UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Murillo Lozano Rubinho de Araujo

Corpos de Funções Algébricas e Teoria dos Códigos

São José do Rio Preto
2023

Murillo Lozano Rubinho de Araujo

Corpos de Funções Algébricas e Teoria dos Códigos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Parham Salehyan

São José do Rio Preto
2023

A663c

Araujo, Murillo Lozano Rubinho de
Corpos de funções algébricas e teoria dos códigos / Murillo Lozano Rubinho de Araujo. -- São José do Rio Preto, 2023
149 p. : il.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto
Orientador: Parham Salehyan

1. Matemática. 2. Corpos de funções algébricas. 3. Teorema de Riemann-Roch. 4. Extensões de Kummer e de Artin-Schreier. 5. Cota de Hasse-Weil. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Murillo Lozano Rubinho de Araujo

Corpos de Funções Algébricas e Teoria dos Códigos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Comissão Examinadora

Prof. Dr. Parham Salehyan
Orientador

Prof. Dr. Trajano Pires da Nóbrega Neto
IBILCE - UNESP

Prof. Dr. Herivelto Martins Borges Filho
ICMC - USP

São José do Rio Preto
13 de março de 2023

Aos meus pais, meu irmão e meus amigos,
dedico.

AGRADECIMENTOS

A presente dissertação de mestrado não poderia chegar a bom porto sem o precioso apoio de várias pessoas, as quais quero agradecer aqui:

Aos meus pais, por todo apoio desde sempre, tanto financeiro quanto emocional. À minha mãe, Rosana, por ser um exemplo de bondade, de compreensão e de amor, além de jamais medir esforços para sempre me proporcionar o melhor que eu poderia ter na vida. Ao meu pai, José Antônio, que apesar de todas as divergências que possamos ter, sempre se fez presente e batalhou para que tivéssemos as melhores oportunidades possíveis. Ao meu irmão, João Pedro, por ter alegrado minha vida nos últimos 14 anos e meio, além de ter me ensinado o significado de um novo amor: o fraterno. À toda minha família que sempre me deu apoio, em especial, minha tia Rose e minha tia Lucilene.

Ao professor Parham Salehyan, pelos últimos 5 anos que me orientou, e por ter me ensinado muito, não apenas de matemática, mas sobre a vida. Agradeço por viabilizar este trabalho, e por ter sido uma grande inspiração durante os últimos anos.

Ao meu melhor amigo, Guilherme Zahra, pela amizade incrível que construímos durante os últimos dois anos. Agradeço por ouvir meus desabafos, por me apoiar nos momentos mais difíceis, e por estar sempre presente nos momentos bons e ruins. Você foi fundamental para mim durante esse tempo, e sei que sem seu apoio não teria chegado até aqui.

Ao meu amigo Eduardo Martins, por todos os momentos felizes e divertidos que compartilhamos juntos, pelo apoio durante meu último ano de graduação, e por ser um verdadeiro irmão de outra mãe.

À minha amiga Milena Zacheo, por aguentar todas as minhas manias, pelas horas de risadas que damos juntos sempre que nos reunimos, por simplesmente estar do meu lado e sendo uma ótima companhia.

À minha amiga Ana Rossafa, por ter sido durante tantos anos a melhor vizinha de apartamento, por sempre me aconselhar e me consolar quando as coisas davam

errado.

À minha amiga Maria Clara Taddone, por ter vivido a maior parte dos últimos 6 anos comigo. Agradeço por ser minha dupla de disciplina, de área de pesquisa, de PET, e de vida. Que possamos sempre ter um ao outro.

À minha amiga Ana Rita Barbas, por aguentar todos os meus surtos, por ouvir meus áudios imensos e pelas horas e horas de conversas que tivemos. Mesmo longe, tenho a certeza de que nossa amizade sempre será algo especial para nós, e agradeço sempre por todo apoio até aqui.

Aos meus estimados amigos: Eduardo Scabora, por tornar minha vida leve, por topar todas as loucuras junto comigo e por estar sempre disponível para me ajudar; Rafael Araujo, pelos momentos engraçados e divertidos que vivemos diariamente, além de me proporcionar as melhores risadas e discussões; Carlos Augusto, por viver em pé de guerra comigo, sempre me contrariando e vice-versa, e ser uma companhia sempre agradável de se estar junto (ou quase sempre); Victória Ratzat, pelos seis longos anos de amizade, por todas as jantas e almoços que fizemos juntos, e pelos roles mais aleatórios em que nos metemos e pela cumplicidade que temos; Ana Gabriela Wicher, pelas conversas e desabafos que sempre temos, além de termos um humor extremamente igual e sermos tão parecidos.

À todos os amigos que fiz estando em Rio Preto, em especial, a Maria Fernanda, Sérgio Verde, Pedro Melo, Marcos Vinícius, por cada jogatina realizada em diversas noites, além de várias risadas e bons momentos; Larissa Soilo, Isabela Pereira e Gabriela Assis, pelas risadas, resenhas e conversas, além de fazerem parte do grupo intitulado "Panasonic". Aos meus amigos Sara Pereira e Mateus Pereira, que mesmo distantes no dia a dia, sempre foram exemplos de amizade e me apoiaram em todas as escolhas. Por fim, mas não menos importante, agradeço Aldimir Bruzadin, Álvaro Helena, Ana Carolina Batista, Ana Julia Gomes, Bruna Andrade, Daiane Donegá, Eduardo Morais, Gabriel Freitas, Gabriel Leone, Issac Sanches, Juliana Marques, Juliana Marques Souza, Larissa Astorini, Larissa Pastri, Linara Fachini, Maiara Martins, Mayara Cristina, Rebeca Esperança, Tarcísio Perfecto, Thaynara Bonfim e Yasmin Moura.

Aos professores do IBILCE, com os quais tanto aprendi. Em especial, ao professor Weber Pereira, por ter sido um grande amigo e sempre ter me aconselhado em

diversos momentos durante a graduação; à professora Luci Any, por ter sido minha primeira orientadora na graduação e por ter sido como uma mãe no meu primeiro ano de faculdade; à professora Michelle Morgado, por todo apoio emocional durante esses últimos anos, por ter escutado todas as minhas queixas e angústias, além de sempre ter acreditado em mim; à professora Juliana Precioso, por todo apoio durante meu período como petiano, por ter me ensinado a gostar de análise, e ainda, ter lecionado o melhor curso que tive durante a graduação; à professora Maria Gorete, com quem pude ter várias conversas sobre matemática e sobre a vida, além de ter me divertido muito na sua companhia; e também, à professora Ermínia, que sempre me apoiou e confiou no meu potencial e por quem tenho um carinho muito especial.

Por fim, à Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto, IBILCE, onde vivi os melhores anos da minha vida, onde conheci as pessoas mais incríveis, e também, onde descobri o meu amor pela matemática.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Se você pode sonhar,
você pode fazer.
Walt Disney

RESUMO

A teoria de curvas algébricas possui diversas aplicações na matemática. Quando as estudamos sobre corpos finitos, obtemos aplicações na teoria de códigos, criptografia e geometria finita.

Neste trabalho, tratamos da parte algébrica desta teoria, e nosso principal objeto de estudo são os corpos de funções algébricas, os quais veremos a princípio, sobre corpos arbitrários. Posteriormente, restringiremos para corpos finitos, e estaremos interessados no número de lugares racionais que um corpo de funções possui, e uma cota superior para este número. Serão apresentados também resultados que estimam seu gênero. As aplicações destes resultados culminam na existência de curvas maximais, e um código bastante importante: os códigos de Goppa.

Palavras-chave: Corpos de funções algébricas. Teorema de Riemann-Roch. Extensões de Kummer e de Artin-Schreier. Cota de Hasse Weil. Gênero.

ABSTRACT

The algebraic curves theory has several applications in mathematics. When we study them over finite fields, we get applications in code theory, cryptography and finite geometry.

In this work, we deal with the algebraic part of this theory, and our main object of study are the algebraic functions fields, which we will see at first, over arbitrary fields. Later, we will restrict to finite fields, and we will be interested in the number of rational places that a function field has, and an upper bound for this number. Results that estimate its genus will also be presented. The applications of these results culminate in the existence of maximal curves, and a very important code: the Goppa codes.

Keywords: Algebraic function fields. Riemman-Roch theorem. Kummer and Artin-Schreier extensions. Hasse-Weil bound, Genus.

Sumário

1 Introdução

O estudo de curvas algébricas é um tópico essencial na área da geometria algébrica, a qual ocupa um papel central na matemática moderna, e tem conexões com áreas diversas, como análise complexa, topologia e teoria dos números. Nesta dissertação de mestrado, o foco principal será estudar os corpos de funções algébricas, e é baseado nas referências [1] e [2].

No primeiro capítulo, iniciamos com a definição de um corpo de funções algébricas, e estaremos interessados em estudar os conceitos de lugares, valorizações discretas, anéis de valorização e divisores associados a ele. Com isso, introduzimos o espaço de Riemann-Roch. O problema envolvendo esse espaço consiste em determinar sua dimensão, e para isso, introduzimos o gênero de um corpo de funções. Os principais resultados deste capítulo consistem no teorema de Riemann-Roch, o teorema da Dualidade e o teorema da Aproximação Forte.

O capítulo seguinte é destinado às aplicações da teoria do capítulo 1. Estaremos interessados na construção de códigos corretores de erros, utilizando corpos de funções algébricas. Mais precisamente, nos códigos de Goppa e BCH, que na prática são os mais utilizados. Além do que veremos neste capítulo, outras aplicações destes resultados podem ser encontrados em [5], [8], [10] e [11].

No capítulo 3, estaremos interessados em estudar extensões de corpo de funções algébricas, além de relacionar conceitos da teoria de corpos com as estruturas até então vistas. Veremos a definição de bases integrais locais, as quais estão diretamente associadas à extensões de lugares e de anéis de valorização. Alguns resultados clássicos como a fórmula do gênero de Hurwitz e o teorema do diferente de Dedekind serão demonstrados neste capítulo. Por fim, serão introduzidas por fim, duas extensões especiais de Galois: as de Kummer e as de Artin-Schreier. Um aprofundamento de ambas pode ser encontrado em [12] e [13].

No último capítulo desta dissertação, estudaremos o comportamento dos corpos de funções sobre corpos finitos, e a sua relação com a função de Zeta e a hipótese de Riemann. Um dos resultados centrais será a cota de Hasse-Weil para corpos de funções, a qual nos fornece uma cota superior e inferior para o números de lugares de grau 1 de $F/\mathbb{F}_q$. Concluimos com as melhorias desta cota, quando estivermos sob hipóteses adicionais, além de relacionais estes resultados com a hipótese de Riemann.

2 Corpos de funções algébricas

Neste capítulo, introduziremos alguns resultados e definições sobre corpos de funções algébricas como valorização, lugares, divisores, gênero de uma curva algébrica e em seguida, veremos o teorema de Riemann-Roch e algumas de suas aplicações: o teorema das lacunas de Weierstrass, o teorema de Clifford e o teorema de Hurwitz.

Ao longo deste capítulo, K sempre denotará um corpo arbitrário (posteriormente, será necessária a finitude do corpo K para resultados mais específicos de nossa teoria).

2.1 Corpos de funções algébricas e lugares

Iniciamos esta seção com a definição de corpo de funções algébricas, e em seguida veremos alguns exemplos.

Definição 2.1. *Um corpo de funções algébricas de uma variável sobre o corpo K é uma extensão $F \supseteq K$ tal que $F/K(x)$ é finita, para algum $x \in F$ transcendente sobre K.*

Essa definição diz que um corpo de funçoes algébricas é uma extensão finita do corpo de funções racionais.

Exemplo 2.2. *O exemplo mais simples de um corpo de funções algébricas é o corpo das funções racionais: F/K é chamado racional se $F = K(x)$ para algum $x \in F$ que é transcendente sobre K. Aqui, cada elemento não nulo $z \in K(x)$ tem um única representação*

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

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

Exemplo 2.3. *Considere o anel $K[x, y]$ e a cúspide dada pela equação polinomial $y^2 - x^3 = 0$. Seja $I = \langle y^2 - x^3 \rangle$. Quando fazemos o quociente, obtemos o corpo de frações $\dfrac{K[x,y]}{\langle y^2 - x^3 \rangle}$. Este é um corpo de funções de uma variável sobre K, e pode ser escrito como $K(x)(\sqrt{x^3})$, neste caso de grau 2 sobre $K(x)$, ou como $K(y)(\sqrt[3]{y^2})$, de grau 3 sobre $K(y)$.*

A fim de facilitar a escrita, diremos que F/K é simplesmente um corpo de funções. Claramente, quando consideramos o conjunto $\widetilde{K} = \{z \in F \mid z \text{ é algébrico sobre } K\}$, este é um subcorpo de F, visto que dados $a, b \in \widetilde{K}$, então $a + b, a \cdot b, a^{-1} \in \widetilde{K}, a \neq 0$.

