7] (Proposição 3.3).

Assim, demonstramos o último caso necessário.

Lema 6.4.8 (Caso 5). *Para cada $(\alpha, \beta) \in \mathcal{K}$, a reta tangente $\tau_{\alpha,\beta} = y - \alpha^q x + \beta^q$ é boa.*

Demonstração. Primeiramente, notemos que, como $(\alpha, \beta) \in \mathcal{K}$, temos ainda que $(-\alpha, \beta^q) \in \mathcal{K}$. Assim, podemos tomar $(d, e) = (-\alpha, \beta^q)$ no Lema 6.4.6. Nesse caso, garantimos a existência de um automorfismo $\sigma \in Aut(H/\mathbb{F}_{q^2})$ tal que $\sigma(x) = x - \alpha$ e $\sigma(y) = y - \alpha^q x + \beta^q = \tau_{\alpha,\beta}$.

A efeito de notação, façamos $\tau := \tau_{\alpha,\beta}$ e $x_\alpha = x - \alpha$.

Ao aplicarmos o automorfismo $\sigma \in Aut(H/\mathbb{F}_{q^2})$ obtido acima na equação (6.7), obtemos:

$$\sigma(y) = \tau = (\tau - \zeta^j x_\alpha) \prod_{i=0,\, i\neq j}^{q} \left(\frac{\tau - \zeta^i x_\alpha}{\tau - 1 - \zeta^i}\right). \tag{6.10}$$

Como σ é um automorfismo, temos que o mesmo preserva pontos de tangência. Dessa forma, usando que $y - \zeta^i x$ e $y - 1 - \zeta^i$ são retas não tangentes para $0 \leq i \neq j \leq q$, segue que o mesmo vale para $\sigma(y - \zeta^i x) = \tau - \zeta^i x_\alpha$ e $\sigma(y - 1 - \zeta^i) = \tau - 1 - \zeta^i$. Mais ainda, temos que, fixado i, tais retas se intersectam em um único ponto, a saber na imagem do ponto de interseção entre $y - \zeta^i x$ e $y - 1 - \zeta^i$ via o automorfismo σ. Assim, o vetor correspondente ao quociente de tais funções, com $0 \leq i \neq j \leq q$, é um vetor minimal. Por outro lado, sabemos, pelo caso 2, que $\tau - \zeta^j x_\alpha$ é uma reta boa.

Portanto, pela equação (6.10), concluímos que o divisor de τ é uma combinação linear de vetores minimais e, consequentemente, τ é uma reta boa. □

Finalmente, somos capazes de demonstrar que o reticulado $L_{\mathcal{P}}$ sobre o corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$ é bem arredondado. Necessitamos apenas de um importante resultado auxiliar, o qual será crucial na demonstração. Conforme é mostrado em [16] (Corolário 7.5), sabe-se que toda função em $\mathcal{O}_{\mathcal{P}}^*$ é o produto de funções da forma $ax + by + c$ e seus inversos.

Teorema 6.4.9 (Reticulado Bem Arredondado). *O reticulado $L_{\mathcal{P}}$ é gerado por seus vetores minimais e, portanto, é bem arredondado.*

Demonstração. Pela caracterização do reticulado $L_{\mathcal{P}}$ (Corolário 4.1.15), sabemos que o mesmo é isomorfo ao grupo $Princ(\mathcal{P})$. Como toda função de $\mathcal{O}_{\mathcal{P}}^*$ é igual ao produto de retas da forma $ax + by + c$ e de seus inversos, temos, então, que o reticulado $L_{\mathcal{P}}$ é gerado pelos divisores das retas do corpo Hermitiano. Sob essa óptica, é suficiente mostrarmos que cada divisor como esse pode ser visto como uma combinação linear inteira de vetores minimais.

Lembramos que uma reta $f = ax + by + c$ é dita *boa* se o divisor de f é uma combinação inteira de vetores minimais. Nosso objetivo, assim, é provarmos que todas as retas do corpo Hermitiano são boas.

Destacamos que os casos de 1 a 5, apresentados na sequência de lemas anteriores (lemas 6.4.2 a 6.4.8) contemplam todas as retas existentes no corpo de funções Hermitiano. Assim, demonstramos que todas as retas estão associadas a vetores minimais do reticulado $L_{\mathcal{P}}$.

