MARLENNHI MAGDA MORENO VILLANUEVA

Corpos de Funções Algébricas e Códigos AG em dois pontos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

2026

MARLENNHI MAGDA MORENO VILLANUEVA

Corpos de Funções Algébricas e Códigos AG em dois pontos

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

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria algébrica.

Orientador: Prof. Dr. Alonso Sepúlveda Castellanos.

UBERLÂNDIA - MG

2026

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

V718 Villanueva, Marlennhi Magda Moreno, 1995-
2026 Corpos de Funções Algébricas e Códigos AG em dois pontos [recurso eletrônico] / Marlennhi Magda Moreno Villanueva. - 2026.

Orientador: Alonso Sepúlveda Castellanos .
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2026.228
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. I. , Alonso Sepúlveda Castellanos,1980-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

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

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 158 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.ppmat.ime.ufu.br - pgmat@ime.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 129, PPGMAT				
Data:	24/02/2026	Hora de início:	14:00	Hora de encerramento:	15:30
Matrícula do Discente:	12412MAT014				
Nome do Discente:	Marlennhi Magda Moreno Villanueva				
Título do Trabalho:	Corpos de Funções Algébricas e Códigos AG em dois pontos				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Lacunas Puras e Semigrupos de Weierstrass				

Reuniu-se na Sala 1F 119 (Sala Multiuso do Instituto de Matemática e Estatística) - Bloco 1F (Campus Santa Mônica) da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Erik Rojas Mendonza - Universidade Federal do Rio de Janeiro /UFRJ, Guilherme Chaud Tizziotti - Universidade Federal de Uberlândia / UFU e Alonso Sepúlveda Castellanos - Instituto de Matemática e Estatística - IME/UFU orientador da candidata.

Iniciando os trabalhos o presidente da mesa, Dr. Alonso Sepúlveda Castellanos , apresentou a Comissão Examinadora e a candidata, agradeceu a presença do público, e concedeu à discente a palavra para a exposição do seu trabalho.

A duração da apresentação da discente e o tempo de arguição e resposta foram conforme as normas do Programa. A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir a candidata. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidata:

Aprovada.

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

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

interna da UFU.

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

Documento assinado eletronicamente por **Erik Antonio Rojas Mendoza**, **Usuário Externo**, em 24/02/2026, às 15:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alonso Sepulveda Castellanos**, **Professor(a) do Magistério Superior**, em 25/02/2026, às 12:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 25/02/2026, às 14:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7044911** e o código CRC **8C9C4661**.

Referência: Processo nº 23117.006759/2026-31 SEI nº 7044911

Dedicatória

A Deus,

à minha família,

com amor e gratidão.

Agradecimentos

Primeiramente, agradeço ao Instituto de Matemática e Estatística da Universidade Federal de Uberlândia (IME - UFU), por me permitir fazer parte dele e acolher-me ao longo de meus estudos do mestrado, por todas as oportunidades. Especialmente, ao corpo docente do Programa de Pós-graduação em Matemática, pelos conhecimentos compartilhados e pela formação oferecida.

Agradeço ao Prof. Dr. Alonso Sepúlveda Castellanos pela orientação e paciência.

Agradeço à minha família, que foi meu principal suporte durante este período. Ao meu pai, Luis Moreno Torre, e à minha mãe, Virginia Villanueva Solorzano, pelo amor e pela tranquilidade que sempre me transmitiram. Às minhas irmãs, Margoth, Yadira e Miriam, pela motivação, pelo apoio emocional, pela fortaleza e pela confiança constantes. Aos meus avós, Elias, Pompeya e Rosalia, que em paz descansem, meus anjos, por serem minha guia. Aos meus tios, Yolanda Maguiña e Manuel Yauri, pelas palavras de incentivo para alcançar todos os meus objetivos e pelo apoio. À meu tio Benigno Maguiña e família, por sempre estar.

Agradeço aos meus amigos e colegas do mestrado, especialmente Mateus Fernando, Carlos, Victor Patrick, Silas, Matheus Felipe, Matheus Deodato, Ially, José, Fernanda e Marcos, pela ajuda, pelas conversas e os conhecimentos compartilhados.

Agradeço à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo auxílio financeiro durante o mestrado.

Moreno, V. M. M. *Corpos de Funções Algébricas e Códigos AG em dois pontos.* 2026. (121 p) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Nesta dissertação estudamos corpos de funções algébricas e sua aplicação na construção de códigos algébrico geométricos, com ênfase nos códigos de dois pontos sobre a curva norma-traço. Apresentamos os fundamentos teóricos necessários, incluindo lugares, valorizações, divisores e o Teorema de Riemann-Roch, e discutimos exemplos relevantes como os códigos Hermitianos. Por fim, investigamos os parâmetros dos códigos de dois pontos sobre a curva norma-traço, destacando suas vantagens em relação aos códigos clássicos de um ponto.

Palavras-chave: Corpos de funções algébricas, Códigos algébrico geométricos, Semigrupo de Weierstrass.

Moreno, V. M. M. *Corpos de Funções Algébricas e Códigos AG em dois pontos.* 2026. (121 p) Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Abstract

In this dissertation, we study algebraic function fields and their application to the construction of algebraic–geometric codes, with emphasis on two-point codes on the norm–trace curve. We present the necessary theoretical foundations, including places, valuations, divisors, and the Riemann–Roch Theorem, and discuss relevant examples such as Hermitian codes. Finally, we investigate the parameters of two-point codes on the norm–trace curve, highlighting their advantages over classical one-point codes.

Keywords: Algebraic function fields, Algebraic–geometric codes, Weierstrass semigroup.

Sumário

Notações

Nesta seção reunimos as principais notações utilizadas ao longo desta dissertação.

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$
$\mathbb{Z}$	Conjunto dos números inteiros.
K	Corpo de constantes.
F/K	Corpo de funções algébricas em uma variável sobre K.
$[F : K]$	Grau da extensão de corpos.
$\tilde{K}$	Corpo de constantes do corpo de funções.
$K(x)$	Corpo de funções racionais.
P, Q	Lugares do corpo de funções.
$\mathbb{F}_P$	Conjunto dos lugares do corpo de funções.
$\mathcal{O}$	Anel de valorização do corpo de funções.
v	Valorização discreta do corpo de funções.
D, G	Divisores do corpo de funções.
$Div(F)$	Conjunto de divisores do corpo de funções.
(f)	Divisor associado ao elemento $f \in F$.
$(f)_0$	Divisor de zeros associado ao elemento $f \in F$.
$(f)_\infty$	Divisor de polos associado ao elemento $f \in F$.
$Supp\, D$	Suporte do divisor D.
$\mathscr{L}(D)$	Espaço de Riemann-Roch associado ao divisor D.
$\ell(D)$	Dimensão do espaço $\mathscr{L}(D)$ sobre o corpo K.
g	Gênero do corpo de funções (ou da curva correspondente).
ω, η	Diferenciais de Weil.
$C_{\mathscr{L}}(D, G)$	Código AG associado aos divisores D e G.
$C_\Omega(D, G)$	Código AG associado as diferenciais de Weil.
d	Distância mínima do código $C_{\mathscr{L}}(D, G)$

Introdução

A teoria de códigos é utilizada em diversas áreas do conhecimento, como matemática, computação, engenharia elétrica e estatística. Na matemática, está ligada com a álgebra, onde estruturas algébricas são utilizadas para descrever e analisar códigos. Os códigos são sistemas de símbolos usados para representar informações de maneira estruturada. O objetivo desta teoria é desenvolver métodos que permitam transmitir dados de forma segura e eficiente, mesmo havendo ruído ou interferência, como erros na transmissão, bits trocados ou sinais perdidos de uma mensagem enviada por meio de rádio, internet ou satélite. Os códigos detectam e corrigem erros, recuperam a informação original e permitem reduzir o tamanho da informação, como em internet, Wi-Fi, CDs, QR codes, códigos de barras, cartões de crédito, criptografia, entre outros.

A teoria dos códigos corretores de erros, fundamental para a transmissão e o armazenamento confiável de informações, foi estudada em 1948 por Shannon [19], quem estabeleceu limites teóricos para a comunicação em canais ruidosos. Nas décadas seguintes, foram desenvolvidos métodos construtivos para códigos com bons parâmetros (comprimento, dimensão e distância mínima), com destaque para os códigos de Hamming, e posteriormente os códigos de Reed-Solomon.

No início da década de 1980, surgiu como uma generalização dos códigos lineares, a teoria dos códigos algébrico geométricos (códigos AG). Esses códigos foram introduzidos pelo matemático Valerii Goppa, cujos trabalhos permitiram construir códigos com parâmetros superiores aos limites clássicos, a partir das informações geométricas das curvas envolvidas e da teoria dos corpos de funções. Posteriormente, diversas pesquisas consolidaram a importância dos corpos de funções algébricas e das curvas com muitos pontos racionais. Nesse contexto, a curva norma-traço é uma família de curvas definidas sobre o corpo finito, que apresenta muitos pontos racionais e uma estrutura algébrica rica, sendo uma boa candidata para a construção de códigos eficientes. Desde então, os códigos AG têm sido objeto de intensa pesquisa, tanto do ponto de vista teórico quanto aplicado, com desdobramentos em áreas como criptografia, computação

quântica, autenticação e armazenamento distribuído.

Esta dissertação está baseada no livro de Stichtenoth [18]. Esse texto aborda os fundamentos da teoria de corpos de funções, divisores, espaços de Riemann-Roch e tópicos avançados. O teorema de Riemann-Roch, em particular, fornece a base para o cálculo da dimensão dos espaços de funções associados a divisores, sendo essencial para determinar os parâmetros dos códigos AG. Além disso, a estrutura dos semigrupos de Weierstrass em um ou mais pontos de uma curva desempenha papel fundamental na análise dos parâmetros dos códigos, especialmente na determinação da distância mínima e da dimensão dos códigos em dois pontos.

Nosso objetivo principal é investigar as propriedades e determinar os parâmetros dos códigos de dois pontos sobre a curva norma-traço, analisando sua relação com os códigos AG clássicos.

A dissertação está dividida em quatro capítulos principais. No primeiro capítulo, estudamos as noções preliminares de álgebra abstrata necessárias para a leitura do texto, bem como a notação que será utilizada. No segundo capítulo, apresentamos definições e resultados importantes da teoria de corpos de funções algébricas. Estudaremos os conceitos de lugares, valorizações discretas, anéis de valorização e divisores. Isso permite definir o espaço de Riemann-Roch. O principal resultado deste capítulo é o teorema de Riemann–Roch, que permite determinar a dimensão do espaço. Além disso, estudamos o corpo de funções racionais, como exemplo central. No terceiro capítulo, apresentamos definições e propriedades fundamentais sobre os códigos AG. Para isso, introduzimos a definição de códigos sobre o corpo finito $\mathbb{F}_q$, onde q é um número primo. Em seguida, discutimos os principais resultados relacionados aos códigos AG, especialmente sua dimensão e distância mínima. Além disso, apresentamos como exemplo os códigos Hermitianos, onde fazemos uma análise detalhada das suas propriedades estruturais. No quarto capítulo, abordamos os códigos de dois pontos sobre a curva norma-traço, onde exploraremos a flexibilidade adicional obtida ao considerar divisores com suporte em dois pontos racionais distintos, o que permite melhorar os parâmetros em relação aos códigos de um ponto, e como exemplo exploramos os códigos Hermitianos.

A dissertação procura oferecer uma base sólida para futuras pesquisas em álgebra, especialmente em teoria de códigos.

Marlennhi

Uberlândia-MG, 24 de fevereiro de 2026.

Capítulo 1

Preliminares

Neste capítulo, apresentamos as noções básicas que serão usadas ao longo deste trabalho. Essas definições e resultados são ferramentas importantes pois permitem estabelecer uma linguagem clara e precisa, que sustenta toda a argumentação matemática desenvolvida nos capítulos seguintes. Podem ser encontradas em livros de Álgebra ou Álgebra abstrata, tais como [10], [7], [8], [16], [17] e [18].

Em álgebra, frequentemente estudamos aplicações (homomorfismos) entre estruturas (grupos, anéis, espaços vetoriais) para comparar seus comportamentos, ou seja, para analisar semelhanças e diferenças estruturais.

Neste contexto, é relevante descrever o conjunto dos elementos da estrutura de partida que correspondem ao elemento neutro da estrutura de chegada, assim como caracterizar os elementos desta última que são atingidos. Tais descrições dão origem às noções de núcleo e imagem.

Definição 1.0.1. Sejam A, B espaços vetoriais e $\varphi : A \longrightarrow B$ uma aplicação. Então:

- O núcleo (ou kernel) da aplicação é definido por $\ker(\varphi) := \{a \in A \mid \varphi(a) = 0\}$.
- A imagem da aplicação é definida por $Im\,(\varphi) := \{\varphi(a) \in B \mid a \in A\}$.

Os conceitos de núcleo e imagem estão relacionados, e é formalizada pelo Primeiro Teorema de Isomorfismo.

Teorema 1.0.2. Seja $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então $\ker(\varphi)$ é um subgrupo normal de G e $\dfrac{G}{\ker(\varphi)} \cong Im\,(\varphi)$.

Demonstração. Veja [16, Teorema 2.18]. □

Agora, introduzimos a definição de R-módulo pois o conjunto das diferenciais de Weil, fundamentais para a definição do códigos AG, assume naturalmente a estrutura de um módulo sobre o corpo de funções.

Definição 1.0.3. Seja R um anel. Um módulo sobre R (ou R-módulo) é um grupo aditivo M, junto com uma aplicação $R \times M \to M$ tal que para cada par (x, m) com $x \in R$ e $m \in M$ associamos um elemento $xm \in M$, satisfazendo quatro condições:

i) Se e é o elemento unitário de R, então $em = m$, para todo $m \in M$.

ii) Se $x \in R$ e $m_1, m_2 \in M$, então $x(m_1 + m_2) = xm_1 + xm_2$.

iii) Se $x, y \in R$ e $m \in M$, então $(x + y)m = xm + ym$.

iv) Se $x, y \in R$ e $m \in M$, então $(xy)m = x(ym)$.

As sequências exatas ocupam um papel central na teoria de módulos, pois permitem descrever a relação entre submódulos, quocientes e homomorfismos. Elas se revelam uma ferramenta fundamental para demostrar o Teorema 2.5.7.

Definição 1.0.4. Uma sequência exata curta é uma sequência da forma $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ tal que $Im\,(\varphi) = \ker(\psi)$.

A seguir, apresentamos as definições e propriedades importantes sobre o extensão de corpo.

Definição 1.0.5. Seja K um corpo. Um corpo F é chamado de extensão de corpos de K (ou simplesmente uma extensão) se K for um subcorpo de F, e é denotado por F/K.

Se F é um corpo e $X \subset F$. Então, o subcorpo (respectivamente subanel) gerado por X é a interseção de todos os subcorpos (respectivamente subanéis) de F que contém X. Se F é uma extensão de K e $X \subset F$, então o subcorpo (respectivamente subanel) gerado por $K \cup X$ é chamado de subcorpo gerado por X sobre K, e é denotado por $K(X)$ (respectivamente $K[X]$).

- Se $X = \{u\}$, então $K(u)$ é chamado de extensão simples de K.
- Se $X = \{u_1, u_2, \ldots, u_n\}$, então o subcorpo $K(X)$ (respectivamente subanel $K[X]$) é denotado por $K(u_1, u_2, \ldots, u_n)$ (respectivamente $K[u_1, u_2, \ldots, u_n]$).

Note que, $K[u_1, u_2, \ldots, u_n]$ é um anel de polinômios em n variáveis sobre K.

Teorema 1.0.6. Se F é uma extensão do corpo K, $u, u_1, \ldots, u_n \in F$. Então

(i) O subanel $K[u]$ consiste de todos os elementos da forma $f(u)$, onde f é um polinômio com coeficientes em K. O subanel $K[u_1, \ldots, u_m]$ consiste de todos os elementos da forma $f(u_1, \ldots, u_m)$, onde f é um polinômio em m variáveis com coeficientes em K.

(ii) O subcorpo $K(u)$ consiste de todos os elementos da forma $\dfrac{f(u)}{g(u)} = f(u)g(u)^{-1}$, onde f, g são polinômios e $g(u) \neq 0$.

Definição 1.0.7. Seja F/K uma extensão de corpos. Um elemento $u \in F$ é algébrico sobre K se u é raiz de um polinômio não nulo $f \in K[x]$. Caso contrario, dizemos que u é transcendente sobre K. Se todo elemento de F é algébrico sobre K, dizemos que a extensão F/K é algébrica.

Teorema 1.0.8. Sejam F/K uma extensão de corpos e $u \in F$. Seja $\varphi : K[x] \longrightarrow F$ o homomorfismo avaliação em u, dado por $f(x) \mapsto f(u)$. Então

a) $Im(\varphi) = K[u]$ e $K \subset K[u] \subset F$.

b) u é transcendente sobre K, se e somente se, $\ker(\varphi) = \{0\}$.

c) Se u é algébrico sobre K, então $\ker(\varphi)$ é gerado por um polinômio irredutível e mônico (e portanto é um ideal maximal).

d) A aplicação $\phi : K[x]/\ker(\varphi) \longrightarrow K[u]$ definida por $\phi(f(x)) = f(u)$ é um isomorfismo. Dessa forma, se u é transcendente sobre K, então $K[u] = K[x]$ e se u é algébrico, então $K[u]$ é subcorpo de F.

Demonstração. Veja [4, Teorema V.2, Corolário V.2]. □

Definição 1.0.9. Sejam F/K uma extensão de corpos, $u \in F$ elemento algébrico sobre K e seja $\varphi : K[x] \longrightarrow F$ o homeomorfismo do teorema anterior. O gerador mônico de $\ker(\varphi)$ é chamado de polinômio minimal de u sobre K e é denotado por m_u.

Se F é uma extensão de K, então $1_F = 1_K$. Além disso, F é um espaço vetorial sobre K. A dimensão desse espaço vetorial é denotado por $[F : K]$. Dizemos que F é uma extensão de dimensão finita de K, se $[F : K]$ é finita.

Teorema 1.0.10. Sejam F/K uma extensão de corpos. Então

a) Se F/K é finita, então F/K é algébrico.

b) Se $u \in F$ é algébrico sobre K e grau $(m_u) = n$, então $\{1, u, u^2, \ldots, u^{n-1}\}$ é uma base do espaço vetorial $K[u]$ sobre K e $[K[u] : K] = n$.

c) Se $u \in F$ é transcendente, então $K[u]/K$ é uma extensão infinita.

Demonstração. Veja [8, Teorema 11.9.] e [4, Proposição V.5]. □

Teorema 1.0.11. Seja F uma extensão de E e E uma extensão de K. Então

$$[F : K] = [F : E][E : K]$$

Além disso, $[F : K]$ é finita se e somente se $[F : E]$ e $[E : K]$ são finitas.

Demonstração. Veja [7, Teorema V.1.2.]. □

Corolário 1.0.12. Seja F/K uma extensão finita. Para todo $u \in F$, tem-se que grau (m_u) divide $[F : K]$.

Corolário 1.0.13. Sejam F/K uma extensão finita e $u \in F$. Então, $F = K[u]$ se, e somente se, grau $(m_u) = [F : K]$.

Demonstração. Veja [4, Teorema V.4]. □

Corolário 1.0.14. Sejam $K \subseteq F \subseteq L$ extensões de corpos e sendo que F/K é uma extensão algébrica. Se $u \in L$ é algébrico sobre F, então u é algébrico sobre K.

Capítulo 2

Corpos de funções algébricas

Neste capítulo apresentamos os conceitos fundamentais da teoria de corpos de funções algébricas, os quais desempenham um papel central em diversas áreas da Matemática, como a teoria dos números, a geometria algébrica e a teoria de códigos.

Introduzimos as definições básicas e resultados importantes sobre anel de valorização, valorização discreta, lugares, divisores, Teorema de Riemann-Roch e algumas consequências. Além disso, estudamos como exemplo central, o corpo de funções algébricas racional. Sendo [18] o texto guia desta investigação, e complementado com as dissertações [14] e [20].

O objetivo principal é estabelecer a base teórica para os posteriores desenvolvimentos nos próximos capítulos. Dessa forma, buscamos garantir uma compreensão rigorosa e coerente da estrutura dos corpos de funções.

Os corpos de funções algébricas estão relacionados ao estudo de curvas algébricas e seus pontos. Cada lugar de um corpo de funções pode ser interpretado geometricamente como um ponto em uma curva associada. Essa perspectiva será retomada nos seguintes capítulos.

2.1 Lugares

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

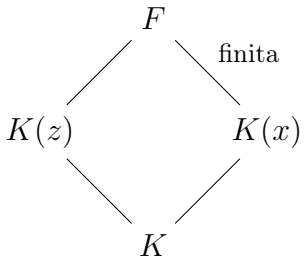
O conjunto $\tilde{K} := \{z \in F \mid z \text{ é algébrico sobre } K\}$ é um subcorpo de F, pois as somas, produtos e inversos de elementos algébricos também são algébricos e assim $\tilde{K}$ é fechado para a subtração e multiplicação de F e todo elemento não nulo em $\tilde{K}$ possui um inverso em $\tilde{K}$. O corpo $\tilde{K}$ é chamado de corpo de constantes de F/K. Como todo elemento de K é algébrico

sobre K, então $K \subseteq \tilde{K} \subseteq F$.

Seja F/K um corpo de funções. Os elementos de F que são transcendentes sobre K são caracterizados da seguinte maneira:

Proposição 2.1.2. $z \in F$ é transcendente sobre K se, e somente se, $[F : K(z)]$ é finito.

Demonstração. Seja F/K o corpo de funções algébricas. Então, F é uma extensão algébrica finita de $K(x)$ para algum $x \in F$ que é transcendente sobre K. Então dado $z \in F$, vale a inclusão $K \subset K(z) \subset F$.



($\Rightarrow$) Seja $z \in F$ transcendente sobre K. Como $F/K(x)$ é uma extensão finita então, é uma extensão algébrica. Por outro lado, como $z \in F$ temos z é algébrico sobre $K(x)$. Assim, existem $a_0(x), a_1(x), \cdots, a_m(x) \in K[x]$, onde $a_m(x) \neq 0$ tal que

$$a_0(x) + a_1(x)z + \cdots + a_m(x)z^m = 0,\ m \geq 1$$

Como z é transcendente sobre K, existe algum $i \in \{1, \cdots, m\}$ tal que $a_i(x)$ não é constante. Logo $a_0(x) + a_1(x)z + \cdots + a_m(x)z^m \in K(z)[x]$, o que implica que x é algébrico sobre $K(z)$. Desse modo, temos $[K(x, z) : K(z)] < \infty$ e como $[F : K(x, z)] < \infty$, pelo Teorema 1.0.11, obtemos $[F : K(z)] < \infty$.

($\Leftarrow$) Suponhamos que $z \in F$ é algébrico sobre K, então $[K(z) : K] < \infty$. Pela hipótese, temos $[F : K(z)] < \infty$ e assim, pelo Teorema 1.0.11 temos $[F : K] < \infty$. Novamente, pelo Teorema 1.0.11 obtemos $[K(x) : K] < \infty$, o que é uma contradição pois x é um elemento transcendente sobre K. □

Exemplo 2.1.3. Um exemplo simples de um corpo de funções algébricas é o corpo de funções racional. O corpo de funções F/K é chamado de racional se $F = K(x)$, para algum $x \in F$ transcendente sobre K. Temos

$$K(x) := \left\{ \frac{f(x)}{g(x)} \in F \middle| f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

Seja $z \in K(x)\backslash\{0\}$, então $z = \dfrac{f(x)}{g(x)}$ e z tem uma única representação da forma $z = a\prod_i p_i(x)^{n_i}$, com $0 \neq a \in K$, onde os polinômios $p_i(x) \in K[x]$ são mônicos, distintos dois a dois e irredutíveis com os $n_i \in \mathbb{Z}$.

Definição 2.1.4. Um anel de valorização do corpo de funções algébricas F/K é um anel $\mathcal{O}$ do corpo F com as seguintes propriedades:

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

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

Exemplo 2.1.5. Seja o corpo de funções racional $K(x)/K$ e seja $p(x) \in K[x]$ um polinômio irredutível. O conjunto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \middle| f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}$$

é um anel de valorização do corpo de funções $K(x)/K$.

Demonstração. Temos $\mathcal{O}_{p(x)} \subset K(x)$. Primeiro, vamos mostrar que $\mathcal{O}_{p(x)}$ é um anel.
De fato, sejam $z_1, z_2 \in \mathcal{O}_{p(x)}$, ou seja,

$$z_1 = \frac{f_1(x)}{g_1(x)} \in K(x) : f_1(x), g_1(x) \in K[x], g_1(x) \neq 0, p(x) \text{ não divide } g_1(x),$$

$$z_2 = \frac{f_2(x)}{g_2(x)} \in K(x) : f_2(x), g_2(x) \in K[x], g_2(x) \neq 0, p(x) \text{ não divide } g_2(x).$$

Logo

$$z_1 z_2 = \left(\frac{f_1(x)}{g_1(x)}\right)\left(\frac{f_2(x)}{g_2(x)}\right) = \frac{f_1(x)g_2(x) - f_2(x)g_1(x)}{g_1(x)g_2(x)} \in K(x)$$

onde $g_1(x)g_2(x) \neq 0$ e $p(x)$ não divide $g_1(x)g_2(x)$. Assim $z_1 z_2 \in \mathcal{O}_{p(x)}$, logo $\mathcal{O}_{p(x)}$ é um anel.
Agora, vamos verificar que é um anel de valorização.

(i) Seja $a \in K$. Podemos escrever $a = \dfrac{a}{1}$ e temos $p(x) \nmid 1$, uma vez que se $p(x)$ divide 1, então existe um polinômio $q(x) \in K[x]$ tal que $p(x)q(x) = 1$. Assim grau $(p(x)) = 0$. Mas, isso não é possível pois $p(x)$ é irredutível. Dessa forma, $a \in \mathcal{O}_{p(x)}$. Logo, $K \subset \mathcal{O}_{p(x)}$. Como o polinômio $p(x) \in \mathcal{O}_{p(x)}$ e $p(x) \notin K$, então $\mathcal{O}_{p(x)} \neq K$. Assim $K \subsetneq \mathcal{O}_{p(x)}$.
Por outro lado, temos $\mathcal{O}_{p(x)} \subset K(x)$. Observe que $\dfrac{1}{p(x)} \in K(x)$ mas não pertence a $\mathcal{O}_{p(x)}$, pois $p(x)$ divide a $p(x)$. Logo $\mathcal{O}_{p(x)} \neq K(x)$. Assim, $\mathcal{O}_{p(x)} \subsetneq K(x)$.
Portanto $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$.

(ii) Seja $z = \dfrac{f(x)}{g(x)} \in K(x) = F$.

- Se $p(x) \nmid g(x)$ então $z = \dfrac{f(x)}{g(x)} \in \mathcal{O}_{p(x)}$.
- Se $p(x) \mid g(x)$ então existe um polinômio $q(x) \in K[x]$ tal que $p(x)q(x) = g(x)$. Assumimos, sem perda de generalidade, que $\text{mdc}(f(x), g(x)) = 1$. Assim, $p(x)$ não divide $f(x)$. Portanto, se $p(x)$ divide $g(x)$ então $p(x)$ não divide $f(x)$, o que implica que $\dfrac{g(x)}{f(x)} \in \mathcal{O}_{p(x)}$, ou seja, o inverso de $\dfrac{f(x)}{g(x)}$ está no anel $\mathcal{O}_{p(x)}$.

□

Proposição 2.1.6. Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K. Então:

a) $\mathcal{O}$ é um anel local, isto é, o anel $\mathcal{O}$ tem um único ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^*$, onde

$$\mathcal{O}^* := \{z \in \mathcal{O} \mid \text{ existe } w \in \mathcal{O} \text{ tal que } zw = 1\}$$

é o grupo de unidades de $\mathcal{O}$.

b) Para $0 \neq x \in F$, $x \in P$ se, e somente se, $x^{-1} \notin \mathcal{O}$.

c) Para o corpo $\tilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$ de constantes de F/K, temos $\tilde{K} \subset \mathcal{O}$ e $\tilde{K} \cap P = \{0\}$

Demonstração. a) Afirmamos que $P = \mathcal{O} \setminus \mathcal{O}^*$ é um ideal de $\mathcal{O}$.

De fato, seja $P \neq \emptyset$, pois $\mathcal{O} \neq \emptyset$.

Sejam $x \in P$ e $z \in \mathcal{O}$. Suponhamos que $xz \in \mathcal{O}^*$, então existe $w \in \mathcal{O}$ tal que $(xz)w = 1$. Logo $x(zw) = 1$, ou seja, $x \in \mathcal{O}^*$. Isso é uma contradição, pois $x \in P$. Portanto $xz \in P$.

Sejam $x, y \in P$. Como $\dfrac{x}{y} \in F$, temos que $\dfrac{x}{y} \in \mathcal{O}$ ou $\dfrac{y}{x} \in \mathcal{O}$, pois $\mathcal{O}$ é um anel de valorização. Sem perda de generalidade, assumimos que $\dfrac{x}{y} \in \mathcal{O}$, e como $1 \in \mathcal{O}$ segue que $1 + \dfrac{x}{y} \in \mathcal{O}$. Assim $x + y \in P$ pois $x + y = y\left(1 + \dfrac{x}{y}\right)$, com $y \in P$. Portanto, P é um ideal de $\mathcal{O}$.

Agora, mostramos que P é o único ideal maximal de $\mathcal{O}$.

De fato, seja I um ideal de $\mathcal{O}$ tal que $P \subset I \subset \mathcal{O}$ e $P \neq I$. Assim, existe $z \in I$ tal que $z \in \mathcal{O}^*$. Como I é o ideal de $\mathcal{O}$, temos $zz^{-1} = 1 \in I$. Logo $J = \mathcal{O}$. Portanto, P é maximal.

Suponhamos que J é outro ideal maximal de $\mathcal{O}$. Se $J \subset P \subset \mathcal{O}$, então $P = J$ pois P é maximal. Se $P \subset J \subset \mathcal{O}$ então $J = \mathcal{O}$ ou $J = P$, pois P é maximal. Portanto, P é o único ideal maximal.

b) Seja $x \in F \setminus \{0\}$. Pela hipótese, temos $x \in P$. Então $x \in \mathcal{O} \setminus \mathcal{O}^*$, ou seja, $x \notin \mathcal{O}^*$. Isso implica que, $x^{-1} \notin \mathcal{O}$.

Reciprocamente, como $\mathcal{O}$ é um ideal de valorização temos que se $x \notin \mathcal{O}^*$, então $x \in \mathcal{O}$. Logo $x \in \mathcal{O} \setminus \mathcal{O}^* = P$.

c) Seja $0 \neq z \in \tilde{K} \subset F$. Suponhamos que $z \notin \mathcal{O}$. Como $\mathcal{O}$ é um anel de valorização, temos que $z^{-1} \in \mathcal{O}$. Como o inverso de um elemento algébrico é algébrico, ou seja,

z^{-1} é algébrico. Logo $z^{-1} \in \tilde{K}$. Isto é, existe um polinômio $f(x) \in K[x] \setminus \{0\}$ tal que $f(z^{-1}) = 0$. Sem perda de generalidade, temos $f(x) = a_r x^r + \cdots + a_1 x + 1$. Logo

$$\begin{aligned} 0 = f(z^{-1}) &= a_r z^{-r} + \cdots + a_1 z^{-1} + 1 \\ -1 &= a_r z^{-r} + \cdots + a_1 z^{-1} \\ z &= -\left(a_r z^{-r+1} + \cdots + a_1\right) \end{aligned}$$

e como $z^{-1} \in \mathcal{O}$, segue que $z \in \mathcal{O}$, o qual é uma contradição. Assim, $\tilde{K} \subseteq \mathcal{O}$.

Se $z \neq 0$ está em $\tilde{K}$, então o inverso de z também está. Logo, como $\tilde{K} \subseteq \mathcal{O}$, temos que $z, z^{-1} \in \mathcal{O}$, ou seja, $z \in \mathcal{O}^*$. Assim, $z \notin P$. Portanto $\tilde{K} \cap P = \{0\}$.

□

Lema 2.1.7. Seja $\mathcal{O}$ um anel de valorização do corpo de funções algébricas F/K, P seu ideal maximal e o elemento não nulo $x \in P$. Sejam $x_1, \ldots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, para $i = 1, ..., n$. Então $n \leq [F : K(x)] < \infty$.

Demonstração. Seja $0 \neq x \in P$ e $\tilde{K} \cap P = \{0\}$. Então $x \notin \tilde{K}$, ou seja, x não é algébrico sobre K. Logo, x é transcendente sobre K. Assim $[F : K(x)]$ é finito ($[F : K(x)] < \infty$).

Agora, vamos mostrar que $n \leq [F : K(x)]$. Para isso, é suficiente provar que $x_1, \ldots, x_n$ são linearmente independentes sobre $K(x)$, assim se $x_1, \ldots, x_n$ gerarem F teremos $n = [F : K(x)]$, e se não gerarem F teremos $n \leq [F : K(x)]$.

Suponhamos que $x_1, \ldots, x_n \in P$ são linearmente dependentes sobre $K(x)$, ou seja, existe uma combinação linear não trivial, isto é, existem $\phi_1, \ldots, \phi_n \in K(x)$ (não todos zeros) tais que

$$\sum_{i=1}^{n} \phi_i x_i = \phi_1 x_1 + \cdots + \phi_n x_n = 0.$$

Podemos supor que os ϕ_i são expressões polinomiais em x e que x não divide todos os ϕ_i. Se x dividisse ϕ_i, então existiria $g_i \in K[x]$ tal que $\phi_i = x g_i$, para todo $i = 1, ..., n$. Logo

$$\sum_{i=1}^{n} \phi_i x_i = \sum_{i=1}^{n} x g_i x_i = x \sum_{i=1}^{n} g_i x_i = 0$$

como $x \neq 0$, temos que $\sum_{i=1}^{n} g_i x_i = 0$.

Definimos $a_i := \phi_i(0)$ o termo constante de ϕ_i. Assim $a_1 = \phi_1(0), a_2 = \phi_2(0), \ldots, a_n = \phi_n(0)$.

Fixamos $j \in \{1, ..., n\}$ tal que $a_j \neq 0$ e $a_i = 0$ para todo $i > j$. Logo $\sum_{i \neq j}^{n} \phi_i x_i = -\phi_j x_j$, com $\phi_i \in \mathcal{O}$, para todo $i = 1, ..., n$.

Para $j > i$, pela hipótese, temos $x_i \in x_{i+1}P$, para todo $i = 1, ..., n$ e $x_1 = x$. Lembremos que

$x_{i+1}P = \{x_{i+1}z : z \in P\}$ e $x_i = x_{i+1}z, z \in P$. Assim, temos

$$\begin{aligned} 0 \neq x = x_1 \in x_2P \to x_1 = x_2z, z \in P \to x_2 \neq 0; \\ 0 \neq x_2 \in x_3P \to x_2 = x_3z, z \in P \to x_3 \neq 0, x_1 \in x_3P; \\ 0 \neq x_3 \in x_4P \to x_3 = x_4z, z \in P \to x_4 \neq 0, x_1 \in x_4P; \\ \vdots \\ 0 \neq x_{n-1} \in x_nP \to x_{n-1} = x_nz, z \in P \to x_n \neq 0. \end{aligned}$$

Além disso, $x_i = x_jP$, para todo $i < j$.

Logo, existe um elemento $x_j \neq 0$ invertível em $\mathcal{O}$. Então, de $\sum_{i\neq j}^{n} \phi_i x_i = -\phi_j x_j$ temos

$$-\phi_j = \sum_{i\neq j}^{n} \phi_i \frac{x_i}{x_j} = \sum_{i>j}^{n} \phi_i \frac{x_i}{x_j} + \sum_{i<j}^{n} \phi_i \frac{x_i}{x_j} = \sum_{i>j}^{n} x g_i \frac{x_i}{x_j} + \sum_{i<j}^{n} \phi_i \frac{x_i}{x_j}$$

Como $x, \frac{x_i}{x_j} \in P$ e $\phi_i \in \mathcal{O}$ então $\sum_{i>j}^{n} x g_i \frac{x_i}{x_j} \in P$ e $\sum_{i<j}^{n} \phi_i \frac{x_i}{x_j} \in P$. Portanto, $\phi_j \in P$.

Por outro lado, temos que $\phi_j = a_j + xg_j$, com $g_j \in K[x]$ e $x \in P$. Dai, $a_j \in P$, e como $a_j \in K$ tem-se $a_j \in P \cap K$. Mas, pela Proposição 2.1.6, temos $K \subset \tilde{K}$ e $\tilde{K} \cap P = \{0\}$, então, em particular, temos $K \cap P = \{0\}$. Isso implica uma contradição pois $a_j \neq 0$. Portanto, $x_1, \ldots, x_n \in P$ são linearmente independentes sobre $K(x)$ e deste modo $n \leq [F : K(x)]$. □

Teorema 2.1.8. Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K e $P = \mathcal{O} \setminus \mathcal{O}^*$ o seu único ideal maximal. Então:

a) P é um ideal principal.

b) Se $P = t\mathcal{O}$ então qualquer $0 \neq z \in F$ tem uma única representação da forma $z = t^n u$, para algum $n \in \mathbb{Z}$, com $u \in \mathcal{O}^*$.

c) $\mathcal{O}$ é um domínio de ideal principal. Mais precisamente, se $P = t\mathcal{O}$ e $\{0\} \neq I \subseteq \mathcal{O}$ é um ideal então $I = t^n\mathcal{O}$ para algum $n \in \mathbb{N}$.

Demonstração. a) Seja $0 \neq x_1 \in P$. Suponha que P não é ideal principal de $\mathcal{O}$. Então, $P \neq x_1\mathcal{O}$. Logo, existe $0 \neq x_2 \in P$ tal que $x_2 \notin x_1\mathcal{O}$. Isso implica que $x_1^{-1}x_2 \notin \mathcal{O}$, pois se pertencesse teríamos $x_2 = x_1x_1^{-1}x_2 \in x_1\mathcal{O}$, o qual é uma contradição pois $x_2 \in P \setminus x_1\mathcal{O}$. Portanto, pela Proposição 2.1.6(b), temos que $(x_1^{-1}x_2)^{-1} \in P$, ou seja, $x_1x_2^{-1} \in P$. Daí, $x_1x_2^{-1} = p, p \in P$. Logo $x_1 = x_2p$, o qual implica que $x_1 \in x_2P$.

Mediante a indução, geramos uma sequencia infinita $\{x_1, x_2, \ldots\}$ de elementos em P, com

$x_i \in x_{i+1}P$, para todo $i \in \mathbb{N}$. Isto, contradiz o Lema 2.1.7 uma vez que teríamos o grau da extensão $F/K(x)$ não sendo finito.

Portanto, P é ideal principal.

b) Pela hipótese, temos $P = t\mathcal{O}$. Seja $z \in F \setminus \{0\}$. Como $\mathcal{O}$ é um anel de valorização, então $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Assumimos, sem perda de generalidade, que $z \in \mathcal{O}$.

- Se $z \in \mathcal{O}^*$, ou seja, se z é um elemento invertível de $\mathcal{O}$, temos $z = t^0 z$.
- Se $z \notin \mathcal{O}^*$, ou seja, $z \in P$. Existe um $m \in \mathbb{N}$ máximo tal que $m \geq 1$ com $z = t^m z$ e considere a sequencia $z = x_1, x_2 = t^{m-1}, x_3 = t^{m-2}, \ldots, x_m = t$ com os elementos de P e com $x_i \in x_{i+1}P$, para $i = 1, \ldots, m-1$.

  Logo $z = x_1 \in x_2 P$, então $z \in t^{m-1}t\mathcal{O} = t^m\mathcal{O}$. Assim $z = t^m u$, com $u \in \mathcal{O}$. Então, pelo Lema 2.1.7 o grau da extensão é finita, ou seja, $[F : K(x)] = m$. Logo u é unidade de $\mathcal{O}$, pois caso contrario, $u \in P = t\mathcal{O}$, o qual implica que $u = tw$, com $w \in \mathcal{O}$. Daí $z = t^m tw = t^{m+1}w$, com $w \in \mathcal{O}$, ou seja, $z \in t^{m+1}\mathcal{O}$. O qual é uma contradição, pois m é máximo. Portanto, $z = t^m u$, com $u \in \mathcal{O}^*$.

Agora, mostramos a unicidade. Suponhamos que $z = t^m u$ e $z = t^n w$, com $u, w \in \mathcal{O}^*$. Considerando que $m \geq n$, teríamos $t^m u = t^n w$. Daí, $t^{m-n}uw^{-1} = 1$. Isso implica que $m = n$ e $u = w$.

c) Seja $\{0\} \neq I \subseteq \mathcal{O}$ um ideal. Vamos mostrar que $I = t^n\mathcal{O}$.

Definimos o conjunto $A := \{r \in \mathbb{N} : t^r \in I\}$.

Note que $A \neq \emptyset$, pois se $0 \neq x \in I \subseteq \mathcal{O} \subseteq F$, e pelo item b), temos $x = t^r u$, com $u \in \mathcal{O}^*$. Daí $t^r = zu^{-1} \in I$, ou seja, $r \in A$.