O conjunto $\widetilde{K}$ é chamado de *corpo das constantes* (ou fecho algébrico) de F/K . Assim, como existe $x \in F$ tal que x é transcendente sobre K, então valem as inclusões

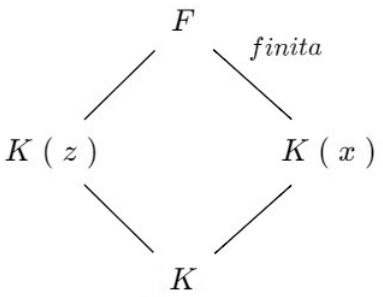
$$K \subseteq \widetilde{K} \subsetneq F.$$

A seguir, veremos uma maneira de caracterizar os elementos de F que são transcendentes sobre K, o que nos auxiliará nas demonstrações de resultados posteriores.

Proposição 2.4. *Seja F/K um corpo de funções algébricas. Então,*

$$z \in F \text{ é transcendente sobre } K \iff \text{a extensão } F/K(z) \text{ é finita.}$$

Demonstração: Primeiramente, note que do fato de F/K ser um corpo de funções, então F é uma extensão finita de $K(x)$, para algum x transcendente sobre K. Então, dado $z \in F$, vale a inclusão $K \subset K(z) \subset F$. Observe o diagrama a seguir:



($\Rightarrow$): Seja $z \in F$ transcendente sobre K. Como a extensão $F/K(x)$ é finita, então é algébrica. Por outro lado, como $z \in F$, então z é algébrico sobre $K(x)$. Assim, existem $a_0(x), a_1(x), \ldots, a_m(x) \in K[x], a_m(x) \neq 0$ tais que $a_m(x)z^m + \cdots + a_1(x)z + a_0(x) = 0$, para algum $m \geq 1$. Como z é transcendente sobre K, existe algum i tal que $a_i(x)$ é não constante.

Agora, reescreva $a_m(x)z^m + \cdots + a_1(x)z + a_0(x) \in K(z)[x]$, e isto mostra que x é algébrico sobre $K(z)$. Desse modo, $[K(x,z) : K(z)] < \infty$, e como $[F : K(x,z)] < \infty$, pelo teorema da multiplicidade dos graus, vale que $[F : K(z)] < \infty$, como gostaríamos de mostrar.

($\Leftarrow$) Reciprocamente, suponha por absurdo que $z \in F$ é algébrico sobre K. Então $[K(z) : K] < \infty$. Por hipótese, $[F : K(z)] < \infty$, e assim, temos $[F : K] < \infty$. Novamente pelo teorema da multiplicidade dos graus, temos que $[K(x) : K] < \infty$, o que é absurdo, uma vez que x é transcendente sobre K. Portanto, z é de fato transcendente sobre K.

■

Veremos agora a definição de anel de valorização, que será um conceito importante para a definição de lugares e de valorizações discretas.

Definição 2.5. *Um anel de valorização de um corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ que satisfaz*

(a)$K \subsetneq \mathcal{O} \subsetneq F$

(b) Para cada $z \in F^*$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Essa definição é motivada pela seguinte observação no caso de um corpo de funções racionais $K(x)$: dado um polinômio mônico e irredutível $p(x) \in K[x]$, consideramos o conjunto

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

Nessas condições, $\mathcal{O}_{p(x)}$ é um anel de valorização. De fato, temos $K \subseteq \mathcal{O}_{p(x)}$, e ainda, $x \in \mathcal{O}_{p(x)}$, mas $x \notin K$, uma vez que x é transcendente sobre K. Logo, $K \subsetneqq \mathcal{O}_{p(x)}$. Por outro lado, $\mathcal{O}_{p(x)} \subseteq K(x)$, pela definição de $\mathcal{O}_{p(x)}$. Agora, note que $\dfrac{1}{p(x)} \in K(x)$, mas $\dfrac{1}{p(x)} \notin \mathcal{O}_{p(x)}$, e assim a inclusão é estrita. Portanto, $K \subsetneqq \mathcal{O}_{p(x)} \subsetneqq K(x)$.

Agora considere $z = \dfrac{f(x)}{g(x)} \in K(x)$ com fatoração completa, ou seja, $\text{mcd}(f(x), g(x)) = 1$. Se $z \in \mathcal{O}_{p(x)}$, então não há o que mostrar. Suponha que $z \notin \mathcal{O}_{p(x)}$. Assim, $g(x)$ é divisível por $p(x)$, e como z possui uma fatoração completa, segue que $z^{-1} \in \mathcal{O}_{p(x)}$, como gostaríamos de mostrar.

Do que mostramos acima, segue que $\mathcal{O}_{p(x)}$ é um anel de valorização. Claramente se $p \neq q$, então $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Proposição 2.6. *Seja $\mathcal{O}$ um anel de valorização de um corpo de funções F/K. Então*
(a) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ tem um único ideal maximal $P = \mathcal{O}\backslash\mathcal{O}^*$, onde $\mathcal{O}^* = \{z \in \mathcal{O} \mid z \text{ e invertível em } \mathcal{O}\}$.
(b) Seja $0 \neq x \in F$. Então, $x \in P \iff x^{-1} \notin \mathcal{O}$.
(c) Seja $\widetilde{K}$ o corpo de constantes de F/K. Então $\widetilde{K} \subseteq \mathcal{O}$ e $\widetilde{K} \cap P = \{0\}$.

Demonstração: (a) Mostremos inicialmente que P é um ideal de $\mathcal{O}$. Sejam $x \in P$ e $z \in \mathcal{O}$. Se $xz \in \mathcal{O}^*$, então x seria invertível, o que não ocorre pois $x \in P$. Logo, $xz \notin \mathcal{O}^*$, e portanto, $xz \in P$.

Agora, considere $x, y \in P$. Então, x e y não são invertíveis. Sem perda de generalidade, assumimos que $x/y \in \mathcal{O}$, e segue que $1 + x/y \in \mathcal{O}$ também. Desse modo, $x + y = y(1 + x/y) \in P$, pelo que mostramos acima. Logo, P é um ideal de $\mathcal{O}$.

Mostrado isto, segue que P é maximal e único uma vez que um ideal próprio não pode conter um elemento invertível.

(b) Segue da seguinte equivalência:

$$x \in P \iff x \text{ não é invertível em } \mathcal{O} \iff x^{-1} \notin \mathcal{O}.$$

(c) Seja $z \in \widetilde{K}$ e assuma que $z \notin \mathcal{O}$. Como $\mathcal{O}$ é um anel de valorização, então $z^{-1} \in \mathcal{O}$. Por outro lado, como z é algébrico sobre $\widetilde{K}$, então z^{-1} também o é, ou seja, existem $a_1, \ldots, a_r \in K$ tais que

$$a_r \left(z^{-1}\right)^r + \cdots + a_1 z^{-1} + 1 = 0 \Longrightarrow z^{-1}\left(a_r (z^{-1})^{r-1} + \cdots + a_1\right) = -1 \Longrightarrow$$
$$\Rightarrow z = -\left(a_r (z^{-1})^{r-1} + \cdots + a_1\right),$$

e assim, $z \in K[z^{-1}] \subseteq \mathcal{O}$, o que contradiz a hipótese. Portanto, concluimos que $\widetilde{K} \subseteq \mathcal{O}$.

Agora, resta mostrar que $\widetilde{K} \cap P = \{0\}$. Suponhamos que exista $x \neq 0$ na interseção acima. Como $x \in \widetilde{K}$, então existem $a_1, \ldots, a_n \in K$ tais que

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

e assim, x seria invertível em $\mathcal{O}$, o que contradiz o fato de $x \in P$. Logo, $x = 0$, e isso conclui a prova de que $\widetilde{K} \cap P = \{0\}$.

■

A seguir, temos um lema que será utilizado mais adiante na demonstração de alguns resultados importantes, além de motivar a definição de anel de valorização discreta.

Lema 2.7. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K, P seu ideal maximal e $0 \neq x \in P$. Sejam ainda $x_1, \ldots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, com $i = 1, \ldots, n-1$. Então, $n \leq [F : K(x)] < \infty$.*

Demonstração: Pelas proposições 2.4 e 2.6 item (3), segue que $F|K(x)$ é uma extensão finita, ou seja, $[F : K(x)] < \infty$. Resta mostrar que $n \leq [F : K(x)]$. Para isso, é suficiente mostrar que os x_i's do enunciado do lema, com $i = 1, \ldots n$, são linearmente independentes sobre $K(x)$. Sejam $\varphi_1(x), \ldots, \varphi_n(x) \in K(x)$ tais que $\sum_{i=1}^{n} \varphi_i(x)x_i = 0$. Assumimos que todos os $\varphi_i(x)$ são polinômios em x e que x não divide todos eles. Denotamos $a_i = \varphi_i(0)$, e definimos para cada $j \in \{1, \ldots, n\}$, $a_j \neq 0$ e $a_i = 0$ para $i > j$. Assim,

$$\sum_{i=1}^{n} \varphi_i(x)x_i = 0 \Longrightarrow \sum_{i \neq j}^{n} \varphi_i(x)x_i + \varphi_j(x)x_j = 0 \Longleftrightarrow \sum_{i \neq j}^{n} \varphi_i(x)x_i = -\varphi_j(x)x_j,$$

com $\varphi_i(x) \in \mathcal{O}$, para $i = 1, \ldots, n$ (já que $x = x_i \in P$), $x_i \in x_jP$, para $i < j$ e $\varphi_i(x) = xg_i(x)$, para $i > j$, onde $g_i(x)$ é um polinômio em x. Dividindo a equação acima por x_j, obtemos

$$\sum_{i \neq j} \varphi_i(x)x_i = -\varphi_j(x)x_j \Longrightarrow \left(\sum_{i \neq j} \varphi_i(x)x_i\right) \cdot \frac{1}{x_j} = -\varphi_j(x) \Longrightarrow$$
$$\sum_{i<j} \varphi_i(x)\frac{x_i}{x_j} + \sum_{i>j} xg_i(x)\frac{x_i}{x_j} = \varphi_j(x).$$

Os termos do lado esquerdo pertencem a P, e logo $\varphi_j(x) \in P$. Agora, note que $\varphi_j(x) = a_j + xg_j(x)$, onde $g_j(x) \in K[x] \subseteq \mathcal{O}$ e $x \in P$. Assim,

$$a_j = \varphi_j(x) - xg_j(x) \in K.$$

Desse modo, $0 \neq a_j \in K \cap P \subset \widetilde{K} \cap P$, o que contradiz a proposição 2.6 item (3). Logo $\varphi_i(x) = 0$, para todo $i = 1, \ldots, n$. Portanto, $x_1, \ldots, x_n$ são linearmente independentes, e concluimos que $[F : K(x)] \geq n$, como gostaríamos de demonstrar.

■

Demonstrado o lema acima, provaremos um teorema a seguir que nos fornece em seguida a definição de anel de valorização discreta.

Teorema 2.8. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K e P seu ideal maximal. Então*

(a) P é um ideal principal.

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

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

Demonstração: (a) Suponhamos que P não é um ideal principal e considere $0 \neq x_1 \in P$. Como P não é principal, então $P \neq x_1\mathcal{O}$, e assim, existe $x_2 \in P \backslash x_1\mathcal{O}$. Afirmamos que $x_2x_1^{-1} \notin \mathcal{O}$. De fato, se $x_2x_1^{-1} \in \mathcal{O}$, teríamos $x_2 \in x_1\mathcal{O}$, o que é absurdo pela escolha de x_2. Novamente, pela proposição 2.6 item 2, como $x_2x_1^{-1} \notin \mathcal{O}$, então $x_2^{-1}x_1 \in P$, e portanto, $x_1 \in x_2P$. Analogamente, podemos encontrar x_3 tal que $x_2 \in x_3P$.