Desse modo, mostramos que $L_{\mathcal{P}}$ é gerado por seus vetores minimais; mais precisamente, por divisores da forma (f_1/f_2) em que f_1 e f_2 são retas distintas que satisfazem uma das condições exibidas no Teorema 6.4.1. Por consequência, está provado que $L_{\mathcal{P}}$ é um reticulado bem arredondado. □

6.5 ESTIMATIVA DO NÚMERO DE VIZINHOS

Por fim, apresentaremos uma estimativa para o número de vetores minimais em $L_{\mathcal{P}}$ (*kissing number*) e calcularemos o volume exato de tal reticulado.

Ao estabelecermos que $L_{\mathcal{P}}$ é gerado por seus vetores minimais, podemos nos perguntar quantos são tais vetores, ou seja, qual o valor do *kissing number* deste reticulado. Ao contrário do reticulado obtido através de um corpo de funções elípticas, no caso do corpo de funções Hermitiano, não apresentaremos um valor exato para esse número, mas sim, um limite inferior para o mesmo.

Teorema 6.5.1 (Limite Inferior para o Número de vetores Minimais de $L_{\mathcal{P}}$). *O reticulado $L_{\mathcal{P}}$ contém, no mínimo, $q^7 - q^5 + q^4 - q^2$ vetores minimais.*

Demonstração. Primeiramente, consideremos o caso em que $q = 2$. Neste caso, decorre do Teorema 6.1.6, que o gênero do corpo de funções Hermitiano é igual a 1 e, conforme analisado anteriormente, o corpo de funções $H/\mathbb{F}_{q^2}$ torna-se um corpo de funções elípticas. Por outro lado, sabemos que $H/\mathbb{F}_{q^2}$ é um corpo de funções maximal, ou seja, $n = q^2 + 1 + 2gq$ (Definição 2.4.11). Assim, fazendo $q = 2$, obtemos $n = 9$ lugares racionais. Como tal corpo possui apenas um 2-ponto de torsão, segue do cálculo feito para o número de vetores minimais no corpo de funções elípticas (Teorema 5.5.2) que o mesmo é dado por:

$$\frac{9(9-1)(9-3)}{4} = 108,$$

o que equivale a $2^7 - 2^5 + 2^4 - 2^2$.

Dessa forma, podemos considerar $q > 2$.

Queremos obter uma estimativa para o número de funções da forma $f = f_1/f_2$, em que f_1 e f_2 são retas distintas satisfazendo uma das condições do Teorema 6.4.1. Assim, consideraremos cada um dos casos apresentados em tal teorema.

Caso 1: Se ambas as retas f_1 e f_2 são da forma $x - \alpha$, sendo $\alpha \in \mathbb{F}_{q^2}$, então existem $q^2(q^2-1)$ funções da forma f.

Caso 2: Consideremos que uma das funções é da forma $x - \alpha$ e a outra é uma reta não tangente (da forma $y + bx + c$) e que as mesmas possuem exatamente um ponto de interseção. Sabemos que as funções dadas por $f_1 = x - a$ e $f_2 = y - b - m(x - a)$ satisfazem a condição anterior, desde que $m \in \mathbb{F}_{q^2}$ seja tal que $m \neq \alpha^q$ (pela Proposição 6.2.7 (**2**)) e $(a, b) \in \mathcal{K}$. Neste caso, temos que, escolhido o valor de a (sendo q^2 possibilidades), o valor de b pode ser escolhido de exatamente q formas, visto que $b^q + b = a^{q+1}$ e que f_2 contém $q + 1$ pontos distintos de $\mathcal{K}$. Ainda, como $c \neq a^{q+1}$, existem $q^2 - 1$ formas de escolher seu valor. Assim, totalizam $q^3(q^2 - 1)$ possibilidades para f. Por outro lado, como a função $1/f$ tem divisor $-(f)$, segue que a mesma está também associada a um vetor minimal de $L_{\mathcal{P}}$. Desse modo, este caso 2 produz, no mínimo, $2q^3(q^2 - 1)$ vetores minimais de $L_{\mathcal{P}}$. Destacamos que a igualdade não é garantida necessariamente, tendo em vista que as retas f_1 e f_2 tomadas como acima são, somente, exemplos de retas que satisfazem as condições exigidas. Consequentemente, é possível existir outras funções com tais características.