Como $A \subseteq \mathbb{N}$, então existe o elemento mínimo de A, chamamos $n := min(A)$. Assim $t^n \in I$ e seja $p \in \mathcal{O}$, logo $t^n p \in I$ (pois I é ideal). Desta forma $t^n\mathcal{O} \subseteq I$.

Por outro lado, seja $0 \neq y \in I$. Por b) temos que $y = t^s w$, com $w \in \mathcal{O}^*$ e $s \geq 0$. Então $t^s = yw^{-1} \in I$ e $s \geq n = min(A)$. Logo $y = t^n t^{s-n} w \in t^n\mathcal{O}$. desta forma $I \subseteq t^n\mathcal{O}$.

Portanto $I = t^n\mathcal{O}$.

□

Definição 2.1.9. Seja F/K um corpo de funções algébricas.

a) Um lugar P do corpo de funções F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Todo elemento $t \in P$ tal que $P = t\mathcal{O} = \{tp : p \in \mathcal{O}\}$ é chamado um elemento primo de P, também denominado parâmetro local, uniformizante local ou variável uniformizante.

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

Se $\mathcal{O}$ é um anel de valorização de F/K e P é seu ideal maximal, então $\mathcal{O}$ é determinado unicamente por P, isto é, $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$, pela Proposição 2.1.6(b). Assim $\mathcal{O}_P := \mathcal{O}$ é chamado o anel de valorização do lugar P ou anel de valorização associado ao lugar P.

Definição 2.1.10. Uma valorização discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ tal que possui as seguintes propriedades:

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

b) $v(xy) = v(x) + v(y)$ para todos $x, y \in F$.

c) $v(x + y) \geq \min\{v(x), v(y)\}$ para todos $x, y \in F$.

d) Existe um elemento $z \in F$ com $v(z) = 1$.

e) $v(a) = 0$ para todo $0 \neq a \in K$.

Neste contexto, o simbolo ∞ representa algum elemento que não é um valor inteiro, tal que $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ para todos m, n números inteiros.

Proposição 2.1.11. A valorização discreta é uma função sobrejetora.

Demonstração. De fato, pela propriedade a) temos $v(0) = \infty$, pela propriedade d) existe um elemento $z \in F$ tal que $v(z) = 1$ e pela propriedade e) temos que para qualquer elemento a não nulo em $K \subseteq F$ tem-se $v(a) = 0$. Em particular, para $a = 1$ temos

$$0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}).$$

Então $-v(z) = v(z^{-1})$. Assim, um número inteiro $p > 1$ pode ser expressado como

$$p = 1 + 1 + \cdots + 1 = v(z) + v(z) + \cdots + v(z) = v(zz \cdots z) = v(z^p).$$

Logo

$$-p = -v(z^p) = -v(z) - v(z) - \cdots - v(z) = v(z^{-1}) + v(z^{-1}) + \cdots + v(z^{-1}) = v(z^{-p}).$$

Assim, $\mathbb{Z} \subset v(F)$. Portanto, a valorização discreta é sobrejetiva. □

Lema 2.1.12 (Desigualdade triangular)**.** Seja v uma valorização discreta de F/K e $x, y \in F$ com $v(x) \neq v(y)$. Então, $v(x + y) = min\{v(x), v(y)\}$.

Demonstração. Seja $a \in K \setminus \{0\}$. Para todo $y \in F$, pelas propriedades b) e e), temos

$$v(ay) = v(a) + v(y) = 0 + v(y) = v(y).$$

Em particular, isto cumpre para $a = -1$, ou seja, temos $v(-y) = v(y)$.
Pela hipótese, temos $v(x) \neq v(y)$, isto é, $v(x) < v(y)$ ou $v(x) > v(y)$. Assumimos, sem perda de generalidade, que $v(x) < v(y)$.
Suponhamos que $v(x + y) \neq \min\{v(x), v(y)\} = v(x)$. Então, pela propriedade c), temos $v(x + y) \geq \min\{v(x), v(y)\} = v(x)$. Logo $v(x + y) > v(x)$. Assim

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

Daí $v(x) > v(x)$, o qual é absurdo. □

Definição 2.1.13. Para qualquer lugar P do corpo de funções algébricas F/K, associamos a função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ (que se provará ser uma valorização discreta de F/K, no Teorema 2.1.15) que é definida da seguinte forma: Escolha um elemento primo t para P. Então, pelo Teorema 2.1.8, todo $0 \neq z \in F$ tem uma representação única $z = t^n u$, com $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Definimos $v_P(z) := n$ e $v_P(0) := \infty$.

Observação 2.1.14. A Definição 2.1.13 depende somente de P, não da escolha de t.

Teorema 2.1.15. Seja F/K um corpo de funções.

a) Para cada lugar $P \in \mathbb{P}_F$, a função v_P definida em 2.1.13 é uma valorização discreta de F/K. Além disso, temos

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\},$$

$$\mathcal{O}_P^* = \{z \in F : v_P(z) = 0\},$$

$$P = \{z \in F : v_P(z) > 0\}.$$

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

c) Por outro lado, suponha que v é uma valorização discreta de F/K. Então, o conjunto $P = \{z \in F : v(z) > 0\}$ é um lugar de F/K e $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ é o anel de valorização correspondente.

d) Cada anel de valorização $\mathcal{O}$ de F/K é um subanel próprio maximal de F.

Demonstração. a) Afirmamos que v_P é uma valorização discreta.

De fato, vamos a verificar as propriedades dadas na Definição 2.1.10.

a) $v_P(x) := \infty \Leftrightarrow x = 0$, pela definição de v_P.

b) Sejam $x, y \in F$, então $x = t^n u_1$, $y = t^m u_2$, com $u_1, u_2 \in O_P^*$ e $n, m \in \mathbb{Z}$. Logo $v_P(x) = n$ e $v_P(y) = m$. Por outro lado, temos $xy = t^n u_1 t^m u_2 = t^{n+m} u_1 u_2$, com $u_1 u_2 \in \mathcal{O}_P^*$. Logo, $v_P(xy) = n + m = v_P(x) + v_P(y)$.

c) Sejam $x, y \in F$, então $x = t^n u_1$, $y = t^m u_2$, com $u_1, u_2 \in \mathcal{O}_P^*$ e $n, m \in \mathbb{Z}$. Logo $v_P(x) = n$ e $v_P(y) = m$. Assumimos, sem perda de generalidade, que $n \leq m < \infty$. Então $x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n} u_2) = t^n z$, com $z \in \mathcal{O}_P$.

- Se $z = 0$, então $x + y = 0$. Consequentemente

$$v_P(x + y) = \infty > n = min\{v_P(x), v_P(y)\}.$$

- Se $z = t^k u$ com $k \geq 0$ e $u \in \mathcal{O}_P^*$. Então $x + y = t^n(t^k u) = t^{n+k} u$. Assim,

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

d) Tomando $z = tu$ com $u \in O_P^*$, temos $v_P(z) = 1$.

e) Seja $0 \neq a \in K$. Como $K \subset \mathcal{O}_P \subset F$, então $a \in \mathcal{O}_P^*$. Logo $a = t^0 a$, ou seja, $v_P(a) = 0$.

Agora, vamos mostrar $\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\}$.

De fato, seja $0 \neq z \in \mathcal{O}_P \subset F$. Como $\mathcal{O}_P$ é um anel de valorização, temos $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$. Além disso, como $P = t\mathcal{O}_P$, pelo Teorema 2.1.8 (b), temos que $z \in F$ tem uma única representação da forma $z = t^n u$, para algum $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Logo $v_P(z) = n$.

Suponha que $z \in \mathcal{O}_P$. Vamos mostrar que $n \geq 0$.

Note que $t \in P$. Então, pela Proposição 2.1.6(b), temos que $t^{-1} \notin \mathcal{O}_p$. Isso implica que $t^{-2} \notin \mathcal{O}_p$, pois caso contrario $t^{-2}t = t^{-1} \in P$ pois P é ideal, e assim $tt^{-1} = 1 \in P$, ou seja, $P = \mathcal{O}_P$, o qual é absurdo.

Por indução, obtemos $t^{-n} \notin \mathcal{O}_p$ para todo $n \in \mathbb{N}$.

Se $z = t^n w$, com $w \in \mathcal{O}_P^*$ e $n < 0$, então $zw^{-1} = t^n \in \mathcal{O}_P$. Isto contradiz o feito acima. Portanto $n \geq 0$ e daí $v_P(z) = n \geq 0$.

Por outro lado, seja $z \in F$ tal que $v_P(z) = n \geq 0$. Então $z = t^n w$, com $w \in \mathcal{O}_P^*$. como $t \in P \subset \mathcal{O}_P$, temos que $t^n \in \mathcal{O}_P$. Logo $z \in \mathcal{O}_P$.

Agora, mostramos que $O_P^* = \{z \in F : v_P(z) = 0\}$.

De fato, seja $0 \neq z \in \mathcal{O}_P^*$. Logo $z = t^0 z$ e assim $v_P(z) = 0$.

Logo, como $P = \mathcal{O}_P \setminus \mathcal{O}_P^*$, temos

$$P = \{z \in F : v_P(z) \geq 0\} - \{z \in F : v_P(z) = 0\} = \{z \in F : v_P(z) > 0\}.$$

b) ($\Rightarrow$) Seja $x \in F$ um elemento primo para P, então $P = x\mathcal{O}_P$. Assim $P = x\mathcal{O}_P = t\mathcal{O}_P$, com t primo para P. Então $x = tw$, com $w \in \mathcal{O}_P^*$ e daí $v_P(x) = 1$.
($\Leftarrow$) Pela hipótese, temos $v_P(x) = 1$, ou seja, $x = tu$, onde $u \in \mathcal{O}_P^*$ e t é elemento primo para P. Logo $P = t\mathcal{O}_P = tu\mathcal{O}_P = x\mathcal{O}_P$, ou seja, x é elemento primo para P.

c) Seja v uma valorização discreta de F/K.
Primeiro, mostramos que $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ é o anel.

- Sejam $x, y \in \mathcal{O}_P$. Então $x, y \in F$ com $v(x) \geq 0$, $v(y) \geq 0$. Logo

$$v(xy) = v(x) + v(y) \geq 0,$$
$$v(x + y) \geq min\{v(x), v(y)\} \geq 0.$$

  Assim $xy \in \mathcal{O}_P$ e $x + y \in \mathcal{O}_P$. Portanto, $\mathcal{O}_P$ é fechado em F.

- Seja 1_F o elemento neutro para a multiplicação de F. Então, $v(1_F) = 0$ pois F é corpo. Assim, $1_F \in \mathcal{O}_P$.

- Seja 0_F o elemento neutro para a adição de F. Então, $v(0_F) = \infty \geq 0$, ou seja, $0_F \in \mathcal{O}_P$.

- Seja $-x$ o oposto aditivo do $x \in \mathcal{O}_P$. Então,

$$v(-x) = v(-1_F x) = v(-1_F) + v(x) = v(x) \geq 0.$$

  Logo $-x \in \mathcal{O}_P$.

Agora, vamos mostrar que $\mathcal{O}_P$ é um anel de valorização.

(i) $K \subsetneq \mathcal{O}_P \subsetneq F$
Seja $0 \neq a \in K$, então $v(a) = 0$. Logo $a \in \mathcal{O}_P$. Assim $K \subset \mathcal{O}_P$. Pela propriedade d), existe $z \in F$ tal que $v(z) = 1 \geq 0$. Então $z \in \mathcal{O}_P$ e $z \notin K$, ou seja, $z \in \mathcal{O}_P \setminus K$. Assim $K \subsetneq \mathcal{O}_P$.
É claro que $\mathcal{O}_P \subset F$.
Seja $x \in \mathcal{O}_P$, com $v(x) > 0$. Então $x \in F$ e $0 = v(1_F) = v(xx^{-1}) = v(x) + v(x^{-1})$. Daí $v(x^{-1}) = -v(x) < 0$. Ou seja $x^{-1} \notin \mathcal{O}_P$. Logo $\mathcal{O}_P \subsetneq F$.

(ii) Para todo $z \in F$, temos que $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$.
Seja $z \in F$. Suponha que $zz^{-1} \notin \mathcal{O}_P$. Então $0 > v(zz^{-1}) = v(1_F) = 0$, o qual é absurdo. Assim $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$.

Agora, mostramos que $P = \{z \in F : v(z) > 0\}$ é um lugar de F/K, ou seja, mostraremos que P é um ideal maximal de $\mathcal{O}_P$.

- Mostraremos que P é ideal.

  De fato, sejam $x, z \in P$ e $y \in \mathcal{O}_P$, então $v(x) > 0$, $v(z) > 0$ e $v(y) \geq 0$. Logo

  $$v(xy) = v(x) + v(y) > 0,$$
  $$v(x + z) \geq \min\{v(x), v(z)\} > 0.$$

  Assim $xy \in P$ e $x + z \in P$. Portanto, P é ideal de $\mathcal{O}_P$.

- Agora, mostramos que P é ideal maximal.

  Seja I outro ideal de $\mathcal{O}_P$ tal que $P \subset I \subseteq \mathcal{O}_P$. Como $P \neq I$, então existe $t \in I$ tal que $t \notin P$, com $v(t) = 0$. Logo, pela proposição 2.1.6(b), temos $t^{-1} \in \mathcal{O}_P$. Daí, $tt^{-1} = 1 \in I$, ou seja, $I = \mathcal{O}_P$.

d) Seja $\mathcal{O}$ o anel de valorização de F/K. Considere P o ideal maximal de $\mathcal{O}$, v_P valorização discreta associada a P e $z \in F \setminus \{0\}$. Vamos mostrar que $F = \mathcal{O}[z]$.

Seja $y \in F$.

Como $z \notin \mathcal{O}$ temos $v_P(z) < 0$ e como $\mathcal{O}$ é um anel de valorização, temos $z^{-1} \in \mathcal{O}$. Logo $v_P(z^{-1}) \geq 0$. Por outro lado $v_P(z^{-1}) = -v_P(z)$. Portanto $v_P(z^{-1}) > 0$. Assim $z^{-1} \in P = t\mathcal{O}$ e daí $z^{-1} = tp$, com $p \in \mathcal{O}$ e t elemento primo para P.

Logo, para $k \geq 0$ suficientemente grande

$$v_P(yz^{-k}) = v_P(y(tp)^k) = v_P(y) + kv_P(tp) = v_P(y) + k(1 + v_P(p))$$
$$\geq v_P(y) + k(1 + 0) = v_P(y) + k.$$

Chamando $w = yz^{-k}$ temos $w \in \mathcal{O}$ e daí $y = wz^k$. Assim $y \in \mathcal{O}[z]$. Portanto $F \subset \mathcal{O}[z]$. E como $\mathcal{O}[z] \subset F$ temos $\mathcal{O}[z] = F$.

□

De acordo ao Teorema 2.1.15, os lugares, anéis de valorização e valorizações discretas de um corpo de funções algébricas F/K são essencialmente a mesma coisa.

Sejam P um lugar de F/K e $\mathcal{O}_P$ o anel de valorização. O anel de classes de resíduos é $\mathcal{O}_P/P$ e como P é ideal maximal, então $\mathcal{O}_P/P$ é corpo.
Para $x \in \mathcal{O}_P$, definimos $x(P) \in \mathcal{O}_P/P$ como a classes de resíduos de x módulo P.
Para $x \in F \setminus \mathcal{O}_P$, tomamos $x(P) = \infty$. Note que o simbolo ∞ é definido aqui de maneira diferente como usado na Definição 2.1.10.

Pela Proposição 2.1.6(c), temos que $\tilde{K} \subset \mathcal{O}_P$ e $\tilde{K} \cap P = \{0\}$. Logo $K \cap P = \{0\}$ pois $K \subset \tilde{K}$. Também, a aplicação de classes de resíduos $\mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ induz uma injeção de K em $\mathcal{O}_P/P$. Consideremos sempre que K é subcorpo de $\mathcal{O}_P/P$ via esta injeção. Observe que este argumento também se aplica para $\tilde{K}$ em vez de K e assim podemos considerar $\tilde{K}$ como subcorpo de $\mathcal{O}_P/P$.

Definição 2.1.16. Seja $P \in \mathbb{P}_F$ (P é um lugar de F/K).

a) $F_P := \mathcal{O}_P/P$ é o corpo de classes de resíduos de P. A aplicação $x \longmapsto x(P)$ de F para $F_P \cup \{\infty\}$ é chamada de aplicação de classes de resíduos com respeito a P. As vezes também se usa a notação $x(P) := x + P$, com $x \in \mathcal{O}_P$.

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

A seguir, veremos um resultado que garante que o grau do lugar P é sempre finito.

Proposição 2.1.17. Se P é um lugar de F/K e $0 \neq x \in P$ então, grau $(P) \leq [F : K(x)] < \infty$.

Demonstração. Como $0 \neq x \in P$ e $\tilde{K} \cap P = \{0\}$, então $x \notin \tilde{K}$, ou seja, x é transcendente sobre K. Assim $[F_P : K]$ é finito.
Agora, vamos mostrar que $[F_P : K] \leq [F : K(x)]$.
Para isso, é suficiente mostrar que para quaisquer elementos $z_1, z_2, \ldots, z_n \in \mathcal{O}_P$, cujas classes de resíduos $z_1(P), z_2(P), \ldots, z_n(P) \in \mathcal{O}_P/P$ são linearmente independentes sobre K, são linearmente independentes sobre $K(x)$.
Suponhamos que $z_1, z_2, \ldots, z_n \in \mathcal{O}_P$ não são linearmente independentes, ou seja, existe uma combinação não trivial tal que

$$\sum_{i=1}^{n} \phi_i z_i = 0, \text{ com } \phi_i \in K(x), \text{ para todo } i = 1, \ldots, n.$$

Assumimos, sem perda de generalidade, que os ϕ_i são expressões polinomiais em x e nem todas são divisíveis por x, isto é, $\phi_i = a_i + x g_i$ onde $a_i \in K$ e $g_i \in K(x)$, com $a_i \neq 0$ para alguns $i \in 1, \ldots, n$.
Note que se $a_i = 0$ para todo $i \in 1, \ldots, n$, teríamos $\phi_i = x g_i$ e daí

$$\sum_{i=1}^{n} \phi_i z_i = \sum_{i=1}^{n} x g_i z_i = x \sum_{i=1}^{n} g_i z_i = 0 \ \Rightarrow \sum_{i=1}^{n} g_i z_i = 0.$$

Como $x \in P$ e $g_i \in K(x) \subseteq \mathcal{O}_P$. Logo $x g_i \in P$, pois P é um ideal. Isso implica que $\phi_i - a_i \in P$. Assim $\phi_i(P) = a_i(P) = a_i$, com $a_i \notin P$ e $a_i \in K$.

Em $\sum_{i=1}^{n} \phi_i z_i = 0$, aplicamos a função de classes de resíduos, obtendo assim

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

Como existe $a_j \neq 0$ para algum $j \in 1, \ldots, n$, segue que $z_1(P), z_2(P), \ldots, z_n(P)$ são linearmente dependentes, o qual é uma contradição.

Portanto $z_1, \ldots, z_n$ são linearmente independentes sobre $K(x)$, e logo $[F_P : K] \leq [F : K(x)]$. □

Corolário 2.1.18. O corpo $\tilde{K}$ de constantes F/K é uma extensão de corpos finita de K.

Demonstração. Usaremos o fato que $\mathbb{P}_F$ não é vazio (o qual será provado no Corolário 2.1.22). Seja P um lugar de F/K. Mediante a aplicação de classes de resíduos $\mathcal{O}_P \to \mathcal{O}_P/P$, consideramos $\tilde{K}$ subcorpo de $\mathcal{O}_P/P$. Pela Proposição 2.1.17 temos que $[\mathcal{O}_P/P : K] \leq [F : K(x)] < \infty$, para $0 \neq x \in P$. Desta forma $[\mathcal{O}_P/P : \tilde{K}] \leq \text{grau}\,(P) < \infty$. Segue disto que $\tilde{K}/K$ é uma extensão de corpos finita. □

Observação 2.1.19. Consideremos P um lugar racional de F/K, ou seja, $\text{grau}\,(P) = 1$. Então $K = \mathcal{O}_P/P = F_P$ e a aplicação de classes de resíduos leva F em $K \cup \{\infty\}$. Em particular, se K é um corpo algebricamente fechado então todos os lugares são racionais e assim todo lugar possui grau um. Neste caso, podemos representar um elemento $z \in F$ como uma função

$$\begin{aligned} z\colon \mathbb{P}_F &\longrightarrow K \cup \{\infty\} \\ P &\longmapsto z + P \end{aligned}$$

Por essa razão, F/K é chamado de corpo de funções. Os elementos de K interpretados como as funções no sentido definido acima, são funções constantes e por isto é chamado de corpo das constante de F.

Definição 2.1.20. Seja $z \in F$ e P um lugar de F/K. Dizemos que P é um zero de z se $v_P(z) > 0$; P é um polo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, P é um zero de z de ordem m; se $v_P(z) = m < 0$, P é um polo de z de ordem m.

No seguinte teorema, o Lema de Zorn é a ferramenta fundamental para a demonstração, especificamente para garantir a existência de um anel maximal em conjuntos que satisfazem a condição de cadeia.

Teorema 2.1.21. Seja F/K um corpo de funções algébricas e seja R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R. Então, existe um lugar P de F/K tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.

Demonstração. Consideremos o conjunto

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

onde $IS = \{\sum a_v s_v \mid a_v \in I, s_v \in S\}$ é um ideal de S.
Como $R \in \mathcal{F}$, temos que $\mathcal{F} \neq \emptyset$ e $\mathcal{F}$ é indutivamente ordenado por inclusão. De fato, se $\mathcal{H} \subseteq \mathcal{F}$ é um subconjunto totalmente ordenado de $\mathcal{F}$, então

$$T := \cup \{S \mid S \in \mathcal{H}\}$$

é um subanel de $\mathcal{F}$ com $R \subseteq T$. Vamos verificar que $IT \neq T$.
Suponha que $IT = T$. Temos que $1 \in T$, pois T é subanel. Então,

$$1 = \sum a_v s_v, \text{ com } a_v \in I, s_v \in T.$$

Como $\mathcal{H}$ é totalmente ordenado, existe $S_0 \in \mathcal{H}$ (S_0 subanel de F) tal que $s_1, \ldots, s_n \in S_0$. Assim

$$1 = \sum_{v=1}^{n} a_v s_v \in IS_0$$

o qual é uma contradição. Portanto, $T \in \mathcal{F}$ e T é majorante de $\mathcal{H}$.
Pelo Lema de Zorn, $\mathcal{F}$ possui um elemento maximal, isto é, existe um anel $\mathcal{O} \subseteq F$ tal que $R \subseteq \mathcal{O} \subseteq F$ e $I\mathcal{O} \neq \mathcal{O}$ e $\mathcal{O}$ é maximal com respeito dessas propriedades. Vamos mostrar $\mathcal{O}$ é um anel de valorização de F/K.
Como $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$ temos que $\mathcal{O} \subsetneq F$ e $I \subseteq \mathcal{O} \setminus \mathcal{O}^*$.
Seja $z \in F$. Suponha que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Então $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Assim, existem $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ tais que

$$\sum_{i=0}^{n} a_i z^i = 1 \text{ e } \sum_{i=0}^{m} b_i z^{-i} = 1$$

Note que $n, m \geq 1$, pois caso contrario $a_0 = 1$ e $b_0 = 1$, ou seja, $1 \in I\mathcal{O}$ o que implicaria $I\mathcal{O} = \mathcal{O}$. Suponhamos que m e n são os menores inteiros positivos e que $n \geq m$. Logo, multiplicando por $(1 - b_0)$ à primeira equação e por $a_n z^n$ à segunda equação, obtemos:

$$\begin{aligned} 1 - b_0 &= \sum_{i=0}^{n} (1 - b_0) a_i z^i \\ &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \end{aligned}$$

e

$$
\begin{aligned}
a_n z^n &= \sum_{i=0}^{m} (a_n z^n) b_i z^{-i} \\
a_n z^n &= (a_n z^n) b_0 + (a_n z^n) b_1 z^{-1} + (a_n z^n) b_2 z^{-2} + \cdots + (a_n z^n) b_m z^{-m} \\
a_n z^n &= a_n b_0 z^n + a_n b_1 z^{n-1} + a_n b_2 z^{n-2} + \cdots + a_n b_m z^{n-m} \\
0 &= -a_n z^n + a_n b_0 z^n + a_n b_1 z^{n-1} + a_n b_2 z^{n-2} + \cdots + a_n b_m z^{n-m} \\
0 &= a_n (b_0 - 1) z^n + a_n b_1 z^{n-1} + a_n b_2 z^{n-2} + \cdots + a_n b_m z^{n-m}.
\end{aligned}
$$

Agora, somando ambas equações

$$
\begin{aligned}
1 - b_0 &= (1 - b_0) a_0 + (1 - b_0) a_1 z + \cdots + (1 - b_0) a_n z^n - a_n (1 - b_0) z^n + \sum_{i=0}^{m} a_n b_i z^{n-i} \\
1 - b_0 &= (1 - b_0) a_0 + (1 - b_0) a_1 z + \cdots + (1 - b_0) a_{n-1} z^{n-1} + \sum_{i=1}^{m} a_n b_i z^{n-i} \\
1 &= b_0 + (1 - b_0) a_0 + (1 - b_0) a_1 z + \cdots + (1 - b_0) a_{n-1} z^{n-1} + \sum_{i=1}^{m} a_n b_i z^{n-i} \\
1 &= \underbrace{b_0 + (1 - b_0) a_0}_{c_0} + \underbrace{(1 - b_0) a_1}_{c_1} z + \cdots + \underbrace{a_{n-1}(1 - b_0)}_{c_{n-1}} z^{n-1},
\end{aligned}
$$

onde $c_i \in I\mathcal{O}$, mas isso é uma contradição pois n é mínimo. Assim, para todo $z \in F$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Portanto, $\mathcal{O}$ é anel de valorização. □

O seguinte corolário garante que todo $z \in F$ tal que $z \notin \tilde{K}$ possui pelo menos um zero e um polo.

Corolário 2.1.22. Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então z tem pelo menos um zero e pelo menos um polo. Em particular, $\mathbb{P}_F$ não é vazio.

Demonstração. Considere o anel $R = K[z]$ e $I = zK[z]$ é o ideal de R.
De fato, $I \neq \emptyset$ pois $z = z.1 \in I$, com $1 \in K \subset K(z)$ e dados $x, y \in I$, $h \in R$ temos que $x = zf$ e $y = zg$, com $f, g \in K[z]$. Então $x + y = z(f + g)$ e $xh = zfh$, com $f + g, fh \in K[z]$. Assim $x + y \in I$ e $xh \in I$. Portanto I é um ideal de R.
Assim temos o anel $R = K[z]$ de F, com $k \subseteq K[z] = R \subseteq F$ e $I = zK[z]$ ideal próprio não nulo de $R = K[z]$. Então, pelo Teorema 2.1.21, existe um lugar P de F/K tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Como $z \in I$, então $z \in P$. Logo, pelo Teorema 2.1.15, temos $v_p(z) > 0$. Portanto, P é um zero de z.
Por outro lado, temos que z é transcendente sobre K, logo z^{-1} é transcendente sobre K. Então $K[z^{-1}]$ é anel de F e $zK[z^{-1}]$ é ideal de $K[z^{-1}]$. Logo, pelo Teorema 2.1.21, existe um lugar Q

de F/K tal que $z^{-1} \in Q$. Logo, pela Proposição 2.1.6(b), temos $z \notin \mathcal{O}_Q$, ou seja, $v_P(z) < 0$. Portanto Q é um polo de z. □

2.2 Corpo de funções algébricas racional

Na seção anterior, estudamos corpos de funções para um corpo arbitrário. Agora, vamos estudar valorizações e lugares no caso do corpo de funções algébricas racional, ou seja, quando $F = K(x)$, onde x transcendente sobre K.

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

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \middle| f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\} \tag{2.1}$$

de $K(x)/K$, com ideal maximal dado por

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \middle| f(x), g(x) \in K[x], p(x) \text{ divide } f(x), p(x) \text{ não divide } g(x) \right\}. \tag{2.2}$$

No Exemplo 2.1.5, verificamos que $\mathcal{O}_{p(x)}$ é um anel de valorização de $K(x)/K$.
No caso particular, quando o polinômio $p(x)$ é linear, ou seja, $p(x) = x - \alpha$, com $\alpha \in K$, podemos abreviar e escrever $P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}$.

Existe outro anel de valorização de $K(x)/K$ dado por

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in K[x], \text{grau}\,(f(x)) \leq \text{grau}\,(g(x)) \right\} \tag{2.3}$$

com ideal maximal dado por

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in K[x], \text{grau}\,(f(x)) < \text{grau}\,(g(x)) \right\} \tag{2.4}$$

Agora vamos a verificar que $\mathcal{O}_\infty$ é um anel de valorização de $K(x)/K$.

(i) $K \subsetneq \mathcal{O}_\infty \subsetneq K(x)$
Seja $a \in K$. Logo $a = \dfrac{a}{1} \in \mathcal{O}_\infty$, pois grau $(a) = 0 =$ grau (1); e $K \neq \mathcal{O}_\infty$, pois $\dfrac{1}{x} \in \mathcal{O}_\infty$ mas não pertence a K, pois caso contrario, teríamos $x \in K$, ou seja, x seria algébrico sobre K, o que significaria uma contradição pois x é transcendente. Também, $\mathcal{O}_\infty \neq K(x)$ pois $x \in K(x)$ e $x \notin \mathcal{O}_\infty$, caso contrario grau $(1) \geq$ grau (x).

(ii) Seja $z \in K(x)$. Então $z = \dfrac{f(x)}{g(x)}$.
Suponha que $z \notin \mathcal{O}_\infty$, assim grau $(f(x)) >$ grau $(g(x))$. Logo $z^{-1} = \dfrac{g(x)}{f(x)} \in \mathcal{O}_\infty$.

P_∞ é chamado de lugar infinito de $K(x)$. Observe que estos rótulos dependem da escolha especifica do elemento x que origina $K(x)/K$. Por exemplo $K(x) = K\left(\frac{1}{x}\right)$ e o lugar infinito com respeito a $\frac{1}{x}$ é o lugar P_0 com respeito a x.
De fato,

$$\begin{aligned}
P_\infty &= \left\{ \frac{f\left(\frac{1}{x}\right)}{g\left(\frac{1}{x}\right)} \mid f\left(\frac{1}{x}\right), g\left(\frac{1}{x}\right) \in K\left[\frac{1}{x}\right], \text{grau}\left(f\left(\frac{1}{x}\right)\right) < \text{grau}\left(g\left(\frac{1}{x}\right)\right) \right\} \\
&= \left\{ \frac{a_0 + a_1\left(\frac{1}{x}\right) + \cdots + a_n\left(\frac{1}{x}\right)^n}{b_0 + b_1\left(\frac{1}{x}\right) + \cdots + b_m\left(\frac{1}{x}\right)^m} \mid b_m \neq 0, m > n \right\} \\
&= \left\{ \frac{\left(\frac{1}{x}\right)^n (a_0x^n + a_1x^{n-1} + \cdots + a_n)}{\left(\frac{1}{x}\right)^m (b_0x^m + b_1x^{m-1} + \cdots + b_m)} \mid b_m \neq 0, m > n \right\} \\
&= \left\{ (x)^{(m-n)} \frac{\tilde{f(x)}}{\tilde{g(x)}}; x \nmid \tilde{g(x)}, m > n \right\} = P_0.
\end{aligned}$$

Proposição 2.2.1. Seja $F = K(x)$ o corpo de funções racional.

a) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ um lugar definido por (2.2), onde $p(x)$ é um polinômio irredutível. Então $p(x)$ é um elemento primo para P e a valorização discreta correspondente v_P pode ser descrita da seguinte forma: Se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n \frac{f(x)}{g(x)}$, com $n \in \mathbb{Z}$, $f(x), g(x) \in K(x)$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo de classes de resíduos $K(x)_P = \mathcal{O}_P/P$ é isomorfo a $K(x)/\langle p(x)\rangle$, e o isomorfismo está dado por

$$\begin{array}{rcl} \phi\colon K(x)/\langle p(x)\rangle & \longrightarrow & K(x)_P \\ f(x) \mod p(x) & \longmapsto & f(x)(P) \end{array}$$

Consequentemente grau $(P) =$ grau $(p(x))$.

b) No caso especial $p(x) = x - \alpha$, com $\alpha \in K$, o grau do lugar $P = P_\alpha$ é igual a um, e a aplicação de classes de resíduos está dada por $z(P) = z(\alpha)$, para $z \in K(x)$ onde $z(\alpha)$ é definido da seguinte forma: escreva $z = \frac{f(x)}{g(x)}$ com polinômios $f(x), g(x) \in K[x]$ primos entre si. Então,

$$z(\alpha) = \begin{cases} \frac{f(\alpha)}{g(\alpha)}, \text{ se } g(\alpha) \neq 0; \\ \infty, \text{ se } g(\alpha) = 0. \end{cases}$$

c) Seja $P = P_\infty$ o lugar infinito de $K(x)/K$ definido por (2.4). Então grau de P_∞ é igual a um, e um elemento primo para P_∞ é $t = \dfrac{1}{x}$. A valorização discreta correspondente v_∞ está dada por

$$v_\infty\left(\frac{f(\alpha)}{g(\alpha)}\right) = \text{grau}\,(g(x)) - \text{grau}\,(f(x))$$

onde $f(x), g(x) \in K[x]$. A aplicação de classes de resíduos correspondente para P_∞ é definida da seguinte forma: se

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}, \text{ com } a_n, b_m \neq 0$$

Então

$$z(\infty) = \begin{cases} \dfrac{a_n}{b_m}, \text{ se } n = m; \\ 0, \text{ se } n < m; \\ \infty, \text{ se } n > m. \end{cases}$$

d) K é todo o corpo de constantes de $K(x)/K$.

Demonstração. a) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$, com $p(x) \in K[x]$ irredutível. O ideal $P_{p(x)}$ esta contida no anel de valorização $\mathcal{O}_{p(x)}$. Como $p(x) = (p(x))^1 \cdot 1$, então $v_P(p(x)) = 1$. Assim, $p(x)$ é primo para P, pelo Teorema 2.1.15(2).

Consideremos o homomorfismo

$$\begin{aligned} \phi\colon K[x] &\longrightarrow K(x)_P \\ f(x) &\longmapsto f(x) + P \end{aligned}$$

Determinamos o núcleo

$$\begin{aligned} \ker(\phi) &= \{f(x) \in K[x]; \phi(f(x)) = 0\} = \{f(x) \in K[x]; f(x) + P = 0\} \\ &= \{f(x) \in K[x]; f(x) \in P\} = \langle p(x) \rangle. \end{aligned}$$

Agora, verificamos que ϕ é sobrejetora.

Dado $z \in \mathcal{O}_{p(x)}$. Escrevemos $z = \dfrac{u(x)}{v(x)}$, onde $u(x), v(x) \in K[x]$ e $p(x) \nmid v(x)$. Logo $mdc(p(x), v(x)) = 1$ e existem $a(x), b(x) \in K[x]$ tal que

$$a(x)p(x) + b(x)v(x) = 1.$$

Assim,

$$z = z \cdot 1 = \frac{u(x)}{v(x)}(a(x)p(x) + b(x)v(x)) = \frac{u(x)}{v(x)}(a(x)p(x)) + u(x)b(x).$$

Aplicando a função de classes de resíduos, temos

$$z(P) = z + P = (u(x)b(x)) + P \in Im(\phi).$$

Logo, pelo teorema do isomorfismo, temos

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

Consequentemente, grau $(P) := [K(x)_P : K] = \text{grau}\,(p(x))$.

b) Temos $P = P_\alpha$ e pelo item (a), grau $(P_\alpha) = \text{grau}\,(p(x)) = 1$. Se $f(x) \in K[x]$. Então $p(x) \mid (f(x) - f(\alpha))$, ou seja, $x - \alpha \mid (f(x) - f(\alpha))$. Aplicando a função de classes de resíduos, temos $f(x)(P) = \underbrace{(f(x) - f(\alpha))(P)}_{\in P_\alpha} + f(\alpha)(P) = f(\alpha)(P)$.
Seja $z \in \mathcal{O}_{p(x)}$, então $z = \dfrac{f(x)}{g(x)}$, onde $f(x), g(x) \in K[x]$ e $p(x) = x - \alpha \nmid g(x)$.
Logo $g(x)(P) = g(\alpha) \neq 0$ e assim

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

Se $g(\alpha) = 0$, temos $z(\alpha) = \infty$.

c) Como $F = K(x)$, temos que grau $(P) = [F_{P_\infty} : K] = 1$.
Vamos a mostrar que v_∞ é uma valorização discreta.

i) $v_\infty\left(\dfrac{f(x)}{g(x)}\right) = \infty \Leftrightarrow \text{grau}\,(g(x)) - \text{grau}\,(f(x)) = \infty \Leftrightarrow \text{grau}\,(f(x)) = -\infty$. Logo $f(x) = 0$, o que implica que $\dfrac{f(x)}{g(x)} = 0$.

ii) Consideramos $\dfrac{f_1(x)}{g_1(x)}$ e $\dfrac{f_2(x)}{g_2(x)}$, então

$$\begin{aligned} v_\infty\left(\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)}\right) &= v_\infty\left(\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}\right) \\ &= \text{grau}\,(g_1(x)g_2(x)) - \text{grau}\,(f_1(x)f_2(x)) \\ &= \text{grau}\,(g_1(x)) + \text{grau}\,(g_2(x)) - \text{grau}\,(f_1(x)) - \text{grau}\,(f_2(x)) \\ &= \text{grau}\,(g_1(x)) - \text{grau}\,(f_1(x)) + \text{grau}\,(g_2(x)) - \text{grau}\,(f_2(x)) \\ &= v_\infty\left(\frac{f_1(x)}{g_1(x)}\right) + v_\infty\left(\frac{f_2(x)}{g_2(x)}\right). \end{aligned}$$

iii) Consideramos $\frac{f_1(x)}{g_1(x)}$ e $\frac{f_2(x)}{g_2(x)}$, então

$$\begin{aligned} v_\infty\left(\frac{f_1(x)}{g_1(x)}+\frac{f_2(x)}{g_2(x)}\right) &= v_\infty\left(\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)}\right) \\ &= \text{grau}\,(g_1(x)g_2(x)) - \text{grau}\,(f_1(x)g_2(x)+f_2(x)g_1(x)) \\ &\geq \text{grau}\,(g_1(x)g_2(x)) - \max\{\text{grau}\,(f_1(x)g_2(x)), \text{grau}\,(f_2(x)g_1(x))\} \\ &= \text{grau}\,(g_1(x)) + \text{grau}\,(g_2(x)) - \max\{\text{grau}\,(f_1(x)) + \text{grau}\,(g_2(x)), \\ &\quad \text{grau}\,(f_2(x)) + \text{grau}\,(g_1(x))\} \\ &= \min\{\text{grau}\,(g_1(x)) - \text{grau}\,(f_1(x)), \text{grau}\,(g_2(x)) - \text{grau}\,(f_2(x)) \\ &= \min\left\{v_\infty\left(\frac{f_1(x)}{g_1(x)}\right), v_\infty\left(\frac{f_2(x)}{g_2(x)}\right)\right\}. \end{aligned}$$

iv) Basta tomar $\frac{1}{x} \in K(x)$, pois $v_\infty\left(\frac{1}{x}\right) = \text{grau}\,(x) - \text{grau}\,(1) = 1$.

v) Seja $a \in K$, então $a = \frac{a}{1}$. Logo $v_\infty(a) = \text{grau}\,(1) - \text{grau}\,(a) = 0$.

Portanto v_∞ é uma valorização discreta.

Agora, vamos a mostrar que $t = \frac{1}{x}$ é elemento primo para P_∞.

Note que $t = \frac{1}{x} \in P_\infty$. Considere $z = \frac{f(x)}{g(x)} \in P_\infty$, ou seja, $\text{grau}\,(f(x)) < \text{grau}\,(g(x))$.

Assim $z = \frac{1}{x}\frac{xf(x)}{g(x)}$. Note que $\text{grau}\,(f(x)) \leq \text{grau}\,(g(x))$. Isso implica que $\frac{xf(x)}{g(x)} \in \mathcal{O}_\infty$.

Assim, $z \in \frac{1}{x}\mathcal{O}_\infty$. Portanto, $\frac{1}{x}$ é um gerador do lugar infinito, isto é, t é primo para P_∞.

d) Seja P um lugar de $K(x)/K$, de grau igual a um (podemos considerar $P = P_\alpha$, com $\alpha \in K$. Então $K(x)_P = K$. Temos $\tilde{K} \subseteq K(x)$. Considerando o homomorfismo do item (a), temos $K \subseteq \tilde{K} \subseteq K(x)_P = K$. Portanto $K = \tilde{K}$.

□

Teorema 2.2.2. Não existem outros lugares do corpo de funções racional $K(x)/K$ diferente dos lugares $P_{p(x)}$ e P_∞.