Por indução, conseguimos uma sequência infinita de elementos $x_1, x_2, x_3, \ldots$ em P tal que $x_i \in x_{i+1}P$, $\forall i \geq 1$, o que contraria o lema 2.7, uma vez que $[F : K(x)] < \infty$. Portanto, concluimos que P é um ideal principal.

(b) Para a demonstração deste item, mostremos a existência dessa representação. Seja $0 \neq z \in F$. Como $\mathcal{O}$ é anel de valorização, sem perda de generalidade, assumimos que $z \in \mathcal{O}$. Se $z \in \mathcal{O}^*$, então $z = t^0 z$, e não há o que mostrar. Suponha que $z \notin \mathcal{O}^*$, ou seja, $z \in P$ pela definição do ideal maximal. Assim, pelo lema 2.7, existe $m \geq 1$, m maximal, tal que $z \in t^m\mathcal{O}$, uma vez que a sequência

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

é limitada. Assim, escrevemos $z = t^m u$, com $u \in \mathcal{O}$. Resta mostrar que $u \in \mathcal{O}^*$. Suponha que $u \notin \mathcal{O}^*$, ou seja, $u \in P = t\mathcal{O}$, isto é, $u = tw$, com $w \in \mathcal{O}$. Desse modo,

$$z = t^m u = t^m tw = t^{m+1}w \subseteq t^{m+1}\mathcal{O},$$

o que contradiz o fato de m ser maximal. Logo, devemos ter $u \in \mathcal{O}^*$, e isto conclui a existência da representação. A unicidade desta representação segue do fato de termos m ser maximal e u ser invertível.

(c) Seja $\{0\} \neq I \subset \mathcal{O}$ um ideal. Mostremos que existe $n \in \mathbb{N}$ tal que $I = t^n\mathcal{O}$. Considere o conjunto $A = \{r \in \mathbb{N} \mid t^r \in I\}$.

Notamos primeiramente que $A \neq \emptyset$. De fato, se $0 \neq x \in I$, então pelo item anterior $x = t^r u$, com $u \in \mathcal{O}^*$, e portanto $xu^{-1} = t^r$. Como $x \in I$, então $xu^{-1} = t^r \in I$.

Seja $n := \min(A)$. Afirmamos que $I = t^n\mathcal{O}$. De fato, como $t^n \in I$, do fato de I ser ideal, segue a inclusão $t^n\mathcal{O} \subseteq I$. Reciprocamente, seja $y \in I$. Pelo item anterior, existe $s \geq 0$ e $w \in \mathcal{O}^*$ tal que $y = t^s w$. Pela minimalidade de n, temos $s \geq n$, e ainda, $t^s \in I$. Reescrevendo y de uma maneira adequada, obtemos

$$y = t^{s-n}.t^n.w = t^n.(t^{s-n}.w) \in t^n\mathcal{O},$$

e segue que $I \subseteq t^n\mathcal{O}$, e portanto vale a igualdade.

■

Definição 2.9. *Um anel que possui as propriedades (a), (b) e (c) do teorema 2.8 é chamado de um anel de valorização discreta.*

Definido o conceito de anel de valorização discreta, podemos definir o conceito de lugar, objeto principal de estudo nessa seção, e de parâmetro local.

Definição 2.10. *Seja F/K um corpo de funções.*

a) Um lugar P de F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de $F|K$. Todo elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado de parâmetro local ou elemento primo de P.

b) $\mathbb{P}_F := \{P \mid P$ 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 unicamente determinado por P, isto é, $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Assim definimos $\mathcal{O}_P = \mathcal{O}$ como o anel de valorização do lugar P.

Definição 2.11. *Uma valorização discreta de F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ que satisfaz:*
a) $v(x) = \infty \Longleftrightarrow x = 0$;
b) $v(xy) = v(x) + v(y)$, $\forall x, y \in F$;
c) $v(x + y) \geq \min\{v(x), v(y)\}$, $\forall x, y \in F$;
d) existe $z \in F$ tal que $v(z) = 1$;
e) $v(a) = 0$, $\forall a \in K$, $a \neq 0$.

Observação 2.12. *O símbolo ∞ serve para denotar um elemento não pertencente a $\mathbb{Z}$ tal que $\infty + \infty = \infty + n = \infty$, $\forall n \in \mathbb{Z}$ e $\infty > m$, $\forall m \in \mathbb{Z}$.*

Observação 2.13. *Seja $n \in \mathbb{Z}$. Pelo item d) da definição acima, existe $z \in F$ tal que $v(z) = 1$. Do item b), segue que $v(z^n) = v(z) + \cdots + v(z) = 1 + \cdots + 1 = n$. Portanto, v é sobrejetora.*

Veremos agora como se comporta a propriedade c) da definição de valorização discreta, para o caso em que $v(x) \neq v(y)$.

Lema 2.14. *(Desigualdade triangular estrita) Sejam v uma valorização discreta de F/K e $x, y \in F$ tais que $v(x) \neq v(y)$. Então $v(x + y) = \min\{v(x), v(y)\}$.*

Demonstração: Primeiramente, note que se $a \in K$, então $v(ay) = v(a) + v(y) = v(y)$, pelos itens (b) e (e) da definição 2.11. Em particular, $v(y) = v(-y)$.

Por hipótese, $v(x) \neq v(y)$. Sem perda de generalidade, suponha que $v(x) < v(y)$ e que $v(x + y) \neq \min\{v(x), v(y)\}$. Então, pelo item (c) da definição 2.11, $v(x + y) > \min\{v(x), v(y)\} = v(x)$. Por fim, temos

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

o que é absurdo. Portanto, $v(x + y) = \min\{v(x), v(y)\}$.

■

Definição 2.15. *A cada lugar $P \in \mathbb{P}_F$, associamos a função $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ da seguinte forma: escolhemos um parâmetro local t de P. Então, cada $0 \neq z \in F$ possui uma representação única da forma $z = t^n u$, com $u \in \mathcal{O}_P^*$ e $n \in \mathbb{Z}$. Desse modo, colocamos $v_P(z) = n$ e $v_P(0) = \infty$.*

Observamos que a definição anterior depende unicamente de P, e não da escolha do parâmetro local t. De fato, seja t' um outro parâmetro local para P. Então, $P = t\mathcal{O} = t'\mathcal{O}$. Desse modo, pelo item (b) do teorema 2.8, $t = t'w$, para algum $w \in \mathcal{O}_P^*$. Assim,

$$t^n u = (t'w)^n u = (t')^n w^n u = (t')^n (w^n u), \text{ onde } w^n u \in \mathcal{O}_P^*.$$

Logo, teremos $v_P(t^n u) = n = v_P((t')^n (w^n u))$, o que garante que a definição não depende do parâmtro escolhido.

Teorema 2.16. *Seja F/K um corpo de funções. Então*
(a) Para cada lugar $P \in \mathbb{P}_F$, a função v_P da definição anterior é uma valorização discreta de F/K. Mais ainda, temos:

$$\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\},$$
$$P = \{z \in F \mid v_P(z) > 0\}.$$

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

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

(d) Todo anel de valorização de F/K é um subanel próprio e maximal de F.

Demonstração: (a) Mostremos que v_P satisfaz as 5 propriedade da definição de valorização discreta.

(i) Segue da definição de v_P que $v_P(x) = \infty \iff x = 0$.

(ii) Sejam $x, y \in F$ e t um parâmetro local de P. Logo, $x = t^m u$, $y = t^n v$, com $m, n \in \mathbb{Z}$ e $u, v \in \mathcal{O}_P^*$. Temos

$$v_P(xy) = v_P(t^m u t^n v) = v_P(t^{m+n} uv) = m + n = v_P(x) + v_P(y).$$

(iii) Sejam $x, y \in F$ com $v_P(x) = n$ e $v_P(y) = m$. Assumimos que $n \leq m < \infty$ e $x = t^n u_1$, $y = t^m u_2$, com $u_1, u_2 \in \mathcal{O}_P^*$. Logo,

$$x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n} u_2) = t^n z,$$

onde $z = u_1 + t^{m-n} u_2 \in \mathcal{O}_P$. Se $z = 0$, então $v_P(x + y) = v_P(0) = \infty > \min\{m, n\}$. Suponha que $z \neq 0$. Então $z = t^k u$, com $k \geq 0$ e $u \in \mathcal{O}_P^*$. Assim,

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

pois $n \leq m$.

(iv) Tomando $z = t$, temos $z = t^1 \cdot 1$, com $1 \in \mathcal{O}_P^*$, e portanto $v_P(t) = 1$.

(v) Seja $a \in K$, $a \neq 0$. Assim, claramente $a = t^0.a$, e $a \in \mathcal{O}_P^*$. Desse modo, $v_P(a) = 0$.

De (i), (ii), (iii), (iv) e (v) segue que v_P é uma valorização discreta de F/K.

Agora, provemos que $P = \{z \in F \mid v_P(z) > 0\}$. Suponha que exista $z \in P$ tal que $v_P(z) \leq 0$. Então, $z = t^n u$, com $u \in \mathcal{O}^*$ e $n \leq 0$. Assim, $u = t^{-n} z$. Agora, como $t, z \in P$, então $t^{-n} z = u \in P$, o que é absurdo pois u é invertível. Logo, $P \subseteq \{z \in F \mid v_P(z) > 0\}$. Para a outra inclusão, considere $z \in F$ tal que $v_P(z) > 0$. Se $v_P(z) = \infty$, então $z = 0 \in P$. Se $v_P(z) = n \in \mathbb{Z}$, então $z = t^n u$, com $u \in \mathcal{O}^*$ e $n \in Z$, e assim, $z \in t\mathcal{O} = P$. Portanto, segue a igualdade dos conjuntos.

Por outro lado, para todo $z \in F$, pela proposição 2.6, item (b), $z \in \mathcal{O} \iff z^{-1} \notin P \iff v_P(z^{-1}) \leq 0 \iff v_P(z) \geq 0$. Portanto, $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$. Do que fizemos, segue que $\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$.

(b) Se $x \in F$ é um parâmetro local, então $x = x \cdot 1$, com $1 \in \mathcal{O}_P^*$. Logo $v_P(x) = 1$.

Reciprocamente, considere t um parâmetro local para P, ou seja $P = t\mathcal{O}$ e sejam $a \in P$ e $v_P(x) = 1$. Queremos mostrar que x é um parâmetro local para P. Como $a \in P = t\mathcal{O}$, então $a = t \cdot o$, com $o \in \mathcal{O}$. Agora, como $v_P(x) = 1$, então $x = t \cdot u$, com $u \in \mathcal{O}^*$. Assim, $a = x \cdot u \cdot o$. Definindo $w := u \cdot o$, segue que $a = x \cdot w$, com $w \in \mathcal{O}$, e portanto, x é parâmetro local de P.

(c) Segue diretamente do que foi feito no item (a).

(d) Sejam $\mathcal{O}$ um anel de valorização de F/K, P seu ideal maximal, v_P a valorização discreta associada a P e $z \in F \backslash \mathcal{O}$.

Mostremos que $F = \mathcal{O}[z]$. Claramente $\mathcal{O}[z] \subseteq F$, uma vez que $\mathcal{O} \subset F$ e $z \in F$. Para a outra inclusão, considere $y \in F$. Então, $v_P(yz^{-k}) \geq 0$, para k suficientemente grande (isto vale pois como $z \notin \mathcal{O}$, então $z^{-1} \in P$, e segue que $v_P(z^{-1}) > 0$). Logo, definimos $w := yz^{-k}$ e temos $w \in \mathcal{O}$, pois $v_P(w) \geq 0$. Então $w = yz^{-k} \Leftrightarrow y = wz^k \in \mathcal{O}[z]$, ou seja, $F \subseteq \mathcal{O}[z]$. Portanto, $\mathcal{O}[z] = F$, como gostaríamos de mostrar.

■

Pelo que vimos no teorema acima, lugares, valorizações discretas e anéis de valorização estão associados às mesmas estruturas.