Caso 3: Consideremos que ambas as retas f_1 e f_2 são não tangentes (da forma $y - bx + c$) e com um ponto de interseção pertencente a $\mathcal{K}$. Suponhamos que o ponto comum $(a, b) \in \mathcal{K}$ é dado. Então, as retas $f_1 = y - b - m_1(x - a)$ e $f_2 = y - b - m_2(x - a)$ satisfazem as condições acima, bastando considerar m_1 e m_2 elementos distintos em $\mathbb{F}_{q^2}$ e ambos

diferentes de a^q (Proposição 6.2.7 (**2**)). Procedendo de modo semelhante ao caso anterior, obtemos, no mínimo, $q^3(q^2-1)(q^2-2)$ possibilidades para a função f. Novamente, a igualdade não é garantida pelo fato de as retas tomadas serem apenas exemplos que cumprem as condições iniciais.

Por fim, precisamos mostrar que nenhuma das funções f foi contada duas vezes; mais precisamente, não foram inclusas em dois casos distintos. Nesse contexto, devemos provar que as formas f_1/f_2 obtidas acima são únicas. Para tanto, consideremos:

$$\frac{f_1}{f_2} = \frac{f_3}{f_4},$$

em que ambos os pares f_1, f_2 e f_3, f_4 satisfazem uma da condições do Teorema 6.4.1.

Assim $f_1f_4 - f_2f_3 = 0$ constitui uma equação polinomial nas variáveis x e y cujo grau d em y é, no máximo, 2. Como $H/\mathbb{F}_{q^2}$ não é um corpo de funções racionais, segue que d não pode ser 1. Considerando, agora, $d = 2$, vemos que o polinômio $f_1f_4 - f_2f_3$ deve ser irredutível, pois, caso contrário, y teria grau 1. Por outro lado, como o polinômio minimal de y sobre $\mathbb{F}_{q^2}(x)$ tem grau q, temos que $q = 2$. No entanto, estamos considerando $q > 2$. Logo $d \neq 2$, resultando que a única possibilidade é $d = 0$, ou seja, as funções f_i são da forma $x - a_i$ para todo $i = 1, 2, 3, 4$. Por meio de um cálculo direto, segue que $f_1 = f_3$ e $f_2 = f_4$, concluindo a unicidade das funções obtidas.

Portanto, somando o número de funções da forma $f = f_1/f_2$ satisfazendo os casos anteriores, obtemos que existem, no mínimo

$$q^2(q^2-1) + 2q^3(q^2-1) + q^3(q^2-1)(q^2-2) = q^7 - q^5 + q^4 - q^2$$

vetores minimais em $L_{\mathcal{P}}$, como queríamos. □

6.6 VOLUME E DENSIDADE DE EMPACOTAMENTO

Para o cálculo do volume do reticulado $L_{\mathcal{P}}$ sobre o corpo de funções Hermitiano, lembramos que, conforme feito no Teorema 4.1.17, sabemos que, para todo corpo de funções $F/\mathbb{F}_{q^2}$, as seguintes desigualdades se verificam:

$$vol(L_{\mathcal{P}}) \leq \sqrt{n}h_F \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g,$$

em que h_F é o número de classes de divisores de F.

Neste caso em específico, provaremos que vale a igualdade.

Teorema 6.6.1 (**Volume de** $L_{\mathcal{P}}$). *O volume do reticulado $L_{\mathcal{P}}$ é igual a* $\sqrt{q^3+1} \cdot (q+1)^{q^2-q}$.

Demonstração. Mostraremos que, ao considerarmos o corpo de funções hermitiano, garantimos que o grupo $Div^0(\mathcal{P})/Princ(\mathcal{P})$ é isomorfo ao próprio grupo da classe de divisores de grau zero, isto é, o grupo $Cl^0(H)$.

Primeiramente, afirmamos que o grupo $Cl^0(H)$ é isomorfo a $\mathbb{Z}_{q+1}^{q^2-q}$.

Para tanto, utilizaremos o estudo do L-polinômio de $H/\mathbb{F}_{q^2}$. Como já exposto, sabemos que:

$$L_H(t) = \prod_{i=1}^{2g}(1 - \alpha_i t),$$

em que os complexos α_i são inteiros algébricos, inversos das raízes de $L_H(t)$, que satisfazem $\alpha_{g+1} = \overline{\alpha_i}$.