Demonstração. Seja P um lugar de $K(x)/K$. Temos duas possibilidades:

Caso 1: Suponha que $x \in \mathcal{O}_P$. Então $K[x] \subseteq \mathcal{O}_P$.

Definimos $I := K[x] \cap P$. Assim, I é um ideal de $K[x]$, e mais, é primo. Assim, a aplicação de classe de resíduos induz uma injeção $\frac{K[x]}{I} \hookrightarrow K(x)_P$, o que garante que $I \neq \{0\}$.

Logo, existe um polinômio mônico e irredutível $p(x) \in K[x]$ tal que

$$I = K[x] \cap P = f(x)K[x].$$

Agora, dado $g(x) \in K[x]$, com $p(x) \nmid g(x)$ temos $g(x) \notin I$, e como $g(x) \in K[x]$ devemos ter que $g(x) \notin P$. Logo, pela Proposição 2.1.6(b), temos $g(x)^{-1} \in \mathcal{O}_P$. Logo

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

Dado que os anéis de valorização são subanéis próprios e maximais de $K(x)$, portanto, $\mathcal{O}_{p(x)} = \mathcal{O}_P$. Assim, o lugar P coincide com o lugar $P_{p(x)}$.

Caso 2: Suponha que $x \notin \mathcal{O}_P$. Então $x^{-1} \in \mathcal{O}_P$. Logo $K[x^{-1}] \subseteq \mathcal{O}_P$. Além disso, pela Proposição 2.1.6(b), $x^{-1} \in P$. Daí $x^{-1} \in P \cap K[x^{-1}]$ e $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$.

Logo, temos que

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \middle| f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \mid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + \cdots + a_n x^{-n}}{b_0 + \cdots + b_m x^{-m}} \middle| b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} \middle| b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \middle| u(x), v(x) \in K[x], \text{grau}\,(u(x)) \leq \text{grau}\,(v(x)) \right\} = \mathcal{O}_\infty.
\end{aligned}$$

Pela maximalidade do anel de valorizações, $\mathcal{O}_P = \mathcal{O}_\infty$. Logo, segue que $P = P_\infty$. Portanto, $P = P_{p(x)}$ ou $P = P_\infty$. □

Corolário 2.2.3. Os lugares de $K(x)/K$ de grau um estão em correspondência biunívoca com $K \cup \{\infty\}$.

2.3 Independência de valorizações

O principal resultado desta seção é o teorema da aproximação fraca, chamada também como teorema da independência.

Teorema 2.3.1 (Teorema da Aproximação Fraca)**.** Sejam F/K um corpo de funções e $P_1, \ldots, P_n$ lugares dois a dois distintos de F/K; sejam $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então, existe algum elemento $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$, para $i = 1, \ldots, n$.

Demonstração. Para simplificar, vamos considerar $v_i = v_{P_i}$. A demonstração deste teorema é construtiva e é feita em vários passos:

- **Passo 1:** Existe algum $u \in F$ com $v_1(u) > 0$ e $v_i(u) < 0$, para $i = 2, \ldots, n$.

  De fato, por indução.

  Para $n = 2$: Como $P_1 \neq P_2$ temos $\mathcal{O}_{P_1} \not\subseteq \mathcal{O}_{P_2}$ e $\mathcal{O}_{P_2} \not\subseteq \mathcal{O}_{P_1}$, pois os anéis de valorização

são anéis maximais de F. Assim, podemos encontrar $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Logo $v_1(y_1) \geq 0$, $v_1(y_2) < 0$, $v_2(y_1) < 0$ e $v_2(y_2) \geq 0$.
Definimos $u := \dfrac{y_1}{y_2}$, então

$$v_1(u) = v_1(y_1) - v_1(y_2) > 0 \text{ e } v_2(u) = v_2(y_1) - v_2(y_2) < 0.$$

Para $n > 2$: Usamos a hipótese de indução: existe um elemento $y \in F$ tal que $v_1(y) > 0$ e $v_2(y) < 0, \ldots, v_{n-1}(y) < 0$.

- Se $v_n(y) < 0$ a demonstração está concluída.
- No caso em que $v_n(y) \geq 0$, escolhemos $z \in F$ tal que $v_1(z) > 0$ e $v_n(z) < 0$.
  Definimos $u := y + z^r$, com $r \geq 1$ é escolhido da forma que $rv_i(z) \neq v_i(y)$, para todo $i = 1, \ldots, n-1$. Daí, segue que $v_1(u) = v_1(y + z^r) \geq \min\{v_1(y), rv_1(z)\} > 0$, e como $rv_i(z) \neq v_i(y)$, pelo Lema 2.1.12 temos,

  $$v_i(u) = v_1(y + z^r) = \min\{v_i(y), rv_i(z)\} < 0$$

  para todo $i = 2, \ldots, n$.

- **Passo 2:** Existe algum $w \in F$ tal que $v_1(w-1) > r_i$ e $v_i(w) > r_i$, para $i = 2, \cdots, n$.
  Considere u como no passo 1 e defina $w = (1+u^s)^{-1}$. Para $s \in \mathbb{N}$ suficientemente grande

  $$\begin{aligned} v_1(w-1) &= v_1\left((1+u^s)^{-1} - 1\right) = v_1\left(-u^s(1+u^s)^{-1}\right) \\ &= v_1(-u^s) - v_1(1+u^s). \end{aligned}$$

  Como $u \in P_1 \subseteq \mathcal{O}_{P_1}$ e $\mathcal{O}_{P_1}$ é um anel local, então $1 + u^s \in \mathcal{O}_{P_1}^*$. Logo $v_1(1+u^s) = 0$. Assim $v_1(w-1) = v_1(u^s) = sv_1(u) > 0$. Portanto, para s suficientemente grande temos

  $$v_1(w-1) = sv_1(u) > r_1.$$

  Agora, analisamos $v_i(w)$, para $i = 2, \ldots, n$.
  Como $w = (1+u^s)^{-1}$ então $v_i(w) = -v_i(1+u^s)$. Assim,

  $$v_i(1+u^s) = \min\{v_i(1), sv_i(u)\} = sv_i(u) < 0$$

  o que implica que $v_i(w) = -sv_i(u) > 0$. Logo, para s suficientemente grande $v_i(w) > r_i$.

- **Passo 3:** Dados $y_1, \ldots, y_n \in F$, existe $z \in F$ tal que $v_i(z - y_i) > r_i$, para todo $i = 2, \ldots, n$.
  Considere $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s$, para todo $i, j \in \{1, \ldots, n\}$. Pelo passo 2, existem

$w_1, \ldots, w_n \in F$ com $v_i(w_i - 1) > r_i - s$ e $v_i(w_j) > r_i - s$, para $j \neq i$.

Definimos $z := \sum_{j=1}^{n} y_j w_j$, logo

$$\begin{aligned} v_i(z - y_i) &= v_i\left(\sum_{j=1}^{n} y_j w_j - y_i\right) = v_i\left((y_i w_i - y_i) + \sum_{j \neq i}^{n} y_j w_j\right) \\ &= v_i\left(y_i(w_i - 1) + \sum_{j \neq i}^{n} y_j w_j\right) \\ &\geq \min\left\{v_i(y_i) + v_i(w_i - 1), v_i\left(\sum_{j \neq i}^{n} y_j w_j\right)\right\} \\ &\geq \min\left\{v_i(y_i) + v_i(w_i - 1), \min_{j \neq i}\{v_i(y_i) + v_i(w_j)\}\right\} > r_i. \end{aligned}$$

Finalmente, fazemos a demonstração do teorema.

Dados $x_1, \ldots, x_n \in F$. Pelo Passo 3, existe um elemento $z \in F$ tal que $v_i(z - x_i) > r_i$, para todo $i = 1, \ldots, n$. Escolhemos $z_i \in F$ tal que $v_i(z_i) = r_i$ (basta um elemento de valor r_i em F). Para $z_1, \ldots, z_n \in F$, pelo Passo 3, existe $z' \in F$ tal que $v_i(z' - x_i) > r_i$, para todo $i = 1, \ldots, n$. Então

$$v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i.$$

Definindo $x := z + z'$ temos $v_i(x - x_i) = v_i((x - x_i) + z') = \min\{v_i(z - x_i), v_i(z')\} = r_i$. □

Corolário 2.3.2. Todo corpo de funções possui infinitos lugares.

Demonstração. Seja F/K o corpo de funções algébricas. Suponhamos que F/K possui finitos lugares, ou seja, $P_1, \ldots, P_n$ são todos os lugares do corpo de funções. Pelo Teorema 2.3.1, existe algum elemento $0 \neq x \in F$ com $v_{P_i}(x) > 0$, para $i = 1, \ldots, n$. Então, x é transcendente sobre K, uma vez que possui zeros, mas x não tem polos, o que contradiz ao Corolário 2.1.22. □

Proposição 2.3.3. Seja F/K corpo de funções algébricas e $P_1, \ldots, P_n$ zeros do elemento $x \in F$. Então

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \text{grau}\,(P_i) \leq [F : K(x)]$$

Demonstração. Denotamos $v_i = v_{P_i}$, $f_i = \text{grau}\,(P_i)$ e $e_i = v_i(x)$.

No Teorema 2.3.1, considere $x_k = 0$, para todo $k = 1, \ldots, n$, $r_i = 1$, $r_k = 0$ para todo $k \neq i$. Então, para cada i, existe $t_i \in F$ tal que

$$v_i(t_i) = 1 \ , \ v_k(t_i) = 0 \ \forall k \neq i.$$

Para cada i fixo, escolhamos $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ formam uma base de F_{P_i} sobre K.

Fixamos i, j. Consideremos $x_i = s_{ij}$ e $x_k = 0$, para todo $k \neq i$. Aplicando o Teorema 2.3.1, existem $z_{ij} \in F$ tal que $v_k(z_{ij} - x_k) = r_k$; $k = 1, \ldots, f_i$, isto é, se $k = i$ temos

$$v_i(z_{ij} - x_i) = v_i(z_{ij} - s_{ij}) = r_i = 1$$

e se $k \neq i$ temos

$$v_k(z_{ij} - x_k) = v_k(z_{ij} - 0) = v_k(z_{ij}) = e_k.$$

Como $v_i(z_{ij} - s_{ij}) = 1 > 0$, então $z_{ij} - s_{ij} \in P_i$.

Como $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ é uma base de F_{P_i}, então $s_{ij}(P_i) \neq 0(P_i)$, para todo j. Dessa forma $s_{ij} \notin P_i$, para todo j, tal que $z_{ij} - s_{ij} \in P_i$. Logo $z_{ij}(P_i) = s_{ij}(P_i)$. Portanto $z_{i1}(P_i), \ldots, z_{if_i}(P_i)$ é uma base de F_{P_i}, para todo j.

Afirmamos que os elementos $t_i^a z_{ij}$, $1 \leq i \leq r$, $1 \leq j \leq f_i$, $0 \leq a < e_i$ são linearmente independentes sobre $K(x)$. Temos um total de $\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} \text{grau}\,(P_i) \cdot v_i(x)$ elementos.

Suponhamos que os elementos $t_i^a z_{ij}$ são linearmente dependentes. Assim existe uma combinação linear não trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija} t_i^a z_{ij} = 0, \text{ onde } \varphi_{ija} \in K(x). \tag{3.1}$$

Sem perda de generalidade, podemos supor que $\varphi_{ija} \in K[x]$ e nem todo φ_{ija} é divisível por x. Assim, existem $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$ tais que

$$x \mid \varphi_{ija}, \text{ para todo } a < c \text{ e para } j \in \{1, \ldots, f_k\}, \tag{3.2}$$

$$x \nmid \varphi_{kjc}, \text{ para algum } j \in \{1, \ldots, f_k\}. \tag{3.3}$$

Multiplicando a equação (3.1) por t_k^{-c} obtemos

$$0 = \sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija} t_i^a z_{ij} t_k^{-c} \tag{3.4}$$

$$= \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{kja} t_k^{a-c} z_{kj} + \sum_{i \neq k} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija} t_i^a z_{ij} t_k^{-c}. \tag{3.5}$$

Agora, aplicando a valorização discreta $v_k = v_{p_k}$ na equação (3.4).

Note que $\varphi_{ija} \in K[x]$; $K \subsetneq \mathcal{O}_{P_k}$, $x \in P_k$. Assim $K[x] \subseteq \mathcal{O}_{P_k}$. Logo $v_k(\varphi_{ija}) \geq 0$. Logo

- Para $i \neq k$ temos

$$\begin{aligned} v_k(\varphi_{ija} t_i^a z_{ij} t_k^{-c}) &= v_k(\varphi_{ija}) + v_k(t_i^a) + v_k(z_{ij} + v_k(t_k^{-c}) \\ &\geq 0 + a v_k(t_i) + v_k(z_{ij}) - c v_k(t_k) \\ &= a \cdot 0 + e_k - c \cdot 1 = e_k - c > 0. \end{aligned}$$

- Para $i = k$ temos

$$\begin{aligned} v_k(\varphi_{kja} t_k^a z_{kj} t_k^{-c}) &= v_k(\varphi_{kja} t_k^{a-c} z_{kj}) = v_k(\varphi_{kja}) + v_k(t_k^{a-c}) + v_k(z_{kj}) \\ &\geq 0 + (a-c) v_k(t_k) + e_k = (a-c) \cdot 1 + e_k \\ &\geq e_k - c > 0. \end{aligned}$$

Logo, da equação 3.5, obtemos:

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} = -\left(\sum_{j=1}^{f_k} \sum_{a \neq c}^{e_i - 1} \varphi_{kja} t_k^{a-c} z_{kj} + \sum_{i \neq k} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \varphi_{ija} t_i^a z_{ij} t_k^{-c} \right) = -S. \tag{3.6}$$

Assim $v_k(S) > 0$. Isso implica que $\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k$. Logo $\sum_{j=1}^{f_k} \varphi_{kjc}(P_k) z_{kj}(P_k) = 0(P_k) = 0$ sobre K. Mas, existe $j \in \{1, \ldots, f_k\}$ tal que $\varphi_{kjc} = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$, com $\alpha_0 \neq 0$. Então

$$\varphi_{kjc}(P_k) = \alpha_0(P_k) = \alpha_0 \in K.$$

Assim, obtivemos uma combinação linear não trivial de elementos da base de $\mathcal{O}_{P_i}/P_i$, o que implica uma contradição. □

2.4 Divisores

A partir daqui, F/K denotará um corpo de funções algébricas em uma variável, tal que K é o corpo de constantes de F/K, ou seja, $K = \tilde{K}$.

Definição 2.4.1. O grupo divisor de F/K é definido como o grupo abeliano livre gerado pelos lugares de F/K e é denotado por $Div(F)$. Os elementos de $Div(F)$ são chamados de divisores de F/K. Em outras palavras, um divisor é uma soma formal

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ com } n_P \in \mathbb{Z} \text{ e quase todos } n_P = 0.$$

O suporte de D está definido como $Supp\, D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$.

Algumas vezes, será conveniente escrever $D = \sum_{P \in S} n_P P$, onde $S \subset \mathbb{P}_F$ é um conjunto finito com $Supp\, D \subset S$.

Definição 2.4.2. Se D é um divisor tal que $D = P$, para $P \in \mathbb{P}_F$, então D é chamado de divisor primo.

Dados dois divisores $D = \sum_{P\in\mathbb{P}_F} n_P P$ e $D' = \sum_{P\in\mathbb{P}_F} n'_P P$, definimos a adição

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

e o elemento neutro é o divisor $0 := \sum_{P\in\mathbb{P}_F} n_P P$, onde $n_P = 0$, para todo P.

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P\in\mathbb{P}_F} n_P P \in Div(F)$, definimos $v_Q(D) := n_Q$; logo

$$Supp\, D = \{P \in \mathbb{P}_F \mid v_p(D) \neq 0\} \text{ e } D = \sum_{P\in Supp\, D} v_P(D)P.$$

Definição 2.4.3. Uma ordem parcial em $Div(F)$ é definida por

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2), \text{ para todo } P \in \mathbb{P}_F.$$

Se $D_1 \leq D_2$ e $D_1 \neq D_2$ simplesmente podemos escrever $D_1 < D_2$, e se $D \geq 0$ dizemos que D é um divisor positivo ou efetivo.

Definição 2.4.4. Seja $D \in Div(F)$, o grau do divisor D é definido como

$$\text{grau } D := \sum_{P\in\mathbb{P}_F} v_P(D) \cdot \text{grau}\,(P).$$

Definição 2.4.5. Seja $0 \neq x \in F$ e denotamos por $\mathcal{Z}$ o conjunto de zeros e $\mathcal{N}$ o conjunto de polos de x em $\mathbb{P}_F$. Então definimos

$$(x)_0 := \sum_{P\in\mathcal{Z}} v_P(x)P, \text{ o divisor de zeros de } x,$$
$$(x)_\infty := \sum_{P\in\mathcal{N}} (-v_P(x))P, \text{ o divisor de polos de } x,$$
$$(x) := (x)_0 - (x)_\infty, \text{ o divisor principal de } x.$$

Note que, dado $P \in \mathcal{Z}$ um zero de x, temos $v_P(x) > 0$ e assim $(x)_0 \geq 0$. E dado $P \in \mathcal{N}$ um polo de x, temos $v_P(x) < 0$, logo $-v_P(x) > 0$ e portanto $(x)_\infty \geq 0$ e

$$(x) = \sum_{P\in\mathbb{P}_F} v_P(x)P. \tag{2.5}$$

Os elementos $0 \neq x \in F$ os quais são constantes, são caracterizados por

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

De fato, se $x \in K = \tilde{K}$, então $x \notin P$, pois $K \cap P = \{0\}$. Assim, $x \in \mathcal{O}_P^*$. Logo, pelo Teorema 2.1.15, tem-se $v_p(x) = 0$, para todo $P \in \mathbb{P}_F$. Isso implica, $(x) = 0$. Reciprocamente, se $(x) = 0$, temos $v_P(x) = 0$ para todo lugar P de F/K e assim x não é transcendente sobre K, pois se fosse teria pelo menos um zero e um polo, logo $x \in K = \tilde{K}$.

Definição 2.4.6. O conjunto de divisores $Princ(F) := \{(x) \mid 0 \neq x \in F\}$ é chamado de grupo dos divisores principais de F/K.

Este é um subgrupo de $Div(F)$, pois dado $0 \neq x, y \in F$, temos

$$\begin{aligned}(x) + (y) &= \sum_{P \in \mathbb{P}_F} v_P(x)P + \sum_{P \in \mathbb{P}_F} v_P(y)P = \sum_{P \in \mathbb{P}_F} (v_P(x) + v_P(y))P \\ &= \sum_{P \in \mathbb{P}_F} v_P(xy)P = (xy).\end{aligned}$$

O grupo quociente

$$Cl(F) := Div(F)/Princ(F)$$

é chamado grupo das classes dos divisores. Para um divisor $D \in Div(F)$, o elemento correspondente no grupo quociente $Cl(F)$ é denotado por $[D]$.

Definição 2.4.7. Dois divisores $D, D' \in Div(F)$ são equivalentes e se escreve $D \sim D'$ se $[D] = [D']$, isto é, $D = D' + (x)$, para algum $x \in F \setminus \{0\}$. ($D \sim D' \Leftrightarrow [D] = [D']$ é uma relação de equivalência).

Definição 2.4.8. Dado $A \in Div(F)$, o espaço de Riemann-Roch associado ao divisor A é definido por

$$\mathscr{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

Observação 2.4.9. Seja $A \in Div(F)$. Então,

a) $x \in \mathscr{L}(A) \iff v_P(x) \geq -v_P(A)$, para todo $P \in \mathbb{P}_F$.

b) $\mathscr{L}(A) \neq \{0\} \iff$ existe $A' \in Div(F)$ tal que $A' \sim A$ e $A' \geq 0$.

Demonstração. a) Dado $P \in \mathbb{P}_F$,

$$\begin{aligned}x \in \mathscr{L}(A) &\iff (x) \geq -A \iff \sum_{P \in \mathbb{P}_F} v_P(x)P \geq -\sum_{P \in \mathbb{P}_F} v_P(A)P \\ &\iff \sum_{P \in \mathbb{P}_F} v_P(x)P \geq \sum_{P \in \mathbb{P}_F} (-v_P(A))P \iff v_P(x)P \geq -v_P(A), \forall P \in \mathbb{P}_F.\end{aligned}$$

b) Seja $A \in Div(F)$,

$$\begin{aligned}\mathscr{L}(A) \neq \{0\} &\iff \text{existe } x \in \mathscr{L}(A) \text{ com } x \neq 0 \\ &\iff (x) \geq -A \iff (x) + A \geq 0.\end{aligned}$$

Assim, basta tomar $A' = (x) + A$ para ter $A' \sim A$ e $A' \geq 0$.

□

Lema 2.4.10. Seja $A \in Div(F)$. Então:

a) $\mathscr{L}(A)$ é um espaço vetorial sobre K.

b) Se $A \sim A'$, então $\mathscr{L}(A) \simeq \mathscr{L}(A')$, como espaços vetoriais.

Demonstração. a) Sejam $x, y \in \mathscr{L}(A)$ e $a \in \mathbb{K}$. Para todo $P \in \mathbb{P}_F$ temos

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A),$$
$$v_P(ax) = v_P(a) + v_P(x) \geq -v_P(A),$$

e pela Observação 2.4.9(a), temos $x+y \in \mathscr{L}(A)$ e $ax \in \mathscr{L}(A)$.

b) Pela hipótese, $A = A' + (z)$, para algum $0 \neq z \in F$.
Considere a aplicação

$$\begin{aligned} \phi\colon \mathscr{L}(A) &\longrightarrow F \\ x &\longmapsto xz \end{aligned}$$

- ϕ é linear.
  Sejam $x, y \in \mathscr{L}(A)$ e $\lambda \in K$ temos

$$\phi(x+\lambda y) = (x+\lambda y)z = xz + \lambda yz = \phi(x) + \lambda\phi(y).$$

- A imagem de ϕ está contida no $\mathscr{L}(A')$.

$$\begin{aligned} x \in \mathscr{L}(A) &\iff (x) + A \geq 0 \iff (x) + (z) + A' \geq 0 \\ &\iff (xz) \geq -A' \iff xz \in \mathscr{L}(A') \iff \phi(x) \in \mathscr{L}(A') \\ &\iff Im(\phi) \subseteq \mathscr{L}(A'). \end{aligned}$$

Agora, definimos a seguinte aplicação

$$\begin{aligned} \phi'\colon \mathscr{L}(A') &\longrightarrow F \\ x &\longmapsto xz^{-1} \end{aligned}$$

ϕ' é linear e a imagem de ϕ' está contida no $\mathscr{L}(A)$. Além disso,

$$(\phi \circ \phi')(x) = \phi(xz^{-1}) = xz^{-1}z = x, \ \forall x \in \mathscr{L}(A'),$$
$$(\phi' \circ \phi)(x) = \phi'(xz) = xzz^{-1} = x, \ \forall x \in \mathscr{L}(A).$$

Portanto ϕ é um isomorfismo entre $\mathscr{L}(A)$ e $\mathscr{L}(A')$.

□

Lema 2.4.11. Seja $A \in Div(F)$.

a) $\mathscr{L}(0) = K$.

b) Se $A < 0$ então $\mathscr{L}(A) = \{0\}$.

Demonstração. a) Para $0 \neq x \in K$ temos $(x) = 0$, logo $x \in \mathscr{L}(0)$ e isso implica que $K \subset \mathscr{L}(0)$. Por outro lado, se $0 \neq x \in \mathscr{L}(0)$ então $(x) \geq 0$ e assim $v_P(x) \geq 0$ para todo lugar P. Logo, x não possui polos e então, pelo Corolário 2.1.22, x não pode ser transcendente sobre K. Assim $x \in \tilde{K} = K$. Portanto $\mathscr{L}(0) \subset K$.

b) Suponha que existe um elemento $x \neq 0$ em $\mathscr{L}(A)$, para $A < 0$. Assim $(x) \geq -A > 0$ e com isso $x \in K = \tilde{K}$ sendo então transcendente sobre K. Além disso, $(x) > 0$ implica que x não possui polos, o qual é absurdo.

□

Lema 2.4.12. Sejam $A, B \in Div(F)$ e $A \leq B$. Então $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ e

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \text{grau } B - \text{grau } A.$$

Demonstração. Seja $x \in \mathscr{L}(A)$. Então $(x) \geq -A$ e como pela hipótese $A \leq B$, logo temos $(x) \geq -B$. Logo $x \in \mathscr{L}(B)$. Portanto $\mathscr{L}(A) \subseteq \mathscr{L}(B)$.
Como $B \geq A$, temos $B = A + P$, para algum lugar $P \in \mathbb{P}_F$. O caso geral segue por indução. Escolhemos $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + 1$.
Seja a aplicação

$$\begin{aligned} \psi\colon \mathscr{L}(B) &\longrightarrow F_P \\ x &\longmapsto xt + P \end{aligned}$$

ψ está bem definida, pois para cada $x \in \mathcal{L}(B)$, temos $v_P(x) \geq -v_P(B)$, pela Observação 2.4.9, ou seja, $v_P(x) \geq -v_P(t)$. Então $v_P(x) + v_P(t) \geq 0$. Assim $v_P(xt) \geq 0$. Logo $xt \in \mathcal{O}_P$.
Além disso, ψ é linear sobre K, pois trata-se de operações envolvendo lugares e valorizações.
Determinamos o núcleo da aplicação

$$\begin{aligned} \ker(\psi) &= \{x \in \mathscr{L}(B) \mid \psi(x) = 0\} = \{x \in \mathscr{L}(B) \mid xt + P = 0\} \\ &= \{x \in \mathscr{L}(B) \mid xt \in P\} = \{x \in \mathscr{L}(B) \mid v_P(xt) > 0\} \\ &= \{x \in \mathscr{L}(B) \mid v_P(x) + v_P(t) > 0\} = \{x \in \mathscr{L}(B) \mid v_P(x) > v_P(t)\} \\ &= \{x \in \mathscr{L}(B) \mid v_P(x) \geq v_P(A)\} = \{x \in \mathscr{L}(B) \mid x \in \mathscr{L}(A)\} = \mathscr{L}(A). \end{aligned}$$

Assim, ψ induz um isomorfismo $\mathscr{L}(B)/\mathscr{L}(A) \longrightarrow Im(\psi)$ e como $Im(\psi) \subseteq F_P$ então

$$\dim(\mathscr{L}(B)/\mathscr{L}(A)) \leq \dim(F_P) = \text{grau}\,(P) = \text{grau}\,(B - A) \leq \text{grau}\,(B) - \text{grau}\,(A).$$

□

Proposição 2.4.13. Para cada $A \in Div(F)$, o espaço vetorial $\mathscr{L}(A)$ tem dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos, então

$$\dim(\mathscr{L}(A)) \leq \text{grau}\,(A_+) + 1.$$

Demonstração. Seja $A \in Div(F)$. Pelo Lema 2.4.10(a), temos que $\mathscr{L}(A)$ é um espaço vetorial sobre o corpo K. Mostraremos que $\mathscr{L}(A)$ tem dimensão finita.
Pela hipótese $A = A_+ - A_-$, com A_+ e A_- divisores positivos, então $A \leq A_+$. Pela hipótese $A_+ \geq 0$, logo, pelo Lema 2.4.12, segue

$$\dim(\mathscr{L}(A_+)/\mathscr{L}(0)) \leq \text{grau } A_+ - \deg 0 = \text{grau } A_+.$$

Agora, pelo Lema 2.4.11, temos que $\mathscr{L}(0) = K$, ou seja, $\dim(\mathscr{L}(0)) = \dim K = 1$. Daí, temos

$$\begin{aligned}\dim(\mathscr{L}(A)) &\leq \dim(\mathscr{L}(A_+)) = \dim(\mathscr{L}(A_+)) - \dim(\mathscr{L}(0)) + 1 \\ &= \dim(\mathscr{L}(A_+)/\mathscr{L}(0)) + 1 \leq \text{grau}\,(A_+) + 1.\end{aligned}$$

Portanto $\dim(\mathscr{L}(A)) \leq \text{grau}\,(A_+) + 1$. □

Definição 2.4.14. Seja $A \in Div(F)$. A dimensão do espaço de Riemann-Roch associado ao divisor A é definida por

$$\ell(A) := \dim(\mathscr{L}(A)).$$

Teorema 2.4.15. Todos os divisores principais possuem grau zero. Mais precisamente, para todo $x \in F/K$, $(x)_0$ o divisor de zeros de x e $(x)_\infty$ o divisor de polos de x. Então

$$\text{grau } (x)_0 = \text{grau } (x)_\infty = [F : K(x)].$$

Demonstração. Sejam $[F : K(x)] = n$ e $B := (x)_\infty = \sum_{i=1}^{r}(-v_{P_i}(x))P_i = \sum_{i=1}^{r}(v_{P_i}(x^{-1}))P_i$, onde $P_1, \cdots, P_r$ são todos os polos de x. Assim, P_i é um zero de x^{-1}. Logo, pela Proposição 2.3.3 tem-se

$$\text{grau } B = \sum_{i=1}^{r}(v_{P_i}(x^{-1})) \cdot \text{grau}\,(P_i) \leq [F : K(x)] = n.$$

Assim grau $B \leq n$. Mostramos agora que grau $B \geq n$.
Como $[F : K(x)] = n$, escolhemos uma base $\{u_1, \ldots, u_n\}$ de $F/K(x)$ e um divisor $C \geq 0$ tal que $(u_j) \geq -C$, para todo $j = 1, \ldots, n$.
Seja $m \geq 0$. Note que, para $0 \leq t \leq m$ e $j = 1, \ldots, n$ temos

$$\begin{aligned}v_P(x^t u_j) &= t v_P(x) + v_P(u_j) \geq -t v_P(B) - v_P(C) \\ &\geq -m v_P(B) - v_P(C) \geq v_P(mB + C).\end{aligned}$$

Assim $x^t u_j \in \mathscr{L}(mB + C)$.

Como $u_1, \ldots, u_n$ são linearmente independentes sobre $K(x)$, então $u_1, \ldots, u_n$ são linearmente sobre K. Isto implica, que os $x^t u_j$ são linearmente independentes sobre K, para $0 \leq t \leq m$ e $j = 1, \ldots, n$.

Portanto, $\ell(mB + C) = \dim(\mathscr{L}(mB + C)) \geq n(m + 1)$, para $m \geq 0$.

Consideremos $c :=$ grau C. Pela Proposição 2.4.13, para todo $m \geq 0$, temos

$$\begin{aligned} \ell(mB + C) &\leq m \,\text{grau}\, B + c + 1 \\ n(m + 1) \leq \ell(mB + C) &\leq m \,\text{grau}\, B + c + 1 \\ nm + n - c - 1 &\leq m \,\text{grau}\, B \\ n - c - 1 &\leq m(\text{grau}\, B - n). \end{aligned}$$

Para m suficientemente grande, temos grau $B \geq n$. Portanto grau $B = n$.

Por outro lado, como $(x)_0 = (x^{-1})_\infty$, concluímos que

$$\text{grau}\ (x)_0 = \text{grau}\ (x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$$

e como $(x) = (x)_0 - (x)_\infty$ então grau $(x) = 0$. □

Corolário 2.4.16. Sejam $A, A' \in \text{Div}(F)$

a) Se $A \sim A'$. Então $\ell(A) = \ell(A')$ e grau $A =$ grau A'.

b) Se grau $A < 0$, então $\ell(A) = 0$.

c) Se grau $A = 0$, então são equivalentes:

   (i) A é principal;

   (ii) $\ell(A) \geq 1$;

   (iii) $\ell(A) = 1$.

Demonstração. a) Como $A \sim A'$, pelo Lema 2.4.10(b), $\mathscr{L}(A)$ e $\mathscr{L}(A')$ são isomorfos como espaços vetoriais sobre K e portanto tem a mesma dimensão, ou seja, $\ell(A) = \ell(A')$.
Por outro lado, como $A \sim A'$, pela definição, temos $A = A' + (x)$ para algum $x \in F \setminus \{0\}$. Pelo Teorema 2.4.15, temos grau $(x) = 0$, o que implica que grau $A =$ grau A'.

b) Suponha que $\ell(A) > 0$, ou seja, $\mathscr{L}(A) \neq \{0\}$. Então, pela Observação 2.4.9(b), existe $A' \in Div(F)$ tal que $A \sim A'$ e $A' \geq 0$, logo $A > 0$. Assim grau $A \geq 0$, o que contradiz a hipótese. Portanto $\ell(A) = 0$.

c) Seja $A \in Div(F)$.

(i) $\implies$ (ii): Pela hipótese, A é um divisor principal, então $A = (x)$ para $x \in F \setminus \{0\}$ e como

$$(x^{-1}) = \sum_{P \in \mathcal{Z}} v_P(x^{-1})P - \sum_{P \in \mathcal{N}} v_P(x^{-1})P = -\sum_{P \in \mathcal{Z}} v_P(x)P + \sum_{P \in \mathcal{N}} v_P(x)P = -(x)$$

então, $x^{-1} \in \mathscr{L}(A)$. Logo $\dim(\mathscr{L}(A)) \geq 1$. Portanto $\ell(A) \geq 1$.

(ii) $\implies$ (iii): Pela hipótese, temos $\ell(A) \geq 1$. Assim $\mathscr{L}(A) \neq \{0\}$, logo pela Observação 2.4.9(b), existe $A' \in Div(F)$ tal que $A \sim A'$ e $A' \geq 0$ e pelo item (a) deste corolário, temos grau $A' =$ grau $A = 0$, e como $A' \geq 0$, então $A' = 0$. Assim

$$\ell(A) = \ell(0) = \ell(\mathscr{L}(0)) = \ell(K) = 1.$$

(iii) $\implies$ (i): Temos $\ell(A) = 1$ e grau $A = 0$. Então $\mathscr{L}(A) \neq \{0\}$. Logo existe $z \in \mathscr{L}(A) \setminus \{0\}$ e assim $(z) + A \geq 0$. Dai, pelo Teorema 2.4.15, temos grau $(z) = 0$ e isso implica que grau $((z) + A) = 0$. Logo $(z) + A = 0$, ou seja, $A = -(z) = (z^{-1})$. Portanto A é divisor principal.

□

Proposição 2.4.17. Existe $\gamma \in \mathbb{Z}$ tal que, para todo $A \in \mathrm{Div}(F)$, vale

$$\text{grau } A - \ell(A) \leq \gamma.$$

Demonstração. Sejam $A_1, A_2 \in Div(F)$. Suponhamos que $A_1 \leq A_2$, pelo Lema 2.4.12, temos $\mathscr{L}(A_1) \subseteq \mathscr{L}(A_2)$ e

$$\begin{aligned}
\dim(\mathscr{L}(A_2)/\mathscr{L}(A_1)) &\leq \text{grau } A_2 - \text{grau } A_1 \\
\dim(\mathscr{L}(A_2)) - \dim(\mathscr{L}(A_1)) &\leq \text{grau } A_2 - \text{grau } A_1 \\
\ell(A_2) - \ell(A_1) &\leq \text{grau } A_2 - \text{grau } A_1 \\
\text{grau } A_1 - \ell(A_1) &\leq \text{grau } A_2 - \ell(A_2).
\end{aligned}$$

Fixamos $x \in F \setminus K$ e consideremos $B = (x)_\infty$ o divisor específico,

$$B := (x)_\infty = \sum_{P \in \mathcal{N}}^{r} (-v_P(x))P$$

onde $\mathcal{N}$ é o conjunto dos polos de x em $\mathbb{P}_F$. Pelo que fizemos na demonstração do Teorema 2.4.15, existe $c \geq 0$ tal que $\ell(mB + C) \geq (m + 1)$ grau B, para todo $m \geq 0$, e pelo Lema 2.4.12

temos $\ell(mB + C) \leq \ell(mB) + \text{grau } C$. Logo

$$\begin{aligned}(m+1)\,\text{grau } B &\leq \ell(mB) + \text{grau } C\\ m\,\text{grau } B + \text{grau } B - \text{grau } C &\leq \ell(mB)\\ \text{grau}\,(mB) + [F : K(x)] - \text{grau } C &\leq \ell(mB).\end{aligned}$$

Considerando $\gamma = \text{grau } C - [F : K(x)] \in \mathbb{Z}$, obtemos

$$\text{grau}\,(mB) - \ell(mB) \leq \gamma.$$

Agora, mostraremos que a desigualdade é válida quando substituirmos mB por $A \in Div(F)$ qualquer.

Afirmação: Dado $A \in Div(F)$, existem $A_1, D \in Div(F)$ e existem $m \geq 0$ tal que $A \leq A_1$, $A_1 \sim D$ e $D \leq mB$.

De fato, seja $A_1 \in Div(F)$, com $A_1 \geq 0$ e $A_1 \geq A$. Pelo Lema 2.4.12, para m suficientemente grande, temos

$$\begin{aligned}\ell(mB - A_1) &\geq \ell(mB) - \text{grau } A_1\\ &\geq \text{grau}\,(mB) - \gamma - \text{grau } A_1 > 0.\end{aligned}$$

Logo, existe $0 \neq z \in \mathscr{L}(mB - A_1)$. Assim, definimos $D := A_1 - (z)$, e então $A_1 \sim D$. Como $z \in \mathscr{L}(mB - A_1)$ temos

$$\begin{aligned}A_1 - D = (z) &\geq -(mB - A_1)\\ A_1 - D &\geq -mB + A_1\\ D &\leq mB.\end{aligned}$$

Agora, pela Afirmação, temos

$$\text{grau } A - \ell(A) \leq \text{grau } A_1 - \ell(A_1) = \text{grau } D - \ell(D) \leq \text{grau}\,(mB) - \ell(mB) \leq \gamma.$$

□

Definição 2.4.18. O gênero g do corpo de funções F/K é definido por

$$g := \max\{\text{grau } A - \ell(A) + 1 \mid \ A \in Div(F)\}.$$

Pela Proposição 2.4.17, o conjunto $\{\text{grau } A - \ell(A) + 1 \mid \ A \in Div(F)\}$ é limitado superiormente pelo número inteiro $\gamma + 1$. Assim o gênero g é um número finito.

Observação 2.4.19. O gênero g de F/K é um inteiro não negativo.

Demonstração. Consideremos $A = 0$, então grau $A - \ell(A) + 1 = 0 - \ell(K) + 1 = 0$ e assim $g \geq 0$. □

Teorema 2.4.20 (Teorema de Riemann)**.** Seja F/K um corpo de funções de gênero g. Então:

(a) Para todo divisor $A \in \mathrm{Div}(F)$, $\ell(A) \geq \text{grau } A + 1 - g$.

(b) Existe um inteiro c, dependendo de F/K, tal que $\ell(A) = \text{grau } A + 1 - g$, sempre que grau $A \geq c$.

Demonstração. a) Seja $A \in \mathrm{Div}(F)$. Pela definição de gênero temos

$$g \geq \text{grau } A - \ell(A) + 1 \implies \ell(A) \geq \text{grau } A + 1 - g.$$

b) Seja $A_0 \in \mathrm{Div}(F)$ com $g \geq \text{grau } A_0 - \ell(A_0) + 1$. Definimos $c := \text{grau } A_0 + g$.
Se grau $A \geq c$, então pelo item (a), temos

$$\begin{aligned}\ell(A - A_0) &\geq \text{grau}\,(A - A_0) + 1 - g = \text{grau } A - \text{grau } A_0 + 1 - g \\ &= \text{grau } A + 1 - g \geq c + 1 - c = 1.\end{aligned}$$

Logo $\mathscr{L}(A - A_0) \neq \{0\}$. Assim, existe $0 \neq z \in \mathscr{L}(A - A_0)$, isto é, $(z) + A - A_0 \geq 0$.
Considere o divisor $A' = A + (z)$, pois $A' \sim A$. Então $A' \geq A_0$. Como $A' \sim A$, obtemos

$$\begin{aligned}\text{grau } A - \ell(A) &= \text{grau } A' - \ell(A') \\ \text{grau } A - \ell(A) &\geq \text{grau } A_0 - \ell(A_0) = g - 1 \\ \ell(A) &\leq \text{grau } A + 1 - g.\end{aligned}$$

e portanto, pelo item (a), temos $\ell(A) = \text{grau } A + 1 - g$.

□

Exemplo 2.4.21. O gênero do corpo de funções racional $K(x)/K$ é zero.

Demonstração. Consideremos o lugar P_∞ (definido na equação (2.4)). Pela Proposição 2.2.1(c), tem-se grau $(P_\infty) = 1$.
Considere, para $r \geq 0$, o espaço vetorial $\mathscr{L}(rP_\infty)$.
Note que, para $0 \leq i \leq r$ tem-se

$$(x^i) + rP_\infty = i(x) + rP_\infty = iP_0 - iP_\infty + rP_\infty = i(x) + rP_\infty = iP_O + (r - i)P_\infty \geq 0,$$

logo $\{1, x, \ldots, x^r\} \subseteq \mathscr{L}(rP_\infty)$; e como $1, x, \ldots, x^r$ são linearmente independente em $\mathscr{L}(rP_\infty)$, segue que

$$r + 1 \leq \ell(rP_\infty) = \text{grau}\,(rP_\infty) + 1 - g = r + 1 - g$$

para r suficientemente grande. Logo $g \leq 0$. Por outro lado, pela Observação 2.4.19, temos $g \geq 0$. Portanto $g = 0$. □

2.5 O Teorema de Riemann-Roch

Nesta seção, F/K é um corpo de funções algébricas de gênero g.