Agora, considere P um lugar de F/K e $\mathcal{O}_P$ o seu anel de valorização. Como P é um ideal maximal de $\mathcal{O}_P$, então o anel de classe residual $\mathcal{O}_P/P$ é um corpo. Para $x \in \mathcal{O}_P$, definimos $x(P) \in \mathcal{O}_P/P$ como a classe residual de x módulo P, e para $x \in F \backslash \mathcal{O}_P$, colocamos $x(P) := \infty$. Pela proposição 2.6, sabemos que $K \subseteq \widetilde{K} \subseteq \mathcal{O}_P$ e $K \cap P \subseteq \widetilde{K} \cap P = \{0\}$, e assim, a aplicação $\mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ induz uma aplicação canônica de K em $\mathcal{O}_P/P$. Assim, consideramos K como um subcorpo de $\mathcal{O}_P/P$, via essa injeção. Vale ressaltar que podemos considerar o corpo das constantes $\widetilde{K}$ no lugar de K. Isso nos motiva a seginte definição:

Definição 2.17. *Seja $P \in \mathbb{P}_F$.*
a) $F_P := \mathcal{O}_P/P$ é o corpo de classe residual de P, e a aplicação

$$\begin{aligned} \varphi : F &\longrightarrow F_P \cup \{\infty\} \\ x &\longmapsto x(P) \end{aligned}$$

é chamada aplicação de classe residual com respeito a P. É comum utilizarmos a notação $x + P := x(P)$.
b) $\deg P = [F_P : K]$ é chamado grau de P. Se um lugar P possui grau 1, P é chamado de um lugar racional de $F|K$.

A proposição a seguir nos garante a finitude do grau de P.

Proposição 2.18. *Se P é um lugar de $F|K$ e $0 \neq x \in P$, então*

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

Demonstração: Já vimos pela proposição 2.4 que $[F : K(x)] < \infty$. Mostremos a outra desigualdade. É suficiente mostrar que, para quaisquer $z_1, \ldots, z_n \in \mathcal{O}_P$, cujas classes residuais $z_1(P), \ldots, z_n(P) \in F_P$ são linearmente independentes sobre K, são linearmente independentes sobre $K(x)$.

Suponha que exista uma cominação linear não trivial da forma

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

com $\varphi_i(x) \in K(x)$. Sem perda de generalidade, assumimos que $\varphi_i(x)$ são polinômios em x e nem todos são divisíveis por x, ou seja, $\varphi_i(x) = a_i + g_i(x)$, com $a_i \in K$ e $g_i \in K[x]$, com $a_j \neq 0$, para algum $j = 1, \ldots n$. Como $x \in P$ e $g_i(x) \in \mathcal{O}_P$, então $\varphi_i(x)(P) = a_i(P) = a_i$. Agora, temos

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

e isso contradiz o fato de $z_1(P), \ldots z_n(P)$ serem linearmente independentes sobre K. Portanto, $z_1, \ldots, z_n$ são linearmente independente sobre $K(x)$, e segue que $\deg P \leq [F : K(x)]$.

■

Corolário 2.19. *O corpo $\widetilde{K}$ das constantes de F/K é uma extensão finita de K.*

Demonstração: Seja $P \in \mathbb{P}_F$. Como $\widetilde{K} \hookrightarrow F_P$ via a aplicação $\mathcal{O}_P \longrightarrow F_P$, segue da proposição 2.18 que

$$[K : \widetilde{K}] \leq [F_P : K] = \deg P \leq [F : K(x)] < \infty.$$

■

Observação 2.20. *Seja P um lugar racional de F/K, isto é,* $\deg P = 1$. *Assim, $F_P = K$, e portanto, a aplicação de classe residual com respeito a P é dada por*

$$\begin{aligned} \varphi : F &\longrightarrow K \cup \{\infty\} \\ x &\longmapsto x + P \end{aligned}$$

Em particular, se K é um corpo algebricamente fechado, então todos os lugares tem grau 1. De fato, se K é algebricamente fechado, então toda extensão algébrica é trivial, ou seja, $[F_p : K] = 1$, para todo $P \in \mathbb{P}_F$. Podemos então olhar para $z \in F$ como uma aplicação

$$z : \begin{cases} \mathbb{P}_F \longrightarrow K \cup \{\infty\} \\ P \longmapsto z + P \end{cases}$$

Por essa razão, F/K é chamado de um corpo de funções. Por outro lado, os elementos de K, interpretados como funções pela aplicação acima, são as constantes, e por isto é chamado de corpo das constante de F.

A seguir, veremos a definição de zeros e polos de um elemento $z \in F$. Essa definição é uma generalização desses conceitos vistos na teoria de funções de uma variável complexa.

Definição 2.21. *Sejam $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z, se $v_P(z) > 0$ e que P é um polo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, então P é um zero de ordem m e se $v_P(z) = -m < 0$, então P é um polo de ordem m.*

Até o momento, baseamos nossa teoria na existência de lugares de um corpo de funções. Uma pergunta natural que surge é a seguinte: dado um corpo de funções F/K, sempre existe P um lugar de F/K? O próximo teorema garante que $\mathbb{P}_F \neq \emptyset$.

Teorema 2.22. *Sejam F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Considere $\{0\} \neq I \subsetneq R$ um ideal próprio de R. Então, existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Demonstração: Considere o conjunto $\mathcal{F} := \{S \mid S \text{ é subanel de } F \text{ com } R \subseteq S \text{ e } IS \neq S\}$. Sabemos que IS por definição é o conjuntos de todas as somas finitas da forma $\sum a_\nu s_\nu$ onde $a_\nu \in I, s_\nu \in S$, e que é um ideal de S. Afirmamos que $\mathcal{F} \neq \emptyset$, uma vez que $R \in \mathcal{F}$. Além disso, $\mathcal{F}$ é ordenado pela inclusão. De fato, se $\mathcal{H} \subseteq \mathcal{F}$ é um subconjunto totalmente ordenado de $\mathcal{F}$, então $T := \bigcup\{S \mid S \in \mathcal{H}\}$ é um subanel de F com $R \subseteq T$. Temos que verificar que $IT \neq T$. Suponha que isso seja falso, ou seja, que $IT = T$. Então, $1 = \sum_{\nu=1}^{n} a_\nu s_\nu$, com $a_\nu \in I, s_\nu \in T$. Como $\mathcal{H}$ é totalmente ordenado, então existe $S_0 \in \mathcal{H}$ tal que $s_1, \ldots, s_n \in S_0$, o que implica que $1 = \sum_{\nu=1}^{n} a_\nu s_\nu \in IS_0$, o que é uma contradição. Assim, $T \in \mathcal{F}$ e, claramente, T é majorante de $\mathcal{H}$.

Então pelo lema de Zorn, $\mathcal{F}$ possui um elemento maximal, ou seja, existe $\mathcal{O} \subseteq F$ tal que $R \subseteq \mathcal{O} \subseteq F, I\mathcal{O} \neq \mathcal{O}$, e $\mathcal{O}$ é maximal com relação a essas propriedades. Para concluir a demonstração, resta mostrar que $\mathcal{O}$ é um anel de valorização de F/K.

Por hipótese, $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$, ou seja, $\mathcal{O} \subseteq F$ e $I \subseteq \mathcal{O} \backslash \mathcal{O}^*$. Suponha que exista um elemento $z \in F$ tal que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Desse modo, temos $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}\left[z^{-1}\right] = \mathcal{O}\left[z^{-1}\right]$. Assim, existem $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ tais que

$$1 = a_0 + a_1 z + \cdots + a_n z^n \text{ e}$$
$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}.$$

Agora, note que $m, n \geq 1$, pois caso contrário teríamos $a_0 = 1$ ou $b_0 = 1$, ou seja, $1 \in I\mathcal{O}$, implicando em $I\mathcal{O} = \mathcal{O}$. Ainda, podemos supor que n, m são os menores inteiros positivos que satisfazem as igualdades acima, e sem perda de generalidade, que $m \leq n$. Multiplicando a primeira equação por $1 - b_0$ e a segunda por $a_n z^n$, obtemos

$$1 - b_0 = (1 - b_0)\, a_0 + (1 - b_0)\, a_1 z + \cdots + (1 - b_0)\, a_n z^n \text{ e}$$
$$0 = (b_0 - 1)\, a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}.$$

Somando as duas equaçõs, obtemos $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$, onde $c_i \in I\mathcal{O}$, mas isso é uma contradição, pela minimalidade de n. Assim, para todo $z \in F$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$, e segue que $\mathcal{O}$ é um anel de valorização, o que conclui a demonstração do teorema.

■

O corolário a seguir garante que, todo elemento $z \in F$, que não pertence ao corpo das constantes $\widetilde{K}$, possui pelo menos um zero e um polo.

Corolário 2.23. *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.*

Demonstração: Considere o anel $R = K[z]$ e o ideal $I = zK[z]$. Pelo teorema 2.22, existe $P \in \mathbb{P}_F$ tal que $z \in P$, e portanto, P é um zero de z. Analogamente, prova-se que z^{-1} tem um zero $Q \in \mathbb{P}_F$, ou seja, Q é um polo de z. Em particular, obtemos que $\mathbb{P}_F \neq \emptyset$.

■

2.2 O corpo das funções racionais

Na seção anterior, trabalhamos com corpos de funções mais gerais e alguns resultados acerca deles. Para um entendimento melhor de como funcionam os corpos de funções, abordaremos nesta seção o caso mais simples, em que o corpo de funções é racional, ou seja, quando temos $F = K(x)$, com x transcendente sobre K.

Consideramos $F = K(x)$ ao longo desta seção. Dado um polinômio mônico irredutível $p(x) \in K[x]$, obtemos o anel de valorização

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

de $K(x)|K$, cujo ideal maximal é

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

Claramente $\mathcal{O}_{p(x)}$ é um anel de valorização e $P_{p(x)}$ o seu ideal maximal. Um caso particular, é quando consideramos o polinômio $p(x) = x - \alpha$, com $\alpha \in K$. Nesse caso, escrevemos $P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}$.

Além do anel de valorização $\mathcal{O}_{p(x)}$, é possível definir outro anel de valorização de $K(x)/K$. Considere o conjunto

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

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

De fato, claramente $K \subset \mathcal{O}_\infty$, e ainda, a inclusão é estrita uma vez que $z = \dfrac{1}{x} \in \mathcal{O}_\infty$, mas $z \notin K$. Assim, $K \subsetneq \mathcal{O}_\infty$. Por outro lado, por definição de $\mathcal{O}_\infty$, temos $\mathcal{O}_\infty \subset K(x)$, mas $z = x \in K(x)$ e $z \notin \mathcal{O}_\infty$. Logo, $\mathcal{O}_\infty \subsetneq K(x)$.

Agora, seja $z = \dfrac{f(x)}{g(x)} \in K(x)$. Se $z \in \mathcal{O}_\infty$, não há o que mostrar. Suponha que $z \notin \mathcal{O}_\infty$. Então, $\deg f(x) > \deg g(x)$. Assim, $z^{-1} = \dfrac{g(x)}{f(x)} \in \mathcal{O}_\infty$. Logo, segue que $\mathcal{O}_\infty$ é um anel de valorização de $K(x)/K$.

É fácil verificar que o conjunto $P_\infty = \left\{ \dfrac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\}$ é ideal maximal de $\mathcal{O}_\infty$. O lugar P_∞ é chamado de *lugar infinito de* $K(x)$.

As proposições a seguir nos fornecem uma série de propriedadades de cada um dos dois tipos de anéis de valorizações e seus respectivos lugares definidos acima. Em seguida, mostraremos que esses são os únicos lugares do corpo de funções $K(x)/K$.

Proposição 2.24. *Considere em $K(x)/K$ o lugar $P = P_{p(x)} \in \mathbb{P}_{K(x)}$, onde $p(x) \in K[x]$ é um polinômio mônico e irredutível. Então $p(x)$ é um parâmetro local para P e a valorização v_P correspondente é definida da seguinte forma: se $z \in K[x]\backslash\{0\}$ é escrito da forma $z = p(x)^n \cdot (f(x)/g(x))$, com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. Ainda, o corpo de classe residual $K(x)_P = \mathcal{O}_P/P$ é isomorfo a $K[x]/\langle p(x)\rangle$, e um isomorfismo é dado por*

$$\phi : \begin{cases} K[x]/\langle p(x)\rangle \longrightarrow & K(x)_P \\ f(x) \bmod p(x) \longmapsto & f(x) + P. \end{cases}$$

Consequentemente, $\deg P = [K(x)_P : K] = \deg(p(x))$.