Como o corpo de funções Hermitiano $H/\mathbb{F}_{q^2}$ é maximal, temos que $n = q^2+1+2gq$. Por outro lado, sabemos (Corolário 5.1.16 de [28]) que n satisfaz ainda:

$$n = q^2 + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Igualando tais equações, obtemos:

$$2gq = -\sum_{i=1}^{2g} \alpha_i.$$

Agora, pelo Teorema de Hasse-Weil, temos que $|\alpha_i| = q$. Assim, pela equação acima, segue que $\alpha_i = -q$ para todo $i = 1, \ldots, 2g$. Dessa forma, usando que $2g = q(q-1)$ (condição (**2**) do Teorema 6.1.6), concluímos que o L-polinômio de $H/\mathbb{F}_{q^2}$ é dado por:

$$L_H(t) = \prod_{i=1}^{2g}(1 - \alpha_i t) = (1 + qt)^{2g} = (1 + qt)^{q^2-q}.$$

Então, o número de classe de tal corpo de funções é igual a $h_H = L_H(1) = (1+q)^{q^2-q}$ e, logo, $Cl^0(H) \cong \mathbb{Z}_{q+1}^{q^2-q}$.

Por outro lado, conforme demonstrado no Teorema 7.3 de [16], temos o isomorfismo:

$$\frac{Div^0(\mathcal{P})}{Princ(\mathcal{P})} \cong \mathbb{Z}_{q+1}^{q^2-q}.$$

Destacamos que, na notação de [16], temos $M_0 = Div^0(\mathcal{P})$, $D_K^0 = Cl^0(H)$ e $N_0 = Princ(\mathcal{P})$.

Assim, obtemos:

$$\frac{Div^0(\mathcal{P})}{Princ(\mathcal{P})} \cong \mathbb{Z}_{q+1}^{q^2-q} \cong Cl^0(H).$$

Portanto, por uma abordagem análoga à feita no Teorema 4.1.17, concluímos que:

$$vol(L_{\mathcal{P}}) = \sqrt{n}h_H = \sqrt{q^3+1} \cdot (q+1)^{q^2-q}.$$

□

Corolário 6.6.2. *No caso do corpo de funções elípticas $H/\mathbb{F}_4$ dado pela equação $y^2 + y = x^3$, temos que o volume do reticulado é igual a 27.*

Demonstração. Basta notarmos que, nesse caso tal corpo de funções pode ser visto como o corpo de funções Hermitiano $H/\mathbb{F}_4$. □

Finalmente, a partir do estudo da distância mínima e do volume de $L_{\mathcal{P}}$, podemos calcular a densidade de empacotamento de tal reticulado. Nesse contexto, a fórmula obtida confirma que os reticulados em questão apresentam uma grande densidade de empacotamento ao tomarmos q (e, consequentemente, n) suficientemente grande.

Teorema 6.6.3 (Densidade de Empacotamento de $L_{\mathcal{P}}$). *A densidade de empacotamento do reticulado $L_{\mathcal{P}}$ sobre o corpo de funções Hermitiano é dada por:*

$$\Delta(L_{\mathcal{P}}) = \frac{\left(\sqrt{2q}\right)^{q^3} \omega_{q^3}}{2^{q^3}\sqrt{q^3+1}\cdot(q+1)^{q^2-q}} \tag{6.11}$$

em que ω_{q^3} é o volume da bola unitária (q^3)-dimensional na métrica euclidiana.

Demonstração. Sabemos que, por definição, a densidade do reticulado $L_{\mathcal{P}}$, cujo posto é $n-1$, é dada por:

$$\Delta(L_{\mathcal{P}}) = \frac{d(L_{\mathcal{P}})^{n-1}\omega_{n-1}}{2^{n-1}\det(L_{\mathcal{P}})^{1/2}}$$

em que ω_{n-1} é o volume da bola unitária $(n-1)$-dimensional na métrica euclidiana.

Assim, para a obtenção da equação (6.11), basta utilizarmos que $d(L_{\mathcal{P}}) = \sqrt{2q}$, $vol(L_{\mathcal{P}}) = \sqrt{q^3+1}\cdot(q+1)^{q^2-q}$ e $n = q^3 - 1$. □

REFERÊNCIAS

[1] ABDÓN, M.; QUOOS, L. *On the genera of subfields of the Hermitian function field.* Finite Fields and Their Applications v. 10, p. 271-284, Elsevier, 2004.

[2] ALVES, C. *Reticulados e Códigos.* Tese (Doutorado) - Unicamp, Campinas, 2008.

[3] BEARDON, A. F. *The geometry of discrete groups.* New York: Springer Verlag, 2012.

[4] BÖTCHER, A.; FUKSHANSKY, L.; GARCIA, S.; MAHARAJ, H. *Lattices from Hermitian Function Fields.* Journal of Algebra, v. 447, p. 560-579, Elsevier, 2016.