El teorema de Riemann–Roch permite determinar a dimensão do espaço de Riemann-Roch a partir do gênero do corpo de funções e o grão de um divisor.

Definição 2.5.1. Para $A \in Div(F)$, o inteiro $i(A) := \ell(A) - \text{grau } A + g - 1$ é chamado de índice de especialidade do divisor A.

Pelo Teorema de Riemann, temos $\ell(A) \geq \text{grau } A + g - 1$ e assim $i(A)$ é um inteiro não negativo e $i(A) = 0$ se grau A é suficientemente grande.

Definição 2.5.2. Um adele de F/K é uma aplicação $\alpha : \mathbb{P}_F \longrightarrow F$ dado por $\alpha(P) = \alpha_P$ tal que $\alpha_P \in \mathcal{O}_P$, para quase todos os lugares P de F/K.

Podemos considerar um adele como um elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$ e usaremos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou simplesmente $\alpha = (\alpha_P)$.

Definição 2.5.3. O conjunto $\mathcal{A}_F := \{\alpha \mid \alpha \text{ é um adele de } F/K\}$ é chamado de espaço adele de F/K.

Observação 2.5.4. O espaço $\mathcal{A}_F$ é um espaço vetorial sobre K.

De fato, dados $c \in K$ e $\alpha, \beta \in \mathcal{A}_F$, então $(\alpha + c\beta) : \mathbb{P}_F \longrightarrow F$ é uma aplicação tal que

$$(\alpha + c\beta)(P) = \alpha(P) + (c\beta)(P) = \alpha_P + c\beta_P \in \mathcal{O}_P.$$

Assim $(\alpha + c\beta)$ é um adele de F/K.

O adele principal de um elemento $x \in F$ é o adele cujas componentes são todas iguais a x.

$$\begin{array}{rcl} \alpha\colon \mathbb{P}_F & \longrightarrow & F \\ P & \longmapsto & x \end{array}$$

Note que $\alpha_P = x \in \mathcal{O}_P$ para quase todos os lugares P de F/K, uma vez que $0 \neq x \in F$ tem uma quantidade finita de polos e zeros.

A aplicação que leva $x \in F$ no seu adele principal (x) é uma injeção de F em $\mathcal{A}_F$ e se é uma aplicação bijectora, temos $F \hookrightarrow \mathcal{A}_F$.

$$\begin{array}{ccc} F & \hookrightarrow & \mathcal{A}_F \\ x & \longmapsto & (x) = (x, x, \ldots, x, x, \ldots) \end{array}$$

Dada essa injeção, a valorização discreta v_P associada ao lugar P de F/K se estende para $\mathcal{A}_F$, colocando $v_P(\alpha) := v_P(\alpha_P)$, onde α_P é a componente do adele α. Assim $v_P(\alpha) \geq 0$.

Definição 2.5.5. Seja $A \in Div(F)$. Definimos

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

Observação 2.5.6. O conjunto $\mathcal{A}_F(A)$ é um K- espaço vectorial de $\mathcal{A}_F$.

De fato, dados $\alpha, \beta \in \mathcal{A}_F(A)$ e $0 \neq c \in K$, então $\alpha, \beta \in \mathcal{A}_F$ com $v_P(\alpha) \geq -v_P(A)$ e $v_P(\beta) \geq -v_P(A)$, para todo $P \in \mathbb{P}_F$. Logo

$$\begin{aligned} v_P(\alpha + c\beta) &= v_P(\alpha_P + c\beta_P) \geq \min\{v_P(\alpha_P), v_P(c\beta_P)\} \\ &= \min\{v_P(\alpha_P), v_P(c) + v_P(\beta_P)\} = \min\{v_P(\alpha), v_P(\beta)\} \\ &\geq -v_P(A). \end{aligned}$$

Portanto $(\alpha + c\beta) \in \mathcal{A}_F(A)$.

Teorema 2.5.7. Seja $A \in Div(F)$. Então $i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$.

Demonstração. Vamos dividir a demonstração em diferentes passos.

- **Passo 1**: Sejam $A_1, A_2 \in Div(F)$ e $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e

  $$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \text{grau}\,(A_2 - A_1)$$

  De fato, pela hipótese temos $A_1 \leq A_2$, então $-A_2 \leq -A_1$. Logo $-v_P(A_1) \geq -v_P(A_2)$, para todo $P \in \mathbb{P}_F$; e seja $\alpha \in \mathcal{A}_F(A_1)$, então $\alpha \in \mathcal{A}_F$ tal que $v_P(\alpha) \geq -v_P(A_1)$, para todo $P \in \mathbb{P}_F$. Daí, $v_P(\alpha) \geq -v_P(A_1) \geq -v_P(A_2)$, ou seja, $\alpha \in \mathcal{A}_F(A_2)$. Assim $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.

  Como $A_1 \leq A_2$, suponhamos que $A_2 = A_1 + P$ para algum $P \in \mathbb{P}_F$. O caso geral, segue por indução, análogo ao Lema 2.4.12.

Como v_P é sobrejetora, escolhemos $t \in F$ tal que $v_P(t) = v_P(A_2) = v_P(A_2) + 1$. Consideremos a aplicação linear

$$\begin{aligned} \varphi\colon \mathcal{A}_F(A_2) &\longrightarrow F_P \\ \alpha &\longmapsto t\alpha_P + P \end{aligned}$$

A aplicação φ é bem definida. Agora, determinemos o núcleo:

$$\begin{aligned} \ker(\varphi) &= \{\alpha \in \mathcal{A}_F(A_2) : \varphi(\alpha) = 0\} = \{\alpha \in \mathcal{A}_F(A_2) : t\alpha_P + P = 0\} \\ &= \{\alpha \in \mathcal{A}_F(A_2) : t\alpha_P \in P\} = \{\alpha \in \mathcal{A}_F(A_2) : v_P(t\alpha_P) > 0\} \\ &= \{\alpha \in \mathcal{A}_F(A_2) : v_P(\alpha_P) > -v_P(t)\} = \{\alpha \in \mathcal{A}_F(A_2) : v_P(\alpha_P) > -v_P(A_1)\} \\ &= \mathcal{A}_F(A_1). \end{aligned}$$

Pelo teorema de isomorfismo, temos

$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \dim(Im(\varphi)) = \dim(F_P) = \text{grau}\,(P) = \text{grau}\,(A_2) - \text{grau}\,(A_1).$$

- **Passo 2**: Se $A_1, A_2 \in Div(F)$ tais que $A_1 \leq A_2$, então

$$\dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1)) + F) = \dim[\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)] - \dim(\mathscr{L}(A_2)/\mathscr{L}(A_2)).$$

Consideremos a sequência exata de aplicações lineares:

$$0 \longrightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \xrightarrow{\sigma_2} (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \longrightarrow 0$$

onde σ_1 e σ_2 são aplicações canônicas. A única afirmação não trivial é que o núcleo de σ_2 está na imagem de σ_1.

Seja $\alpha \in \ker(\sigma_2) = \mathcal{A}_F(A_1)$, assim $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$, o que implica $\alpha + \mathcal{A}_F(A_1) + F = 0$. Logo $\alpha \in \mathcal{A}_F(A_1) + F$, ou seja, existe $x \in F$ tal que $x - \alpha \in \mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$. Daí $x \in \mathcal{A}_F(A_2) \cap F = \mathscr{L}(A_2)$.

Por outro lado $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathscr{L}(A_1))$.

Pelo passo 1, obtemos

$$\begin{aligned} \dim[(\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)] &= \dim[\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)] - \dim[\mathscr{L}(A_2)/\mathscr{L}(A_1)] \\ &= \text{grau } A_2 - \text{grau } A_1 - (\ell(A_2) - \ell(A_1)). \end{aligned}$$

- **Passo 3**: Se B é um divisor com $\ell(B) = \text{grau } B + 1 - g$. Então $\mathcal{A}_F = \mathcal{A}_F(B) + F$.

De fato, considere um divisor $B_1 \geq B$. Pelo Lema 2.4.12, obtemos

$$\begin{aligned} \ell(B_1) - \ell(B) &\leq \text{grau } B_1 - \text{grau } B \\ \ell(B_1) &\leq \text{grau } B_1 - \text{grau } B + \ell(B) \\ &= \text{grau } B_1 - \text{grau } B + (\text{grau } B + 1 - g) \\ &= \text{grau } B_1 + 1 - g. \end{aligned}$$

Por outro lado, pelo Teorema de Riemann 2.4.20, temos $\ell(B_1) \geq \text{grau } B_1 + 1 - g$. Logo, para todo $B_1 \geq B$ temos $\ell(B_1) = \text{grau } B_1 + 1 - g$.

Agora, seja $\alpha \in \mathcal{A}_F$ e escolha $B_1 \geq B$ tal que $\alpha \in \mathcal{A}_F(B_1)$. Pelo passo 2, temos

$$\begin{aligned}\dim[(\mathcal{A}_F(B_1) + F)/(\mathcal{A}_F(B) + F)] &= (\text{grau } B_1 - \ell(B_1)) - (\text{grau } B - \ell(B)) \\ &= (g-1) - (g-1) = 0.\end{aligned}$$

Logo $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$ e como $\alpha \in \mathcal{A}_F(B_1)$, então $\alpha \in \mathcal{A}_F(B) + F$.

Portanto $\mathcal{A}_F = \mathcal{A}_F(B) + F$.

Finalmente, seja A um divisor qualquer. Pelo Teorema de Riemann 2.4.20(b) e pelo passo 3, existe $A_1 \geq A$ tal que $\ell(A_1) = \text{grau}\,(A_1) + 1 - g$. E pelo passo 3, temos $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$. Logo, pelo passo 2, obtemos

$$\begin{aligned}\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) &= \dim(\mathcal{A}_F(A_1) + F/(\mathcal{A}_F(A) + F)) \\ &= (\text{grau } A_1 - \ell(A_1)) - (\text{grau } A - \ell(A)) \\ &= g - 1 - \text{grau } A + \ell(A) = i(A).\end{aligned}$$

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

Corolário 2.5.8. $g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Demonstração. Pelo Teorema 2.5.7 temos

$$\dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)) = i(0) = g - 1 - \text{grau } 0 + \ell(0) = g - 1 - 0 + 1 = g.$$

□

O Teorema 2.5.7 pode ser reescrito da seguinte forma: Para todo $A \in Div(F)$ temos

$$\ell(A) = \text{grau } A + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)).$$

Esta é uma versão preliminar do Teorema de Riemann-Roch, o que será provado mais adiante. Agora, introduziremos o conceito de diferencial de Weil, o qual permitira dar outra interpretação do índice de especialidade.

Definição 2.5.9. Uma diferencial de Weil é uma aplicação linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula sobre $\mathcal{A}_F(A) + F$, para algum divisor $A \in Div(F)$. Chamamos

$$\Omega_F := \{\omega \mid \omega \text{ é uma diferencial de Weil de } F/K\}$$

de módulo das diferenciais de Weil de F/K. Dado $A \in Div(F)$, definimos

$$\Omega_F(A) = \{\omega \in \Omega_F \mid \omega \text{ se anula sobre } \mathcal{A}_F(A) + F\}.$$

O conjunto Ω_F é um espaço vetorial sobre K com as operações usuais, e como consequência $\Omega_F(A)$ é um subespaço vetorial de Ω_F.

Lema 2.5.10. Para $A \in Div(F)$ temos $\dim \Omega_F(A) = i(A)$.

Demonstração. Vamos mostrar que o espaço $\Omega_F(A)$ é equivalente ao espaço de formas lineares $Hom_K(\mathcal{A}_F/\mathcal{A}_F(A) + F; K)$.
De fato, seja $w \in \Omega_F(A)$. Assim, w é uma diferencial de Weil que se anula em $\mathcal{A}_F(A) + F$. Então existe $\bar{w}$ tal que

$$\begin{array}{rcl} \bar{\omega}\colon \mathcal{A}_F/\mathcal{A}_F(A) + F & \longrightarrow & K \\ \bar{\alpha} := \alpha + (\mathcal{A}_F(A) + F) & \longmapsto & \bar{\omega}(\bar{\alpha}) = \omega(\alpha) \end{array}$$

Considere $\varphi \in Hom_K(\mathcal{A}_F/\mathcal{A}_F(A) + F; K)$, então

$$\begin{array}{rcl} \varphi\colon \mathcal{A}_F/\mathcal{A}_F(A) + F & \longrightarrow & K \\ \bar{\alpha} := \alpha + (\mathcal{A}_F(A) + F) & \longmapsto & \varphi(\bar{\alpha}) \end{array}$$

Definimos $\phi : \mathcal{A}_F \longrightarrow K$ dado por $\phi(\alpha) = \varphi(\bar{\alpha})$. Então ϕ é linear (pois φ é linear) e ϕ se anula em $\mathcal{A}_F(A) + F$ pois se $\alpha \in \mathcal{A}_F(A) + F$, temos $\bar{\alpha} = \alpha + (\mathcal{A}_F(A) + F) = \bar{0}$. Assim

$$\phi(\bar{\alpha}) = \varphi(\bar{\alpha}) = \varphi(\bar{0}) = 0.$$

Logo $\phi \in \Omega_F(A)$. Agora, definimos o isomorfismo

$$\begin{array}{rcl} \psi\colon \Omega_F(A) & \longrightarrow & Hom_K(\mathcal{A}_F/\mathcal{A}_F(A) + F; K) \\ \omega & \longmapsto & \bar{\omega} \end{array}$$

Logo

$$\dim \Omega_F(A) = \dim Hom_K(\mathcal{A}_F/\mathcal{A}_F(A) + F; K) = \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = i(A)$$

Portanto $\dim \Omega_F(A) = i(A)$. □

Definição 2.5.11. Para $x \in F$ e $\omega \in \Omega_F$. Definimos $x\omega : \mathcal{A}_F \longrightarrow K$ dada por $x\omega(\alpha) := \omega(x\alpha)$.

A aplicação $x\omega$ é uma diferencial de Weil em F/K, pois $x\omega$ é linear e se ω se anula sobre $\mathcal{A}_F(A) + F$, então $x\omega$ se anula sobre $\mathcal{A}_F(A + (x)) + F$.

Proposição 2.5.12. Ω_F é um espaço vetorial unidimensional sobre F.

Demonstração. Pelo Lema 2.5.10, temos $\Omega_F \neq 0$. Então existe $\omega_1 \in \Omega_F$. Vamos mostrar que, para todo $\omega_2 \in \Omega_F$, existe $z \in F$ tal que $\omega_2 = z\omega_1$.

Se $\omega_2 = 0$, basta $z = 0$.

Se $\omega_2 \neq 0$. Sejam $A_1, A_2 \in Div(F)$ tal que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$. Para um divisor B, a ser determinado, consideremos a aplicação linear e injetora, sobre K, para $i = 1, 2$.

$$\begin{aligned} \varphi\colon \mathscr{L}(A_i + B) &\longrightarrow \Omega_F(-B) \\ x &\longmapsto x\omega_i \end{aligned}$$

Afirmamos que, para uma escolha apropriada do divisor B, vale

$$\varphi_1(\mathscr{L}(A_1 + B)) \cap \varphi_2(\mathscr{L}(A_2 + B)) \neq \{0\}.$$

De fato, seja $B > 0$ um divisor de grau suficientemente grande tal que

$$\ell(A_i + B) = \dim(A_i + B) = \text{grau}\,(A_i + B) + 1 - g,$$

para $i = 1, 2$, o que é possível pelo teorema de Riemann.

Definimos $U_i := \varphi(\mathscr{L}(A_i + B)) \subseteq \Omega_F(-B)$. Como grau $(-B) < 0$ então $\ell(-B) = 0$. Logo, pelo Lema 2.5.10, temos

$$\dim(\Omega_F(-B)) = i(-B) = \ell(-B) - \text{grau}\,(-B) - 1 + g = \text{grau}\ B - 1 + g.$$

Como $\varphi_i, i = 1, 2$ é injetora, então $\ker(\varphi_i) = \{0\}$. Assim $\dim(\ker(\varphi_i)) = 0$. Pelo teorema do núcleo - imagem, obtemos

$$\ell(A_i + B) = \dim(\mathscr{L}(A_i + B)) = \dim(\ker(\varphi_i)) + \dim(\varphi_i(\mathscr{L}(A_i + B))) = \ell(\varphi_i(\mathscr{L}(A_i + B))).$$

Logo

$$\begin{aligned} \dim U_1 + \dim U_2 - \dim(\Omega_F(-B)) &= \dim(\mathscr{L}(A_1 + B)) + \dim(\mathscr{L}(A_2 + B)) - \dim(\Omega_F(-B)) \\ &= \text{grau}\,(A_1 + B) + \text{grau}\,(A_2 + B) + 3(1 - g) - \text{grau}\ B \\ &= \text{grau}\ B + [\text{grau}\ A_1 + \text{grau}\ A_2 + 3(1 - g)]. \end{aligned}$$

Como o termo grau A_1 + grau $A_2 + 3(1 - g)$ não depende de B, temos

$$\dim U_1 + \dim U_2 - \dim(\Omega_F(-B)) > 0$$

para B suficientemente grande. Logo $\dim(U_1 \cap U_2) > 0$, ou seja, $U_1 \cap U_2 \neq \{0\}$. Assim existe um elemento em $U_1 \cap U_2$, isto é, dados $x_1 \in \mathscr{L}(A_1 + B)$ e $x_2 \in \mathscr{L}(A_2 + B)$ tem-se $x_1\omega_1 = x_2\omega_2 \neq 0$. Isso implica que $\omega_2 = (x_2^{-1}x_1)\omega_1$, com $x_2^{-1}x_1 \in F$. □

Queremos vincular um divisor para qualquer diferencial de Weil $\omega = 0$. Para isso, fixamos ω, então o conjunto de divisores

$$M(\omega) := \{A \in Div(F) \mid \omega \text{ se anula sobre } \mathcal{A}_F(A) + F\}$$

Lema 2.5.13. Seja $0 \neq \omega \in \Omega_F$. Então, existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.

Demonstração. Pelo teorema de Riemann, item (b), existe c dependendo do corpo de funções F/K tal que $\ell(A) = \text{grau } A + 1 - g$ sempre que $\text{grau}\,(A) \geq c$, para todo $A \in Div(F)$. Por outro lado, pelo Teorema 2.5.7 temos

$$\dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = i(A) = \ell(A) - \text{grau } A + 1 - g.$$

Dessa forma $\dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = 0$, para todo $A \in Div(F)$, isto é, $\mathcal{A}_F = \mathcal{A}_F(A) + F$.
Se $A \in M(\omega)$ então ω se anula em $\mathcal{A}_F(A) + F$, mas $\bar{\omega} \neq 0$ sobre $\mathcal{A}_F(A) + F$. Então grau $A < c$, para todo $A \in M(\omega)$.
Desse modo, podemos escolher $W \in M(\omega)$ de grau máximo, já que temos limitação superior para o grau dos divisores de $M(\omega)$.
Suponha que W não possui as propriedades do lema. Assim, existe algum divisor $A_0 \in M(\omega)$ com $A_0 \nleq W$, isto é, $v_Q(A_0) > v_Q(W)$ para algum $Q \in \mathbb{P}_F$.
Afirmamos que $W + Q \in M(\omega)$.
De fato, seja $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$ um adele e escrevemos $\alpha = \alpha' + \alpha''$, onde

$$\alpha'_P = \begin{cases} \alpha_P, & P \neq Q, \\ 0, & P = Q \end{cases} \quad \text{e} \quad \alpha''_P = \begin{cases} 0, & P \neq Q, \\ \alpha_Q, & P = Q \end{cases}$$

Logo

$$v_P(\alpha_P) \geq -v_P(W + Q) = -v_P(\omega),\ P \neq Q$$
$$v_Q(\alpha_Q) \geq -v_Q(W + Q) \geq -v_Q(A_0).$$

Então $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in \mathcal{A}_F(A_0)$. Portanto,

$$\omega(\alpha) = \omega(\alpha' + \alpha'') = \omega(\alpha') + \omega(\alpha'') = 0.$$

Assim α se anula sobre $\mathcal{A}_F(W + Q) + F$. Logo $W + Q \in M(\omega)$ e $\text{grau}\,(W + Q) = \text{grau } W + 1$ o que contradiz a maximalidade de W. Assim $A_0 \leq W$.
Agora suponha que existe W' de grau máximo. Logo $W \leq W'$ e $W' \leq W$, pois W é maximal. Portanto $W = W'$. □

Definição 2.5.14. a) O divisor (ω) de uma diferencial de Weil $\omega \neq 0$ é o divisor unicamente determinado de F/K satisfazendo:

i) ω se anula sobre $\mathcal{A}_F((\omega)) + F$, e

ii) ω se anula sobre $\mathcal{A}_F(A) + F$ então $A \leq (\omega)$.

b) Para $0 \neq \omega \in \Omega_F$ e $P \in \mathbb{P}_F$, definimos $v_P(\omega) := v_p((\omega))$.

c) Um lugar P é chamado de zero (polo respectivamente) de ω, se $v_P(\omega) > 0$ ($v_P(\omega) < 0$ respectivamente). El diferencial de Weil ω é chamado de regular em P se $v_P(\omega) \geq 0$ e ω é denominado de regular (ou holomórfica) se ω é regular para todos os lugares $P \in \mathbb{P}_F$.

d) Um divisor W é denominado divisor canônico de F/K se $W = (\omega)$, para algum $\omega \in \Omega_F$.

Proposição 2.5.15. Segue da definição

a) $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\}$.

b) $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ é regular}\}$.

c) $\dim \Omega_F(0) = g$.

Demonstração. a) Seja $\alpha \in \Omega_F(A)$, então ω se anula em $\mathcal{A}_F(A) + F$. Logo, pela Definição 2.5.14(a), temos $A \leq (\omega)$. Assim $\Omega_F(A) \subseteq \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\}$.
Por outro lado, dado $\omega = 0$ temos ω se anula em $\mathcal{A}_F(A) + F$, para todo $A \in Div(F)$. Agora, dado $\omega \neq 0$ e $(\omega) \geq A$. Pela definição 2.5.14(a), ω se anula em $\mathcal{A}_F((\omega)) + F$ e como $A \leq (\omega)$, temos $\mathcal{A}_F(A) + F \subseteq \mathcal{A}_F((\omega)) + F$. Logo ω se anula em $\mathcal{A}_F(A) + F$. Assim $\omega \in \Omega_F(A)$. Consequentemente $\{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq A\} \subseteq \Omega_F(A)$.

b) Pelo item a), temos $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } (\omega) \geq 0\}$. Logo $v_P((\omega)) \geq 0$, ou seja, ω é regular. E se, ω é regular temos que $\omega \in \Omega_F(0)$.

c) $\ell(\Omega_F(0)) = \dim(\Omega_F(0)) = i(0)$ e pelo Lema 2.5.10 temos

$$\ell(\Omega_F(0)) = \ell(0) - \text{grau}\,(0) + g - 1 = 1 + g - 1 = g.$$

Portanto $\ell(\Omega_F(0)) = g$.

□

Proposição 2.5.16. a) Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos $(x\omega) = (x) + (\omega)$.

b) Qualquer par de divisores canônicos de F/K são equivalentes.

Demonstração. a) Como $\omega \in \Omega_F$, temos ω é uma diferencial de Weil, e assim ω se anula sobre $\mathcal{A}_F(A) + F$. Logo $x\omega$ se anula sobre $\mathcal{A}_F(A + (x)) + F$. Por outro lado, pela Definição 2.5.14(a), temos ω se anula sobre $\mathcal{A}_F((\omega)) + F$, logo $x\omega$ se anula sobre $\mathcal{A}_F((\omega) + (x)) + F$.

Consequentemente $(\omega) + (x) \leq (x\omega)$.

Da mesma forma, temos $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Assim

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x)$$

Portanto $(x\omega) = (x) + (\omega)$.

b) Sejam $0 \neq \omega_1, \omega_2$ diferenciais de Weil de F/K e W_1, W_2 divisores canônicos de F/K, tal que $W_1 = (\omega_1)$ e $W_2 = (\omega_2)$. Como Ω_F é um espaço vetorial de dimensão um sobre F, existe um elemento $0 \neq z \in F$ tal que $\omega_2 = z\omega_1$. Logo

$$W_1 - W_2 = (\omega_1) - (\omega_2) = (\omega_1) - (z\omega_1) = (\omega_1) - (z) - (\omega_1) = (z^{-1}).$$

Assim $W_1 = (z^{-1}) + W_2$, onde $z^{-1} \in F \setminus \{0\}$. Portanto W_1 e W_2 são equivalentes.

□

Teorema 2.5.17 (Teorema da dualidade)**.** Seja $A \in Div(F)$ um divisor arbitrário e $W = (\omega)$ um divisor canônico de F/K. Então, a aplicação

$$\begin{array}{rccc} \mu\colon & \mathscr{L}(W - A) & \longrightarrow & \Omega_F(A) \\ & x & \longmapsto & x\omega \end{array}$$

é um isomorfismo de espaços vetoriais sobre K. Em particular $i(A) = \ell(W - A)$.

Demonstração. Primeiro, verificamos que μ é bem definida. Para $x \in \mathscr{L}(W - A)$, temos $(x) + W - A \geq 0$. Logo $(x) + (\omega) \geq A$. Assim $(x\omega) = (x) + (\omega) \geq A$. Daí $x\omega \in \Omega_F(A)$. Claramente, μ é linear. Agora, vamos mostrar que é bijetora.

Dados $x, y \in \mathscr{L}(W - A)$, se $\mu(x) = \mu(y)$, temos $x\omega = y\omega$. Logo $(x - y)\omega = 0$, e como $\omega \neq 0$ temos $x = y$. Assim μ é injetora.

Por outro lado, dado ω_1 uma diferencial de Weil, ou seja, $\omega \in \Omega_F(A)$. Pela Proposição 2.5.12, existe $x \in F$ tal que $\omega_1 = x\omega$. Logo $(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A$. Dessa forma $(x) \geq A - W = -(W - A)$. Logo $x \in \mathscr{L}(W - A)$ e $\mu(x) = x\omega = \omega_1$. Portanto, μ é sobrejetiva. □

Teorema 2.5.18 (Teorema de Riemann-Roch)**.** Seja W um divisor canônico de F/K. Então, para cada divisor $A \in Div(F)$, temos

$$\ell(A) = \text{grau } A + 1 - g + \ell(W - A).$$

Demonstração. Do Teorema 2.5.17 temos $\dim \Omega_F(A) = \dim(W - A)$ e pelo Lema 2.5.10 temos $\dim \Omega_F(A) = i(A)$. Então $\ell(A) = \text{grau } A + 1 - g + \ell(W - A)$. □

Corolário 2.5.19. Para um divisor canônico W, temos grau $W = 2g - 2$ e $\ell(W) = g$.

Demonstração. No teorema de Riemann-Roch, para $A = 0$, temos

$$1 = \ell(0) = \text{grau}\,(0) + 1 - g + \ell(W - 0)$$
$$1 = 1 - g + \ell(W)$$

então $\ell(W) = g$; e para $A = W$ obtemos

$$g = \ell(W) = \text{grau}\ W + 1 - g + \ell(W - W)$$
$$g = \text{grau}\ W + 1 - g + \ell(0).$$

Portanto,grau $W = 2g - 2$. □

Teorema 2.5.20. Se A é um divisor de F/K de grau $A \geq 2g-1$, então $\ell(A) = \text{grau}\ A+1-g$.

Demonstração. Pelo teorema de Riemann-Roch, temos $\ell(A) = \text{grau}\ A+1-g+\ell(W-A)$, onde W é um divisor canônico. Como grau $A \geq 2g - 1$ e grau $W = 2g - 2$ então

$$\text{grau}\,(W - A) \leq 2g - 2 - 2g + 1 = -1 < 0.$$

Pelo Corolário 2.4.16(b), segue que $\ell(W - A) = 0$. Assim $\ell(A) = \text{grau}\ A + 1 - g$. □

2.6 Algumas consequências do Teorema de Riemann-Roch

Nesta seção, F/K denota o corpo de funções algébricas de gênero g.

Proposição 2.6.1. Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in Div(F)$ satisfazem

$$\ell(A) = \text{grau}\ A + 1 - g_0 + \ell(W_0 - A)$$

para todo $A \in Div(F)$. Então $g_0 = g$ e W_0 é um divisor canônico.

Demonstração. Na hipótese, para $A = 0$ temos

$$1 = \ell(0) = \text{grau}\,(0) + 1 - g_0 + \ell(W_0 - 0)$$
$$1 = 1 - g_0 + \ell(W_0)$$
$$\ell(W_0) = g_0$$

e para $A = W_0$ obtemos

$$g = \ell(W_0) = \text{grau}\ W_0 + 1 - g_0 + \ell(W_0 - W_0)$$
$$g_0 = \text{grau}\ W + 1 - g_0 + \ell(0)$$
$$\text{grau}\ W_0 = 2g_0 - 2.$$

Seja W um divisor canônico de F/K. Escolhemos um divisor A com

$$\text{grau } A > \max\{2g_0 - 2, 2g - 2\}.$$

Note que grau $A \geq 2g - 1$, então pelo Teorema 2.5.20 temos $\ell(A) = \text{grau } A + 1 - g$ e pela hipótese temos $\ell(A) = \text{grau } A + 1 - g_0$. Assim $g = g_0$.
Finalmente, substituímos $A = W$ na hipótese

$$\begin{aligned} \ell(W) &= \text{grau } W + 1 - g_0 + \ell(W_0 - W) \\ g &= 2g - 2 + 1 - g + \ell(W_0 - W) \\ 1 &= \ell(W_0 - W). \end{aligned}$$

Como grau $(W_0 - W) = 0$, então $W_0 - W$ é principal. Assim $W_0 \sim W$. □

Proposição 2.6.2. Um divisor B é canônico se, e somente se, grau $B = 2g - 2$ e $\ell(B) \geq g$.

Demonstração. Se grau $B = 2g - 2$ e $\ell(B) \geq g$.
Escolhemos W um divisor canônico. Então,

$$\begin{aligned} g \leq \ell(B) &= \text{grau } B + 1 - g + \ell(W - B) \\ &= 2g - 2 + 1 - g + \ell(W - B) \\ &= g - 1 + \ell(W - B). \end{aligned}$$

Assim $\ell(W - B) \geq 1$. Como grau $(W - B) = 0$, pelo Corolário 2.4.16, temos $W - B$ é principal. Isso implica que $W \sim B$. Portanto B é canônico.
O reciproco, já foi mostrado no Corolário 2.5.19. □

Proposição 2.6.3. Para um corpo de funções F/K, as seguintes condições são equivalentes:

a) F/K é racional, isto e, $F = K(x)$ para algum x transcendente sobre o corpo K.

b) F/K tem o gênero 0, e existe algum divisor $A \in Div(F)$ com grau $A = 1$.

Demonstração. a) $\implies$ b): Ver o Exemplo 2.4.21
b) $\implies$ a): Sejam $g = 0$ e $A \in Div(F)$ tal que grau $A = 1$. Então,

$$1 = \text{grau } A \geq 2g - 1 = -1.$$

Pelo Teorema de Riemann $\dim(\mathscr{L}(A)) = \ell(A) = \text{grau } A + 1 - g = 2$. Assim $\mathscr{L}(A) \neq \{0\}$. Pela Observação 2.4.9(b), existe $A' \in Div(F)$ tal que $A' \sim A$ e $A' \geq 0$. Dessa forma $\ell(A') = 2$,

pelo Corolário 2.4.16(a). Logo $\mathscr{L}(A') \neq \{0\}$ e assim, existe $x \in \mathscr{L}(A') \setminus K$ tal que $(x) \neq 0$ e $(x) + A \geq 0$. Como $A' \geq 0$ e grau $A' = 1$, então

$$(x) + A' = (x)_0 - (x)_\infty + A' \geq 0.$$

Isto é possível, se $A' = (x)_\infty$, o divisor de polos de x. Assim, pelo Teorema 2.4.15 temos

$$[F : K(x)] = \text{grau } (x)_\infty = \text{grau } A' = 1.$$

Portanto $F = K(x)$. □

Teorema 2.6.4 (Teorema da Aproximação Forte)**.** Seja $S \subsetneq \mathbb{P}_F$ um subconjunto próprio de $\mathbb{P}_F$ e $P_1, \ldots, P_r \in S$. Suponha que dados $x_1, \ldots, x_r \in F$ e $n_1, \ldots, n_r \in \mathbb{Z}$. Então, existe um elemento $x \in F$ tal que

$$\begin{aligned} v_{P_i}(x - x_i) &= n_i, \text{ para todo } i = 1, \ldots, r; \\ v_P(x) &\geq 0, \text{ para todo } P \in S \setminus \{P_1, \ldots, P_r\}. \end{aligned}$$

Demonstração. Consideremos o adele $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ com

$$\alpha_P := \begin{cases} x_i, & P = P_i, i = 1, \ldots, r. \\ 0, & \text{outro caso} \end{cases}.$$

Escolhemos um lugar $Q \in \mathbb{P}_F \setminus S$ e para $m \in \mathbb{N}$ consideremos o divisor

$$D = mQ - \sum_{i=1}^{r}((n_i + 1)P_i).$$

Para $m > 0$ suficientemente grande, temos

$$\text{grau } D = \text{grau } \left(mQ - \sum_{i=1}^{r}((n_i + 1)P_i) \right) = m \,\text{grau } Q - \sum_{i=1}^{r}((n_i + 1)\,\text{grau}\,(P_i)) \geq c.$$

Logo, pelo Teorema de Riemann, temos $\ell(D) = \text{grau } D + 1 - g$. Assim $i(D) = 0$, o que implica $\mathcal{A} = \mathcal{A}_F(D) + F$. Dessa forma, existe $z \in F$ tal que $z - \alpha \in \mathcal{A}_F(D)$, isto é,

$$v_P(z - \alpha) = v_P(z - \alpha_P) \geq -v_P(D)$$

para todo $P \in \mathbb{P}_F$. Então

$$\begin{aligned} v_{P_i}(z - \alpha_{P_i}) = v_{P_i}(z - x_i) &\geq -(-(n_i + 1)) = n_i + 1, \text{ para } P = P_i, i = 1, \ldots, r; \\ v_P(z - \alpha_P) = v_{P_i}(z - 0) &\geq 0, \text{ para } P \in S \setminus \{P_1, \ldots, P_n\}. \end{aligned}$$

Agora, escolhemos $y_1, \ldots, y_r \in F$, com $v_{P_i}(y_i) = n_i$. Consideremos o adele $\alpha' = (\alpha'_P)_{P \in \mathbb{P}_F}$ com

$$\alpha_P := \begin{cases} y_i, & P = P_i, i = 1, \ldots, r; \\ 0, & \text{outro caso.} \end{cases}$$

Escolhemos um lugar $Q' \in \mathbb{P}_F \setminus S$ e para $m' \in \mathbb{N}$ consideremos o divisor

$$D' = m'Q' - \sum_{i=1}^{r}((n_i + 1)P_i).$$

Para $m > 0$ suficientemente grande, temos

$$\text{grau } D' = \text{grau } \left(m'Q' - \sum_{i=1}^{r}((n_i + 1)P_i) \right) = m' \,\text{grau } Q' - \sum_{i=1}^{r}((n_i + 1)\,\text{grau}\,(P_i)) \geq c'.$$

Logo, pelo Teorema de Riemann, temos $\ell(D') = \text{grau } D' + 1 - g$. Assim $i(D') = 0$, o que implica $\mathcal{A} = \mathcal{A}_F(D') + F$. Dessa forma, existe $y \in F$ tal que $y - \alpha \in \mathcal{A}_F(D)$, isto é,

$$v_P(y - \alpha) = v_P(y - \alpha_P) \geq -v_P(D')$$

para todo $P \in \mathbb{P}_F$. Então

$$\begin{aligned} v_{P_i}(y - \alpha_{P_i}) = v_{P_i}(y - y_i) \geq -(-(n_i)) = n_i, \text{ para } P = P_i, i = 1, \ldots, r; \\ v_P(y - \alpha_P) = v_{P_i}(y - 0) \geq 0, \text{ para } P \in S \setminus \{P_1, \ldots, P_n\}. \end{aligned}$$

Então, para $i = 1, \ldots, r$, temos

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = \min\{v_{P_i}(y - y_i), v_{P_i}(y_i)\} = n_i.$$

Definimos $x := y + z$, então

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = \min\{v_{P_i}(y), v_{P_i}(z - x_i)\} = n_i$$

e

$$v_P(x) = v_P(y + z) \geq \min\{v_P(y), v_P(z)\} \geq 0, P \in S \setminus \{P_1, \ldots, P_r\}.$$

Portanto, existe $x \in F$ tal que $v_{P_i}(x - x_i) = n_i$ e $v_P(x) \geq 0$, para $P \notin S$. □

Proposição 2.6.5. Seja $P \in \mathbb{P}_F$. Então, para cada $n \geq 2g$, existe um elemento $x \in F$ com divisor de polos $(x)_\infty = nP$.

Demonstração. Consideremos o divisor $(n-1)P$, com $n \in \mathbb{N}$ e $n \geq 2g$. Logo

$$\text{grau}\,((n-1)P) = (n-1)\,\text{grau}\,(P) \geq 2g - 1.$$

Pelo Teorema de Riemann-Roch, temos

$$\ell((n-1)P) = \text{grau}\,((n-1)P) + 1 - g = (n-1)\,\text{grau}\,(P) + 1 - g \geq n - g.$$

Similarmente $\text{grau}\,(nP) \geq n \geq 2g \geq 2g-1$. Então,

$$\ell(nP) = \text{grau}\,(nP) + 1 - g = n\,\text{grau}\,(P) + 1 - g \geq n + 1 - g.$$

Assim $\ell((n-1)P) < \ell(nP)$. Isso implica que $\mathscr{L}((n-1)P) \subsetneq \mathscr{L}(nP)$ propriamente, ou seja, existe $x \in \mathscr{L}(nP) \setminus \mathscr{L}((n-1)P)$. Então, $(x) + nP \geq 0$ e $(x) + (n-1)P < 0$. Daí $(x)_0 - (x)_\infty + nP \geq 0$ e $(x)_0 - (x)_\infty + (n-1)P < 0$. Como $Supp\,(x)_0 \cap Supp\,(x)_\infty = \emptyset$, temos $0 \geq -(x)_\infty + nP \geq 0$. Portanto $(x)_\infty = nP$. □

Definição 2.6.6. Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado de ordem de polo de P se existe um elemento $x \in F$, com $(x)_\infty = nP$. Caso contrario, se não existe tal x, o inteiro n é chamado de lacuna de P.

Temos a seguinte caracterização de uma lacuna:

Proposição 2.6.7. Seja $i \in \mathbb{N}_0$. Então i é uma lacuna se, e somente, se $\mathscr{L}((i-1)P) = \mathscr{L}(iP)$.

Demonstração. Seja i uma lacuna de P. Então i não é uma ordem de polo de P. Sabemos que $\mathscr{L}((n-1)P) \subseteq \mathscr{L}(nP)$. Se existe algum elemento $x \in \mathscr{L}(iP) \setminus \mathscr{L}((i-1)P)$, teríamos que $(x)_\infty = iP$, o que seria uma contradição. Portanto $\mathscr{L}((i-1)P) = \mathscr{L}(iP)$.
Reciprocamente, suponhamos que i não é uma lacuna de P, ou seja, existe um elemento $x \in F$ com $(x)_\infty = iP$. Logo

$$(x) + iP = (x)_0 - (x)_\infty + iP = (x)_0 \geq 0,$$

$$(x) + iP - P = (x)_0 - (x)_\infty + iP - P = (x)_0 - P.$$

Assim $x \in \mathscr{L}(iP)$, e como $P \in Supp\,(x)_\infty$ e $P \notin Supp\,(x)_0$ temos $x \notin \mathscr{L}((i-1)P)$. Logo $\mathscr{L}((i-1)P) \neq \mathscr{L}(iP)$, o que contradiz a hipótese. Portanto, i é uma lacuna de P. □

Teorema 2.6.8 (Teorema das lacunas de Weierstrass)**.** Suponha que F/K tem gênero $g > 0$ e P um lugar de F/K de grau um. Então existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. Além disso, $i_1 = 1$ e $i_g \leq 2g-1$.