Demonstração: O fato de $p(x)$ ser um parâmetro local para P segue do teorema 2.16, uma vez que $p(x) = p(x)^1 \cdot 1$, ou seja, $v_P(p(x)) = 1$, e portanto, é um parâmetro local. Ainda, a aplicação definida no enunciado é claramente uma valorização.

Considere o homomorfismo

$$\phi : \begin{cases} K[x] \longrightarrow K(x)_P \\ f(x) \longmapsto f(x) + P \end{cases}$$

Vamos determinar o núcleo da aplicação ϕ. Temos

$$\operatorname{Ker}\phi = \{f(x) \in K[x] \mid \phi(f(x)) = 0\} = \{f(x) \in K[x] \mid f(x) + P = 0\} = \{f(x) \in K[x] \mid f(x) \in P\} = \langle p(x)\rangle.$$

Ainda, temos ϕ sobrejetora, uma vez que, 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, $\text{mdc}(p(x), v(x)) = 1$, e segue que existem $a(x), b(x) \in K[x]$ tais que $a(x)p(x) + b(x)v(x) = 1$. Assim,

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

ou seja, $z(P) = z + P = (b(x)u(x)) + P \in \text{Im}(\phi)$. Pelo teorema do isomorfismo, temos

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

Ainda $\deg P = [K(x)_P : K] = \deg(p(x))$.

■

Proposição 2.25. *Nas condições da proposição anterior, considere o caso em que $p(x) = x - \alpha$, com $\alpha \in K$. Então $\deg P = 1$ e a aplicação de classe residual é dada por $z(P) = z(\alpha)$, para $z \in K(x)$, onde $z(\alpha)$ é definido da seguinte forma: escreva $z = \dfrac{f(x)}{g(x)}$, onde $f(x), g(x) \in K[x]$ são primos entre si. Então*

$$z(\alpha) = \begin{cases} \dfrac{f(x)}{g(x)}, & g(\alpha) \neq 0 \\ \infty, & g(\alpha) = 0 \end{cases}.$$

Demonstração:

Nesse caso, temos $P = P_\alpha$, com $\alpha \in K$. Claramente $\deg P = 1$, pois pela proposição 2.24, temos $\deg P = [K(x)_P : K] = \deg(p(x)) = 1$.

Se $f(x) \in K[x]$, então $(x - \alpha) \mid (f(x) - f(\alpha))$, e consequentemente

$$f(x)(P) = (f(x) - f(\alpha))(P) + (f(\alpha))(P) = (f(\alpha))(P),$$

pois $f(x) - f(\alpha) \in P_\alpha$. Seja $z \in \mathcal{O}_P$ arbitrário. Então

$$z = \frac{f(x)}{g(x)}, \text{ com } f(x), g(x) \in K[x] \text{ e } p(x) = x - \alpha \nmid g(x).$$

Logo, $g(x)(P) = g(\alpha) \neq 0$, e temos $z(P) = \dfrac{f(x)(P)}{g(x)(P)} = \dfrac{f(\alpha)}{g(\alpha)} = z(\alpha), g(\alpha) \neq 0$. Se $g(\alpha) = 0$, colocamos $z(\alpha) = \infty$ e o resultado segue.

■

Proposição 2.26. *Seja $P = P_\infty$ o lugar infinito de $K(x)/K$. Então $\deg P_\infty = 1$ e um parâmetro local para P_∞ é $t = 1/x$. A valorização discreta correspondente v_∞ é dada por*

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

onde $f(x), g(x) \in K[x]$. A aplicação de classe residual correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$, para $z \in K(x)$, onde $z(\infty)$ é definida da seguinte maneira: escreva

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

Então,

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

Demonstração: Como $F = K(x)$, então F é corpo de funções racionais, e portanto, $[F_{P_\infty} : K] = 1$, ou seja $\deg P_\infty = 1$.

Para concluir a demonstração, resta verificar que $t = 1/x$ é um parâmetro local, uma vez que a valorização v_∞ está bem definida e é de fato uma valorização, e ainda, a aplicação de classe residual corresponde de fato a P_∞.

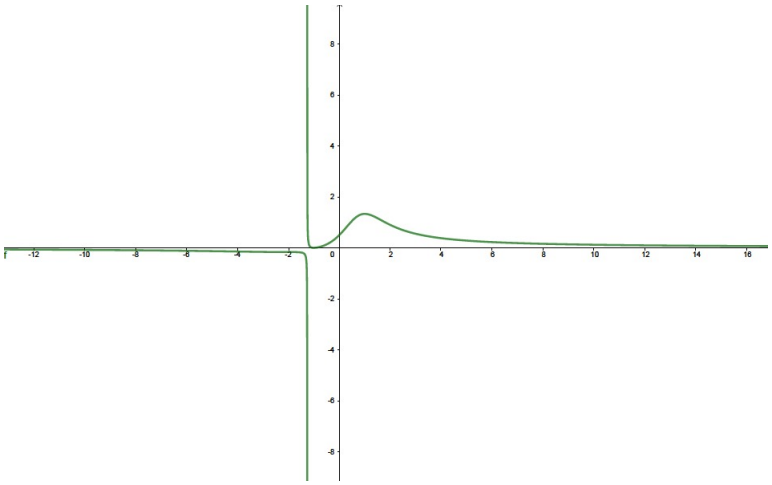
Note primeiramente que, pela definição de P_∞, temos $1/x \in P_\infty$. Agora, considere $z = \dfrac{f(x)}{g(x)} \in P_\infty$, ou seja $\deg(f(x)) < \deg(g(x))$.

Assim, obtemos $z = \dfrac{1}{x}.\dfrac{xf(x)}{g(x)}$. Agora, note que $\deg(xf(x)) \leq \deg(g(x))$, e assim, $\dfrac{xf(x)}{g(x)} \in \mathcal{O}_\infty$. Segue que $z \in \left(\dfrac{1}{x}\right)\mathcal{O}_\infty$.

Portanto $\dfrac{1}{x}$ é um gerador do lugar infinito, ou seja, $\dfrac{1}{x}$ é um parâmetro local para P_∞.

■

Com essa última proposição, podemos fazer uma relação com a teoria de cáclulo diferencial e integral, sobre cálculo de limite de funções racionais. Sejam $f(x) = x^2 + 2x + 1$ e $g(x) = x^3 + 2$, e considere $z = \dfrac{f(x)}{g(x)}$. Pela proposição 2.26, como $\deg(f(x)) = 2 < 3 = \deg(g(x))$, temos $z(\infty) = 0$, que coincide com $\lim\limits_{x\to\infty} \dfrac{f(x)}{g(x)}$. Veja a figura a seguir.



Os casos em que os graus são iguais ou o grau do numerador é maior que do numerador, seguem de maneira análoga.

Proposição 2.27. *Considere $K(x)/K$ o corpo das funções racionais. Então K é o corpo das constantes completo de $K(x)/K$, isto é, K é algebricamente fechado em F.*

Demonstração: Considere P um lugar de $K(x)|K$ de grau 1 (basta considerar $P = P_\alpha$, com $\alpha \in K$). Então, $K(x)_P = K$. Agora, o corpo das constantes $\widetilde{K}$ de $K(x)$ está contido em $K(x)_P$. De fato, como $\widetilde{K} \subseteq K(x)$, basta considerarmos a homomorfismo definido na proposição 2.24. Assim, temos $K \subseteq \widetilde{K} \subseteq K(x)_P = K$, ou seja $K = \widetilde{K}$, como queríamos mostrar.

■

Finalizamos essa seção com o teorema a seguir, que caracteriza todos os lugares no corpo de funções racionais $K(x)/K$, os definidos no início desta seção.

Teorema 2.28. *Não existem outros lugares do corpo de funções racionais $K(x)/K$ diferentes dos lugares $P_{p(x)}$ e P_∞ definidos no início desta seção.*

Demonstração: Seja P um lugar de $K(x)/K$. Temos duas possibilidades: $x \in \mathcal{O}_P$ ou $x \notin \mathcal{O}_P$. Vamos dividir a demonstração nesses dois casos.

Caso 1*:* Suponha que $x \in \mathcal{O}_P$. Logo, $K[x] \subseteq \mathcal{O}_P$. Definimos $I := K[x] \cap P$. Note que I é um ideal de $K[x]$, e mais ainda, é primo. Desse modo, a aplicação de classe residual induz uma injeção $K[x]/I \hookrightarrow K(x)_P$, o que garante que $I \neq \{0\}$. Disto, segue que existe um único polinômio mônico e irredutível $p(x) \in K[x]$ tal que $I = K[x] \cap P = p(x) \cdot K[x]$. Agora, dado $g(x) \in K[x]$, com $p(x) \nmid g(x)$, temos que $g(x) \notin I$, e como $g(x) \in K[x]$, devemos ter $g(x) \notin P$, o que implica que $1/g(x) \in \mathcal{O}_P$, pela proposição 2.6. Logo, temos

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

Pelo teorema 2.16, os anéis de valorização são subanéis próprios e maximais de $K(x)$, e portanto, $\mathcal{O}_P = \mathcal{O}_{p(x)}$, e segue que o lugar P coincide com o lugar $P_{p(x)}$.

Caso 2*:* Suponhamos agora que $x \notin \mathcal{O}_P$. Como $\mathcal{O}_P$ é um anel de valorização, segue que $x^{-1} \in \mathcal{O}_P$, e assim, $K[x^{-1}] \subseteq \mathcal{O}_P$. Ainda, como $x \notin \mathcal{O}_P$, temos $x^{-1} \in P$, ou seja, $x^{-1} \in P \cap K[x^{-1}]$ e $P \cap K\left[x^{-1}\right] = x^{-1}K\left[x^{-1}\right]$. Como fizemos no caso 1, temos

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f\left(x^{-1}\right)}{g\left(x^{-1}\right)} \mid f\left(x^{-1}\right), g\left(x^{-1}\right) \in K\left[x^{-1}\right], x^{-1} \nmid g\left(x^{-1}\right) \right\} \\
&= \left\{ \frac{a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}} \mid b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} \mid b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \mid u(x), v(x) \in K[x], \deg u(x) \leq \deg v(x) \right\} \\
&= \mathcal{O}_\infty.
\end{aligned}$$

Novamente, pela maximalidade do anel de valorização, temos $\mathcal{O}_P = \mathcal{O}_\infty$, e segue que $P = P_\infty$. Portanto, temos $P = P_{p(x)}$ ou $P = P_\infty$, como gostaríamos de demonstrar.

■

2.3 Independência de valorizações

Nesta seção enunciaremos alguns resultados que serão úteis na construção do espaço de Riemann-Roch, o qual veremos na seção seguinte. As demonstrações dos resultados enunciados aqui serão omitidas, mas podem ser encontradas em [1].

O principal resultado desta seção é o teorema da aproximação fraca, o qual essencialmente diz que, dadas $v_1, \ldots, v_n$ valorizações discretas distintas duas a duas de um corpo de funções F/K e $z \in F$, mesmo que saibamos os valores de $v_1(z), \ldots, v_{n-1}(z)$, não é possível concluir nada sobre $v_n(z)$.

Teorema 2.29. *(Aproximação fraca) Sejam F/K um corpo de funções, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K, $x_1, \ldots, x_n \in F$ e $r_1, \ldots, r_n \in \mathbb{Z}$. Então, existe $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \text{ com } i = 1, \ldots, n.$$

Como consequência imediata do teorema 2.29, temos o corolário a seguir, que nos garante a existência de uma infinidade de lugares de um corpo de funções.

Corolário 2.30. *Todo corpo de funções possui infinitos lugares.*

Na próxima seção, veremos que um elemento $x \in F$, transcendente sobre K, possui a mesma quantidade de zeros e polos. A proposição a seguir desempenha um papel importante na demonstração do resultado citado anteriormente.

Proposição 2.31. *Sejam F/K um corpo de funções e $P_1, \ldots, P_r$ zeros de um elemento $x \in F$. Então*

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

Para encerrar esta seção, temos um corolário importante, que garante a finitude do número de polos e zeros de um elemento $x \in F$.

Corolário 2.1. *Em um corpo de funções F/K, todo elemento $0 \neq x \in F$ tem uma quantidade finita de zeros e polos.*

2.4 Divisores

A partir desta seção, e ao longo deste capítulo, F/K denotará sempre um corpo de funções algébricas de uma variável tal que K é algebricamente fechado em F.