[5] CAMPELLO, A. *Reticulados, Projeções e Aplicações à Teoria da Informação.* Tese (Doutorado) - Unicamp, Campinas, 2014.

[6] CARLOS, T.B. *Abordagem algébrica e geométrica de reticulados.* Tese (Doutorado) - Unicamp, Campinas, 2007.

[7] CASTELLANOS, A. S.; TIZZIOTTI, G. C. *On the Automorphism Group of Generalized Hermitian Codes.* IEEE Transactions on Information Theory v. 59, p. 6642-6645, IEEE, 2013.

[8] COHN, H.; KUMAR, A.; MILLER, S. D.; RADCHENKO, D.; VIAZOVSKA, M. *The sphere packing problem in dimension 24.* Annals of Mathematics. Second series, v. 185, n. 3, p. 1017-1033, 2017.

[9] CONWAY, J.H.; SLOANE, N. J.A. *Sphere packings, lattices and groups.* Springer Science & Business Media, v. 290, 2013.

[10] DADUSH, D.; REGEV, O. *Lattices, Convexity & Algorithms: Lecture 1.* Department of Computer Science New York University, 2013. Disponível em `https://cs.nyu.edu/courses/spring13/CSCI-GA.3033-013/lectures/lecture-1.pdf`. Acesso em: 21 mar. 2019.

[11] DADUSH, D.; REGEV, O. *Lattices, Convexity & Algorithms: Lecture 3.* Department of Computer Science New York University, 2013. Disponível em `https://cs.nyu.edu/courses/spring13/CSCI-GA.3033-013/lectures/lecture-3.pdf`. Acesso em: 21 mar. 2019.

[12] DIAS, M.P.A.C. *Reticulados Bem Arredondados e Reticulados Semi-Estáveis no* $\mathbb{R}^2$. Tese (Mestrado) - Unesp, Rio Claro, 2018.

[13] FUKSHANSKY, L.; MAHARAJ, H. *Lattices from Elliptic Curves over Finite Fields.* Finite Fields and Their Applications, v. 28, p. 67-78, Elsevier, 2014.

[14] FULTON, W. *Algebraic Curves: An Introduction to Algebraic Geometry.* WA Benjamin Incorporated, 3ed, 2008.

[15] GOLDWASSER, S.; MICCIANCIO, D. *Complexity of lattice problems: a cryptographic perspective.* The Kluwer International Series in Engeneering as Computer Science, v. 671, Kluwer Academic Publishers, 2002.

[16] HISS, G. *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups.* Indagationes Mathematicae v. 15, p. 223-243, Elsevier, 2004.

[17] JORGE, G. C. *Reticulados q-ários e algébricos.* Tese (Doutorado) - Unicamp, Campinas, 2012.

[18] LIDL, R.; NIEDERREITER, H. *Finite Fields.* Cambridge University Press, v. 20, 1997.

[19] LIMA, R. F. *Topologia e Análise no Espaço* $\mathbb{R}^n$. Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

[20] MARTINET, J. *Perfect Lattices in Euclidean Spaces.* Springer Science & Business Media, v. 327, 2013.

[21] MCMULLEN, C. *Minkowski's Conjecture, Well-Rounded Lattices and Topological Dimension.* Journal of the American Mathematical Society, v. 18, p. 711-714, 2005.

[22] ROGERS, C.A. *Packing and Covering.* Cambridge University Press, 1964.

[23] ROMIK, D. *Complex Analysis Lecture Notes.* University of California at Davis, 2016.

[24] ROSENBLOOM, M.Y.; TSFASMAN, M.A. *Multiplicative lattices in global fields.* Inventiones Mathematicae v. 101, p. 687-696, Springer-Verlag, 1990.

[25] SALEHYAN, P. *Introdução às Curvas Elípticas e Aplicações.* 30º Colóquio Brasileiro de Matemática, IMPA, 2015.

[26] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves.* Springer Science & Business Media, v. 106, 2009.

[27] STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem.* Massachussets: A K Peters, 2002.

[28] STICHTENOTH, H. *Algebraic Function Fields and Codes.* Springer Science & Business Media, v. 254, 2009.

[29] VIAZOVSKA, M. S. *The sphere packing problem in dimension 8.* Annals of Mathematics. Second series, v. 185, n. 3, p. 991-1015, 2017.

[30] TSFASMAN, M.; VLADUT, S. G. *Algebraic-geometric Codes.* Springer Science & Business Media, v. 58, 2013.

[31] WALLENBORN, L. A. *Elliptic Curves, Divisors and Lines.* 2010.