Demonstração. Pela Proposição 2.6.5, qualquer n é uma lacuna de P se $n \leq 2g-1$ e 0 é uma ordem de polo de P pois tomando $0 \in F$ observamos que $(0)_\infty = 0 = 0P$.
Consideremos a sequência de espaços vetoriais

$$K = \mathscr{L}(0) \subseteq \mathscr{L}(P) \subseteq \mathscr{L}(2P) \subseteq \cdots \subseteq \mathscr{L}((2g-1)P)$$

onde $\ell(0) = \dim K = 1$ e como grau $(P) = 1$ temos grau $((2g-1)P) = 2g-1 \geq 2g-1$. Logo, pelo Teorema 2.5.20, temos

$$\ell((2g-1)P) = \text{grau}\,((2g-1)P) + 1 - g = 2g - 1 + 1 - g = g$$

e pelo Lema 2.4.12, para todo i, temos

$$\ell(iP) - \ell(i-1)P) \leq \text{grau}\,(iP) - \text{grau}\,((i-1)P) = i - i + 1 = 1.$$

Tomando a dimensão de cada espaço vetorial da sequência, obtemos exatamente $g-1$ números $1 \leq i \leq 2g-1$ com $\mathscr{L}((i-1)P) \subsetneq \mathscr{L}(iP)$. Os g números $0 \leq i \leq 2g-1$ restantes tal que $\mathscr{L}((i-1)P) = \mathscr{L}(iP)$ são lacunas de P, pela Proposição 2.6.7.
Finalmente, mostramos que 1 é uma lacuna de P. Suponha que 1 é uma ordem de polo de P e como as ordens de polo de P formam um semigrupo aditivo, então qualquer $n \in \mathbb{N}$ é uma ordem de polo de P, ou seja, não há lacunas, o que é absurdo, pois $g > 0$ (g tem lacunas). Portanto, 1 é uma lacuna de P. □

Seja A um divisor de F/K. Se grau $A < 0$ temos $\ell(A) = 0$, pelo Lema 2.4.11, e logo $\mathscr{L}(A) = \{0\}$. Se grau $A > 2g-2$ temos $\ell(A) = \text{grau}\ A + 1 - g$, pelo Teorema 2.5.18. Dessa forma, a dimensão do espaço de Riemann-Roch associado ao divisor A depende do grau A e o gênero de F/K, caso grau $A \geq 2g-1$.

Definição 2.6.9. Um divisor $A \in Div(F)$ é chamado não especial se o índice de especialidade de A for $i(A) = 0$; caso contrario, A é chamado especial.

Proposição 2.6.10. De acordo com a Definição 2.6.9, temos:

a) A é não especial se, e somente se, $\ell(A) = \text{grau}\ A + 1 - g$.

b) Se grau $A > 2g-2$ então, A é não especial.

c) A propriedade de que um divisor A seja especial ou não especial, depende somente da classe $[A]$ de A no grupo de classes de divisores.

d) Divisores canônicos são especiais.

e) Cada divisor A com $\ell(A) > 0$ e grau $A < g$ são especiais.

f) Se A é não especial e $B \geq A$ então B é não especial.

Demonstração. a) Seja A um divisor não especial. Assim

$$i(A) = 0 \Leftrightarrow 0 = \ell(A) - \text{grau}\ A - 1 + g \Leftrightarrow \ell(A) = \text{grau}\ A + 1 - g$$

b) Pela hipótese, temos grau $A > 2g-2$, ou seja, grau $A \geq 2g-1$. Logo, pelo Teorema 2.5.20, temos $\ell(A) = \text{grau } A + 1 - g$. Isso implica que $i(A) = 0$, e dessa forma A é não especial.

c) Seja $A \sim A'$. Então, pelo Corolário 2.4.16(a), temos $\ell(A) = \ell(A')$ e grau A = grau A'. Assim $i(A) = i(A')$.

d) Seja W um divisor canônico. Então $i(W) = \ell(W - W) = \ell(0) = 1 \neq 0$. Logo W é especial.

e) Para $A \in Div(F)$ com $\ell(A) > 0$, temos $1 \leq \ell(A) = \text{grau } A + 1 - g + i(A)$. Assim $g - \text{grau } A \leq i(A)$. E como grau $A < g$ então $i(A) > 0$. Dessa forma, A é especial.

f) Como A é não especial, então $i(A) = 0$. Assim $0 = i(A) = \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F)$. Logo $\mathcal{A}_F = \mathcal{A}_F(A) + F$. Como $A \leq B$ então $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$. Logo $\mathcal{A}_F \subseteq \mathcal{A}_F(B) + F$, e como $\mathcal{A}_F(B) + F \subseteq \mathcal{A}_F$, temos $i(B) = \dim(\mathcal{A}_F/\mathcal{A}_F(B) + F) = 0$. Portanto B é não especial.

□

Proposição 2.6.11. Suponha que $T \subseteq \mathbb{P}_F$ é um conjunto de lugares de grau um tal que $|T| \geq g$. Então, existe um divisor $B \geq 0$ não especial com grau $B = g$ e $Supp\, B \subseteq T$.

Demonstração. Primeiro mostraremos a seguinte afirmação

Afirmação: Dados g lugares distintos $P_1, \ldots, P_g \in T$ e um divisor $A \geq 0$ com $\ell(A) = 1$ e grau $A \leq g - 1$, existe algum $j \in \{1, \ldots, g\}$ tal que $\ell(A + P_j) = 1$.

De fato, suponhamos que a afirmação é falsa, ou seja, $\ell(A + P_j) > 1$ para todo j, e como $\ell(A) = 1$, existem elementos $z_j \in \mathscr{L}(A + P_j) \setminus \mathscr{L}(A)$ para $j = 1, \ldots, g$. Logo $z_j \in \mathscr{L}(A + P_j)$ e $z_j \notin \mathscr{L}(A)$. Então

$$v_{P_j}(z_j) = -v_{P_j}(A) - 1,$$
$$v_{P_i}(z_j) = -v_{P_i}(A), \text{ para todo } i \neq j.$$

Como $v_{P_j}(z_j) \neq v_{P_i}(z_i)$, então pela desigualdade triangular estrita temos que $1, z_1, \ldots, z_g$ são linearmente independentes sobre K.

Escolhemos um divisor $D \geq A + P_1 + \cdots + P_g$ com grau $D = 2g - 1$. Então $z_1, \ldots, z_g \in \mathscr{L}(D)$, e isso implica que $\ell(D) \geq g + 1$, mas pelo Teorema de Riemann-Roch, temos

$$\ell(D) = \text{grau } D + 1 - g = 2g - 1 + 1 - g = g$$

e assim, obtemos $g \geq g+1$, o que é absurdo. Portanto $\ell(A+P_j)=1$.
Agora, mostramos a proposição. Pela afirmação, encontramos divisores

$$0 < P_{i_1} < P_{i_1}+P_{i_2} < \cdots < P_{i_1}+\cdots+P_{i_g} =: B$$

com $i_v \in \{1,\ldots,g\}$ (não necessariamente distintos) tal que $\ell(P_{i_1}+\cdots+P_{i_j})=1$, para todo $j=1,\ldots,g$. Assim $\ell(B)=1$ e como grau $B+1-g=g+1-g=1$, então $\ell(B)=$ grau $B+1-g$. Portanto B é não especial. □

Lema 2.6.12. Suponha que $A, B \in Div(F)$ tal que $\ell(A)>0$ e $\ell(B)>0$. Então

$$\ell(A)+\ell(B) \leq 1+\ell(A+B).$$

Demonstração. Pela hipótese temos $\ell(A)>0$ e $\ell(B)>0$, então $\mathscr{L}(A)\neq\{0\}$ e $\mathscr{L}(B)\neq\{0\}$. Logo, pela Observação 2.4.9(b), existem $A', B' \in Div(F)$ tais que $A'\sim A$, $B'\sim B$, $A'\geq 0$ e $B'\geq 0$. Definimos o conjunto

$$X := \{D \in Div(F) \mid D \leq A' \text{ e } \mathscr{L}(D)=\mathscr{L}(A)\}.$$

Assim $X\neq\emptyset$, pois $A'\in X$. Como grau $D\geq 0$, para todo $D\in X$, então existe algum divisor $D_0\in X$ de grau mínimo. Logo $\ell(D_0-P)<\ell(D_0)$, para todo $P\in\mathbb{P}_F$.
Assumimos que K é um corpo infinito. Consideremos $Supp\, B'=\{P_1,\ldots,P_r\}$. Desse modo $\mathscr{L}(D_0-P_i)\subsetneq\mathscr{L}(D_0)$, para $i=1,\ldots,r$.
Lembremos que todo espaço vetorial sobre um corpo infinito não é uma união finita de subespaços próprios. Então podemos considerar

$$z \in \mathscr{L}(D_0) \setminus \bigcup_{i=1}^{r} \mathscr{L}(D_0-P_i).$$

Consideremos a aplicação

$$\begin{aligned} \varphi\colon \mathscr{L}(B') &\longrightarrow \mathscr{L}(D_0+B')/\mathscr{L}(A') \\ x &\longmapsto xz \mod \mathscr{L}(A') \end{aligned}$$

φ é linear. Determinamos o núcleo da aplicação

$$\begin{aligned} \ker(\varphi) &= \{x\in\mathscr{L}(B') \mid \varphi(x)=0\} = \{x\in\mathscr{L}(B') \mid xz \mod \mathscr{L}(A')=0\} \\ &= \{x\in\mathscr{L}(B') \mid xz\in\mathscr{L}(D_0)\}. \end{aligned}$$

Como $z\notin\mathscr{L}(D_0-P_i)$, para todo $i=1,\ldots,r$, então z tem polos em $P_i\in Supp\, B'$ e para que $xz\in\mathscr{L}(D_0)$, não debe ter zeros nem polos nos P_i, isto é, x deve ser constante. Portanto

$\ker(\varphi) = K$.

Logo, pelo Teorema de isomorfismo, temos

$$\mathscr{L}(B')/\ker(\varphi) \cong Im\,(\varphi) \subseteq \mathscr{L}(D_0 + B')/\mathscr{L}(A').$$

Então

$$\begin{aligned}\ell(B') - \dim K &\leq \ell(D_0 + B') - \ell(A') = \ell(D_0 + B') - \ell(D_0)\\ \ell(B') + \ell(D_0) &\leq \ell(D_0 + B') + 1.\end{aligned}$$

Logo

$$\begin{aligned}\ell(A) + \ell(B) = \ell(A') + \ell(B') = \ell(D_0) + \ell(B') &\leq \ell(D_0 + B') + 1\\ &= \ell(A' + B') + 1 = \ell(A + B) + 1.\end{aligned}$$

Portanto $\ell(A) + \ell(B) \leq 1 + \ell(A + B)$. □

Teorema 2.6.13 (Teorema de Clifford)**.** Para todo $A \in Div(F)$, com $0 \leq \text{grau } A \leq 2g - 2$ temos $\ell(A) \leq 1 + \frac{1}{2}\,\text{grau } A$.

Demonstração. Para $\ell(A) = 0$ temos $0 \leq 1 + \frac{1}{2}\,\text{grau } A$, pois $0 \leq \text{grau } A$.
Seja W um divisor canônico. Então, pelo Teorema de Riemann-Roch, temos

$$\ell(A) = \text{grau } A + 1 - g + \ell(W - A).$$

Se $\ell(W - A) = 0$, então

$$\begin{aligned}\ell(A) = \text{grau } A + 1 - g &= \frac{1}{2}\,\text{grau } A + 1 + \frac{1}{2}\,\text{grau } A - \frac{1}{2}2g\\ &= \frac{1}{2}\,\text{grau } A + 1 + \frac{1}{2}\,(\text{grau } A - 2g)\,.\end{aligned}$$

Como grau $A \leq 2g - 2$, temos grau $A - 2g \leq -2$. Logo $\ell(A) < 1 + \frac{1}{2}\,\text{grau } A$.
Em caso que $\ell(A) > 0$ e $\ell(W - A) > 0$, pelo Lema 2.6.12, temos

$$\ell(A) + \ell(W - A) \leq 1 + \ell(A + W - A) = 1 + \ell(W) = 1 + g$$

e pelo Teorema de Riemann-Roch, temos $\ell(A) - \ell(W - A) = \text{grau } A + 1 - g$. Logo

$$\begin{aligned}2\ell(A) &= 1 + g + \text{grau } A + 1 - g = 2 + \text{grau } A\\ \ell(A) &\leq 1 + \frac{1}{2}\,\text{grau } A.\end{aligned}$$

□

2.7 Componentes locais das diferenciais de Weil

Na secção 2.5, consideramos a injeção $F \hookrightarrow \mathcal{A}_F$ como sendo a aplicação que leva $x \in F$ ao seu adele correspondente. Agora, vamos introduzir, para qualquer lugar P do corpo de funções F/K, outra injeção de F em $\mathcal{A}_F$.

Definição 2.7.1. Seja P um lugar do corpo de funções F/K.

a) Para $x \in F$, dado $i_P \in \mathbb{A}_F$ o adele cuja P-componente é x e todas as demais componentes são iguais a zero.

b) Para uma diferencial de Weil $\omega \in \Omega_F$, sua componente local é definida como sendo a função

$$\begin{aligned} \omega_P \colon F &\longrightarrow K \\ x &\longmapsto \omega_P(x) := \omega(i_P(x)) \end{aligned}$$

A aplicação ω_P é linear sobre K.

Proposição 2.7.2. Seja ω uma diferencial de Weil e $\alpha = \alpha_P$ um adele do corpo de funções F/K. Então $\omega_P(\alpha_P) \neq 0$, para uma quantidade finita de lugares P e $\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P)$. Em particular, $\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0$.

Demonstração. Veja [18, Proposição I.7.2.]. □

Proposição 2.7.3. Seja P um lugar do corpo de funções F/K.

a) Seja $\omega \neq 0$ uma diferencial de Weil. Então

$$v_P(\omega) = \max\{r \mid r \in \mathbb{Z} \text{ e } \omega_P(x) = 0, \text{ para todo } x \in F \text{ com } v_P(x) \geq -r\}.$$

Em particular, $\omega_P \neq 0$.

b) Se ω e ω' são diferenciais de Weil do corpo de funções e $\omega_P = \omega'_P$, para algum lugar P, então $\omega = \omega'$.

Demonstração. Veja [18, Proposição I.7.3.]. □

Capítulo 3

Códigos Algébrico Geométricos

Neste capítulo, descrevemos a teoria de códigos usando corpos de funções algébricas. Começamos com uma introdução dos conceitos desta teoria. Em seguida, definimos os códigos AG e desenvolvemos suas principais propriedades.

3.1 Códigos lineares

Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideremos o espaço vetorial n - dimensional $\mathbb{F}_q^n$, cujos elementos são n- uplas da forma $(a_1, \ldots, a_n)$, com $a_i \in \mathbb{F}_q$ para todo $i = 1, \ldots, n$.

Definição 3.1.1 (Distância de Hamming)**.** Sejam $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ em $\mathbb{F}_q^n$. A distância de Hamming é definida por

$$d(a, b) := |\{i : a_i \neq b_i\}|.$$

A distância de Hamming é uma métrica.

Definição 3.1.2. O peso de um elemento $a \in \mathbb{F}_q$ é definido por

$$\mathrm{wt}(a) := d(a, 0) = |\{i : a_i \neq 0\}|.$$

Definição 3.1.3. Um código linear C de comprimento n sobre o alfabeto $\mathbb{F}_q$ é um subespaço linear de $\mathbb{F}_q^n$. Os elementos de C são chamados de palavras do código. O número $n \in \mathbb{N}$ é chamado de comprimento do código C e $k = \dim C$ é a dimensão do C como $\mathbb{F}_q$-espaço vetorial.

Um código $[n, k]$ é um código de comprimento n e dimensão k.

Definição 3.1.4. A distância mínima de um código $C \neq \emptyset$ é definida como

$$d(C) := \min\{d(a, b) \mid a, b \in C, a \neq b\} = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}.$$

Um código $[n, k]$ com distância mínima $d = d(C)$ será referido como um código $[n, k, d]$.

Observação 3.1.5. De forma mais geral, podemos definir um código como um subconjunto arbitrário não vazio $C \subseteq A^n$, onde $A \neq \emptyset$ é um conjunto finito. Consideramos apenas códigos lineares.

Definição 3.1.6. Seja C um código $[n, k]$ sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$, cujas linhas formam uma base para C.

Definição 3.1.7. Sejam $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ em $\mathbb{F}_q^n$. O produto interno canônico é definido por $\langle a, b\rangle = \sum_{i=1}^{n} a_i b_i$.

Definição 3.1.8. Seja $C \subseteq \mathbb{F}_q^n$ um código linear. Então, o código dual de C é definido por

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

O código C é chamado de auto-dual se $C = C^{\perp}$, e é chamado de auto-ortogonal se $C \subseteq C^{\perp}$.

Definição 3.1.9. Uma matriz geradora H de $C^{\perp}$ é chamada a matriz de teste de paridade do código C.

Note que, a matriz de teste de paridade de um código $[n, k]$ é uma matriz de ordem $(n-k)\times n$, com $(n-k)$ linhas e n colunas; e temos $C := \{u \in \mathbb{F}_q^n \mid H \cdot u^t = 0\}$, onde u^t denota a transposta de u.

Desta forma, uma matriz de teste de paridade verifica se um vetor $u \in \mathbb{F}_q^n$ é uma palavra-código ou não.

Proposição 3.1.10 (Cota de Singleton)**.** Para um código $[n, k, d]$, temos $k + d \leq n + 1$.

Demonstração. Considere o espaço vetorial $E \subseteq \mathbb{F}_q^n$ dado por

$$E := \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid a_i = 0, \text{ para todo } i \geq d\}.$$

Seja $a \in E$. Então $a_i = 0$ para todo $i \geq d$. Pela Definição 3.1.2, o peso de a é

$$\mathrm{wt}(a) = |\{i : a_i \neq 0\}|.$$

Logo $\mathrm{wt}(a) \leq d - 1$.

Como $d = d(C) = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$, temos $E \cap C = \{0\}$, pois se existe $0 \neq a \in (E \cap C)$, teríamos $\mathrm{wt}(a) < d$ e então, $d = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\} < d$. Logo $\dim(E \cap C) = 0$.

Da Álgebra Linear, temos

$$\dim(C + E) = \dim C + \dim E - \dim(E \cap C) = \dim C + \dim E$$

Como $C + E \subseteq \mathbb{F}_q^n$, então $\dim(C + E) \leq n$. Logo $n \geq k + (d - 1)$. Portanto $n + 1 \geq k + d$. □

Em geral, obter cotas para a distância mínima de um código dado não é um problema muito fácil. Uma das razões para o interesse em códigos algébricos geométricos, é que esta classe de códigos se consegue avaliar uma boa cota para a distância mínima.

3.2 Códigos Algébrico Geométricos

Vamos fixar as notações para toda a seção.

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

Definição 3.2.1. O código algébrico geométrico $C_{\mathscr{L}}(D, G)$ associado com os divisores D e G, é definido por

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

Note que esta definição faz sentido: para $f \in \mathscr{L}(G)$ temos $v_{P_i}(f) + v_{P_i}(G) \geq 0$, para todo $i = 1, \ldots, n$ e como $Supp\, G \cap Supp\, D = \emptyset$, então $v_{P_i}(G) = 0$. Logo $v_{P_i}(f) \geq 0$, e daí $f \in \mathcal{O}_{P_i}$, para $i = 1, \ldots, n$. A classe de resíduos $f(P_i)$ de f módulo P_i é um elemento do corpo de classes de resíduos de P_i, e como grau $(P_i) = 1$, o corpo de classes de resíduos é $\mathbb{F}_q$. Logo $f(P_i) \in \mathbb{F}_q$.

A aplicação de avaliação $\mathrm{ev}_D : \mathscr{L}(G) \longrightarrow \mathbb{F}_q^n$ é dada por

$$\mathrm{ev}_D(f) := (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n. \tag{3.1}$$

A aplicação ev_D é $\mathbb{F}_q$- linear e $C_{\mathscr{L}}(D, G)$ é a imagem de $\mathscr{L}(G)$ mediante esta aplicação.

Teorema 3.2.2. $C_{\mathscr{L}}(D, G)$ é um código $[n, k, d]$ com parâmetros satisfazendo

$$k = \ell(G) - \ell(G - D) \quad \text{e} \quad d \geq n - \text{grau}\,(G).$$

Demonstração. Consideremos a aplicação de avaliação definida em (3.1).
Como $Im(\mathrm{ev}_D(f)) = C_{\mathscr{L}}(D, G)$, então ev_D é uma aplicação linear e sobrejetora (de $\mathscr{L}(G)$ para $C_{\mathscr{L}}(D, G)$). Observemos que o núcleo é

$$\begin{aligned}\ker(\mathrm{ev}_D) &= \{f \in \mathscr{L}(G) \mid \mathrm{ev}_D(f) = 0\} = \{f \in \mathscr{L}(G) \mid f(P_i) = 0, \forall\, i = 1, \ldots, n\} \\ &= \{f \in \mathscr{L}(G) \mid f \in P_i, \forall\, i = 1, \ldots, n\} = \{f \in \mathscr{L}(G) \mid v_{P_i}(f) > 0, \forall\, i = 1, \ldots, n\}.\end{aligned}$$

Por outro lado, dado $f \in \mathscr{L}(G-D)$, temos $v_{P_i}(f) + v_{P_i}(G-D) \geq 0$, para todo $i = 1, \ldots, n$. Logo

$$v_{P_i}(f) \geq -v_{P_i}(G-D) = -v_{P_i}(G) + v_{P_i}(D) = 0 + v_{P_i}(D) = v_{P_i}(D).$$

Como $D = P_1 + \cdots + P_n$, então $v_{P_i}(f) \geq v_{P_i}(D) > 0$, para todo $i = 1, \ldots, n$. Além disso, como $G - D \leq G$, temos $\mathscr{L}(G-D) \subseteq \mathscr{L}(G)$. Logo $f \in \mathscr{L}(G)$ e $v_{P_i}(f) > 0$, para todo $i = 1, \ldots, n$, ou seja, $f \in \ker(\mathrm{ev}_D)$. Portanto, $\mathscr{L}(G-D) \subseteq \ker(\mathrm{ev}_D)$.

Agora, seja $f \in \ker(\mathrm{ev}_D)$, isto é, $f \in \mathscr{L}(G)$ e $v_{P_i}(f) > 0$, para todo $i = 1, \ldots, n$. Note que

$$\begin{aligned}
&\{f \in F \mid v_P(f) + v_P(G) - v_P(D) \geq 0, \forall\, P\} \\
&\supseteq \{f \in \mathscr{L}(G) \mid v_{P_i}(f) - v_{P_i}(D) \geq 0, \forall\, i = 1, \ldots, n\} \\
&\supseteq \{f \in \mathscr{L}(G) \mid v_{P_i}(f) > 0, \forall\, i = 1, \ldots, n\}.
\end{aligned}$$

Assim $f \in \mathscr{L}(G-D)$ e $\ker(\mathrm{ev}_D) \subseteq \mathscr{L}(G-D)$. Dessa forma $\ker(\mathrm{ev}_D) = \mathscr{L}(G-D)$.

Pelo teorema de Núcleo - Imagem, temos

$$\begin{aligned}
\dim(\mathscr{L}(G)) &= \dim(\ker(\mathrm{ev}_D)) + \dim(Im(\mathrm{ev}_D)) \\
\ell(G) &= \dim(\mathscr{L}(G-D)) + \dim(C_{\mathscr{L}}(D,G)) \\
\ell(G) &= \ell(G-D) + k.
\end{aligned}$$

Assim $k = \ell(G) - \ell(G-D)$.

A asserção referente à distância mínima d faz sentido somente se $C_{\mathscr{L}}(D,G) \neq \{0\}$. Assumimos que este código é não trivial.

Escolha $0 \neq f \in \mathscr{L}(G)$ com wt $(\mathrm{ev}_D(f)) = d$. Dessa forma, temos $n-d$ entradas nulas em $\mathrm{ev}_D(f) = (f(P_1), \ldots, f(P_n))$. Suponhamos que $f(P_{i_1}) = f(P_{i_2}) = \cdots = f(P_{i_{(n-d)}}) = 0$. Então $f \in P_{i_j}$, para todo $j = 1, \ldots, n-d$. Logo $v_{P_{i_j}}(f) > 0$, para todo $j = 1, \ldots, n-d$. Dessa forma, os $n-d$ lugares de $F/\mathbb{F}_q$ são zeros de x.

Assim $0 \neq f \in \mathscr{L}\left(G - \left(P_{i_1} + P_{i_2} + \cdots + P_{i_{(n-d)}}\right)\right)$. Então

$$\ell\left(G - \left(P_{i_1} + P_{i_2} + \cdots + P_{i_{(n-d)}}\right)\right) \neq 0$$

e, pelo Corolário 2.4.16(b), temos

$$0 \leq \text{grau}\left(G - \left(P_{i_1} + P_{i_2} + \cdots + P_{i_{(n-d)}}\right)\right) = \text{grau } G - (n-d) = \text{grau } G - n + d.$$

Dessa forma $d \geq n - \text{grau } G$. □

Corolário 3.2.3. Suponha que o grau de G é estritamente menor do que n. Então, a aplicação da avaliação $\mathrm{ev}_D : \mathscr{L}(G) \longrightarrow C_{\mathscr{L}}(D,G)$ é injetora e temos

a) $C_{\mathscr{L}}(D,G)$ é um código $[n,k,d]$ com $d \geq n - \text{grau } G$ e $k = \ell(G) \geq \text{grau } G + 1 - g$. Consequentemente, $k + d \geq n + 1 - g$.

b) Se tivermos ainda, a hipótese adicional $2g - 2 < \text{grau } G < n$, então $k = \text{grau } G + 1 - g$.

c) Se $\{f_1, \ldots, f_k\}$ é base de $\mathscr{L}(G)$, então

$$M = \begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{bmatrix}$$

é uma matriz geradora para $C_{\mathscr{L}}(D,G)$.

Demonstração. Temos grau $G < n$, então grau $(G - D) < n - n = 0$. Logo, pelo Corolário 2.4.16, temos $\ell(G-D) = 0$. Assim $\mathscr{L}(G-D) = \{0\}$ e como $\ker(\text{ev}_D) = \mathscr{L}(G-D)$, concluímos que ev_D é injetora.
Agora, pelo Teorema 3.2.2, temos $C_{\mathscr{L}}(D,G)$ é um código $[n,k,d]$, satisfazendo

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

Logo, pelo Teorema de Riemann, temos $k = \ell(G) \geq \text{grau } G + 1 - g$. Somando, obtemos $k + d \geq n + 1 - g$, o que mostra o item a).
Pela hipótese, temos grau $G > 2g - 2 \geq 2g - 1$. Então, pelo Teorema 2.5.20, $\ell(G) = \text{grau } G + 1 - g$. Assim $k = \text{grau } G + 1 - g$, o que mostra o item b).
Finalmente, temos $\{f_1, \ldots, f_k\}$ é base de $\mathscr{L}(G)$. Como a aplicação de avaliação ev_D leva de base em base, assim o conjunto $\{\text{ev}_D(f_1), \text{ev}_D(f_2), \ldots, \text{ev}_D(f_k)\}$ é uma base de $C_{\mathscr{L}}(D,G)$, ou seja, as k linhas de M são linearmente independentes em $C_{\mathscr{L}}(D,G)$ que geram o código. Portanto, a matriz M é geradora de $C_{\mathscr{L}}(D,G)$. □

Definição 3.2.4. O inteiro $d^* := n - \text{grau } G$ é denominado a distância mínima designada do código $C_{\mathscr{L}}(D,G)$.

O Teorema 3.2.2, afirma que a distância mínima de um código AG não pode ser menor que a distância designada, ou seja, $d \geq d^*$.

Observação 3.2.5. Suponha que $\ell(G) > 0$ e $d^* = n - \text{grau } G > 0$. Então $d^* = d$ se, e somente se, existe um divisor D satisfazendo $0 \leq D' \leq D$, grau $D' = \text{grau } G$ e $\ell(G - D') > 0$.

Demonstração. ($\Rightarrow$) Temos $d^* = d$.

Seja a aplicação da avaliação $\mathrm{ev}_D : \mathscr{L}(G) \longrightarrow C_{\mathscr{L}}(D,G)$. Então existe $0 \neq f \in \mathscr{L}(G)$ tal que a palavra - código $\mathrm{ev}_D(f) = (f(P_1), \ldots, f(P_n)) \in C_{\mathscr{L}}(D,G)$ possui $n - d = n - d^* = \text{grau } G$ componentes nulas, isto é, existem $i_1, \ldots, i_{\text{grau } G}$ tal que $f(P_{i_j}) = 0$, para $j = 1, \ldots, \text{grau } G$.

Consideremos $D' := \sum_{j=1}^{\text{grau } G} P_{i_j}$. Então

$$\text{grau } D' = \text{grau} \left(\sum_{j=1}^{\text{grau } G} P_{i_j} \right) = \sum_{j=1}^{\text{grau } G} \text{grau } P_{i_j} = \text{grau } G$$

e como P_{i_j} são pontos de D e $D = P_1 + \cdots + P_n$, temos $0 \leq D' \leq D$. Além disso, como $0 \neq f \in \mathscr{L}(G - D')$ então $\ell(G - D') > 0$.

($\Leftarrow$) Seja um divisor D satisfazendo $0 \leq D' \leq D$, grau $D' = $ grau G e $\ell(G - D') > 0$.

Como $\ell(G - D') > 0$ então $\mathscr{L}(G - D') \neq \{0\}$. Assim existe $0 \neq f \in \mathscr{L}(G - D')$. Então, para $P \in Supp\, D$,

$$0 \leq v_P(f) + v_P(G - D') = v_P(f) + v_P(G) - v_P(D')$$

como $0 \leq D' \leq D$, temos $v_P(f) + v_P(G) \geq 0$, para $P \in Supp\, D'$. Assim $f \in \mathscr{L}(G)$ e $(f(P_1), \ldots, f(P_n)) \in C_{\mathscr{L}}(D,G)$. □

Outro código pode ser associado aos divisores G e D, usando as componentes locais da diferencial de Weil. Para $A \in Div(F)$, $\Omega_F(A)$ é o espaço das diferenciais de Weil ω, com $(\omega) \geq A$. Isto é um espaço vetorial de dimensão finita sobre $\mathbb{F}_q$, de dimensão $i(A)$ (índice de especialidade). Para uma diferencial de Weil ω num lugar $P \in \mathbb{P}_F$, a aplicação $\omega_P : F \longrightarrow \mathbb{F}_q$ denota componente local de ω em P.

Definição 3.2.6. Sejam G e $D = P_1 + \cdots + P_n$ divisores de F/K. Então definimos o código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ por

$$C_\Omega(D,G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G - D)\}.$$

Teorema 3.2.7. $C_\Omega(D,G)$ é um código $[n, k', d']$ com parâmetros satisfazendo

$$k' = i(G - D) - i(G) \text{ e } d' \geq \text{grau } G - (2g - 2).$$

Tendo a hipótese adicional grau $G > 2g - 2$, temos $k' = i(G - D) \geq n + g - 1 - \text{grau } G$. Além disso, se $n > \text{grau } G > 2g - 2$, então $k' = n + g - 1 - \text{grau } G$.

Demonstração. Sejam $P \in \mathbb{P}_F$ um lugar de grau um e ω um diferencial de Weil com $v_P(\omega) \geq -1$. Afirmamos que

$$\omega_P(1) = 0 \iff v_P(\omega) \geq 0 \tag{3.2}$$

De fato, pela Proposição 2.7.3, temos para $r \in \mathbb{Z}$ vale

$$v_P(\omega) \geq r \iff \omega_P(f) = 0, \forall f \in F \text{ com } v_P(f) \geq -r. \tag{3.3}$$

($\Leftarrow$) Suponhamos que $v_P(\omega) \geq 0 \overset{(3.3)}{\Rightarrow} \omega_P(f) = 0, \forall f \in F$ com $v_P(f) \geq 0$. Em particular, $\omega_P(1) = 0$.

($\Rightarrow$) Suponhamos que $\omega_P(1) = 0$. Seja $f \in F$ com $v_P(f) \geq 0$.
Como grau $P = 1$, podemos escrever $f = a + y$, com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Então

$$\omega_P(f) = \omega_P(a + y) = \omega_P(a) + \omega(y) = a\omega_P(1) + \omega_P(y) = \omega_P(y).$$

Como $v_P(y) \geq 1$ e $v_P(\omega) \geq -1 \overset{(3.3)}{\Rightarrow} \omega_P(y) = 0$. Logo $v_P(\omega) \geq 0$.

Agora, consideremos a aplicação linear sobre $\mathbb{F}_q$.

$$\begin{aligned} \phi_D \colon \Omega_F(G - D) &\longrightarrow C_\Omega(D, G) \\ \omega &\longmapsto (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \end{aligned}$$

Como $Im\,(\phi_D) = C_\Omega(D, G)$, temos ϕ_D é sobrejetora. Vamos a determinar o núcleo da aplicação

$$\ker(\phi_D) = \{\omega \in \Omega_F(G - D) \mid \phi_D(\omega) = 0\}.$$

Seja $0 \neq \omega \in \ker(\phi_D)$, então $\omega \in \Omega_F(G - D)$ tal que $\omega_{P_1}(1) = 0$, para todo $i = 1, \ldots, n$. Logo, pela Proposição 2.5.15, temos $(\omega) \geq G - D$. Como $Supp\, G \cap Supp\, D = \emptyset$, obtemos

$$v_{P_i}(\omega) \geq v_{P_i}(G - D) = v_{P_i}(G) - v_{P_i}(D) = 0 - 1 = -1.$$

Logo, pela afirmação (3.2), $v_{P_i}(\omega) \geq 0$, para todo $i = 1, \ldots, n$.

Pelo Teorema de Núcleo - Imagem, temos

$$\begin{aligned} \dim(\Omega_F(G - D)) &= \dim(\ker(\phi_D)) + \dim(Im\,(\phi_D)) \\ \dim(\Omega_F(G - D)) &= \dim(\Omega_F(G)) + \dim(C_\Omega(D, G)) \\ i(g - D) - i(G) &= \dim(C_\Omega(D, G)) = k'. \end{aligned}$$

Seja $\phi_D(\omega) = (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \in C_\Omega(D, G)$ com peso $m > 0$. Então $\omega_{P_i}(1) = 0$ para os índices $i_1, i_2, \ldots, i_{n-m}$. Logo

$$\omega \in \Omega_F\left(G - \left(D - \sum_{j=1}^{n-m} P_{i_j}\right)\right) \Rightarrow (\omega) \geq G - \left(D - \sum_{j=1}^{n-m} P_{i_j}\right).$$

Assim

$$\begin{aligned}
\text{grau}\,(\omega) &\geq \text{grau}\,\left(G-\left(D-\sum_{j=1}^{n-m}P_{i_j}\right)\right)\\
2g-2 &\geq \text{grau}\,G-\left(\text{grau}\,D-(n-m)\,\text{grau}\,P_{i_j}\right)=\text{grau}\,G-(n-n+m)\\
2g-2 &\geq \text{grau}\,G-m\\
m &\geq \text{grau}\,G-2g+2.
\end{aligned}$$

Em particular, se d' é a distância mínima então $d' \geq \text{grau}\,G-2g+2$.
Se grau $G > 2g-2$, pelo Teorema 2.5.17, temos $i(G)=0$ e pelo Teorema de Riemann-Roch

$$\begin{aligned}
k' = i(G-D) &= \ell(G-D)-\text{grau}\,(G-D)-1+g\\
&= \ell(G-D)-\text{grau}\,G-n-1+g\\
&\geq n+g-1-\text{grau}\,G.
\end{aligned}$$

Se $n > \text{grau}\,G > 2g-2$, temos $\text{grau}\,(G-D) < n-n=0$. Logo $\ell(G-D)=0$. Assim

$$\begin{aligned}
k' = i(G-D) &= \ell(G-D)-\text{grau}\,(G-D)-1+g\\
&= \ell(G-D)-\text{grau}\,G-n-1+g\\
&= n+g-1-\text{grau}\,G.
\end{aligned}$$

□

Teorema 3.2.8. Os códigos $C_{\mathscr{L}}(D,G)$ e $C_{\Omega}(D,G)$ são duais entre si, isto é, $C_{\Omega}(D,G) = C_{\mathscr{L}}(D,G)^{\perp}$.

Demonstração. Sejam $P \in \mathbb{P}_F$ de grau um, ω um diferencial de Weil com $v_P(\omega) \geq -1$ e um elemento $f \in F$ com $v_P(f) \geq 0$.
Consideremos $f = a+y$, com $a = f(P) \in \mathbb{F}_q$ e $v_P(y) > 0$, então

$$\omega_P(f) = \omega_P(a)+\omega_P(y) = a\omega_P(1)+0 = f(P)\cdot\omega_P(1).$$

Consideremos $Im\,(\text{ev}_D) = C_{\mathscr{L}}(D,G)$ e $Im\,(\phi) = C_{\Omega}(D,G)$, onde

$$\begin{aligned}
\text{ev}_D\colon \mathscr{L}(G) &\longrightarrow \mathbb{F}_q^n\\
f &\longmapsto (f(P_1),\ldots,f(P_n))
\end{aligned}$$

e

$$\begin{aligned}
\phi\colon \Omega_F(G-D) &\longrightarrow \mathbb{F}_q^n\\
\omega &\longmapsto (\omega_{P_1}(1),\ldots,\omega_{P_n}(1))
\end{aligned}$$

Vamos a mostrar que $C_\Omega(D,G) \subseteq C_{\mathscr{L}}(D,G)^\perp$.

Sejam $\omega \in \Omega_F(G-D)$ e $f \in \mathscr{L}(G)$. Então ω se anula em $\mathcal{A}_F(G-D)+F$, assim $\omega(f)=0$. Logo

$$0 = \omega(f) = \sum_{P \in \mathbb{P}_F} \omega_P(f).$$

Agora, considere $Q \notin \{P_1, \ldots, P_n\}$. Note que

$$v_Q(f) \geq -v_Q(G) \text{ e}$$
$$v_Q(G-D) = v_Q(G) - v_Q(D) = v_Q(G).$$

Como $\omega \in \Omega_F(G-D)$, temos $v_Q(\omega) \geq v_Q(G) \geq -v_Q(f)$ e pela Proposição 2.7.3(a) temos

$$v_Q(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P(f) = 0, \forall f \in F \text{ com } v_Q(f) \geq -r\},$$

logo $\omega_Q(f)=0$. Daí

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

Como $v_{p_i}(f) \geq 0$ e grau $P_i = 1$, para todo $i = 1, \ldots, n$, então $\omega_{P_i}(f) = f(P_i) \cdot \omega_{P_i}(1)$. Logo

$$0 = \sum_{i=1}^{n} \omega_{P_i}(f) = \sum_{i=1}^{n} f(P_i) \cdot \omega_{P_i}(1) = \langle (f(P_1), \ldots, f(P_n)), (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \rangle.$$

Portanto $C_\Omega(D,G) \subseteq C_{\mathscr{L}}(D,G)^\perp$.

Pelo Teorema 3.2.7, temos

$$\begin{aligned}
\dim C_\Omega(D,G) &= i(G-D) - i(G) \\
&= \ell(G-D) - \text{grau}\,(G-D) - 1 + g - \ell(G) + \text{grau}\; G + 1 - g \\
&= \ell(G-D) - \ell(G) + \text{grau}\; D \\
&= -[\ell(G) - \ell(G-D)] + n \\
&= n - \dim C_{\mathscr{L}}(D,G) \\
&= \dim C_{\mathscr{L}}(D,G)^\perp.
\end{aligned}$$

Portanto, os códigos $C_{\mathscr{L}}(D,G)$ e $C_\Omega(D,G)$ são duais entre si. □

Lema 3.2.9. Existe uma diferencial de Weil η tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$, para todo $i = 1, \ldots, n$.

Demonstração. Escolha uma diferencial de Weil arbitrário $\omega_0 \neq 0$. Dados os lugares $P_1, \ldots, P_n$ de $F/\mathbb{F}_q$ distintos dois a dois, $r_i = -v_{P_i}(\omega_0) - 1$, para $i = 1, \ldots, n$, então pelo Teorema de

aproximação fraca (Teorema 2.3.1), existe $f \in F$ tal que $v_{P_i}(f) = r_i$, para $i = 1, \ldots, n$.
Considerando $\omega = f\omega_0$, temos

$$v_{P_i}(\omega) = v_{P_i}(f\omega_0) = v_{P_i}(f) + v_{P_i}(\omega_0) = -v_{P_i}(\omega_0) - 1 + v_{P_i}(\omega_0) = -1.$$

Assim $v_{P_i}(\omega) < 0$, e pela afirmação (3.2), temos $\omega_{P_i}(1) \neq 0$, para $i = 1, \ldots, n$.
Definimos $a_i = \omega_{P_i}(1) \in K \subset F$, $i = 1, \ldots, n$. Pelo passo 3 do Teorema da Aplicação Fraca, existe $g \in F$ tal que $v_{P_i}(y - a_i) > 0$. Segue que $v_{P_i}(y) = 0$ e $g(P_i) = a_i$, para $i = 1, \ldots, n$.
Consideremos $\eta := y^{-1}\omega$, então

$$v_{P_i}(\eta) = v_{P_i}(y^{-1}\omega) = v_{P_i}(y^{-1}) + v_{P_i}(\omega) = -v_{P_i}(y) + v_{P_i}(\omega) = -0 + (-1) = -1$$

e

$$\eta_{P_i}(1) = (y^{-1}\omega)_{P_i}(1) = \omega_{P_i}(y^{-1} \cdot 1) = y^{-1}(P_i) \cdot \omega_{P_i}(1) = a_i^{-1} \cdot a_i = 1.$$

□

Proposição 3.2.10. Seja η uma diferencial de Weil tal que $v_{P_i}(\eta) = -1$ e $\eta_{P_i}(1) = 1$, para $i = 1, \ldots, n$. Então $C_{\mathscr{L}}(D, G)^{\perp} = C_{\Omega}(D, G) = C_{\mathscr{L}}(D, H)$, com $H = D - G + (\eta)$.