Nesta seção, definiremos um conceito importante em nossa teoria: os divisores, os quais aparecem na definição do espaço de Riemann-Roch. Além disso, definiremos o conceito de gênero de um corpo de funções, para que possamos demonstrar o teorema de Riemann-Roch mais adiante.

Definição 2.32. *O grupo divisor de F/K é definido como o grupo abeliano livre gerado pelos lugares de F/K, e denotado por* $\mathrm{Div}(F)$.

Os elementos de $\mathrm{Div}(F)$ são chamados de *divisores* de F/K. Em outra palavras, um divisor é uma soma formal do tipo

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ com } n_P \in \mathbb{Z}, \text{ e } n_P \neq 0 \text{ apenas para uma quantidade finita.}$$

O *suporte* de D é definido por $\operatorname{supp} D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}$. Algumas vezes, escreveremos $D = \sum_{P \in S} n_P P$, onde $S \subseteq \mathbb{P}_F$ é um conjunto finito tal que $\operatorname{supp} D \subseteq S$.

Definição 2.33. *Se um divisor D é tal que $D = P$, para $P \in \mathbb{P}_F$, chamamos D de divisor primo.*

Podemos definir uma adição entre dois divisores, e ainda, exibir um elemento neutro para essa operação.

Dados $D = \sum_{P \in \mathbb{P}_F} n_P P$ e $D' = \sum_{P \in \mathbb{P}_F} n'_P P$, definimos $D + D' := \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$. Além disso, definimos o divisor zero por $0 := \sum_{P \in \mathbb{P}_F} r_P P$ onde $r_P = 0$, para todo r_P. Claramente $D + 0 = 0 + D = D$, para todo $D \in \operatorname{Div}(F)$. Agora, dados $Q \in \mathbb{P}_F$ e $D = \sum_{P \in \mathbb{P}_F} n_P P \in \operatorname{Div}(F)$, definimos $v_Q(D) = n_Q$. Assim, podemos reescrever o suporte de D como

$$\operatorname{supp} D = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \quad \text{e} \quad D = \sum_{P \in \operatorname{supp} D} v_P(D) \cdot P.$$

Para nossa teoria, é interessante que tenhamos em $\operatorname{Div}(F)$ uma relação de ordem. Para isso, definimos a seguinte relação de maneira natural: dados $D_1, D_2 \in \operatorname{Div}(F)$ dizemos que $D_1 \leq D_2$ se, e somente se, $v_P(D_1) \leq v_P(D_2)$, para todo $P \in \mathbb{P}_F$. Claramente a relação "$\leq$" é de ordem parcial.

No caso em que tivermos $D_1 \leq D_2$ e $D_1 \neq D_2$, podemos escrever simplesmente $D_1 < D_2$, e se $D \geq 0$, dizemos que D é um *divisor positivo* ou *efetivo*.

Definição 2.34. *Dado $D \in \operatorname{Div}(F)$, definimos o grau de D por* $\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P$.

Da forma que definimos grau de um divisor, existe $\varphi : \operatorname{Div}(F) \longrightarrow \mathbb{Z}$ homomorfismo: basta associarmos cada divisor D ao seu grau. Agora, a cada ponto $x \in F$, podemos considerar um divisor associado a x, o qual denotaremos por $\langle x \rangle$. Isso nos motiva a seguinte definição:

Definição 2.35. *Sejam $0 \neq x \in F$, Z o conjunto de zeros de x em $\mathbb{P}_F$ e N o conjunto dos polos de x em $\mathbb{P}_F$. Definimos*

$$\langle x \rangle_0 := \sum_{P \in Z} v_P(x) P, \text{ como o zero divisor de } x,$$

$$\langle x \rangle_\infty := \sum_{P \in N} (-v_P(x))\, P, \text{ como o polo divisor de } x,$$

$$\langle x \rangle := \langle x \rangle_0 - \langle x \rangle_\infty \text{ como o divisor principal de } x.$$

Segue diretamente da definição anterior que $\langle x \rangle_0 \geq 0$ e $\langle x \rangle_\infty \geq 0$. Ainda, temos que $\langle x \rangle = \sum_{P \in \mathbb{P}_F} v_P(x) P$. Além disso, os elementos não nulos $x \in F$ que são constantes são caracterizados por $x \in K \Leftrightarrow \langle x \rangle = 0$. Esse fato segue diretamente do corolário 2.23, assumindo que K é algebricamente fechado sobre F.

Considere agora o conjunto $\operatorname{Princ}(F) := \{\langle x \rangle \mid 0 \neq x \in F\}$. Temos $\operatorname{Princ}(F)$ um subrupo de $\operatorname{Div}(F)$, uma vez que, para quaisquer $0 \neq x, y \in F$, temos

$$\langle xy\rangle = \sum v_P(xy)P = \sum \left(v_P(x) + v_P(y)\right) P = \sum v_P(x)P + \sum v_P(y)P = \langle x\rangle + \langle y\rangle.$$

Definição 2.36. *O conjunto* $\mathrm{Princ}(F) := \{\langle x\rangle \mid 0 \neq x \in F\}$ *é chamado de grupo dos divisores principais de* F/K.

O grupo quociente $\mathrm{Cl}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$ é chamado *grupo de classe divisora* de F/K. Dado $D \in \mathrm{Div}(F)$, o elemento correspondente a D em $\mathrm{Cl}(F)$ é denotado por $[D]$ ou $\overline{D}$, e chamado de *classe de* D.

Veremos agora a definição de divisores equivalentes, a qual será bastante utilizada no desenvolvimento desta teoria.

Definição 2.37. *Dados* $D, D' \in \mathrm{Div}(F)$, *dizemos que* D *e* D' *são equivalentes, e denotamos por* $D \sim D'$, *se* $\overline{D} = \overline{D'}$, *isto é, existe* $x \in F$ *não nulo tal que* $D = D' + \langle x\rangle$.

Claramente $\sim$ da definição anterior é uma relação de equivalência. A seguir, definimos o espaço de Riemann-Roch, que será nosso objeto central de estudo de agora em diante.

Definição 2.38. *Dado* $A \in \mathrm{Div}(F)$, *definimos o espaço de Riemann-Roch associado a* A *por*

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

Essa definição tem a seguinte interpretação: Se $A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, onde $n_i, m_j > 0$, então

$$\mathcal{L}(A) = \{x \in F \mid \langle x\rangle \geq -A\} \cup \{0\} = \left\{x \in F \mid \langle x\rangle \geq -\left(\sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j\right)\right\} \cup \{0\} =$$
$$\left\{x \in F \mid \langle x\rangle \geq \sum_{i=1}^{r}(-n_i)P_i + \sum_{j=1}^{s} m_j Q_j\right\} \cup \{0\}.$$

Logo, x tem zeros de ordem $\geq m_j$ em Q_j, com $j = 1, \ldots, s$ e tem polos somente nos lugares P_i, cujas ordens em P_i são limitadas por n_i, com $i = 1, \ldots r$.

A observação a seguir tem uma demonstração bastante simples, porém será bastante usada no decorrer da seção.

Observação 2.39. *Seja* $A \in \mathrm{Div}(F)$. *Então*
(a) $x \in \mathcal{L}(A) \iff v_P(x) \geq -v_P(A)$, *para todo* $P \in \mathbb{P}_F$.
(b) $\mathcal{L}(A) \neq \{0\} \iff$ *existe* $A' \in \mathrm{Div}(F)$ *tal que* $A' \sim A$ *e* $A' \geq 0$.

Demonstração: (a) Temos

$$x \in \mathcal{L}(A) \Leftrightarrow \langle x\rangle \geq -A \Leftrightarrow \sum_{P\in\mathbb{P}_F} v_P(x)P \geq -\sum_{P\in\mathbb{P}_F} v_P(A)P \Leftrightarrow$$
$$\Leftrightarrow \sum_{P\in\mathbb{P}_F} v_P(x)P \geq \sum_{P\in\mathbb{P}_F} (-v_P(A))P \Leftrightarrow\Leftrightarrow v_P(x) \geq -v_P(A),\ \forall\ P \in \mathbb{P}_F.$$

(b) $\mathcal{L}(A) \neq \{0\} \Leftrightarrow$ existe $x \in \mathcal{L}(A)$ com $x \neq 0 \Leftrightarrow \langle x\rangle \geq -A \Leftrightarrow \langle x\rangle + A \geq 0$. Assim, basta tomarmos $A' = \langle x\rangle + A$, e teremos $A \sim A'$ por definição, e $A' \geq 0$.

■

Quando consideramos o espaço de Riemann-Roch associado a um divisor A, podemos definir neste conjunto, uma adição e uma multiplicação por escalar, de maneira usual. O próximo resultado nos garante que o conjunto $\mathcal{L}(A)$ é um K-espaço vetorial. Além disso, obtemos uma condição suficiente para que dois espaços de Riemann-Roch sejam isomorfos.

Lema 2.40. *Seja $A \in \mathrm{Div}(F)$. Então:*
(a) $\mathcal{L}(A)$ é um espaço vetorial sobre K.
(b) Se $A \sim A'$, então $\mathcal{L}(A) \simeq \mathcal{L}(A')$, como espaços vetoriais.

Demonstração: (a) Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$. Pela observação 2.39(a), $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A)$ e $v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A)$. Assim, também pela observação 2.39(a), concluimos que $x+y$ e ax estão em $\mathcal{L}(A)$. Como as operações são fechadas em $\mathcal{L}(A)$, segue que o conjunto é um K-espaço vetorial, uma vez que as propriedades para ser espaço vetorial se restringem a operações entre divisores e valorizações.

(b) Seja $A' \in \mathrm{Div}(F)$ com $A' \sim A$. Logo, existe $z \in F$ não nulo tal que $A = \langle z \rangle + A'$. Afirmamos que $\mathcal{L}(A) \simeq \mathcal{L}(A')$. Considere a aplicação

$$\varphi : \begin{cases} \mathcal{L}(A) \longrightarrow F \\ \quad x \longmapsto xz \end{cases} .$$

Afirmamos que φ é linear. De fato, $\varphi(ax+y) = (ax+y)z = (ax)z + yz = a(xz) + yz = a\varphi(x) + \varphi(y)$, $\forall\ x, y \in \mathcal{L}(A)$ e $\forall\ a \in K$. Além disso, observe que

$$\begin{aligned} x \in \mathcal{L}(A) \Leftrightarrow \langle x \rangle + A \geq 0 \Leftrightarrow \langle x \rangle + \langle z \rangle + A' \geq 0 \Leftrightarrow \langle xz \rangle \geq -A' \Leftrightarrow xz \in \mathcal{L}(A') \\ \Leftrightarrow \varphi(x) \in \mathcal{L}(A') \Leftrightarrow \mathrm{Im}\,\varphi \subseteq \mathcal{L}(A'). \end{aligned}$$

Agora, definindo

$$\varphi' : \begin{cases} \mathcal{L}(A') \longrightarrow F \\ \quad x \longmapsto xz^{-1} \end{cases} ,$$

segue de maneira análoga que φ' é linear, e ainda

$$\begin{aligned} (\varphi \circ \varphi')(x) &= \varphi(xz^{-1}) = xz^{-1}z = x, \forall x \in \mathcal{L}(A') \quad \text{e} \\ (\varphi' \circ \varphi)(x) &= \varphi(xz) = xzz^{-1} = x, \forall x \in \mathcal{L}(A) \end{aligned}$$

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

■

Sabendo que o conjunto $\mathcal{L}(A)$ possui estrutura de espaço vetorial. Uma pergunta natural que surge é o valor da dimensão deste espaço, que é exatamente o problema de Riemann-Roch. Os próximos resultados que apresentaremos serão todos com o intuito de mostrar que o espaço $\mathcal{L}(A)$ tem dimensão finita, e ainda, que existe uma cota superior para sua dimensão, que é de fato atingida. A seguir, temos dois lemas que serão utilizados em demonstrações futuras.

Lema 2.41. *(a) $\mathcal{L}(0) = K$*
(b) Se $A < 0$, então $\mathcal{L}(A) = \{0\}$.

Demonstração: (a) Ja vimos que se $0 \neq x \in K$, então $\langle x \rangle = 0$, ou seja, $\langle x \rangle \geq 0$, e portanto $x \in \mathcal{L}(0)$. Reciprocamente, dado $0 \neq x \in \mathcal{L}(0)$, temos $\langle x \rangle \geq 0$. Assim, x não tem nenhum polo. Pelo corolário 2.23, devemos ter $x \in K$. Portanto, $K = \mathcal{L}(0)$.

(b) Seja $A < 0$ e assuma que exista $0 \neq x \in \mathcal{L}(A)$. Logo, $\langle x \rangle \geq -A > 0$, o que implica que x tem pelo menos um zero e nenhum polo, o que é absurdo pelo corolário 2.23. Portanto, $\mathcal{L}(A) = \{0\}$.

■

Lema 2.42. *Sejam $A, B \in \mathrm{Div}(F)$ e $A \leq B$. Então $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A$.*

Demonstração: Seja $x \in \mathcal{L}(A)$. Então, $\langle x \rangle \geq -A \geq -B \Rightarrow x \in \mathcal{L}(B)$. Mostremos que vale a outra afirmação. Como $B \geq A$, colocamos $B = A + P$, para algum $P \in \mathbb{P}_F$. O caso geral segue por indução. Escolhemos $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + 1$. Assim, para cada $x \in \mathcal{L}(B)$, temos $v_P(x) \geq -v_P(B)$, pela observação 2.39(a), ou seja, $v_P(x) \geq -v_P(t) \Rightarrow v_P(x) + v_P(t) \geq 0 \Rightarrow v_P(xt) \geq 0$. Pelo teorema 2.16, segue que $xt \in \mathcal{O}_P$. Assim, temos bem definida a aplicação

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

Claramente ψ é linear sobre K, pois trata-se de operações envolvendo lugares e valorizações. Vamos determinar o núcleo desta aplicação. Temos

$$\begin{gathered} \mathrm{Ker}(\psi) = \{x \in \mathcal{L}(B) \mid \psi(x) = 0\} = \{x \in \mathcal{L}(B) \mid xt + P = 0\} = \{x \in \mathcal{L}(B) \mid xt \in P\} = \\ = \{x \in \mathcal{L}(B) \mid v_P(xt) > 0\} = \{x \in \mathcal{L}(B) \mid v_P(x) > -v_P(t)\} = \\ = \{x \in \mathcal{L}(B) \mid v_P(x) > -v_P(A)\} = \{x \in \mathcal{L}(B) \mid x \in \mathcal{L}(A)\} = \mathcal{L}(A). \end{gathered}$$

Portanto, $\mathrm{Ker}(\psi) = \mathcal{L}(A)$. Assim, ψ induz um K-monomorfismo $\mathcal{L}(B)/\mathcal{L}(A) \longrightarrow F_P$. Disto, segue que

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim(F_P) = \deg P = \deg(B - A) = \deg B - \deg A.$$

■

Utilizando esses dois lemas, iremos agora demonstrar uma proposição que nos fornece uma primeira cota superior para a dimensão do espaço $\mathcal{L}(A)$.

Proposição 2.43. *Para cada $A \in \mathrm{Div}(F)$, o espaço vetorial $\mathcal{L}(A)$ tem dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos, então $\dim(\mathcal{L}(A)) \leq \deg A_+ + 1$.*

Demonstração: Vamos mostrar primeiramente que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Seja $x \in \mathcal{L}(A)$. Então $\langle x \rangle \geq -A = -(A_+ - A_-) = -A_+ + A_- \geq -A_+$, ou seja, $x \in \mathcal{L}(A_+)$. Logo, $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$.

Assim, é suficiente mostrar que $\dim(\mathcal{L}(A_+)) \leq \deg(A_+) + 1$. Como $A_+ \geq 0$ por hipótese, pelo lema 2.42, temos $\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq \deg A_+ - \deg 0 = \deg A_+$. Agora, pelo lema 2.41, temos $\mathcal{L}(0) = K$, ou seja, $\dim(\mathcal{L}(0)) = \dim K = 1$. Assim,

$$\begin{gathered} \dim(\mathcal{L}(A)) \leq \dim(\mathcal{L}(A_+)) = \dim(\mathcal{L}(A_+)) - \dim(\mathcal{L}(0)) + 1 = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1 \leq \\ \deg(A_+) + 1. \end{gathered}$$

■

Demonstrada esta proposição, faz sentido a próxima definição.

Definição 2.44. *Seja $A \in \mathrm{Div}(F)$. O inteiro $\ell(A) := \dim(\mathcal{L}(A))$ é chamado de dimensão do divisor A.*

Como falamos anteriormente, um dos mais importantes problemas da teoria de corpos de funções algébricas é calcular a dimensão de um divisor. A resposta para esse problema será dada na próxima seção, pelo teorema de Riemann-Roch.

Teorema 2.45. *Todos os divisores principais possuem grau zero. De fato, pata todo $x \in F/K$,*

$$\deg(\langle x\rangle_0) = \deg(\langle x\rangle_\infty) = [F : K(x)].$$

Demonstração: Sejam $n = [F : K(x)]$ e $B := \langle x\rangle_\infty = \sum_{i=1}^{r}(-v_{P_i}(x))P_i = \sum_{i=1}^{r}(v_{P_i}(x^{-1}))P_i$, onde $P_1, \ldots, P_r$ são todos os polos de x (segue da interpretação feita após a definição do conjunto $\mathcal{L}(A)$). Então, pela proposição 2.31,

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

Mostremos que $n \leq \deg B$. Como $[F : K(x)] = n$, escolha uma base $\{u_1, \ldots, u_n\}$ de $F/K(x)$ e um divisor $C \geq 0$ tal que $\langle u_j\rangle \geq -C$, para todo $j = 1, \ldots n$, ou seja, $u_j \in \mathcal{L}(C)$.

Agora, note que $x^i u_j \in \mathcal{L}(mB + C)$, para $0 \leq i \leq m$ e $1 \leq j \leq n$. De fato,

$$v_P(x^i u_j) = iv_P(x) + v_P(u_j) \geq -iv_P(B) - v_P(C) \geq -mv_P(B) - v_P(C) = -v_P(mB + C).$$

Agora, como esses elementos são todos linearmente independentes sobre $K(x)$, temos $\ell(mB + C) \geq n(m + 1)$, para todo $m \geq 0$. Colocamos $c := \deg C$. Pela proposição 2.43, temos

$$n(m + 1) \leq \ell(mB + C) \leq \deg(mB + C) + 1 = m \deg B + c + 1.$$

Portanto, $m(\deg B - n) \geq n - c - 1$, $\forall\ m \in \mathbb{N}$. Como o lado direito da desigualdade não depende de m, então a desiguldade só é satisfeita quando $\deg B - n \geq 0$, ou seja $\deg B \geq n$. Portanto, $\deg B = n$, e mostramos que $\deg(\langle x\rangle_\infty) = [F : K(x)]$. Agora, como $\langle x\rangle_0 = \langle x^{-1}\rangle_\infty$, segue que

$$\deg(\langle x\rangle_0) = \deg(\langle x^{-1}\rangle_\infty) = [F : K(x^{-1})] = [F : K(x)].$$

Em particular, todos os divisores principais possuem grau zero, já que $\deg(\langle x\rangle_0) = \deg(\langle x\rangle_\infty)$.

■

Como consequência desse teorema, temos o seguinte corolário.

Corolário 2.46. *(a) Sejam $A, A' \in \mathrm{Div}(F)$ tais que $A \sim A'$. Então $\ell(A) = \ell(A')$ e $\deg A = \deg A'$.*

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

(c) Se $\deg A = 0$, então são equivalentes:

(i) A é principal;

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

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

Demonstração: (a) Sejam A e A' divisores com $A \sim A'$. Pelo lema 2.40, $\mathcal{L}(A) \simeq \mathcal{L}(A')$, ou seja, $\ell(A) = \ell(A')$. O fato de $\deg A = \deg A'$ segue do teorema 2.45.

(b) Suponha que $\ell(A) > 0$, ou seja, $\mathcal{L}(A) \neq \{0\}$. Pela observação 2.39, existe $A' \in \mathrm{Div}(F)$ com $A \sim A'$ e $A' \geq 0$. Pelo item (a), temos $\deg A = \deg A' \geq 0$, o que contraria a hipótese de $\deg A < 0$. Portanto, segue que $\ell(A) = 0$.

(c) $(i) \Rightarrow (ii)$: Se $A = \langle x \rangle$ é principal, então $x^{-1} \in \mathcal{L}(A)$. Assim, $\dim(\mathcal{L}(A)) \geq 1$, ou seja $\ell(A) \geq 1$.

$(ii) \Rightarrow (iii)$: Como $\ell(A) \geq 1$, então $\mathcal{L}(A) \neq \{0\}$, e pela observação 2.39, existe $A' \geq 0$ tal que $A \sim A'$. Pelo item (a), $\deg A' = \deg A = 0$. Como $A' \geq 0$, então $A' = 0$. Pelo lema 2.41, segue que $\ell(A) = \ell(A') = \ell(0) = \dim(\mathcal{L}(0)) = \dim(K) = 1$.

$(iii) \Rightarrow (i)$: Suponha $\ell(A) = 1$ e $\deg A = 0$. Então, $\mathcal{L}(A) \neq \{0\}$, e assim, existe $0 \neq z \in \mathcal{L}(A)$. Assim, $\langle z \rangle + A \geq 0$. Logo, $\deg(A + \langle z \rangle) = 0$, ou seja $A + \langle z \rangle = 0 \Rightarrow A = -\langle z \rangle = \langle z^{-1} \rangle$. Portanto, A é principal.

■

O próximo resultado nos fornece uma cota inferior para $\ell(A)$, semelhante a desigualdade $\ell(A) \leq 1 + \deg(A)$, vista na proposição 2.43.

Proposição 2.47. *Existe $\gamma \in \mathbb{Z}$ tal que para todo $A \in \mathrm{Div}(F)$, é válida a desigualdade*

$$\deg(A) - \ell(A) \leq \gamma.$$

Demonstração: Observamos primeiramente que, para quaisquer divisores A_1 e A_2, temos

$$A_1 \leq A_2 \Rightarrow \dim(\mathcal{L}(A_2)|\mathcal{L}(A_1)) \leq \deg(A_2) - \deg(A_1) \Rightarrow \dim(\mathcal{L}(A_2)) - \dim(\mathcal{L}(A_1)) \leq \deg(A_2) - \deg(A_1) \Rightarrow \deg(A_1) - \ell(A_1) \leq \deg(A_2) - \ell(A_2).$$

Fixe agora $x \in F/K$ e considere $B = \langle x \rangle_\infty = \sum_{P \in N} (-v_P(x))P$, onde N é o conjunto dos polos de x em $\mathbb{P}_F$. Pelo que fizemos na demonstração do teorema 2.45, existe $C \geq 0$ tal que $\ell(mB + C) \geq (m+1) \cdot \deg(B)$, para todo $m \geq 0$. Ainda, pelo lema 2.42, $\ell(mB + C) \leq \ell(mB) + \deg(C)$. Combinando ambas as desigualdades, obtemos

$$(m+1)\deg(B) \leq \ell(mB) + \deg(C) \Rightarrow \ell(mB) \geq m\deg(B) + \deg(B) - \deg(C) = \deg(mB) + ([F : K(x)] - \deg(C)) \Rightarrow \deg(mB) - \ell(mB) \leq \gamma,$$

onde $\gamma = \deg(C) - [F : K(x)] \in \mathbb{Z}$.

Nosso objetivo agora é mostrar que a desigualdade acima é válida quando substituirmos mB por $A \in \mathrm{Div}(F)$ qualquer.

Afirmação 1: Dado um divisor A, existem divisores A_1 e D e um inteiro $m \geq 0$ tal que $A \leq A_1$, $A_1 \simeq D$ e $D \leq mB$.