Demonstração. Como $v_{P_i}(\eta) = -1$ para todo i então $(\eta) = -D + N$, $P_i \notin Supp\, N$. Logo

$$Supp\, H = Supp\,(D - G + (\eta)) = Supp\,(D - G - D + N) = Supp\,(N - G).$$

Assim $Supp\, H \cap Supp\, D = \emptyset$. Então, o código $C_{\mathscr{L}}(D, G)$ pode ser definido.
Como η é canônico, pelo Teorema da dualidade 2.5.17, existe um isomorfismo entre espaços vetoriais sobre K.

$$\begin{aligned} \mu \colon \mathscr{L}(H) &\longrightarrow \Omega_F(G - D) \\ f &\longmapsto \mu(f) := f\eta \end{aligned}$$

Para $f \in \mathscr{L}(H) = \mathscr{L}((\eta) - G + D)$ temos

$$(f\eta)_{P_i}(1) = \eta_{P_i}(f \cdot 1) = f(P_i)\eta_{P_i}(1) = x(P_i) \cdot 1.$$

Logo

$$\begin{aligned} C_{\Omega}(D, G) &= \{((f\eta)_{P_1}(1), \cdots, (f\eta)_{P_n}(1)) \mid x \in \mathscr{L}(H)\} \\ &= \{(f(P_1), \cdots, f(P_n)) \mid f \in \mathscr{L}(H)\} \\ &= C_{\mathscr{L}}(D, H). \end{aligned}$$

□

Como consequência imediata da Proposição 3.2.10 podemos fornecer condições suficientes para que um código $C_{\mathscr{L}}(D,G)$ seja auto-dual.

Corolário 3.2.11. Suponha que existe um diferencial de Weil η tal que $(\eta) = 2G - D$ e $\eta_{P_i}(1) = 1$, para $i = 1, \ldots, n$. Então o código $C_{\mathscr{L}}(D,G)$ é auto-dual.
Se $(\eta) \geq 2G - D$ e $\eta_{P_i}(1) = 1$ para $i = 1, \ldots, n$ Então o código $C_{\mathscr{L}}(D,G)$ é auto-ortogonal.

Demonstração. Como $(\eta) = 2G - D$, então $G = D - G + (\eta) =: H$. Logo, pela Proposição 3.2.10, obtemos $C_\Omega(D,G) = C_{\mathscr{L}}(D,G)$.
Se $H = D - G + (\eta)$ então, $C_{\mathscr{L}}(D,G)^\perp = C_{\mathscr{L}}(D,H)$. Mas, se $(\eta) \geq 2G - D \Longrightarrow G \leq D - G + (\eta) = H$, temos $C_{\mathscr{L}}(D,G) \subseteq C_{\mathscr{L}}(D,H) = C_{\mathscr{L}}(D,G)^\perp$. □

Definição 3.2.12. Dois códigos $C_1, C_2 \subseteq \mathbb{F}_q^n$ são chamadas equivalentes se existe um vetor $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$ tal que $C_2 = aC_1$, isto é,

$$C_2 = \{(a_1c_1, \ldots, a_nc_n) \mid (c_1, \ldots, c_n) \in C_1\}.$$

Claramente, os códigos equivalentes tem a mesma dimensão e a mesma distância mínima.

Proposição 3.2.13. Sejam G_1 e G_2 são divisores.

a) Suponha que $G_1 \sim G_2$ e $Supp\, G_i \cap Supp\, D = \emptyset$, para $i = 1, 2$. Então, os códigos $C_\Omega(D,G_1)$ e $C_\Omega(D,G_2)$ são equivalentes. O mesmo vale para $C_{\mathscr{L}}(D,G_1)$ e $C_{\mathscr{L}}(D,G_2)$.

b) Reciprocamente, se um código $C \subseteq \mathbb{F}_q^n$ é equivalente a $C_{\mathscr{L}}(D,G)$ (respectivamente a $C_\Omega(D,G)$) então existe um divisor $G' \sim G$ tal que $Supp\, G' \cap Supp\, D = \emptyset$ e $C = C_{\mathscr{L}}(D,G')$ (respectivamente $C = C_\Omega(D,G')$).

Demonstração. a) Como $G_1 \sim G_2$, então existe $0 \neq z \in F$ tal que $G_2 = G_1 - (z)$ e como $Supp\, G_i \cap Supp\, D = \emptyset$, para $i = 1, 2$, então $v_{P_i}(z) = 0$, para todo $i = 1, \ldots, n$. Logo $a := (z(P_1), \ldots, z(P_n)) \in (\mathbb{F}_q^*)^n$.

Seja a aplicação

$$\begin{aligned} \varphi\colon \mathscr{L}(G_1) &\longrightarrow \mathscr{L}(G_2) \\ f &\longmapsto fz \end{aligned}$$

φ é bijectora. Logo

$$\begin{aligned} C_{\mathscr{L}}(D,G_2) &= \{(fz(P_1), \ldots, fz(P_n) \mid x \in \mathscr{L}(H)\} \\ &= \{(f(P_1), \ldots, f(P_n)) \cdot (z(P_1), \ldots, z(P_n)) \mid x \in \mathscr{L}(H)\} \\ &= aC_{\mathscr{L}}(D,G_1) \end{aligned}$$

e

$$\begin{aligned} C_\Omega(D, G_1) &= \{((x\omega)_{P_1}(1), \cdots, (z\omega)_{P_n}(1)) \mid z\omega \in \Omega_F(G_1 - D)\} \\ &= \{(x(P_1), \cdots, x(P_n)) \cdot (\omega_{P_1}(1), \cdots, \omega_{P_n}(1))\} \\ &= aC_\Omega(D, G_2). \end{aligned}$$

b) Seja $C = aC_{\mathscr{L}}(D, G)$, com $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^*$. Escolhemos $z \in F$ com $z(P_i) = a_i$, para $i = 1, \ldots, n$. Pelo Teorema da aproximação, temos $v_{P_i}(z - a_i) = 1 > 0$.
Se $G' = G - (z)$, temos $C = C_{\mathscr{L}}(D, G')$.
Se $C = aC_\Omega(D, G)$, considerando $G' = G + (z)$ temos $C = C_\Omega(D, G')$.

□

3.3 Códigos Hermitianos

Os códigos Hermitianos são uma classe de códigos AG construídos a partir da curva Hermitiana, a qual desempenha um papel central na teoria por ser uma curva maximal sobre corpos finitos. Essa curva é definida sobre $\mathbb{F}_{q^2}$ e pode ser descrita pela equação afim

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

A principal característica é que possui um grande número de lugares ou pontos racionais, o que permite obter excelentes parâmetros, muitas vezes superiores aos de códigos lineares clássicos.

Esses códigos são amplamente utilizados como referência para a comparação com outras famílias de códigos construídos a partir de curvas algébricas. Sua relevância torna-os ferramentas fundamentais no estudo da codificação baseada em geometria algébrica.

Seja H o corpo de funções associado à curva hermitiana sobre $\mathbb{F}_{q^2}$, isto é,

$$H = \mathbb{F}_{q^2}(x, y), \text{ com } y^q + y = x^{q+1}.$$

O gênero de H é $g = q(q-1)/2$ e H tem $1 + q^3$ lugares de grau um,

- P_∞ o único polo comum de x e y.
- Para cada par $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_H$ de grau um tal que $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.

Para cada $\alpha \in \mathbb{F}_{q^2}$ existem q elementos distintos $\beta \in \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, e portanto, o número de lugares $P_{\alpha,\beta}$ é q^3.

Definição 3.3.1 (Códigos Hermitianos)**.** Para $r \in \mathbb{Z}$ definimos o código $C_r := C_{\mathscr{L}}(D, rP_\infty)$, onde $D = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta}$ é a soma de todos os lugares de grau um (excepto P_∞) do corpo de funções Hermitianas.

Os códigos Hermitianos são códigos de comprimento $n = q^3$. Para $r \leq s$, temos $C_r \subseteq C_s$. Primeiro, estudamos os casos triviais.

- Para $r < 0$, temos grau $(rP_\infty) = r < 0$, e isso implica que $\mathscr{L}(rP_\infty) = 0$. Portanto $C_r = 0$.
- Para $r > q^3 + q^2 - q - 2 = q^3 + 2g - 2$, temos

$$\begin{aligned}\dim C_r &\overset{(3.2.2)}{=} \ell(rP_\infty) - \ell(rP_\infty - D)\\ &\overset{(2.5.18)}{=} \text{grau}\,(rP_\infty) + \ell(P - rQ_\infty) - \text{grau}\,(rP_\infty - D) - \ell(W - rP_\infty + D)\\ &= r + 0 - r + \text{grau}\ D - 0 = \text{grau}\ D = q^3.\end{aligned}$$

  Portanto, $C_r = \mathbb{F}_{q^2}^n$.

Agora, vamos estudar os códigos Hermitianos para $0 < r \leq q^3 + q^2 - q - 2$.

Proposição 3.3.2. O código dual de C_r é $C_r^\perp = C_{q^3+q^2-q-2-r}$. Portanto, C_r é auto - ortogonal se $2r \leq q^3 + q^2 - q - 2$ e é auto - dual para $r = (q^3 + q^2 - q - 2)/2$.

Demonstração. Consideremos $t := \prod_{\alpha\in\mathbb{F}_{q^2}} (x - \alpha) = x^{q^2} - x$.
Afirmamos que t é elemento primo para todos os lugares $P_{\alpha,\beta} \leq D$ e seu divisor principal é $(t) = D - q^3P_\infty$.
De fato, como

$$v_{P_{\alpha_i,\beta}}(t) = v_{P_{\alpha_i,\beta}}\left(\prod_{\alpha\in\mathbb{F}_{q^2}} (x - \alpha)\right) = v_{P_{\alpha_i,\beta}}\left((x - \alpha_i)\prod_{\alpha\neq\alpha_i} (x - \alpha)\right) = 1$$

então, t é elemento primo. Por outro lado, temos $(t) = (t)_0 - (t)_\infty$.
Sabemos que t tem um único polo em P_∞ de ordem q^3, então $(t)_\infty = q^3Q_\infty$; e os zeros de t cumprem $x^{q^2} - x = 0$ se $x \in \mathbb{F}_{q^2}$. Logo $t = 0$ em todos os q^3 lugares que constituem D, o que implica $(t)_0 = D$. Portanto $(t) = D - q^3P_\infty$.
Determinamos o diferencial (veja [18, Capítulo 4]) de t

$$dt = d(x^{q^2} - x) = (q^2x^{q^2-1} - 1)dx = dx.$$

Logo $(dt) = (dx) = (2g - 2)P_\infty = (q^2 - q - 2)P_\infty$ e grau $(dt) =$ grau $(dx) = 2g - 2$, pois é canônico. Logo $C_r = C_{\mathscr{L}}(D, rP_\infty)$ e pelo Teorema 3.2.8, temos $C_r^\perp = C_\Omega(D, rP_\infty)$. Por outro

lado, temos

$$\begin{aligned} C_\Omega(D, rP_\infty) &= C_{\mathscr{L}}(D, D - rP_\infty + (dt) - (t)) \\ &= C_{\mathscr{L}}(D, D - (t) - rP_\infty + (q^2 - q - 2)P_\infty) \\ &= C_{\mathscr{L}}(D, q^3P_\infty - rP_\infty + (q^2 - q - 2)P_\infty) \\ &= C_{\mathscr{L}}(D, (q^3 + q^2 - q - 2 - r)P_\infty) \\ &= C_{q^3+q^2-q-2-r}. \end{aligned}$$

Portanto $C_r^\perp = C_{q^3+q^2-q-2-r}$.
Se $2r \leq q^3 + q^2 - q - 2$, então $r \leq q^3 + q^2 - q - 2 - r$. Assim $C_r \subseteq C_{q^3+q^2-q-2-r} = C_r^\perp$.
Se $r = (q^3 + q^2 - q - 2)/2$, então $r = q^3 + q^2 - q - 2 - r$. Assim $C_r = C_r^\perp$. □

Nosso próximo objetivo é determinar os parâmetros do código C_r. Da Definição 2.6.6, consideremos o conjunto I de ordem de polos de P_∞, isto é,

$$I := \{m \geq 0 \mid \text{existe } z \in H \text{ com } (z)_\infty = mP_\infty\}.$$

As funções com polo apenas em P_∞ são combinações de elementos da forma $x^i y^j$. Assim, tem-se que

$$\mathscr{L}(rP_\infty) = \left\langle x^i y^j \;\middle|\; iq + j(q+1) \leq r,\ 0 \leq i,\ 0 \leq j \leq q-1 \right\rangle.$$

Para $s \geq 0$ temos

$$I(s) := \{m \in I \mid m \leq s\}. \tag{3.4}$$

Então, pelo teorema de Riemann-Roch, para $s \geq 2g - 2 = q^2 - q - 1$ temos

$$\begin{aligned} |I(s)| = |\{m \in I \mid m \leq s\}| &= \dim \mathscr{L}(sP_\infty) = \ell(sP_\infty) \\ &= \text{grau}\,(sP_\infty) + 1 - g + \ell(W - sP_\infty) = s + 1 - g + 0 \\ &= s + 1 - q(q-1)/2. \end{aligned}$$

A partir da Definição 2.6.6, definimos:

Definição 3.3.3 (Semigrupo de Weierstrass)**.** Seja P um lugar de F/K. O seu semigrupo de Weierstrass associado a P é dado por

$$H(P) := \{m \in \mathbb{N}_0 \mid m \text{ é uma ordem de polo de } P\}.$$

Proposição 3.3.4. O semigrupo de Weierstrass de P_∞, no corpo de funções hermitianas é

$$H(P_\infty) = \langle q, q+1 \rangle.$$

Demonstração. Veja [2, Proposição 1.8] □

Da definição acima, obtemos a seguinte descrição de $I(s)$.

$$I(s) = \{m \leq s \mid m = iq + j(q+1), i \leq 0, 0 \leq j \leq q-1\}.$$

Então

$$|I(s)| = |\{(i,j) \in \mathbb{N}_0^2 \mid j \leq q-1, iq + j(q+1) \leq s\}|.$$

Proposição 3.3.5. Suponha que $0 \leq r \leq q^3 + q^2 - q - 2$. Então

a) A dimensão de C_r é dada por

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

onde $s := q^3 + q^2 - q - 2 - r$ e $I(r)$ definida em (3.4).

b) Para $q^2 - q - 2 < r < q^3$ temos $\dim C_r = r + 1 - q(q-1)/2$.

c) A distância mínima d de C_r satisfaz $d \geq q^3 - r$.
Se $0 \leq r < q^3$ e ambos números r e $q^3 - r$ são ordens de polo de P_∞, então, $d = q^3 - r$.

Demonstração. a) Para $0 \leq r < q^3$, pelo Corolário 3.2.3(a) temos

$$\dim C_r = \dim \mathscr{L}(rP_\infty) = |I(r)|$$

Para $q^3 \leq r \leq q^3 + q^2 - q - 2$, como $s = q^3 + q^2 - q - 2 - r$ temos $0 \leq s \leq q^2 - q - 2 < q^3$. Pela Proposição 3.3.2, obtemos $C_r^\perp = C_s$. Logo

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

b) Para $q^2 - q - 2 = 2g - 2 < r < q^3$, pelo Corolário 3.2.3(b) temos

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

c) Pelo Teorema 3.2.2, temos $d \geq q^3 - r$.
Seja $0 \leq r \leq q^3$ e assumimos que r e $q^3 - r$ são ordens de polo de P_∞. Para provar que $d = q^3 - r$, analisaremos três casos:

- Caso 1: $r = q^3 - q^2$.

  Definimos $i := q^2 - q$ elementos distintos $\alpha_1, \ldots, \alpha_i \in \mathbb{F}_{q^2}$. Definimos o elemento

  $$z := \prod_{v=1}^{i}(x - \alpha_v).$$

  Vamos a provar que $z \in \mathscr{L}(rP_\infty)$.

  Para cada $\alpha \in \mathbb{F}_{q^2}$, $x - \alpha = 0$ em $P_{\alpha,\beta}$ com $\beta^q + \beta = \alpha^{q+1}$ tem exatamente q zeros $P_{\alpha,\beta}$ de grau um. Além, $x - \alpha$ tem um único polo em P_∞ de ordem q. Portanto, o divisor principal é

  $$(x - \alpha) = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - qP_\infty.$$

  Como z é produto de i fatores $(x - \alpha_v)$, somamos os divisores

  $$(z) = \sum_{v=1}^{i}(x - \alpha_v) = \sum_{v=1}^{i}\left(\sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - qP_\infty\right) = \sum_{v=1}^{i}\sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - iqP_\infty.$$

  Logo (z) tem iq zeros e a ordem de polo em P_∞ é iq, mas

  $$iq = (q^2 - q)q = q^3 - q^2 = r,$$

  logo $(z)_\infty = iqP_\infty = rP_\infty$. Portanto $z \in \mathscr{L}(rP_\infty)$.

  Dada a aplicação de avaliação

  $$\begin{aligned} \mathrm{ev}_D \colon \mathscr{L}(rP_\infty) &\longrightarrow C_{\mathscr{L}}(D, rP_\infty) \\ z &\longmapsto (z(P_{\alpha_1,\beta}), \ldots, z(P_{\alpha_n,\beta})) \end{aligned}$$

  z se anula em $r = iq$, coordenadas de $\mathrm{ev}_D(z)$, logo

  $$\mathrm{wt}\ (\mathrm{ev}_D(z)) = n - r = q^3 - r = d.$$

- Caso 2: $r < q^3 - q^2$.

  Consideremos $r = iq + j(q + 1)$, com $r \geq 0$ e $0 \leq j \leq q - 1$. Assim

  $$iq < r < q^3 - q^2 \Longrightarrow i < q^2 - q \Longrightarrow i \leq q^2 - q - 1.$$

  Fixamos um elemento $0 \neq \gamma \in \mathbb{F}_q$ e consideremos o conjunto

  $$A := \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^{q+1} \neq \gamma\}.$$

  Para $\gamma \neq 0$, $\alpha^{q+1} = \gamma$ tem exatamente $q + 1$ soluções em $\mathbb{F}_{q^2}^*$. Então

  $$|A| = q^2 - (q + 1) = q^2 - q - 1 \geq i.$$

Logo, escolhemos i elementos distintos $\alpha_1, \ldots, \alpha_i \in A$. Definimos o elemento

$$z_1 := \prod_{v=1}^{i}(x - \alpha_v).$$

Similar ao feito no caso anterior, obtemos que z_1 tem iq zeros $P_{\alpha,\beta}$ e a ordem de polo em Q_∞ é iq, logo $(z_1)_\infty = iqP_\infty$. Portanto $z_1 \in \mathscr{L}(iqP_\infty)$.

Agora, escolhemos j elementos distintos $\beta_1, \ldots, \beta_j \in \mathbb{F}_{q^2}$, com $\beta_u^q + \beta_u = \gamma$, para $u = 1, \ldots, j$.

Para a equação $\beta^q + \beta = \gamma$, existem exatamente q soluções $\beta \in \mathbb{F}_{q^2}$. Definimos o elemento

$$z_2 := \prod_{u=1}^{j}(y - \beta_u).$$

Para cada $\beta \in \mathbb{F}_{q^2}$, $y - \beta_u$ se anula nos pontos (α, β) tal que $\alpha^{q+1} = \beta^q + \beta = \gamma$. Note que, para $\gamma \neq 0$, existem $q+1$ valores $\alpha \in \mathbb{F}_{q^2}$. Além disso, y tem polo de ordem $q+1$ em P_∞. Então, o divisor principal é

$$(y - \beta) = \sum_{\alpha^{q+1}=\gamma} P_{\alpha,\beta} - (q+1)P_\infty.$$

Portanto, cada $y - \beta_u$ tem $q+1$ zeros distintos. Logo z_2 tem $j(q+1)$ zeros distintos e a ordem de polo em P_∞ é $j(q+1)$, logo $(z_2)_\infty = j(q+1)P_\infty$. Assim $z_1 \in \mathscr{L}(j(q+1)P_\infty)$. Então, definindo

$$z := z_1 z_2 = \left(\prod_{v=1}^{i}(x - \alpha_v)\right)\left(\prod_{u=1}^{j}(y - \beta_u)\right).$$

O número de zeros distintos de z é $iq + j(q+1) = r$ e o polo de z em P_∞ tem ordem $iq + j(q+1)$. Dessa forma $(z)_\infty = rP_\infty$, o que implica que $z \in \mathscr{L}(rP_\infty)$.

- Caso 3: $q^3 - q^2 < r < q^3$.

  Definimos $s := q^3 - r$. Então $0 < s < q^2 \leq q^3 - q^2$. Como $q^3 - r$ é uma ordem de polo do semigrupo de Weierstrass em P_∞, temos que s é uma ordens de polo de P_∞. Logo, pelo Caso 2, existe $z \in H$, com $(z) = D' - sP_\infty$, onde D' é um divisor efetivo que satisfaze $0 \leq D' \leq D$ e grau $D' = s$.

  O elemento $u := x^{q^2} - x \in H$ tem como divisor principal $(u) = D - q^3P_\infty$. Então

$$\begin{aligned}(z^{-1}u) &= (z^{-1}) + (u) = -(z) + (u) = -D' + sP_\infty + D - q^3P_\infty \\ &= (D - D') - (q^3 - s)P_\infty = (D - D') - (q^3 - q^3 + r)P_\infty \\ &= (D - D') - rP_\infty.\end{aligned}$$

Assim $D - D'$ é efetivo e grau $(D - D') =$ grau $D -$ grau $D' = q^3 - s = r$. Então, o divisor de polos de $z^{-1}u$ é $(D - D')$ e seu divisor de zeros é rP_∞. Logo, $\mathrm{ev}_D(z^{-1}u) \in C_r$ tem zeros em exatamente r coordenadas. Assim wt $(\mathrm{ev}_D(z^{-1}u)) = q^3 - r = d$.

□

Exemplo 3.3.6. Consideremos $q = 2$. Então o corpo finito é $\mathbb{F}_2 = \{0, 1\}$ e a curva ermitiana é $y^2 + y = x^3$, com gênero $g = 1$. O polinômio $f(x) = x^2 + x + 1$ é irredutível em $\mathbb{F}_2[x]$, pois não tem raízes em $\mathbb{F}_2$, já que $f(0) = 1$ e $f(1) = 1$.

O corpo $\mathbb{F}_{2^2} = \mathbb{F}_4 = \mathbb{F}_2[x]/\langle f(x)\rangle$ é o corpo de extensão de grau 2 de $\mathbb{F}_2$. Em $\mathbb{F}_4$, se cumpre a relação

$$\alpha^2 + \alpha + 1 = 0 \Longrightarrow \alpha^2 = \alpha + 1$$

então, os elementos de $\mathbb{F}_4$ tem a forma $a + b\alpha$ com $a, b \in \mathbb{F}_2$. Assim $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$.

Os pontos afins ou lugares de grau um do corpo de funções hermitianas, são

$$\{(0,0), (0,1), (1,\alpha), (1,\alpha+1), (\alpha,\alpha), (\alpha,\alpha+1), (\alpha+1,\alpha), (\alpha+1,\alpha+1)\}.$$

Note que para cada $x \in \mathbb{F}_4$, existe exatamente 2 valores em $\mathbb{F}_4$ satisfazendo $y^2 + y = x^3$.

Homogenizamos a equação, em coordenadas projetivas $[x : y : z]$:

$$y^2z + yz^2 = x^3$$

Se $z = 0$, temos $0 = x^3 \Longrightarrow x = 0$. Logo, o único lugar no infinito é $P_\infty = [0 : 1 : 0]$. Então,

$$D = P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_7 + P_8 \quad \text{e} \quad G = rP_\infty,\ r \geq 0$$

O espaço de Riemann-Roch é $\mathscr{L}(G) = \{z \in H \mid G + (z) \geq 0\}$, assim

$$\mathscr{L}(rP_\infty) = \langle x^i y^j : i \geq 0, 0 \leq j \leq 1\rangle,\ \text{onde } 2i + 3j \leq r$$

Vamos considerar $r = 4$:

$$\mathscr{L}(4P_\infty) = \langle 1, x, y, x^2\rangle$$

A matriz geradora de $C_4 := C_{\mathscr{L}}(D, 4P_\infty)$ é

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha & \alpha+1 & \alpha & \alpha+1 & \alpha & \alpha+1 \\ 0 & 0 & 1 & 1 & \alpha+1 & \alpha+1 & \alpha & \alpha \end{bmatrix}$$

Além disso, $d \geq n - \deg G = 8 - 4 = 4$, mas como $0 \leq r \leq 8$ e $r = 4 = q^3 - r$ são ordens de polo de P_∞, pois $4 \in H(P_\infty)$, temos que a distancia mínima é exatamente $d = 4$. Por outro lado, como $8 > \deg G = 4 > 2g - 2 = 0$, então $k = \deg G + 1 - g = 4 + 1 - 1 = 4$. Portanto C_4 é um código $[8, 4, 4]$.

Capítulo 4

Códigos AG de dois pontos sobre a curva norma–traço

Nesta seção, analisamos o semigrupo de Weierstrass de dois pontos racionais sobre a curva norma-traço, dando continuidade e aprofundando os resultados obtidos em [11].

As curvas norma-traço são curvas algébricas definidas por relações entre norma e traço em extensões de corpos finitos. Elas são fundamentais nos códigos AG, pois fornecem muitos pontos racionais para avaliação, permitindo construir códigos altamente eficientes e robustos. São consideradas como a generalização das curvas Hermitianas.

As curvas norma-traço foram estudadas em diversos artigos recentes e clássicos, sendo usadas para construir códigos AG em um ponto e variantes mais sofisticadas. Geil em [5], apresenta uma nova construção de códigos e estuda, em particular, códigos associados às curvas norma–traço.

Seja $\mathcal{X}$ uma curva algébrica, não singular, projetiva, geometricamente irredutível, de gênero g sobre o corpo finito $\mathbb{F}_q$.

Seja P um ponto racional (ou lugar) sobre $\mathcal{X}$. Da Definição 3.3.3, temos que o semigrupo

$$H(P) := \{m \in \mathbb{N}_0 \mid \text{ existe } f \in \mathcal{X}(\mathbb{F}_q) \text{ com } (f)_\infty = mP\}$$

é o semigrupo de Weierstrass de P em $\mathcal{X}$. Seu complemento $G(P) := \mathbb{N}_0 \setminus H(P)$ é o conjunto das lacunas de Weierstrass. $G(P)$ tem exatamente g elementos.
Agora, definimos o semigrupo de Weierstrass para dos pontos.

Definição 4.0.1. Dados P_1 e P_2 pontos racionais distintos sobre $\mathcal{X}$. O Semigrupo de Weierstrass de P_1 e P_2 em $\mathcal{X}$ é:

$$H(P_1, P_2) := \left\{(n, m) \in \mathbb{N}_0^2 \mid \text{ existe } f \in \mathcal{X}(\mathbb{F}_q) \text{ com } (f)_\infty = nP_1 + mP_2\right\}.$$

O conjunto $G(P_1, P_2) := \mathbb{N}_0^2 \setminus H(P_1, P_2)$ é chamado de conjunto das lacunas de Weierstrass para o par (P_1, P_2). $G(P_1, P_2)$ é sempre finita e sua cardinalidade depende de P_1 e P_2.

Observação 4.0.2. Se $(m, n) \in H(P_1, P_2)$ então $(n, m) \in H(P_2, P_1)$.

Agora, introduzimos as definições sobre a função traço e a função norma, os quais podem ser aprofundadas em [12]. Eles permitem definir a curva norma-traço.

Definição 4.0.3. Sejam $F = \mathbb{F}_{q^r}$ e $K = \mathbb{F}_q$. Para $a \in F$, a norma $\mathscr{N}_{F/K}(a)$ de a sobre K é definida por

$$\mathscr{N}_{F/K}(a) = a \cdot a^q \cdot \cdots \cdot a^{q^{r-1}} = a^{\frac{q^r-1}{q-1}}.$$

Para $b \in F$, o traço $\mathcal{T}_{F/K}(b)$ de b sobre K é definido por

$$\mathcal{T}_{F/K}(b) = b + b^q + \cdots + b^{q^{r-1}}.$$

Definição 4.0.4. Seja q um número primo e $r \geq 2$ um inteiro. A curva $\mathcal{X}_{q,r}$, definida sobre $\mathbb{F}_{q^r}$ pela equação afim

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$$

é chamada de curva norma-traço.

- Se $r = 2$, então $\mathcal{X}_{q,r}$ é $x^{q+1} = y^q + y$ (curva Hermitiana).
- Os zeros da curva $x^{\frac{q^r-1}{q-1}} - \left(y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y\right) = 0$ em $\mathbb{F}_{q^r}^2$, são os pares $(a, b) \in \mathbb{F}_{q^r}^2$ tal que $\mathscr{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a) = \mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(b)$.
- $\mathcal{X}_{q,r}$ tem um único ponto racional no infinito $P_\infty = (0 : 1 : 0)$.
- A função traço é sobrejetora sobre $\mathbb{F}_q$ e para cada α em $\mathbb{F}_{q^r}$ existem q^{r-1} elementos em $\mathbb{F}_{q^r}$ que tem o mesmo traço, pelo que possui q^{2r-1} pontos racionais afins (veja [5, Lema 2]).
- O gênero de $\mathcal{X}_{q,r}$ é $g = (q^{r-1} - 1)\left(\frac{q^r - 1}{q - 1} - 1\right)/2$.

4.1 Semigrupo de Weierstrass sobre a curva norma–traço

O estudo dos semigrupos de Weierstrass em dois pontos é fundamental porque conecta a geometria algébrica com aplicações práticas em teoria de códigos e curvas algébricas, permitindo construir códigos AG de dois pontos mais eficientes.

Homma e Kim em [6] investigaram semigrupos de Weierstrass em dois pontos sobre as curvas Hermitianas, e mostraram como calcular explicitamente esses conjuntos. Além disso, Matthews em [13] trabalhou na aplicação dos semigrupos de Weierstrass em códigos AG, explorando como a estrutura melhora os parâmetros.

Seja $P_{a,b}$ um zero comum de $x-a$ e $y-b$, onde $a,b \in \mathbb{F}_{q^r}$. Os divisores das funções x e y são dados por

$$(x) = P_{0,0} + \sum_b P_{0,b} - q^{r-1}P_\infty, \ (y) = \frac{q^r-1}{q-1}P_{0,0} - \frac{q^r-1}{q-1}P_\infty, \tag{4.1}$$

onde b são as $q^{r-1}-1$ raízes da equação $t^{q^{r-1}} + \cdots + t + 1 = 0$. Como $|G(P)| = g$, temos

$$H(P_\infty) = \langle q^{r-1}, (q^r-1)/(q-1)\rangle.$$

Note que, para $b \in \mathbb{F}_{q^r}$ tal que $\mathcal{T}_{F/K}(b) = 0$, temos que o semigrupo $H(P_{0,b})$ também é gerado pelos mesmos elementos que gera o semigrupo $H(P_{0,0})$, pelo que mostraremos só para $H(P_{0,0})$.

No caso que $r = 2$ temos a curva hermitiana. Agora, estudamos para o caso $r \geq 3$. Primeiramente, para o caso $q = 2$ e logo, para o caso $q \geq 3$.

4.1.1 Semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ para $q = 2$.

A curva norma-traço tem gênero $g = (2^{r-1}-1)^2$ e $H(P_\infty) = \langle 2^{r-1}, 2^r - 1\rangle$.

Proposição 4.1.1. Seja $\gamma = 2^r - 2$. O semigrupo de Weierstrass de $\mathcal{X}_{2,r}$ em $P_{0,0}$ está dado por

$$H(P_{0,0}) = \left\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma - \left(\frac{\gamma}{2}-1\right)\right\rangle.$$

Demonstração. Temos

$$(x) = P_{0,0} + \sum_b P_{0,b} - 2^{r-1}P_\infty, \ \ (y) = (2^r-1)P_{0,0} - (2^r-1)P_\infty.$$

Então, os divisores das funções racionais $\dfrac{x}{y}$ e $\dfrac{1}{y}$ são

$$\begin{aligned}\left(\frac{x}{y}\right) &= (x) - (y) = P_{0,0} + \sum_b P_{0,b} - 2^{r-1}P_\infty - (2^r-1)P_{0,0} + (2^r-1)P_\infty \\ &= -(2^r-2)P_{0,0} + \sum_b P_{0,b} + (2^{r-1}-1)P_\infty = -\gamma P_{0,0} + \sum_b P_{0,b} + (\frac{\gamma}{2})P_\infty\end{aligned}$$

e

$$\left(\frac{1}{y}\right) = -(y) = -(2^r-1)P_{0,0} + (2^r-1)P_\infty = -(\gamma+1)P_{0,0} + (\gamma+1)P_\infty.$$

Logo, os divisores de polos são

$$\left(\frac{x}{y}\right)_\infty = \gamma P_{0,0} \text{ e } \left(\frac{1}{y}\right)_\infty = (\gamma+1)P_{0,0}.$$

Além disso, dado um inteiro m satisfazendo $0 \leq m \leq 2^{r-2}+2^{r-3}+\cdots+2 = 2^{r-1}-2$ é possível expressar

$$2m+2+1 = 2(m+1)+1 = 2(m+1)-m+(m+1),$$
$$m+2 = 2m-m+2 = 2(m+1)-m.$$

Assim, a função pode ser escrito como

$$\frac{x^{2m+2+1}}{y^{m+2}} = \frac{x^{2(m+1)-m+(m+1)}}{y^{2(m+1)-m}} = \left[\frac{x}{y}\right]^{2(m+1)-m} \cdot x^{m+1}$$

Logo, determinamos o divisor

$$\begin{aligned}
\left(\frac{x^{2m+2+1}}{y^{m+2}}\right) &= [2(m+1)-m]\left(\frac{x}{y}\right) + [m+1](x) \\
&= [m+2]\left(-\gamma P_{0,0} + \sum_b P_{0,b} + (\frac{\gamma}{2})P_\infty\right) + [m+1](P_{0,0} + \sum_b P_{0,b} - (\frac{\gamma}{2}+1)P_\infty) \\
&= [-(m+2)\gamma + (m+1)]P_{0,0} + [2m+3]\sum_b P_{0,b} + -(\frac{\gamma}{2} - (m+1))P_\infty \\
&= -[(2(m+1)-m)\gamma - (m+1)]P_{0,0} + [2m+3]\sum_b P_{0,b} + -(\frac{\gamma}{2} - (m+1))P_\infty.
\end{aligned}$$

Dessa forma, o divisor de polos é

$$\left(\frac{x^{2m+2+1}}{y^{m+2}}\right)_\infty = [(2(m+1)-m)\gamma - (m+1)]P_{0,0}.$$

Logo,

- Para $m=0$: $\left(\frac{x^3}{y^2}\right)_\infty = [2\gamma-1]P_{0,0}$.
- Para $m=1$: $\left(\frac{x^5}{y^3}\right)_\infty = [3\gamma-2]P_{0,0}$.
- Para $m=2$: $\left(\frac{x^7}{y^4}\right)_\infty = [4\gamma-3]P_{0,0}$.

  $\vdots$

- Para $m=2^{r-1}-2$: $\left(\frac{x^{2m+2+1}}{y^{m+2}}\right)_\infty = [\frac{\gamma}{2}\gamma - (\frac{\gamma}{2}-1)]P_{0,0}$.

Portanto, temos $\gamma, \gamma+1, 2\gamma-1, 3\gamma-2, 4\gamma-3, \cdots, \frac{\gamma}{2}\gamma-(\frac{\gamma}{2}-1) \in H(P_{0,0})$.
Mas, os elementos do conjunto $\left\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma-\left(\frac{\gamma}{2}-1\right)\right\rangle$ são

$$\underbrace{0,\ \gamma}_{\gamma-1}, \underbrace{\gamma+1, 2\gamma-1}_{\gamma-3},\ 2\gamma,\ 2\gamma+1, \underbrace{2\gamma+2, 3\gamma-2}_{\gamma-5},\ 3\gamma-1,\ 3\gamma,\ 3\gamma+1,\ 3\gamma+2,$$
$$\underbrace{3\gamma+3, 4\gamma-3}_{\gamma-7},\ 4\gamma-2,\ 4\gamma-1,\ 4\gamma, 4\gamma+1, 4\gamma+2, 4\gamma+3, \ldots,\ \tfrac{\gamma}{2}\gamma-\left(\tfrac{\gamma}{2}-1\right).$$

Note que, entre 0 e γ existem $\gamma-1$ elementos, entre $\gamma+1$ e $2\gamma+2$ existem $\gamma-2$, entre $2\gamma+2$ e $3\gamma-2$, existem $\gamma-3$ elementos que não pertencem a $H(P_{0,0})$, e assim sucessivamente. Dessa forma, a quantidade de elementos que não pertencem no semigrupo é

$$\begin{aligned}|G(P_{0,0})| &= (\gamma-1)+(\gamma-3)+\cdots+3+1 = \left(\frac{\gamma}{2}\right)^2 = \left(\frac{2^r-2}{2}\right)^2 \\ &= \left(2^{r-1}-1\right)^2 = g.\end{aligned}$$

Portanto, concluímos $H(P_{0,0}) = \left\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma-\left(\frac{\gamma}{2}-1\right)\right\rangle$. □

Agora estudamos os semigrupos em dois pontos.
Dados $P_1, P_2 \in \mathcal{X}_{2,r}(\mathbb{F}_{2^r})$, para $\alpha \in G(P_1)$, definimos $\beta_\alpha := \min\{\beta \in \mathbb{N}_0 \mid (\alpha,\beta) \in H(P_1,P_2)\}$. Então $G(P_2) = \{\beta_\alpha \mid \alpha \in G(P_1)\}$ (veja [9, Lema 2.6]).

Sejam $\alpha_1 < \alpha_2 < \cdots < \alpha_g$ a sequência de lacunas em P_1 e $\beta_1 < \beta_2 < \cdots < \beta_g$ a sequência de lacunas em P_2. Definimos a aplicação injetora

$$\begin{aligned}\sigma\colon G(P_1) &\longrightarrow G(P_2) \\ \alpha_i &\longmapsto \beta_{\alpha_i} = \beta_{\sigma(i)}\end{aligned}$$

para todo $i = 1, \ldots, g$, onde σ é uma permutação do conjunto $\{1, \ldots, g\}$. Denotamos por $\sigma(P_1, P_2)$ essa permutação. O gráfico da aplicação entre $G(P_1)$ e $G(P_2)$ denotado por $\Gamma(P_1, P_2)$, é definido por

$$\Gamma(P_1,P_2) := \{(\alpha_i, \beta_{\sigma(i)}) : i = 1, \ldots, g\} = \{(\alpha_i, \beta_{\alpha_i}) : i = 1, \ldots, g\}.$$

O conjunto $\Gamma(P_1, P_2)$ é denominado conjunto gerador minimal do semigrupo de Weierstrass $H(P_1, P_2)$.

Lema 4.1.2. Seja Γ' um subconjunto de $(G(P_1)\times G(P_2)) \cap H(P_1,P_2)$. Se existe uma permutação τ de $\{1, \ldots, g\}$ tal que $\Gamma'(P_1,P_2) = \{(\alpha_i, \beta_{\tau(i)}) : i = 1, \ldots, g\}$, então $\Gamma' = \Gamma(P_1, P_2)$.

Demonstração. Para $\alpha \in G(P_1)$, temos $\beta_\alpha = \min\{\beta \in \mathbb{N}_0 \mid (\alpha,\beta) \in H(P_1,P_2)\}$. Pela hipótese, temos $\Gamma' \subseteq H(P_1,P_2)$, logo $(\alpha_i, \beta_{\tau(i)}) \in H(P_1,P_2)$, para todo $i = 1, \ldots, g$. Isso implica que

$\beta_{\tau(i)} \geq \beta_{\alpha_i} = \beta_{\sigma(i)}$, para $i = 1, \ldots, g$. Logo os conjuntos $\{\beta_{\sigma(i)} : i = 1, \ldots, g\}$ e $\{\beta_{\tau(i)} : i = 1, \ldots, g\}$ são exatamente iguais, ou seja $\beta_{\sigma(i)} = \beta_{\tau(i)}$, para todo $i = 1, \ldots, g$. Assim $\sigma = \tau$. Portanto $\Gamma' = \Gamma(P_1, P_2)$. □

Teorema 4.1.3. Consideremos o semigrupo $H(P_\infty, P_{0,0})$. Então,

$$\beta_{2(i-j)a+j} = (2a-1)j - 2i,\ 1 \leq j \leq i \leq a-1;$$
$$\beta_{(2(i-j)+1)a+j} = (2a-1)j - (2i+1),\ 1 \leq j \leq i \leq a-2;$$

onde $a = 2^{r-1}$.

Demonstração. Vamos a provar a primeira igualdade. Temos os divisores

$$(x) = P_{0,0} + \sum_b P_{0,b} - 2^{r-1}P_\infty,\ (y) = (2^r-1)P_{0,0} - (2^r-1)P_\infty$$

Logo, determinamos as valorizações discretas associadas a P_∞

- $v_{P_\infty}(x) = -2^{r-1} = -a$.
- $v_{P_\infty}(y) = -(2^r-1) = -(2a-1)$.

Assim, x tem um polo de ordem a em P_∞, e y tem um polo de ordem $(2a-1)$ em P_∞. Consideremos a função racional $f_{i,j} = \dfrac{x^{2i}}{y^j}$, com $1 \leq j \leq i \leq a-1$. Então,

$$\begin{aligned} v_{P_\infty}(f_{i,j}) &= 2iv_{P_\infty}(x) - jv_{P_\infty}(y) = 2i(-a) + j(2a-1) = 2aj - 2ai - j \\ &= 2a(j-i) - j < 0. \end{aligned}$$

Assim, $f_{i,j}$ tem um polo de ordem $2a(i-j)+j$ em P_∞.
Por outro lado,

$$v_{P_{0,0}}(f_{i,j}) = 2iv_{P_{0,0}}(x) - jv_{P_{0,0}}(y) = 2i(1) - j(2a-1) = 2i - j(2a-1).$$

como

$$\begin{aligned} j(2a-1) - 2i &= 2aj - j - 2i = 2aj - 2j + j + 2i = 2j(a-1) + j - 2i \\ &= 2j(a-1) - 2(a-1) + 2(a-1) + j - 2i \\ &= (2j-2)(a-1) + 2(a-1) + j - 2i \\ &= 2(j-1)(a-1) + 2(a-1) - 2i + j > 0. \end{aligned}$$

Então $2i - j(2a-1) < 0$. Assim, $f_{i,j}$ tem um polo de ordem $j(2a-1) - 2i$ em $P_{0,0}$.
Temos $H(P_\infty) = \langle 2^{r-1}, 2^r - 1\rangle = \langle a, 2a-1\rangle$. Como $2a(i-j)+j$ não é possível expressar como

combinação linear de a e $2a-1$ temos $2a(i-j)+j \notin H(P_\infty)$. Logo $2a(i-j)+j \in G(P_\infty)$. Por outro lado, da Proposição 4.1.1, para $\gamma = 2^r - 2$, temos

$$H(P_{0,0}) = \langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma - \Big(\frac{\gamma}{2}-1\Big)\rangle.$$

Reescrevendo em termos de a, temos $\gamma = 2a-2 = 2(a-1)$. Logo

$$H(P_{0,0}) = \langle 2(a-1), 2a-1, 4a-5, 6a-8, \ldots, 2(a-1)^2-(a-2)\rangle.$$

Como $j(2a-1)-2i$ não é possível expressar como uma combinação linear dos elementos geradores de $H(P_{0,0})$, então $j(2a-1)-2i \notin H(P_{0,0})$. Logo $j(2a-1)-2i \in G(P_{0,0})$.
Dessa forma, para cada (i,j), com $1 \leq j \leq i \leq a-1$ temos $2a(i-j)+j \in G(P_\infty)$ e $j(2a-1)-2i \in G(P_{0,0})$.
Vamos mostrar que $2a(i-j)+j \neq 2a(i'-j')+j'$ se $i \neq i'$ e $j \neq j'$.
Suponhamos que é falso, isto é, existem dois pares diferentes (i,j) e (i',j') tal que se cumpre $2a(i-j)+j = 2a(i'-j')+j'$.

- Se $i-j = i'-j'$, então

  $$2a(i'-j')+j' = 2a(i-j)+j = 2a(i'-j')+j \Longrightarrow j' = j \Longrightarrow i = i'.$$

  Assim $(i,j) = (i',j')$ - Absurdo.

- Se $i-j \neq i'-j'$. Assumimos que $i-j > i'-j'$. Então, existe algum $0 < m \in \mathbb{N}$ tal que $i-j = i'-j'+m$. Assim

  $$2a(i'-j')+j' = 2a(i-j)+j = 2a(i'-j'+m)+j = 2a(i'-j')+2am+j.$$

  Logo $j' = 2am+j$ - Absurdo, pois $1 \leq j, j' \leq a-1$.

Agora, mostramos que $j(2a-1)-2i \neq j'(2a-1)-2i'$ se $(i,j) \neq (i',j')$.
Suponhamos que é falso. Assim, existem pares diferentes (i,j) e (i',j') tal que se cumpre $j(2a-1)-2i = j'(2a-1)-2i'$. Logo $i \neq i'$ ou $j \neq j'$.

- Suponhamos que $i > i'$, isto é, existe $m \in \mathbb{N}$, $0 \leq m < a-1$ tal que $i = i'+m$. Então

  $$\begin{aligned} j(2a-1)-2i &= j(2a-1)-2(i'+m) = j(2a-1)-2i'-2m \\ j'(2a-1)-2i' &= j(2a-1)-2i'-2m \\ (j-j')(2a-1) &= 2m < 2a-2 < 2a-1. \end{aligned}$$

  Dessa forma $0 \leq j-j' < 1$. Logo $j = j'$. Assim $m = 0$ e portanto $i = i'$ - Absurdo.

- Suponha que $j > j'$, ou seja, existe existe $m \in \mathbb{N}$, $0 < m < a-1$ tal que $j = j' + m$. Então

$$\begin{aligned} j(2a-1) - 2i &= (j'+m)(2a-1) - 2i = j'(2a-1) + m(2a-1) - 2i \\ j'(2a-1) - 2i' &= j'(2a-1) + m(2a-1) - 2i \\ 2(i-i') &= m(2a-1) \end{aligned}$$

mas $m(2a-1) > m(2a-2) = 2m(a-1)$. Logo $i - i' > m(a-1)$ - Absurdo.

Logo, para $1 \leq j \leq i \leq a-1$, temos

$$(f_{i,j})_\infty = \left(\frac{x^{2i}}{y^j}\right)_\infty = [2a(i-j)+j]P_\infty + [j(2a-1)-2i]P_{0,0}.$$

Assim $(2a(i-j)+j, j(2a-1)-2i) \in H(P_\infty, P_{0,0})$.
Então, se $\alpha_l = 2a(i-j)+j$ e $\beta_{l'} = j(2a-1)-2i$, para $l, l' = 1, \ldots, g$, temos

$$(\alpha_l, \beta_{l'}) \in G(P_\infty) \times G(P_{0,0}) \cap H(P_\infty, P_{0,0}).$$

Seja τ uma permutação de $\{1, \ldots, g\}$ tal que $\tau(l) = l'$. Pelo Lema 4.1.2, temos

$$\Gamma' = \{(\alpha_l, \beta_{\tau(l)}) : l = 1, \ldots, g\} = \Gamma(P_\infty, P_{0,0}).$$

Portanto, obtemos $\beta_{2(i-j)a+j} = (2a-1)j - 2i$.
De forma similar, provaremos a segunda igualdade. Consideramos a função $g_{i,j} = \dfrac{x^{2i+1}}{y^j}$, com $1 \leq j \leq i \leq a-2$. Então

$$\begin{aligned} v_{P_\infty}(g_{i,j}) &= (2i+1)v_{P_\infty}(x) - jv_{P_\infty}(y) = (2i+1)(-a) + j(2a-1) \\ &= 2aj - 2ai - a - j = 2a(j-i) - a - j < 0 \end{aligned}$$

e

$$\begin{aligned} v_{P_{0,0}}(g_{i,j}) &= (2i+1)v_{P_{0,0}}(x) - jv_{P_{0,0}}(y) = (2i+1)(1) - j(2a-1) \\ &= 2i + 1 - j(2a-1) < 0. \end{aligned}$$

Assim, $g_{i,j}$ tem um polo de ordem $(2(i-j)+1)a+j$ em P_∞ e um polo de ordem $j(2a-1)-2i-1$ em $P_{0,0}$.
Como $(2(i-j)+1)a+j$ não é possível expressar como combinação linear de a e $2a-1$ temos $(2(i-j)+1)a+j \notin H(P_\infty)$. Também $j(2a-1)-2i-1$ não é possível expressar como uma combinação linear dos elementos geradores de $H(P_{0,0})$, então $j(2a-1)-2i-1 \notin H(P_{0,0})$.
Logo, $(2(i-j)+1)a+j \in G(P_\infty)$ e $j(2a-1)-2i-1 \in G(P_{0,0})$, para cada (i,j) com

$1 \leq j \leq i \leq a-2$.

Vamos mostrar que $(2(i-j)+1)a+j \neq (2(i'-j')+1)a+j'$ se $i \neq i'$ e $j \neq j'$.

Suponhamos que é falso, isto é, existem dois pares diferentes (i,j) e (i',j') tal que se cumpre $(2(i-j)+1)a+j = (2(i'-j')+1)a+j'$.

- Se $i-j = i'-j'$, então

  $$(2(i'-j')+1)a+j' = (2(i-j)+1)a+j = (2(i'-j')+1)a+j \Longrightarrow j' = j \Longrightarrow i = i'.$$

  Assim $(i,j) = (i',j')$ - Absurdo.

- Se $i-j \neq i'-j'$. Assumimos que $i-j > i'-j'$. Então, existe algum $0 < m \in \mathbb{N}$ tal que $i-j = i'-j'+m$. Assim

  $$\begin{aligned}(2(i'-j')+1)a+j' = (2(i-j)+1)a+j &= (2(i'-j'+m)+1)a+j \\ &= (2(i'-j')+1)a+2am+j.\end{aligned}$$

  Logo $j' = 2am+j > a-1$ - Absurdo, pois $1 \leq j, j' \leq a-1$.

Agora, mostramos que $j(2a-1)-2i-1 \neq j'(2a-1)-2i'-1$ se $(i,j) \neq (i',j')$.

Suponhamos que é falso. Assim, existem pares diferentes (i,j) e (i',j') tal que se cumpre $j(2a-1)-2i-1 = j'(2a-1)-2i'-1$. Logo $i \neq i'$ ou $j \neq j'$. Suponhamos que $i > i'$, isto é, existe $m \in \mathbb{N}$, $1 \leq m < a-1$ tal que $i = i'+m$. Então,

$$\begin{aligned}j(2a-1)-2i-1 &= j(2a-1)-2(i'+m)-1 = j(2a-1)-2i'-2m-1 \\ j'(2a-1)-2i'-1 &= j(2a-1)-2i'-2m-1 \\ (j-j')(2a-1) &= 2m < 2a-2 < 2a-1.\end{aligned}$$

Dessa forma $j-j' < 1$.

Logo para $1 \leq j \leq i \leq a-2$, temos

$$(g_{i,j})_\infty = \left(\frac{x^{2i+1}}{y^j}\right)_\infty = [(2(i-j)+1)a+j]P_\infty + [j(2a-1)-2i-1]P_{0,0}.$$

Assim $(2(i-j)+1)a+j, j(2a-1)-2i-1) \in H(P_\infty, P_{0,0})$.

Então, se $\alpha_l = (2(i-j)+1)a+j$ e $\beta_{l'} = j(2a-1)-2i-1$, para $l,l' = 1,\ldots,g$, temos

$$(\alpha_l, \beta_{l'}) \in G(P_\infty) \times G(P_{0,0}) \cap H(P_\infty, P_{0,0}).$$

Seja τ uma permutação de $\{1,\ldots,g\}$ tal que $\tau(l) = l'$. Pelo Lema 4.1.2, temos

$$\Gamma' = \{(\alpha_l, \beta_{\tau(l)}) : l = 1,\ldots,g\} = \Gamma(P_\infty, P_{0,0}).$$

Portanto, obtemos $\beta_{(2(i-j)+1)a+j} = (2a-1)j-(2i+1)$. □

Pela Observação 4.0.2, para $1 \leq j \leq i \leq a-1$ temos

$$(j(2a-1)-2i-1, 2(i-j)+1)a+j) \in H(P_{0,0}, P_\infty)$$

e para $1 \leq j \leq i \leq a-2$ temos

$$(j(2a-1)-2i, 2a(i-j)+j) \in H(P_{0,0}, P_\infty).$$

Exemplo 4.1.4. Consideremos $q=2$ e $r=3$. A curva norma-traço é $\mathcal{X}_{2,3} : x^7-y^4-y^2+y=0$, cujo gênero é $g=9$. Os semigrupos de Weierstrass são os seguintes:

- $H(P_\infty) = \langle 4, 7\rangle$, ou seja, $H(P_\infty) = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, 19, 20, 21, 22, \dots\}$. Então, o conjunto das lacunas é $G(P_\infty) = \{1, 2, 3, 5, 6, 9, 10, 13, 17\}$.

- Pela Proposição 4.1.1 temos $H(P_{0,0}) = \langle 6, 7, 11, 16\rangle$. Então, o conjunto das lacunas é $G(P_{0,0}) = \{1, 2, 3, 4, 5, 8, 9, 10, 15\}$.

- Pelo Teorema 4.1.3 temos o conjunto

$$\Gamma(P_{0,0}, P_\infty) = \{(1, 17), (2, 13), (3, 9), (4, 5), (5, 1), (8, 10), (9, 6), (10, 2), (15, 3)\}.$$

Definição 4.1.5. Dados $u_1 = (\alpha_1, \beta_1) \in \mathbb{N}_0^2$ e $u_2 = (\alpha_2, \beta_2) \in \mathbb{N}_0^2$. O menor limite superior (lub) de u_1 e u_2 é definido por

$$lub(u_1, u_2) := (\max\{\alpha_1, \alpha_2\}, \max\{\beta_1, \beta_2\}).$$

Proposição 4.1.6. Dados $u_1, u_2 \in H(P_1, P_2)$ temos $lub(u_1, u_2) \in H(P_1, P_2)$.

Demonstração. Sejam $u_1 = (\alpha_1, \beta_1)$, $u_2 = (\alpha_2, \beta_2)$.

- Se $\alpha_1 \geq \alpha_2$ e $\beta_1 \geq \beta_2$, então $lub(u_1, u_2) = u_1 \in H(P_1, P_2)$. Da mesma forma, se $\alpha_2 \geq \alpha_1$ e $\beta_2 \geq \beta_1$, então $lub(u_1, u_2) = u_2 \in H(P_1, P_2)$.

- Assumimos que $\alpha_1 > \alpha_2$ e $\beta_2 > \beta_1$. Então

$$lub(u_1, u_2) := (\max\{\alpha_1, \alpha_2\}, \max\{\beta_1, \beta_2\}) = (\alpha_1, \beta_2).$$

Como $u_1, u_2 \in H(P_1, P_2)$, existem f_1 e f_2 funções racionais satisfazendo

$$(f_1)_\infty = \alpha_1 P_1 + \beta_1 P_2 \text{ e } (f_2)_\infty = \alpha_2 P_1 + \beta_2 P_2.$$

Logo

$$\begin{aligned}(f_1+f_2)_\infty &= -\sum_{i=1}^{2}(\min\{v_{P_i}(f_1), v_{P_i}(f_2)\})P_i \\ &= -(\min\{v_{P_1}(f_1), v_{P_1}(f_2)\})P_1 - (\min\{v_{P_2}(f_1), v_{P_2}(f_2)\})P_2 \\ &= -(\min\{-\alpha_1, -\alpha_2\})P_1 - (\min\{-\beta_1, -\beta_2\})P_2 \\ &= \alpha_1 P_1 + \beta_2 P_2.\end{aligned}$$

Dessa forma $lub(u_1, u_2) = (\alpha_1, \beta_2) \in H(P_1, P_2)$.

□

Lema 4.1.7. Sejam P_1, P_2 dois pontos racionais distintos. Então

$$H(P_1, P_2) = \{lub(u_1, u_2) \mid u_1, u_2 \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

Demonstração. Veja [9, Lema 2] □

4.1.2 Semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ para algum q

Consideremos $a = ((q^r-1)/(q-1)) - 1$. Das equações dadas em (4.1) temos

$$\begin{aligned}\left(\frac{x}{y}\right) = (x) - (y) &= P_{0,0} + \sum_b P_{0,b} - q^{r-1}P_\infty - \frac{q^r-1}{q-1}P_{0,0} + \frac{q^r-1}{q-1}P_\infty \\ &= \left(1 - \frac{q^r-1}{q-1}\right)P_{0,0} + \sum_b P_{0,b} + \left(\frac{q^r-1}{q-1} - q^{r-1}\right)P_\infty \\ &= -aP_{0,0} + \sum_b P_{0,b} + \left(\frac{q^{r-1}-1}{q-1}\right)P_\infty\end{aligned}$$

e

$$\left(\frac{1}{y}\right) = -(y) = -\frac{q^r-1}{q-1}P_{0,0} + \frac{q^r-1}{q-1}P_\infty = -(a+1)P_{0,0} + (a+1)P_\infty.$$

Então, os divisores de polo são

$$\left(\frac{x}{y}\right)_\infty = aP_{0,0} \text{ e } \left(\frac{1}{y}\right)_\infty = (a+1)P_{0,0}.$$

Para $0 \le m \le q^{r-2} + q^{r-3} + \cdots + q - 1$, temos

$$mq + q + 1 = (m+1)q + 1 = (m+1)q - m + m + 1 = [(m+1)q - m] + (m+1)$$

$$m(q-1) + q = mq - m + q = (m+1)q - m$$

Assim, a função racional pode ser expressado da seguente forma

$$\frac{x^{mq+q+1}}{y^{m(q-1)+q}} = \left[\frac{x}{y}\right]^{(m+1)q-m} \cdot x^{m+1}$$

e o seu divisor é

$$\begin{aligned}
\left(\frac{x^{mq+q+1}}{y^{m(q-1)+q}}\right) =& [(m+1)q-m]\left(\frac{x}{y}\right) + [m+1](x) \\
=& [(m+1)q-m]\left[-aP_{0,0} + \sum_b P_{0,b} + \left(\frac{q^{r-1}-1}{q-1}\right)P_\infty\right] \\
&+ [m+1]\left[P_{0,0} + \sum_b P_{0,b} - q^{r-1}P_\infty\right] \\
=& [-[(m+1)q-m]a + (m+1)]P_{0,0} + [(m+1)q-m+(m+1)]\sum_b P_{0,b} \\
&+ \left[[(m+1)q-m+(m+1)]\left(\frac{q^{r-1}-1}{q-1}\right) - [m+1]q^{r-1}\right]P_\infty.
\end{aligned}$$

Logo, o divisor de polos é

$$\left(\frac{x^{mq+q+1}}{y^{m(q-1)+q}}\right)_\infty = [[(m+1)q-m]a - (m+1)]P_{0,0}. \tag{4.2}$$

Proposição 4.1.8. O Semigrupo de Weierstrass $H(P_{0,0})$ é dado por

$$H(P_{0,0}) = \langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)\rangle,$$

onde $\lambda = q^{r-2} + q^{r-3} + \cdots + q - 1$.

Demonstração. Seja $0 \leq m \leq q^{r-2} + q^{r-3} + \cdots + q - 1 = \lambda$. Então, substituindo cada valor de m na equação (4.2), obtemos que

$$qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1) \in H(P_{0,0})$$

Além disso, $a, a+1 \in H(P_{0,0})$.

Agora vamos mostrar que $\langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)\rangle$ tem g lacunas.

Note que, escrevendo por extensão o conjunto gerado, podemos identificar as lacunas

$$\underbrace{0, a}_{a-1}, \underbrace{a+1, 2a}_{a-2}, 2a+1, \ldots \underbrace{2a+2, 3a}_{a-3}, 3a+1, 3a+2, \underbrace{3a+3, 4a}_{a-4}, 4a+1, \ldots, \underbrace{4a+4, 5a}_{a-5},$$
$$5a+1, 5a+2, \ldots, \underbrace{5a+5, 6a}_{a-6}, \ldots, \underbrace{(q-2)a+(q-2), (q-1)a}_{a-(q-1)}, (q-1)a+1, \ldots$$
$$\underbrace{(q-1)a+(q-1), qa-1}_{a-(q+1)}, qa, qa+1, \ldots, \underbrace{qa+q, (q+1)a-1}_{a-(q+2)}, \ldots$$

Dessa forma, a quantidade de lacunas é

$$\begin{aligned}
|G(P_{0,0})| =&(a-1)+(a-2)+(a-3)+(a-4)+\cdots+(a-(q-1))+(a-(q+1))+\\
&(a-(q+2))+\cdots+(a-(2q-1))+(a-(2q+1))+(a-(2q+2))+\cdots+\\
&(a-(3q-1))+(a-(3q+1))+(a-(3q+2))+\cdots+(a-(4q-1))\\
&+(a-(4q+1))+(a-(4q+2))+\ldots(q-1)+\cdots+2+1\\
=&(a-1)+(a-2)+(a-3)+(a-4)+\cdots+3+2+1-(a-q)-(a-2q)-\\
&(a-3q)-\cdots-\left(a-\left(\frac{q^{r-1}-1}{q-1}-1\right)q\right)\\
=&\sum_{i=1}^{(a-1)} i-\left(\frac{q^{r-1}-1}{q-1}-1\right)a+q\left(1+2+3+\cdots+\frac{q^{r-1}-1}{q-1}-1\right)\\
=&\frac{(a-1)a}{2}-\left(\frac{q^{r-1}-1}{q-1}-1\right)a+\left(\frac{q^{r-1}-1}{q-1}-1\right)\left(\frac{q^{r-1}-1}{q-1}\right)\frac{q}{2}\\
=&\frac{(a-1)a}{2}-\left(\frac{q^{r-1}-1}{q-1}-1\right)a+\left(\frac{q^{r-1}-1}{q-1}-1\right)\frac{a}{2}\\
=&\frac{(a-1)a}{2}-\left(\frac{q^{r-1}-1}{q-1}-1\right)\frac{a}{2}\\
=&\left(a-\frac{q^{r-1}-1}{q-1}\right)\frac{a}{2}=\left(q\left(\frac{q^{r-1}-1}{q-1}\right)-\frac{q^{r-1}-1}{q-1}\right)\frac{a}{2}\\
=&(q-1)\left(\frac{q^{r-1}-1}{q-1}\right)\frac{a}{2}=(q^{r-1}-1)\frac{a}{2}=g
\end{aligned}$$

Portanto, $H(P_{0,0})=\langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)\rangle$. □

Teorema 4.1.9. Seja q um número primo, $r\geq 3$ e $a=q^{r-1}+q^{r-2}+\cdots+q^2+q$. Consideremos o semigrupo $H(P_{0,0},P_\infty)$. Então, para cada s tal que $1\leq s\leq q^{r-2}+q^{r-3}+\cdots+q+1$ e cada par (i,j) com $1\leq j\leq i\leq a-s$ e $(s-1)q-(s-1)\leq i-j\leq sq-(s+1)$, temos

$$\beta_{(i-j)(a+1)+j}=(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}.$$

Demonstração. Vamos mostrar que se $(i,j)\neq(i',j')$, então $(i-j)(a+1)+j\neq(i'-j')(a+1)+j'$. Suponhamos que é falso. Então, existe $(i,j)\neq(i',j')$ tal que $(i-j)(a+1)+j=(i'-j')(a+1)+j'$.

- Se $i-j=i'-j'$, temos $j=j'$. Logo $i=i'$, o que é uma contradição.
- Se $i-j\neq i'-j'$. Consideremos que $i-j>i'-j'$. Então, existe $m\in\mathbb{N}$ com $1\leq m<q-1$ tal que $i-j=i'-j'+m$. Logo

$$\begin{aligned}
(i-j)(a+1)+j&=(i'-j'+m)(a+1)+j\\
(i'-j')(a+1)+j'&=(i'-j')(a+1)+m(a+1)+j\\
j'&=m(a+1)+j.
\end{aligned}$$

Assim $j' \geq a+1$, o que é absurdo pois $1 \leq j' \leq a-s \leq a-1 < a+1$.

Agora, vamos mostrar que os números $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$ são distintos para distintos pares (i,j).

Suponha que é falso. Então, existe $(i,j) \neq (i',j')$ tal que

$$(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} = (q^{r-1}-(i'-j'+1))(a+1)-j'q^{r-1}.$$

- Se $i-j = i'-j'$ temos $-jq^{r-1} = -j'q^{r-1}$. Então $j = j'$. Logo $i = i'$, o que é uma contradição.

- Se $i-j \neq i'-j'$. Consideremos que $i-j > i'-j'$. Então, existe $m \in \mathbb{N}$ com $1 \leq m < q-1$ tal que $i-j = i'-j'+m$. Logo

$$\begin{aligned}
(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} &= (q^{r-1}-(i'-j'+m+1))(a+1)-jq^{r-1} \\
(q^{r-1}-(i'-j'+1))(a+1)-j'q^{r-1} &= (q^{r-1}-(i'-j'+1))(a+1)+m(a+1)-jq^{r-1} \\
-j'q^{r-1} &= m(a+1)-jq^{r-1} \\
(j-j')q^{r-1} &= m(a+1) \\
(j-j')q^{r-1} &= m(q^{r-1}+q^{r-2}+\cdots+q^2+q+1).
\end{aligned}$$

  Daí $q^{r-1} \mid m(q^{r-1}+q^{r-2}+\cdots+q^2+q+1)$, o qual é uma contradição.

Finalmente, vamos a mostrar que os números $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$ são lacunas em P_∞.

Suponhamos que não são lacunas em P_∞. Então $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} \in H(P_\infty)$, ou seja, existe algum (i_0,j_0) tal que

$$(q^{r-1}-(i_0-j_0+1))(a+1)-j_0q^{r-1} \in \langle q^{r-1}, (q^r-1)/(q-1)\rangle$$

Então, existem $\alpha, \beta \in \mathbb{Z}$ positivos tal que

$$\begin{aligned}
\alpha q^{r-1}+\beta(q^{r-1}+\cdots+q+1) &= (q^{r-1}-(i_0-j_0+1))(a+1)-j_0q^{r-1} \\
\alpha q^{r-1}+\beta(q^{r-1}+\cdots+q+1) &= (q^{r-1}-(i_0-j_0+1))(q^{r-1}+\cdots+q+1)-j_0q^{r-1} \\
(\alpha+j_0)q^{r-1} &= (q^{r-1}-(i_0-j_0+1+\beta))(q^{r-1}+\cdots+q+1).
\end{aligned}$$

Temos $\alpha+j_0 > 0$ e $i_0-j_0+1+\beta > 0$, assim q^{r-1} divide $(q^{r-1}-(i_0-j_0+1+\beta))(q^{r-1}+\cdots+q+1)$, o qual é absurdo, pois $q^{r-1}-(i_0-j_0+1+\beta) < q^{r-1}$ e q é primo.

Pela Proposição 4.1.8, temos $(i-j)(a+1)+j \in G(P_{0,0})$. Logo, o divisor de polos da função racional $f_{i,j} = \dfrac{x^{a+1-j}}{y^{i-j+1}}$ é

$$(f_{i,j})_\infty = [(i-j)(a+1)+j]P_{0,0} + [q^{r-1}-(i-j+1))(a+1)-jq^{r-1}]P_\infty.$$

Dessa forma $((i-j)(a+1)+j, (q^{r-1}-(i-j+1))(a+1)-jq^{r-1}) \in G(P_{0,0})\times G(P_\infty)\cap H(P_{0,0}, P_\infty)$. Sejam $\alpha_1 < \alpha_2 < \cdots < \alpha_g$ e $\beta_1 < \beta_2 < \cdots < \beta_g$ sequencias de lacunas em $P_{0,0}$ e P_∞ respectivamente. Seja τ a permutação de $\{1, \ldots, g\}$ tal que $\beta_{\tau(l)} = (q^{r-1} - (i-j+1))(a+1) - jq^{r-1}$, se $\alpha_l = (i-j)(a+1)+j$, para $l = 1, 2, \ldots, g$. Então

$$\Gamma' = \{(\alpha_l, \beta_{\tau(l)}) : l = 1, 2, \ldots, g\} \subseteq G(P_{0,0}) \times G(P_\infty) \cap H(P_{0,0}, P_\infty)$$

Pelo Lema 4.1.2, $\Gamma' = \Gamma(P_{0,0}, P_\infty)$. Assim $\beta_{(i-j)(a+1)+j} = (q^{r-1} - (i-j+1))(a+1) - jq^{r-1}$. □

4.2 Códigos sobre a curva norma-traço

Nesta secção, mostraremos como a informação sobre o semigrupo de Weierstrass em dois pontos, pode ser usada para melhorar os parâmetros dos códigos AG sobre a curva norma-traço. Para isso, começamos estudando o seguinte teorema, o qual foi demostrado por Matthews em [13].

Teorema 4.2.1. Seja $(\alpha_1, \alpha_2) \in G(Q_1, Q_2)$, com $\alpha_1 \geq 1$ e $\ell(\alpha_1 Q_1 + \alpha_2 Q_2) = \ell((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)$. Suponha que $(\gamma_1, \gamma_2 - t - 1) \in G(Q_1, Q_2)$, para todo $0 \leq t \leq \min\{\gamma_2 - t, 2g-1-(\alpha_1+\alpha_2)\}$. Sejam os divisores $G = (\alpha_1 + \gamma_1 - 1)Q_1 + (\alpha_2 + \gamma_2 - 1)Q_2$ e $D = \sum_{j=1}^{n} P_j$, onde $Q_1, Q_2, P_1, \ldots, P_n$ são pontos racionais distintos sobre a curva $\mathcal{X}$ definida sobre $(\mathbb{F}_q)$. Se a dimensão do código $C_\Omega(D, G)$ é positivo, então sua distância mínima é pelo menos grau $G - 2g + 3$.

Demonstração. Seja $w :=$ grau $G - 2g + 2$. Se existe alguma palavra-código de peso w, então existe uma diferencial de Weil $\eta \in \Omega(G - D)$ com exatamente w polos $P_1, \ldots, P_w$. Então

$$(\eta) \geq G - (P_1 + \cdots + P_w)$$

Como (η) é um divisor canônico, temos

$$2g - 2 = \text{grau}\,(\eta) \geq \text{grau}\; G - w = \text{grau}\; G - \text{grau}\; G + 2g - 2 = 2g - 2$$

Logo $(\eta) = G - (P_1 + \cdots + P_w)$.
Por outro lado, aplicando o Teorema de Riemann-Roch, temos

$$\begin{aligned} \ell(\alpha_1 Q_1 + \alpha_2 Q_2) &= \text{grau}\,(\alpha_1 Q_1 + \alpha_2 Q_2) + 1 - g + \ell(W - (\alpha_1 Q_1 + \alpha_2 Q_2)) \\ &= \alpha_1 + \alpha_2 + 1 - g + \ell(W - (\alpha_1 Q_1 + \alpha_2 Q_2)) \end{aligned}$$

e

$$\begin{aligned} \ell((\alpha_1 - 1)Q_1 + \alpha_2 Q_2) &= \text{grau}\,((\alpha_1 - 1)Q_1 + \alpha_2 Q_2) + 1 - g + \ell(W - ((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)) \\ &= \alpha_1 + \alpha_2 - g + \ell(W - ((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)). \end{aligned}$$

Como pela hipótese $\ell(\alpha_1 Q_1 + \alpha_2 Q_2) = \ell((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)$, então

$$1 + \ell(W - (\alpha_1 Q_1 + \alpha_2 Q_2)) = \ell(W - ((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)).$$

Logo, existe uma função racional h tal que

$$h \in \mathscr{L}(W - ((\alpha_1 - 1)Q_1 + \alpha_2 Q_2)) \setminus \mathscr{L}(W - (\alpha_1 Q_1 + \alpha_2 Q_2)),$$

onde W divisor canônico. Dessa forma,

$$((\alpha_1 - 1)Q_1 + \alpha_2 Q_2) - W \leq (h) < (\alpha_1 Q_1 + \alpha_2 Q_2) - W.$$

Então, $(h) = (\alpha_1 - 1)Q_1 + \alpha_2 Q_2 - W + E$, onde E é efetivo de grau $2g - 1 - (\alpha_1 + \alpha_2)$, com $Q_1 \notin Supp\, E$. Escrevemos $E = E' + tQ_2$, onde E' é efetivo tal que $Q_2 \notin Supp\, E'$. Então, o divisor (h) pode ser expressado como $(h) = (\alpha_1 - 1)Q_1 + (\alpha_2 + t)Q_2 - W + E'$. Logo

$$G - (P_1 + \cdots + P_w) = (\eta) \sim W \sim (\alpha_1 - 1)Q_1 + (\alpha_2 + t)Q_2 + E'.$$

Assim $(\alpha_1 + \gamma_1 - 1)Q_1 + (\alpha_2 + \gamma_2 - 1)Q_2 - (P_1 + \cdots + P_w) \sim (\alpha_1 - 1)Q_1 + (\alpha_2 + t)Q_2 + E'$. Então, existe uma função racional f tal que

$$(\alpha_1 + \gamma_1 - 1)Q_1 + (\alpha_2 + \gamma_2 - 1)Q_2 - (P_1 + \cdots + P_w) + (f) = (\alpha_1 - 1)Q_1 + (\alpha_2 + t)Q_2 + E'$$

$$(f) = -\gamma_1 Q_1 - (\gamma_2 - t - 1)Q_2 + (P_1 + \cdots + P_w) + E'.$$

Se $t \leq \gamma_2 - 1$, o divisor de polos de f seria $(f)_\infty = \gamma_1 Q_1 + (\gamma_2 - t - 1)Q_2$. Logo $(\gamma_1, \gamma_2 - t - 1) \in H(Q_1, Q_2)$, o qual é absurdo, pois $(\gamma_1, \gamma_2 - t - 1) \in G(Q_1, Q_2)$. Logo f tem um divisor de polos $(f)_\infty = \gamma_1 Q_1$, o qual é absurdo, pois γ_1 é uma lacuna em Q_1. □

Teorema 4.2.2. Consideremos o código $C_\Omega(D, G)$ surgindo desde a curva $\mathcal{X}_{q,r}$ definida sobre $\mathbb{F}_{q^r}$, com os divisores $G = (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha_2 + \gamma_2 - 1)P_\infty$ e $D = \sum_{j=1}^{n} P_j$, onde $P_{0,0}, P_\infty, P_1, \ldots, P_n$ são pontos racionais distintos sobre $\mathbb{F}_{q^r}$. Suponha que

a) $\alpha \geq 1$, $(\alpha_1, \alpha) \in G(P_{0,0}, P_\infty)$ e $\ell(\alpha_1 P_{0,0} + \alpha_2 P_\infty) = \ell((\alpha_1 - 1)P_{0,0} + \alpha_2 P_\infty)$.

b) $(\gamma_1 - t - 1, \gamma), (\gamma_1 - t - 1, \gamma + 1), (\gamma_1 - t - 1, \gamma + \frac{q^r - 1}{q - 1}), (\gamma_1, \gamma) \in G(P_{0,0}, P_\infty)$, para todo $0 \leq t \leq \min\{\gamma_1 - 1, 2g - 1 - (\alpha_1 + \alpha)\}$.

Sob essas condições, se a dimensão de $C_\Omega(D, G)$ é positiva, então sua distância mínima é pelo menos grau $G - 2g + 4$.

Demonstração. Pelo Teorema 4.2.2, a distância mínima é pelo menos grau $G - 2g + 3$. Seja $d := grau G - 2g + 3$. Se existe alguma palavra-código $c \in C_\Omega(D, G)$ de peso d, então existe uma diferencial de Weil $\omega \in \Omega(G - D)$ com exatamente d polos simples $P_{i_1}, \ldots, P_{i_d}$. Logo $(\omega) \geq G - (P_{i_1} + \cdots + P_{i_d})$, e como (ω) é um divisor canônico, temos

$$2g - 2 = \text{grau}\,(\omega) \geq \text{grau}\; G - w = \text{grau}\; G - \text{grau}\; G + 2g - 2 = 2g - 2$$

Então $(\omega) = G - (P_{i_1} + \cdots + P_{i_d}) + P$, onde P é um ponto racional sobre $\mathbb{F}_{q^r}$, com $P \neq P_{i_j}$, para $j = 1, \ldots, d$.
Por outro lado, pela hipótese $\ell(\alpha_1 P_{0,0} + \alpha P_\infty) = \ell(\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)$ e aplicando o Teorema de Riemann-Roch, obtemos

$$1 + \ell(W - (\alpha_1 P_{0,0} + \alpha P_\infty)) = \ell(W - ((\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)).$$

Então, existe uma função racional h tal que

$$h \in \mathscr{L}(W - ((\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)) \setminus \mathscr{L}(W - (\alpha_1 P_{0,0} + \alpha P_\infty)),$$

onde W divisor canônico. Dessa forma,

$$((\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)) - W \leq (h) < (\alpha_1 P_{0,0} + \alpha P_\infty) - W.$$

Então, $(h) = (\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} - W + E$, onde E é efetivo tal que $P_{0,0}, P_\infty \notin Supp\, E$ e $0 \leq t \leq 2g - 1 - (\alpha_1 + \alpha)$, pois grau $(h) = 0$. Então

$$G - (P_{i_1} + \cdots + P_{i_d}) + P = (\omega) \sim W \sim (\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} + E$$

e como $G = (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha_2 + \gamma_2 - 1)P_\infty$ existe uma função racional f tal que

$$(\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} + E = (f) + G - (P_{i_1} + \cdots + P_{i_d}) + P$$
$$(\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} + E = (f) + (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha_2 + \gamma_2 - 1)P_\infty - (P_{i_1} + \cdots + P_{i_d}) + P$$

Logo $(f) = -\gamma P_\infty - (\gamma_1 - t - 1)P_{0,0} - P + (P_{i_1} + \cdots + P_{i_d}) + E$. Vamos a mostrar que isso não é possível. Consideremos os casos:

- Caso 1: $t \leq \gamma_1 - 1$.
  - ⋆ Se $P \in Supp\, E$, então $(f)_\infty = \gamma P_\infty + (\gamma_1 - t - 1)P_{0,0}$, o que contradiz o fato que $(\gamma_1 - t - 1, \gamma) \in G(P_{0,0}, P_\infty)$.
  - ⋆ Se $P = P_\infty$, temos $(f)_\infty = (\gamma + 1)P_\infty + (\gamma_1 - t - 1)P_{0,0}$ o que contradiz o fato $(\gamma_1 - t - 1, \gamma + 1) \in G(P_{0,0}, P_\infty)$.

⋆ Se $P = P_{0,0}$, temos $(f)_\infty = \gamma P_\infty + (\gamma_1 - t)P_{0,0}$, então $(\gamma_1 - t - 1, \gamma + 1) \in H(P_{0,0}, P_\infty)$.

⋆ Se $P = P_v$ tal que $P_v \in \{P_{i_1} + \cdots + P_{i_d}\}$ e seja o divisor (y), definido em (4.1), então,

$$\begin{aligned}(f.y) = (f) + (y) &= (f) + \frac{q^r - 1}{q - 1}P_{0,0} - \frac{q^r - 1}{q - 1}P_\infty \\ &= -\left(\gamma + \frac{q^r - 1}{q - 1}\right)P_\infty - (\gamma_1 - t - 1)P_{0,0} - P + (P_{i_1} + \cdots + P_{i_d}) + E + \frac{q^r - 1}{q - 1}P_{0,0}.\end{aligned}$$

Logo

$$(f.y)_\infty = \left(\gamma + \frac{q^r - 1}{q - 1}\right)P_\infty + (\gamma_1 - t - 1)P_{0,0}$$

o que contradiz $(\gamma_1 - t - 1, \gamma + \frac{q^r - 1}{q - 1}) \in G(P_{0,0}, P_\infty)$.

- Caso 2: $\gamma_1 - 1 < t \leq 2g - 1 - (\alpha_1 + \alpha)$.

⋆ Se $P \in Supp\, E$ ou $P = P_{0,0}$, então $(f)_\infty = \gamma P_\infty$. Dessa forma $(\gamma_1 - t - 1, \gamma) \in G(P_{0,0}, P_\infty)$, o qual é absurdo pois $(\gamma_1 - 1) - t < 0$. Portanto γ é uma lacuna.

⋆ Se $P = P_\infty$, então $(f)_\infty = (\gamma + 1)P_\infty$. Logo $\gamma + 1$ é uma lacuna.

⋆ Se $P = P_v$ tal que $P_v \in \{P_{i_1} + \cdots + P_{i_d}\}$, então $\gamma + \frac{q^r - 1}{q - 1}$ é uma lacuna.

Portanto $d \geq$ grau $G - 2g + 4$. □

Definição 4.2.3. Seja $C_\Omega(D, G)$ o código $[n, k, d]$. Definimos sua taxa de informação por $R := k/n$ e sua distância mínima relativa por $\delta := d/n$.

Teorema 4.2.4. Dado m um inteiro tal que $q^r - (q^{r-1} + q^{r-2} + \cdots + q^2 + q) + q \leq m \leq q^r$ e seja o divisor $G = P_{0,0} + (q^{2r-1} + 2g - mq^{r-1} - 4)P_\infty$. Então, existem códigos de dois pontos $C_\Omega(D, G)$ sobre $\mathcal{X}_{q,r}$ de comprimento $|\mathcal{X}_{q,r}| - 2$, tendo parâmetros relativos melhores que códigos de um ponto $C_{\mathscr{L}}(\bar{D}, mq^{r-1}P_\infty)$ sobre $\mathcal{X}_{q,r}$, onde $\bar{D}$ é a soma de todos os q^{2r-1} pontos racionais afins.

Demonstração. Consideremos o código $C_{\mathscr{L}}(\bar{D}, mq^{r-1}P_\infty)$. Os pontos racionais são da forma $(0, \alpha_s^{(0)})$, onde os $\alpha_s^{(0)}$ são as raízes em $\mathbb{F}_{q^r}$ da equação

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = 0$$

ou da forma $(\alpha^j, \alpha_s^{(j)})$, com $0 \leq j \leq q^r - 2$, onde α é o gerador de $\mathbb{F}_{q^r}^*$ e $\alpha_s^{(j)}$ são as raízes em $\mathbb{F}_{q^r}$ da equação

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = \alpha^j.$$

Seja d a distância mínima de $C_{\mathscr{L}}(\bar{D}, mq^{r-1}P_\infty)$. Seja a função $f = \prod_{j=1}^{m}(x - \alpha^j)$. Então, similar à demonstração feita da Proposição 3.3.2, obtemos

$$(f) = \sum_{j=1}^{m}(x - \alpha^j) = \bar{D} - mq^{r-1}P_\infty.$$

Portanto, $f \in \mathscr{L}(mq^{r-1}P_\infty)$. Consequentemente, f tem mq^{r-1} zeros. Então, o peso da palavra-código é $q^{2r-1} - mq^{r-1}$. Por outro lado, pelo Teorema 3.2.2 temos

$$d \geq n - \text{grau}\,(mq^{r-1}P_\infty) = q^{2r-1} - mq^{r-1}.$$

Dessa forma $d = q^{2r-1} - mq^{r-1}$. Logo, pelo Corolário 3.2.3, como $2g-2 < \text{grau}\,(mq^{r-1}P_\infty) < n$, temos

$$k = \text{grau}\,(mq^{r-1}P_\infty) + 1 - g = mq^{r-1} - g + 1.$$

Agora, consideramos o código $C_\Omega(D, G)$ de dois pontos, onde $D = \sum_{j=1}^{q^{2r-1}-1} P_j$, com $P_j \neq P_{0,0}, P_\infty$. Então $n = q^{2r-1} - 1$ e como grau $G = q^{2r-1} + 2g - mq^{r-1} - 3 > 2g - 2$ e para W canônico, temos

$$\begin{aligned}\text{grau}\,(W - G + D) &= \text{grau}\ W - \text{grau}\ G + \text{grau}\ D \\ &= 2g - 2 - q^{2r-1} - 2g + mq^{r-1} + 3 + q^{2r-1} - 1 \\ &= mq^{r-1} - g + 1.\end{aligned}$$

Finalmente, a distância mínima é determinada usando o Teorema 4.2.2.
Note que, pelo Teorema 4.2.1, o par $(\alpha_1, \alpha) = (1, 2g-2) \in G(P_{0,0}, P_\infty)$, e para cada m tal que $q^r - (q^{r-1} + q^{r-2} + \cdots + q^2 + q) + q \leq m \leq q^r$, temos

$$(\gamma_1, \gamma) = (1, q^{2r-1} - mq^{r-1} - 1) \in G(P_{0,0}, P_\infty)$$

pois $q^{2r-1} - mq^{r-1} - 1 < 2g - 2$. Além disso, ambos pares satisfazem a condição

$$(\gamma_1, \gamma_2 - t - 1) \in G(Q_1, Q_2), \text{ para todo } 0 \leq t \leq \min\{\gamma - 1, 2g - 1 - (\alpha_1 + \alpha)\} = 0.$$

Assim, a distância mínima de $C_\Omega(D, G)$ é

$$d' \geq \text{grau}\ G - (2g-3) = q^{2r-1} + 2g - mq^{r-1} - 3 - 2g + 3 = q^{2r-1} - mq^{r-1}.$$

Então, o código C_Ω tem melhores parâmetros relativos R, δ que os correspondentes ao código $C_{\mathscr{L}}((\bar{D}, mq^{r-1}P_\infty)$. □

Agora, vamos mostrar dois exemplos.

Exemplo 4.2.5. Consideremos $q = 3$ e $r = 3$.
A curva norma-traço é $\mathcal{X}_{3,3} : x^{13} - (y^9 + y^3 + y) = 0$, de gênero $g = 48$ sobre $\mathbb{F}_{27}$. Com a notação da Proposição 4.1.8, temos $a = 12$ e $1 \leq s \leq 4$. Logo, os semigrupos de Weierstrass são os seguintes:

- $H(P_\infty) = \langle 9, 13\rangle$. Então, o conjunto das lacunas é $G(P_\infty) = \{$ 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, 29, 30, 32, 33, 34, 37, 38, 41, 42, 43, 46, 47, 50, 51, 55, 56, 59, 60, 64, 68, 69, 73, 77, 82, 86, 95 $\}$.

- $H(P_{0,0}) = \langle 12, 13, 35, 58, 81\rangle$. Então, o conjunto das lacunas é $G(P_{0,0}) = \{$ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 40, 41, 42, 43, 44, 45, 46, 53, 54, 55, 56, 57, 66, 67, 68, 69, 79, 80, 92 $\}$.

Agora, usando o Teorema 4.1.9, obtemos o conjunto

$$\Gamma(P_{0,0}, P_\infty) = \{(1,95), (2,86), (3,77), (4,68), (5,59), (6,50), (7,41), (8,32), (9,23), (10,14), (11,5), (14,82), (15,73), (16,64), (17,55), (18,46), (19,37), (20,28), (21,19), (22,10), (23,1), (27,69), (28,60), (29,51), (30,42), (31,33), (32,24), (33,15), (34,6), (40,56), (41,47), (42,38), (43,29), (44,20), (45,11), (46,2), (53,43), (54,34), (55,25), (56,16), (57,7), (66,30), (67,21), (68,12), (69,3), (79,17), (80,8), (92,4)\}.$$

Por outro lado, pelo Lema 4.1.7, temos

$$H(P_{0,0}, P_\infty) = \{lub(x,y) \mid x, y \in \Gamma(P_{0,0}, P_\infty) \cup (H(P_{0,0}) \times \{0\}) \cup (\{0\} \times H(P_\infty))\}.$$

Consideremos a notação do Teorema 4.2.4. Sejam o divisor $D = \sum P_j$, com $P_j \neq P_{0,0}, P_\infty$, o divisor $\bar{D}$ é a soma de todos os 243 pontos racionais afins e $18 \leq m \leq 27$. Em particular, determinamos os parâmetros dos códigos para $m = 20$. Então, temos os códigos

- $C_{\mathscr{L}}(\bar{D}, 180P_\infty)$ cujos parâmetros são $n = 243$, $k = 133$ e $d = 63$.

- $C_\Omega(D, P_{0,0} + 155P_\infty)$ cujos parâmetros são $n = 242$, $k = 133$ e $d \geq 63$.

Consequentemente, os parâmetros relativos do código $C_\Omega(D, P_{0,0}+155P_\infty)$ são melhores do que $C_{\mathscr{L}}(\bar{D}, 180P_\infty)$.

Exemplo 4.2.6. Consideremos $q = 5$ e $r = 3$.
A curva norma-traço é $\mathcal{X}_{5,3} : x^{31} - (y^{25} + y^5 + y) = 0$, de gênero $g = 360$ sobre $\mathbb{F}_{125}$. Com a notação da Proposição 4.1.8, temos $a = 30$ e $0 \leq s \leq 4$. Logo, os semigrupos de Weierstrass são os seguintes:

- $H(P_\infty) = \langle 25, 31\rangle$. Então, o conjunto das lacunas é $G(P_\infty) = \{$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 53, 54, 55, 57, 58, 59, 60, 61, 63,

64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 76, 77, 78, 79, 80, 82, 83, 84, 85, 86, 88, 89, 90, 91, 92, 94, 95, 96, 97, 98, 99, 101, 102, 103, 104, 105, 107, 108, 109, 110, 111, 113, 114, 115, 116, 117, 119, 120, 121, 122, 123, 126, 127, 128, 129, 130, 132, 133, 134, 135, 136, 138, 139, 140, 141, 142, 144, 145, 146, 147, 148, 151, 152, 153, 154, 157, 158, 159, 160, 161, 163, 164, 165, 166, 167, 169, 170, 171, 172, 173, 176, 177, 178, 179, 182, 183, 184, 185, 188, 189, 190, 191, 192, 194, 195, 196, 197, 198, 201, 202, 203, 204, 207, 208, 209, 210, 213, 214, 215, 216, 219, 220, 221, 222, 223, 226, 227, 228, 229, 232, 233, 234, 235, 238, 239, 240, 241, 244, 245, 246, 247, 251, 252, 253, 254, 257, 258, 259, 260, 263, 264, 265, 266, 269, 270, 271, 272, 276, 277, 278, 282, 283, 284, 285, 288, 289, 290, 291, 294, 295, 296, 297, 301, 302, 303, 307, 308, 309, 313, 314, 315, 316, 319, 320, 321, 322, 326, 327, 328, 332, 333, 334, 338, 339, 340, 344, 345, 346, 347, 351, 352, 353, 357, 358, 359, 363, 364, 365, 369, 370, 371, 376, 377, 378, 382, 383, 384, 388, 389, 390, 394, 395, 396, 401, 402, 407, 408, 409, 413, 414, 415, 419, 420, 421, 426, 427, 432, 433, 438, 739, 440, 444, 445, 446, 451, 452, 457, 458, 463, 464, 469, 470, 471, 476, 477, 482, 483, 488, 489, 494, 495, 501, 502, 507, 508, 513, 514, 519, 520, 526, 532, 533, 538, 539, 544, 545, 551, 557, 563, 564, 569, 570, 576, 582, 588, 594, 595, 601, 607, 613, 619, 626, 632, 638, 644, 657, 663, 669, 688, 694, 719 }.

- $H(P_{0,0}) = \langle 30, 31, 149, 268, 387, 506, 625 \rangle$. Então, o conjunto das lacunas é $G(P_{0,0}) = \{$ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415,

416, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 497, 498, 499, 500, 501, 502, 503, 504, 505, 528, 529, 530, 531, 532, 533, 534, 535, 559, 560, 561, 562, 563, 564, 565, 590, 591, 592, 593, 594, 595, 621, 622, 623, 624, 652, 653, 654, 683, 684, 714}.

Agora, pelo Teorema 4.1.9, obtemos que o conjunto gerador minimal do semigrupo de Weierstrass é $\Gamma(P_{0,0}, P_\infty) = \{$(1,719), (2,694), (3,669), (4,644), (5,619), (6,594), (7,569), (8,544), (9,519), (10,494), (11,469), (12,444), (13,419), (14,394), (15,369), (16,344), (17,319), (18,294), (19,269), (20,244), (21,219), (22,194), (23,169), (24,144), (25,119), (26,94), (27,69),(28,44), (29,19), (32,688), (33,663), (34,638), (35,613), (36,588), (37,563), (38,538), (39,513), (40,488), (41,463), (42,438), (43,413), (44,388), (45,363), (46,338), (47,313), (48,288), (49,263), (50,238), (51,213), (52,188), (53,163), (54,138), (55,113), (56,88), (57,63), (58,38), (59,13), (63,657), (64,632), (65,607), (66,582), (67,557), (68,532), (69,507), (70,482), (71,457), (72,432), (73,407), (74,382), (75,357), (76,332), (77,307), (78,282), (79,257), (80,232), (81,207), (82,182), (83,157), (84,132), (85,107), (86,82), (87,57), (88,32), (89,7), (94,626), (95,601), (96,576), (97,551), (98,526), (99,501), (100,476), (101,451), (102,426), (103,401), (104,376), (105,351), (106,326), (107,301), (108,276), (109,251), (110,226), (111,201), (112,176), (113,151), (114,126), (115,101), (116,76), (117,51), (118,26), (119,1), (125,595), (126,570), (127,545), (128,520), (129,495), (130,470), (131,445), (132,420), (133,395), (134,370), (135,345), (136,320), (137,295), (138,270), (139,245), (140,220), 141,195), (142,170), (143,145), (144,120), (145,95), (146,70), (147,45), (148,20), (156,564), (157,539), (158,514), (159,489), (160,464), (161,439), (162,414), (163,389), (164,364), (165,339), (166,314), (167,289), (168,264), (169,239), (170,214), (171,189), (172,164), (173,139), (174,114), (175,89), (176,64), (177,39), (178,14), (187,533), (188,508), (189,483), (190,458), (191,433), (192,408), (193,383), (194,358), (195,333), (196,308), (197,283), (198,258), (199,233), (200,208), (201,183), (202,158), (203,133), (204,108), (205,83), (206,58), (207,33), (208,8), (218,502), (219,477), (220,452), (221,427), (222,402), (223,377), (224,352), (225,327), (226,302), (227,277), (228,252), (229,227), (230,202), (231,177), (232,152), (233,127), (234,102), (235,77), (236,52), (237,27), (238,2), (249,471), (250,446), (251,421), (252,396), (253,371), (254,346), (255,321), (256,296), (257,271), (258,246), (259,221), (260,196), (261,171), (262,146), (263,121), (264,96), (265,71), (266,46), (267,21), (280,440), (281,415), (282,390), (283,365), (284,340), (285,315), (286,290), (287,265), (288,240), (289,215), (290,190), (291,165), (292,140), (293,115), (294,90), (295,65), (296,40), (297,15), (311,409), (312,384), (313,359), (314,334), (315,309), (316,284), (317,259), (318,234), (319,209), (320,184), (321,159), (322,134), (323,109), (324,84), (325,59), (326,34), (327,9), (342,378), (343,353), (344,328), (345,303), (346,278),

(347,253), (348,228), (349,203), (350,178), (351,153), (352,128), (353,103), (354,78), (355,53), (356,28), (357,3), (373,347), (374,322), (375,297), (376,272), (377,247), (378,222), (379,197), (380,172), (381,147), (382,122), (383,97), (384,72), (385,47), (386,22), (404,316), (405,291), (406,266), (407,241), (408,216), (409,191), (410,166), (411,141), (412,116), (413,91), (414,66), (415,41), (416,16), (435,285), (435,260), (437,235), (437,210), (439,185), (439,160), (441,135), (441,110), (443,85), (443,60), (445,35), (445,10), (466,254), (467,229), (468,204), (469,179), (470,154), (471,129), (472,104), (473,79), (474,54), (475,29), (476,4), (497,223), (498,198), (499,173), (500,148), (501,123), (502,98), (503,73), (504,48), (505,23), (528,192), (529,191), (530,190), (531,189), (532,188), (533,187), (534,186), (535,185), (559,161), (560,160), (561,159), (562,158), (563,157),(564,156), (565,155), (590,130), (591,129), (592,128), (593,127), (594,126), (595,125) (621,99), (622,98), (623,97), (624,96), (652,68), (653,67), (654,66), (683,37), (684,36), (714,6)}.

Por outro lado, pelo Lema 4.1.7, temos

$$H(P_{0,0}, P_\infty) = \{lub(x, y) \mid x, y \in \Gamma(P_{0,0}, P_\infty) \cup (H(P_{0,0}) \times \{0\}) \cup (\{0\} \times H(P_\infty))\}.$$

Similar ao exemplo anterior, podemos verificar que as condições do Teorema 4.2.4 são satisfeitas.

4.2.1 Lacunas puras

Em 2001, Homma e Kim introduziram o conceito de lacuna pura para dois lugares do corpo de funções $F/\mathbb{F}_q$. Elas permitem melhorar estimativas da distância mínima de códigos AG de dois pontos e, em diversos casos, conduzem à construção de códigos com parâmetros superiores aos obtidos por meio de códigos de um ponto.

Na Definição 4.0.1, definimos o semigrupo de Weierstrass $H(P_1, P_2)$ e o conjunto $G(P_1, P_2)$ das lacunas de dois pontos.

Os elementos de $G(P_1, P_2)$ podem ser caracterizados usando os espaços de Riemann-Roch, isto é, um par $(\alpha, \beta) \in \mathbb{N}_0^2$ é uma lacuna em P_1, P_2, se satisfaz

$$\ell(\alpha P_1 + \beta P_2) = \ell(\alpha P_1 + \beta P_2 - P_j), \text{ para algum } j = 1, 2.$$

Definição 4.2.7. Sejam P_1 e P_2 lugares do corpo de funções. O par (α, β) é chamado de lacuna pura sobre P_1, P_2 se satisfaz

$$\ell(\alpha P_1 + \beta P_2) = \ell(\alpha P_1 + \beta P_2 - P_j), \text{ para todo } j = 1, 2$$

ou equivalentemente

$$\ell(\alpha P_1 + \beta P_2) = \ell((\alpha - 1)P_1 + (\beta - 1)P_2).$$

O conjunto das lacunas puras e denotado por $G_0(P_1, P_2)$. Claramente $G_0(P_1, P_2)$ é subconjunto de $G(P_1, P_2)$.

Definição 4.2.8. Sejam $u_1 = (\alpha_1, \beta_1)$ e $u_2 = (\alpha_2, \beta_2)$ elementos de $\Gamma(P_1, P_2)$. O maior limite inferior de u_1 e u_2 é definido por

$$glb(u_1, u_2) = (\min\{\alpha_1, \alpha_2\}, \min\{\beta_1, \beta_2\}).$$

Seja $\preceq$ a ordem parcial natural em $\mathbb{N}_0^2$. Denotamos $u_1 \not\preceq u_2$ se $\alpha_1 > \alpha_2$ ou $\beta_1 > \beta_2$.

O seguinte lema mostra que o conjunto $\Gamma(P_1, P_2)$ é muito importante para determinar o conjunto de lacunas puras.

Lema 4.2.9. Sejam P_1 e P_2 lugares distintos em F. Então

$$G_0(P_1, P_2) = \{glb(u_1, u_2) : u_1, u_2 \in \Gamma(P_1, P_2), u_1 \not\preceq u_2, u_2 \not\preceq u_1\}.$$

Demonstração. Veja [3, Proposição 3.3]. □

Mostramos dois exemplos onde determinarmos os conjuntos de lacunas puras usando o lema.

Exemplo 4.2.10. No Exemplo 4.1.4, para $q = 2$ e $r = 3$, determinamos o conjunto

$$\Gamma(P_{0,0}, P_\infty) = \{(1, 17), (2, 13), (3, 9), (4, 5), (5, 1), (8, 10), (9, 6), (10, 2), (15, 3)\}.$$

Então, o conjunto das lacunas puras é $G_0(P_{0,0}, P_\infty) = \{$(1,1), (1,2), (1,3), (1,5), (1,6), (1,9), (1,10), (1,13), (2,1), (2,2), (2,3), (2,5), (2,6), (2,9), (2,10), (3,1), (3,2), (3,3), (3,5), (3,6), (4,1), (4,2), (4,3), (8,2), (8,3), (8,6), (9,2), (9,3) $\}$.

Exemplo 4.2.11. No Exemplo 4.2.5, determinamos para $q = 3$ e $r = 3$, o conjunto

$$\Gamma(P_{0,0}, P_\infty) = \{(1, 95), (2, 86), (3, 77), (4, 68), (5, 59), (6, 50), (7, 41), (8, 32), (9, 23), (10, 14), (11, 5), (14, 82), (15, 73), (16, 64), (17, 55), (18, 46), (19, 37), (20, 28), (21, 19), (22, 10), (23, 1), (27, 69), (28, 60), (29, 51), (30, 42), (31, 33), (32, 24), (33, 15), (34, 6), (40, 56), (41, 47), (42, 38), (43, 29), (44, 20), (45, 11), (46, 2), (53, 43), (54, 34), (55, 25), (56, 16), (57, 7), (66, 30), (67, 21), (68, 12), (69, 3), (79, 17), (80, 8), (92, 4)\}.$$

Então, o conjunto das lacunas puras é $G_0(P_{0,0}, P_\infty) = \{$(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (1,7), (1,8), (1,10), (1,11), (1,12), (1,14), (1,15), (1,16), (1,17), (1,19), (1,20), (1,21), (1,23), (1,24), (1,25), (1,28), (1,29), (1,30), (1,32), (1,33), (1,34), (1,37), (1,38), (1,41), (1,42), (1,43), (1,46), (1,47), (1,50), (1,51), (1,55), (1,56), (1,59), (1,60), (1,64), (1,68), (1,69), (1,73), (1,77),

(1,82), (1,86), (2,1), (2,2), (2,3), (2,4), (2,5), (2,6), (2,7), (2,8), (2,10), (2,11), (2,12), (2,14), (2,15), (2,16), (2,17), (2,19), (2,20), (2,21), (2,23), (2,24), (2,25), (2,28), (2,29), (2,30), (2,32), (2,33), (2,34), (2,37), (2,38), (2,41), (2,42), (2,43), (2,46), (2,47), (2,50), (2,51), (2,55), (2,56), (2,59), (2,60), (2,64), (2,68), (2,69), (2,73), (2,77), (2,82), (3,1), (3,2), (3,3), (3,4), (3,5), (3,6), (3,7), (3,8), (3,10), (3,11), (3,12), (3,14), (3,15), (3,16), (3,17), (3,19), (3,20), (3,21), (3,23), (3,24), (3,25), (3,28), (3,29), (3,30), (3,32), (3,33), (3,34), (3,37), (3,38), (3,41), (3,42), (3,43), (3,46), (3,47), (3,50), (3,51), (3,55), (3,56), (3,59), (3,60), (3,64), (3,69), (3,68), (3,73), (4,1), (4,2), (4,3), (4,4), (4,5), (4,6), (4,7), (4,8), (4,10), (4,11), (4,12), (4,14), (4,15), (4,16), (4,17), (4,19), (4,20), (4,21), (4,23), (4,24), (4,25), (4,28), (4,29), (4,30), (4,32), (4,33), (4,34), (4,37), (4,38), (4,41), (4,42), (4,43), (4,46), (4,47), (4,50), (4,51), (4,55), (4,56), (4,59), (4,60), (4,64), (5,1), (5,2), (5,3), (5,4), (5,5), (5,6), (5,7), (5,8), (5,10), (5,11), (5,12), (5,14), (5,15), (5,16), (5,17), (5,19), (5,20), (5,21), (5,23), (5,24), (5,25), (5,28), (5,29), (5,30), (5,32), (5,33), (5,34), (5,37), (5,38), (5,41), (5,42), (5,43), (5,46), (5,47), (5,50), (5,51), (5,55), (5,56), (6,1), (6,2), (6,3), (6,4), (6,5), (6,6), (6,7), (6,8), (6,10), (6,11), (6,12), (6,14), (6,15), (6,16), (6,17), (6,19), (6,20), (6,21), (6,23), (6,24), (6,25), (6,28), (6,29), (6,30), (6,32), (6,33), (6,34), (6,37), (6,38), (6,41), (6,42), (6,43), (6,46), (6,47), (7,1), (7,2), (7,3), (7,4), (7,5), (7,6), (7,7), (7,8), (7,10), (7,11), (7,12), (7,14), (7,15), (7,16), (7,17), (7,19), (7,20), (7,21), (7,23), (7,24), (7,25), (7,28), (7,29), (7,30), (7,32), (7,33), (7,34), (7,37), (7,38), (8,1), (8,2), (8,3), (8,4), (8,5), (8,6), (8,7), (8,8), (8,10), (8,11), (8,12), (8,14), (8,15), (8,16), (8,17), (8,19), (8,20), (8,21), (8,23), (8,24), (8,25), (8,28), (8,29), (8,30), (9,1), (9,2), (9,3), (9,4), (9,5), (9,6), (9,7), (9,8), (9,10), (9,11), (9,12), (9,14), (9,15), (9,16), (9,17), (9,19), (9,20), (9,21), (10,1), (10,2), (10,3), (10,4), (10,5), (10,6), (10,7), (10,8), (10,10), (10,11), (10,12), (11,1), (11,2), (11,3), (11,4), (14,1), (14,2), (14,3), (14,4), (14,6), (14,7), (14,8), (14,10), (14,11), (14,12), (14,15), (14,16), (14,17), (14,19), (14,20), (14,21), (14,24), (14,25), (14,28), (14,29), (14,30), (14,33), (14,34), (14,37), (14,38), (14,42), (14,43), (14,46), (14,47), (14,51), (14,55), (14,56), (14,60), (14,64), (14,69), (14,73), (15,1), (15,2), (15,3), (15,4), (15,6), (15,7), (15,8), (15,10), (15,11), (15,12), (15,15), (15,16), (15,17), (15,19), (15,20), (15,21), (15,24), (15,25), (15,28), (15,29), (15,30), (15,33), (15,34), (15,37), (15,38), (15,42), (15,43), (15,46), (15,47), (15,51), (15,55), (15,56), (15,60), (15,64), (15,69), (16,1), (16,2), (16,3), (16,4), (16,6), (16,7), (16,8), (16,10), (16,11), (16,12), (16,15), (16,16), (16,17), (16,19), (16,20), (16,21), (16,24), (16,25), (16,28), (16,29), (16,30), (16,33), (16,34), (16,37), (16,38), (16,42), (16,43), (16,46), (16,47), (16,51), (16,60), (16,55), (16,56), (17,1), (17,2), (17,3), (17,4), (17,6), (17,7), (17,8), (17,10), (17,11), (17,12), (17,15), (17,16), (17,17), (17,19), (17,20), (17,21), (17,24), (17,25), (17,28), (17,29), (17,30), (17,33), (17,34), (17,37),(17,38), (17,42), (17,43), (17,46), (17,47), (17,51), (18,1), (18,2), (18,3),

(18,4), (18,6), (18,7), (18,8), (18,10), (18,11), (18,12), (18,15), (18,16), (18,17), (18,19), (18,20), (18,21), (18,24), (18,25), (18,28), (18,29), (18,30), (18,33), (18,34), (18,37), (18,38), (18,42), (18,43), (19,1), (19,2), (19,3), (19,4), (19,6), (19,7), (19,8), (19,10), (19,11), (19,12), (19,15), (19,16), (19,17), (19,19), (19,20), (19,21), (19,24), (19,25), (19,28), (19,29), (19,30), (19,33), (19,34), (20,1), (20,2), (20,3), (20,4), (20,6), (20,7), (20,8), (20,10), (20,11), (20,12), (20,15), (20,16), (20,17), (20,19), (20,20), (20,21), (20,24), (20,25), (21,1), (21,2), (21,3), (21,4), (21,6), (21,7), (21,8), (21,10), (21,11), (21,12), (21,15), (21,16), (21,17), (22,1), (22,2), (22,3), (22,4), (22,6), (22,7), (22,8), (27,2), (27,3), (27,4), (27,6), (27,7), (27,8), (27,11), (27,12), (27,15), (27,16), (27,17), (27,20), (27,21), (27,24), (27,25), (27,29), (27,30), (27,33), (27,34), (27,38), (27,42), (27,43), (27,47), (27,51), (27,56), (27,60), (28,2), (28,3), (28,4), (28,6), (28,7), (28,8), (28,11), (28,12), (28,15), (28,16), (28,17), (28,20), (28,21), (28,24), (28,25), (28,29), (28,30), (28,33), (28,34), (28,38), (28,42), (28,43), (28,47), (28,51), (28,56), (29,2), (29,3), (29,4), (29,6), (29,7), (29,8), (29,11), (29,12), (29,15), (29,16), (29,17), (29,20), (29,21), (29,24), (29,25), (29,29), (29,30), (29,33), (29,34), (29,38), (29,42), (29,43), (29,47), (30,2), (30,3), (30,4), (30,6), (30,7), (30,8), (30,11), (30,12), (30,15), (30,16), (30,17), (30,20), (30,21), (30,24), (30,25), (30,29), (30,30), (30,33), (30,34), (30,38), (31,2), (31,3), (31,4), (31,6), (31,7), (31,8), (31,11), (31,12), (31,15), (31,16), (31,17), (31,20), (31,21), (31,24), (31,25), (31,29), (31,30), (32,2), (32,3), (32,4), (32,6), (32,7), (32,8), (32,11), (32,12), (32,15), (32,16), (32,17), (32,20), (32,21), (33,2), (33,3), (33,4), (33,6), (33,7), (33,8), (33,11), (33,12), (34,2), (34,3), (34,4), (40,2), (40,3), (40,4), (40,7), (40,8), (40,11), (40,12), (40,16),(40,17), (40,20), (40,21), (40,25), (40,29), (40,30), (40,34), (40,38), (40,43), (40,47), (41,2), (41,3), (41,4), (41,7), (41,8), (41,11), (41,12), (41,16), (41,17), (41,20), (41,21), (41,25), (41,29), (41,30), (41,34), (41,38), (41,43), (42,2), (42,3), (42,4), (42,7), (42,8), (42,11), (42,12), (42,16), (42,17), (42,20), (42,21), (42,25), (42,29), (42,30), (42,34), (43,2), (43,3), (43,4), (43,7), (43,8), (43,11), (43,12), (43,16), (43,17), (43,20), (43,21), (43,25), (44,2), (44,3), (44,4), (44,7), (44,8), (44,11), (44,12), (44,16), (44,17), (45,2), (45,3), (45,4), (45,7), (45,8), (53,3), (53,4), (53,7), (53,8), (53,12), (53,16), (53,17), (53,21), (53,25), (53,30), (53,34), (54,3), (54,4), (54,7), (54,8), (54,12), (54,16), (54,17), (54,21), (54,25), (54,30), (55,3), (55,4), (55,7), (55,8), (55,12), (55,16), (55,17), (55,21), (56,3), (56,4), (56,7), (56,8), (56,12), (57,3), (57,4), (66,3), (66,4), (66,8), (66,12), (66,17), (66,21), (67,3), (67,4), (67,8), (67,12), (67,17), (68,3), (68,4), (68,8), (79,4), (79,8), (80,4)}.

O seguinte resultado permite estimar a distância mínima a partir do conjunto das lacunas puras.

Teorema 4.2.12. Sejam P_1 e P_2 pontos racionais sobre $\mathcal{X}(\mathbb{F}_q)$. Para $t_1, t_2 \in \mathbb{N}$, suponha que

$$\{(k_1, k_2) \mid \alpha \leq k_1 \leq \alpha + t_1, \beta \leq k_2 \leq \beta + t_2\} \subseteq G_0(P_1, P_2).$$

Se $G = (2\alpha + t_1 - 1)P_1 + (2\beta + t_2 - 1)P_2$, então a distância mínima do código $C_\Omega(D, G)$, onde $D = \sum_{j=1}^{q^{2r-1}-1} Q_j$, com $Q_j \neq P_1, P_2$ é dada por $d' \geq \text{grau } G - (2g-2) + t_1 + t_2 + 2$.

Demonstração. Veja [6, Teorema 3.3]. □

Exemplo 4.2.13. No Exemplo 4.2.10, determinamos os elementos de $G_0(P_{0,0}, P_\infty)$ para $q = 2$ e $r = 3$, os quais representamos graficamente

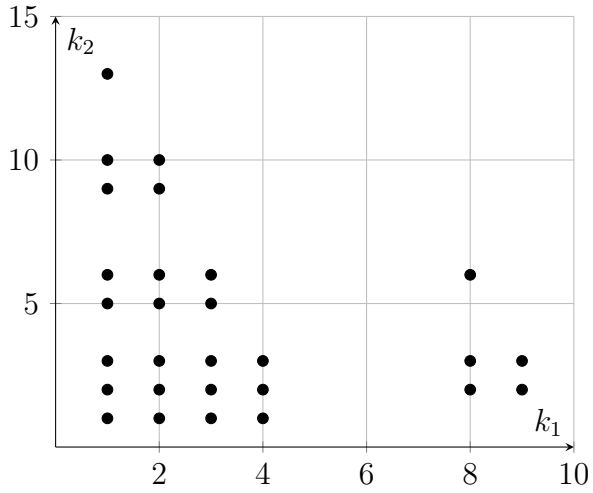


Figura 4.1: Representação gráfica do conjunto das lacunas puras para $q = 2$ e $r = 3$.

Consideremos o seguinte bloco contido em $G_0(P_{0,0}, P_\infty)$

$$(9, 2), (9, 3)$$
$$(8, 2), (8, 3)$$

Então, as variáveis do teorema são $\alpha = 8$, $\beta = 2$, $t_1 = 1$ e $t_2 = 1$. Assim, o divisor

$$G = (2\alpha + t_1 - 1)P_{0,0} + (2\beta + t_2 - 1)P_\infty = 16P_{0,0} + 4P_\infty.$$

Logo, a distância mínima é

$$d' \geq \text{grau } G - (2g-2) + t_1 + t_2 + 2 = 20 - (18-2) + 1 + 1 + 2 = 20 - 16 + 4 = 8.$$

Exemplo 4.2.14. No Exemplo 4.2.11, determinamos os elementos de $G_0(P_{0,0}, P_\infty)$ para $q = 3$ e $r = 3$, os quais representamos graficamente

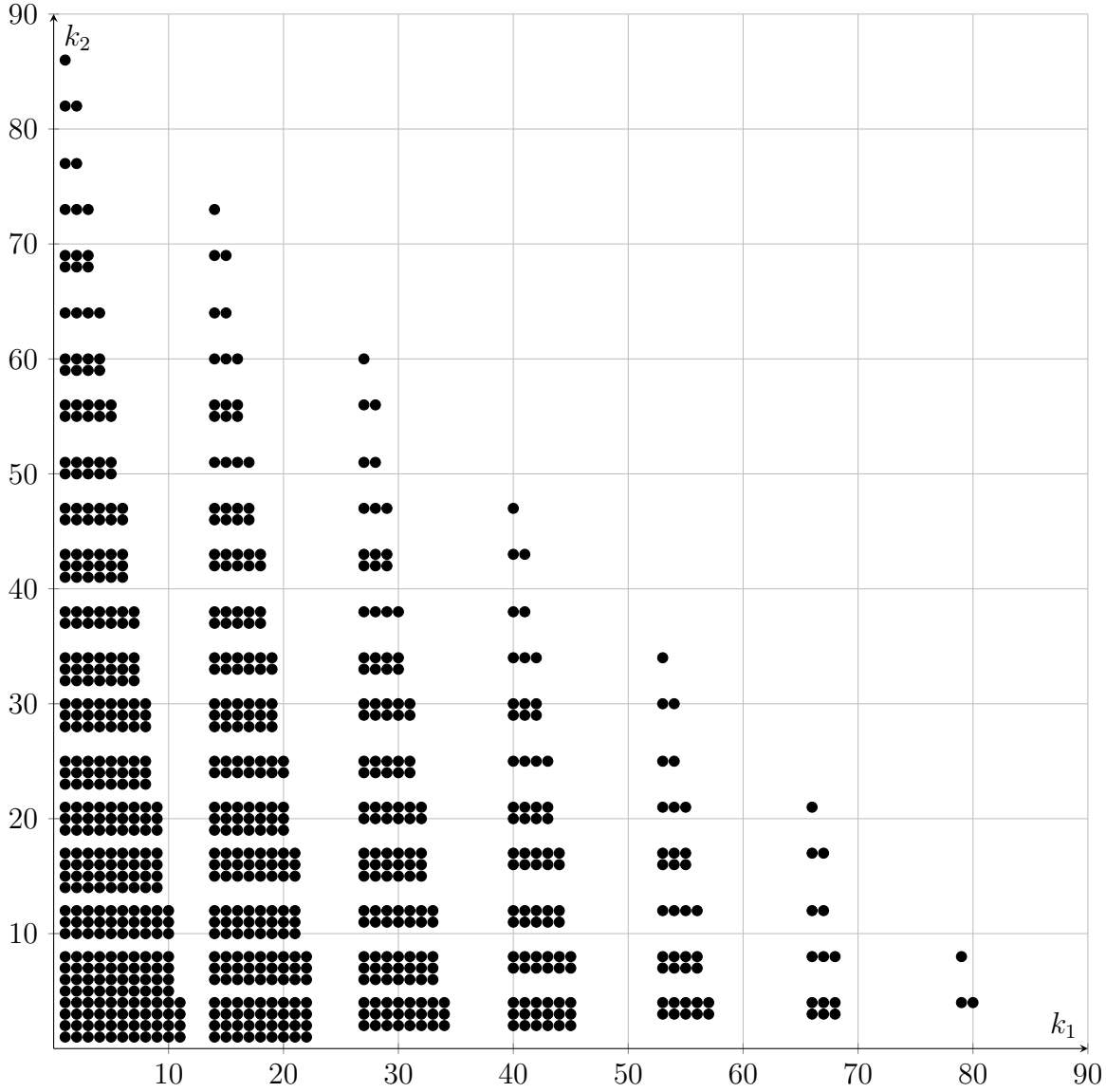


Figura 4.2: Representação gráfica das lacunas puras para $q = 3$ e $r = 3$.

Consideremos o seguinte bloco contido em $G_0(P_{0,0}, P_\infty)$

$$(27, 34), (28, 34), (29, 34), (30, 34)$$
$$(27, 33), (28, 33), (29, 33), (30, 33).$$

Então, as variáveis do teorema são $\alpha = 27$, $\beta = 33$, $t_1 = 3$ e $t_2 = 1$. Assim, o divisor

$$G = (2\alpha + t_1 - 1)P_{0,0} + (2\beta + t_2 - 1)P_\infty = 56P_{0,0} + 66P_\infty.$$

Logo, a distância mínima é

$$d' \geq \text{grau } G - (2g - 2) + t_1 + t_2 + 2 = 122 - (96 - 2) + 3 + 1 + 2 = 34.$$

Considerações finais

Nesta dissertação, exploramos a construção de códigos AG a partir de corpo de funções algébricas, com ênfase nos códigos de dois pontos definidos sobre a curva norma-traço. Revisamos os fundamentos da teoria de corpos de funções, sendo o Teorema de Riemann-Roch essencial para determinar os parâmetros desses códigos.

Os resultados obtidos demonstram que a análise do semigrupo de Weierstrass desempenhou um papel fundamental, fornecendo ferramentas para a determinação de lacunas e lacunas puras. Esta abordagem permitiu a obtenção de códigos de dois pontos com distâncias mínimas superiores em relação aos códigos de um ponto. Adicionalmente, as curvas norma-traço são relevantes devido às suas propriedades estruturais.

Como continuidade deste trabalho, sugere-se a generalização para códigos em n pontos ($n > 2$) e a investigação de outras famílias de curvas com vários pontos racionais. Seria interessante, explorar aplicações práticas dos códigos de dois pontos em cenários reais de transmissão e armazenamento de dados.

Referências Bibliográficas

[1] Camargo, J., *Códigos Algébricos Geométricos*, Monografia de Graduação, IME-UFU, 2019.

[2] Castellanos, A., *Sobre códigos hermitianos generalizados*,Tese de doutorado,IMECC-UNICAMP, 2008.

[3] Castellanos, A., Mendoza, E., Quoos, L., *Weierstrass semigroups, pure gaps and codes on function fields*, Designs, Codes and Cryptography, vol. 92, no 5, p. 1219-1242, 2024. https://doi.org/10.1007/s10623-023-01339-w

[4] Gonçalves, A., *Introdução à álgebra*, Instituto de Matemática Pura e Aplicada, 1979.

[5] Geil, O., *On codes from norm-trace curves*, Finite Fields and Their Applications, vol 9, 351-371,2003. https://doi.org/10.1016/S1071-5797(03)00010-8

[6] Homma, M., Kim, S., *Goppa codes with Weierstrass pairs*, Journal of pure and applied algebra, vol 162, 2-3, 273-290, 2001. https://doi.org/10.1016/S0022-4049(00)00134-1

[7] Hungerford, T., *Algebra*, Berling Heidelberg New York: Springer Verlag, 1973.

[8] Hungerford, T., *Abstract algebra: an introduction*, 2013.

[9] Kim, S.,*On the index of the Weierstrass semigroup of a pair of points on a curve*, Archiv der Mathematik, vol 62, p. 73-82, 1994. https://doi.org/10.1007/BF01200442

[10] Lang, S., *Algebra*, Springer New York, 2005.

[11] Manuera, C., Tizziotti, G. e Torres, F. *Two points codes on Norm - Trace curves*, In: Barbero, Á. (eds) Coding Theory and Applications. Lecture Notes in Computer Science, vol 5228. Springer, Berlin, Heidelberg, 2008. https://doi.org/10.1007/978-3-540-87448-$5_1$4

[12] Morales, G. ,*Uma introdução aos polinômios sobre corpos finitos*, Dissertação de mestrado, IME - UFU, 2025.

[13] Matthews, G., *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography, vol 22, 107–121, 2001. https://doi.org/10.1023/A:1008311518095

[14] Mujica, X., *Introdução aos Corpos de Funções Algébricas com Exemplos de Códigos Auto-Duais*, Dissertação de mestrado, IMECC - UNICAMP, 1997.

[15] Pereira, F., *Códigos Algébrico-Geométricos e suas Aplicações à Teoria de Códigos Quânticos*, Tese de doutorado,CEEI-UFCG, 2019.

[16] Rotman, J. *An introduction to the theory of groups*, Springer Science and Business Media, 2012.

[17] Rotman, J. *Advanced modern algebra*, American Mathematical Soc., 2010.

[18] Stichtenoth, H., *Algebraic Function Fields and Codes*, Berling Heidelberg New York: Spring Verlag, 1993.

[19] Shannon, C. *A mathematical theory of communication*,The Bell system technical journal, v. 27, n. 3, p. 379-423, 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[20] Tognon, C., *Cotas para a distância mínima de códigos de Goppa envolvendo o piso e o teto de um divisor*, Dissertação de mestrado, IME - UFU, 2011.