De fato, escolha $A_1 \in \mathrm{Div}(F)$ com $A_1 \geq 0$ e $A_1 \geq A$. Pelo lema 2.42,

$$\ell(mB - A_1) \geq \ell(mB) - \deg A_1 \geq \deg(mB) - \gamma - \deg(A_1) > 0$$

para m suficientemente grande. Logo como $\ell(mB - A_1) > 0$, existe $0 \neq z \in \mathcal{L}(mB - A_1)$. Assim, definimos $D := A_1 - \langle z \rangle$, e então $A_1 \simeq D$. Ainda, como $z \in \mathcal{L}(mB - A_1)$, temos

$$A_1 - D = \langle z \rangle \geq -(mB - A_1) \Rightarrow A_1 - D \geq -mB + A_1 \Rightarrow D \leq mB.$$

Agora, usando a afirmação 1 que acabamos de mostrar, temos

$$\deg(A) - \ell(A) \leq \deg(A_1) - \ell(A_1) = \deg(D) - \ell(D) \leq \deg(mB) - \ell(mB) \leq \gamma.$$

■

Com o que fizemos acima, podemos definir o gênero de um corpo de funções. Pela proposição anterior, $\max\{\deg(A) - \ell(A) + 1 \mid A \in \mathrm{Div}(F)\}$ existe, pelo princípio da boa ordem. Assim, faz sentido a seguinte definição.

Definição 2.48. *O gênero g de F/K é definido por* $g := \max\{\deg(A) - \ell(A) + 1 \mid A \in \mathrm{Div}(F)\}$.

Observe que g existe pelo Princípio da Boa Ordem. Segue diretamente da definição que g é um inteiro não negativo, basta tomar $A = 0$, e teremos $\deg(0) - \ell(0) + 1 = -\deg(A) + 1 = -1 + 1 = 0$, ou seja, $g \geq 0$.

A seguir, iremos relacionar a dimensão de um divisor A diretamente com o gênero de um corpo de funções.

Teorema 2.49. *(de Riemann) Seja F/K um corpo de funcões de gênero g. Então*
(a) Para todo $A \in \mathrm{Div}(F)$, $\ell(A) \geq \deg(A) + 1 - g$.
(b) Existe um inteiro c, dependendo apenas do corpo F/K, tal que $\ell(A) = \deg(A) + 1 - g$, sempre que $\deg(A) \geq c$.

Demonstração: (a) Seja $A \in \mathrm{Div}(F)$. Então, da definição de gênero, segue que $g \geq \deg(A) - \ell(A) + 1 \Rightarrow \ell(A) \geq \deg(A) + 1 - g$, como queríamos.

(b) Seja $A_0 \in \mathrm{Div}(F)$ com $g = \deg(A_0) - \ell(A_0) + 1$ e defina $c = \deg(A_0) + g$. Se $\deg(A) \geq c$, então

$$\ell(A - A_0) \geq \deg(A - A_0) + 1 - g = \deg(A) - \deg(A_0) + 1 - g \geq c - \deg(A_0) - g + 1 = 1,$$

e portanto, existe $0 \neq z \in \mathcal{L}(A - A_0)$. Considere o divisor $A' = A + \langle z \rangle$. Então, $A' \geq A_0$, e assim, usando o fato que $A \simeq A'$, obtemos

$$\begin{gathered}\ell(A') - \ell(A_0) \leq \deg A' - \deg A_0 \Rightarrow \ell(A) - \ell(A_0) \leq \deg A - \deg A_0 \\ \Rightarrow \ell(A) - \deg A \leq \ell(A_0) - \deg A_0 = g - 1 \Rightarrow \ell(A) \leq \deg A + 1 - g.\end{gathered}$$

Do item (a), vale a igualdade $\ell(A) = \deg(A) + 1 - g$.

■

Exemplo 2.50. *Mostremos que o gênero g do corpo de funções racionais $K(x)/K$ é zero.*

Sejam $P_\infty = \left\{ \dfrac{f(x)}{g(x)} \mid f(x), g(x) \in K[x],\ \deg(f(x)) < \deg(g(x)) \right\}$ o polo divisor de x e $r \geq 0$ suficientemente grande. Considere o espaço de Riemann-Roch associado ao divisor rP_∞, $\mathcal{L}(rP_\infty)$. Os elementos $1, x, \ldots, x^r \in \mathcal{L}(rP_\infty)$, e como eles são linearmente independentes, segue que $r + 1 \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$. Assim, $g \leq 0$, e portanto, $g = 0$.

2.5 O teorema de Riemann-Roch

Nesta seção, F/K denotará um corpo de funções algébricas de gênero g. O principal resultado desta seção será explicitar uma maneira de calcular a dimensão de um divisor qualquer.

Definição 2.51. *Seja $A \in \mathrm{Div}(F)$. O inteiro $i(A) = \ell(A) - \deg(A) + g - 1$ é chamado índice de especialidade de A.*

O teorema 2.49 nos garante que $i(A) \geq 0$ e quando $\deg(A)$ é suficientemente grande, temos $i(A) = 0$. Introduziremos agora a noção de uma adele.

Definição 2.52. *Uma adele de F/K é uma aplicação*

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{P}_F & \longrightarrow & F \\ P & \longmapsto & \alpha_P \end{array} \right.$$

tal que $\alpha_P \notin \mathcal{O}_P$ apenas para um número finito de $P \in \mathbb{P}_F$.

Uma adele é 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 $\alpha = (\alpha_P)$. O conjunto

$$\mathcal{A}_F := \{\alpha \mid \alpha \text{ é uma adele de } F/K\}$$

é chamado de *espaço adele de F/K*. Claramente $\mathcal{A}_F$ é um espaço vetorial sobre K. A *adele principal* de $x \in F$ é a adele cujas componentes são todas iguais a x. Ainda, temos uma injeção $F \hookrightarrow \mathcal{A}_F$.

Com o intuito de utilizar todos os resultados já vistos para valorizações, podemos estender naturalmente os conceitos de valorizações para o espaço das adeles, colocando $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a componente P da adele α.

Definição 2.53. *Seja $A \in \mathrm{Div}(F)$. Definimos $\mathcal{A}_F(A)$ por*

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

Analogamente ao que demonstramos no lema 2.40, segue que o conjunto $\mathcal{A}_F(A)$ é um K-espaço vetorial de $\mathcal{A}_F$. O teorema a seguir relaciona o índice de especialidade de um divisor com as adeles relacionadas a ele.

Teorema 2.54. *Seja $A \in \mathrm{Div}(F)$. Então $i(A) = \dim\left(\mathcal{A}_F / \left(\mathcal{A}_F(A) + F\right)\right)$.*

Demonstração: Dividiremos a demonstração deste teorema em algumas afirmações.
Afirmação 1: Sejam $A_1, A_2 \in \mathrm{Div}(A)$ com $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e

$$\dim\left(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)\right) = \deg A_2 - \deg A_1.$$

Segue trivialmente da definição que $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$. Resta mostrar a igualdade da afirmação.

Como $A_2 \geq A_1$, colocamos $A_2 = A_1 + P$, com $P \in \mathbb{P}_F$. O caso geral segue por indução, analogamente ao lema 2.42. Agora, como v_P é sobrejetora, escolha $t \in F$ tal que $v_P(t) = v_P(A_2) = v_P(A_1) + 1$. Analogamente à demonstração do lema 2.42, consideramos a aplicação linear

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{A}_F(A_2) & \longrightarrow & F_P \\ \alpha & \longmapsto & t\alpha_P + P \end{array} \right. ,$$

a qual está bem definida. Vamos calcular o núcleo de φ. Temos

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

Além disso, φ é claramente sobrejetora. Pelo teorema do isomorfismo, temos

$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \dim(\operatorname{Im}\varphi) = \dim(F_p) = \deg(P) = \deg(A_2 - A_1) = \deg(A_2) - \deg(A_1),$$

o que conclui a afirmação 1.

Afirmação 2: Se $A_1, A_2 \in \operatorname{Div}(F)$ são tais que $A_1 \leq A_2$, então

$$\dim\left(\left(\mathcal{A}_F\left(A_2\right) + F\right) / \left(\mathcal{A}_F\left(A_1\right) + F\right)\right) = \left(\deg A_2 - \ell\left(A_2\right)\right) - \left(\deg A_1 - \ell\left(A_1\right)\right).$$

Inicialmente, consideramos a sequência exata

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

onde σ_1 e σ_2 são aplicações canônicas. Usando a exatidão da sequência e a afirmação 1, obtemos

$$\begin{aligned}\dim\left(\mathcal{A}_F\left(A_2\right) + F\right) / \left(\mathcal{A}_F\left(A_1\right) + F\right) &= \dim\left(\mathcal{A}_F\left(A_2\right)/\mathcal{A}_F\left(A_1\right)\right) - \dim\left(\mathcal{L}\left(A_2\right)/\mathcal{L}\left(A_1\right)\right) \\ &= \left(\deg A_2 - \deg A_1\right) - \left(\ell\left(A_2\right) - \ell\left(A_1\right)\right),\end{aligned}$$

e isso conclui a afirmação 2. Por fim, temos uma última afirmação que relacionará a dimensão de um divisor B específico com o espaço de adele associado a este divisor.

Afirmação 3: Se B é um divisor com $\ell(B) = \deg(B) + 1 - g$, então $\mathcal{A}_F = \mathcal{A}_F(B) + F$.

De fato, considere um divisor $B_1 \geq B$. Pelo lema 2.42,

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

Por outro lado, pelo teorema 2.49, temos $\ell(B_1) = \deg(B_1) + 1 - g$, para todo $B_1 \geq B$. Agora, seja $\alpha \in \mathcal{A}_F$ e escolha $B_1 \geq B$ tal que $\alpha \in \mathcal{A}_F(B_1)$. Pelo afirmação 2 e da construção acima, segue que

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

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

Com essas três afirmações, podemos provar o teorema. Seja A um divisor qualquer. Pelo teorema 2.49, existe $A_1 \geq A$ tal que $\ell(A_1) = \deg(A_1) + 1 - g$. Pela afirmação 3, $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$ e pela afirmação 2, obtemos

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

■

Como consequência imediata deste teorema, obtemos o seguinte corolário.

Corolário 2.55. $g = \dim(\mathcal{A}_F/\mathcal{A}_F(0) + F))$.

Demonstração: Pelo teorema 2.54, temos $\dim(\mathcal{A}_F/\mathcal{A}_F(0)+F)) = i(0) = \ell(0) - \deg(0) + g - 1 = g$.

■

Podemos reescrever o teorema 2.54 como

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

Com isso, vamos introduzir a definição de diferencial de Weil, a qual nos dará uma interpretação diferente do índice de especialidade de um divisor.

Definição 2.56. *Uma diferencial de Weil é uma aplicação linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula em $\mathcal{A}_F(A) + F$, para algum $A \in \mathrm{Div}(F)$.*

Chamamos o conjunto $\Omega_F := \{\omega \mid \omega \text{ é uma diferencial de Weil de } F/K\}$ de *módulo das diferenciais de Weil* de F/K. Agora, dado $A \in \mathrm{Div}(F)$, definimos o conjunto $\Omega_F(A)$ por

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

O conjunto Ω_F é um K-espaço vetorial com as operações definidas de forma usual, e como consequência disso, $\Omega_F(A)$ é um subespaço vetorial de Ω_F. O próximo resultado relaciona o índice de especialidade com o conjunto das diferenciais de Weil.

Lema 2.57. *Seja $A \in \mathrm{Div}(F)$. Então $\dim \Omega_F(A) = i(A)$.*

Demonstração: Considere a aplicação linear

$$\varphi : \begin{cases} \Omega_F(A) & \longrightarrow \quad \mathcal{A}_F/\mathcal{A}_F(A) + F \\ \omega & \longmapsto \quad \omega + (\mathcal{A}_F(A) + F) \end{cases}$$

Claramente φ é sobrejetora e é fácil verificar que $\ker \varphi = \{0\}$. Logo, φ é isomorfismo entre K-espaços vetoriais, e segue do teorema do isomorfismo e do teorema 2.54 que

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

■

Como consequência do lema 2.57, temos $\Omega_F \neq 0$, uma vez que dado $A \in \mathrm{Div}(F)$ com $\deg A \leq -2$, segue que

$$\dim(\Omega_F(A)) = i(A) = \ell(A) - \deg(A) + g - 1 = \ell(A) + g + 1 \geq 1,$$

ou seja, $\Omega_F \neq 0$.

Definição 2.58. *Sejam $x \in F$ e $\omega \in \Omega_F$. Definimos a aplicação $x\omega : \mathcal{A} \longrightarrow K$ por $(x\omega)(\alpha) = \omega(x\alpha)$.*

Segue diretamente da definição acima que $x\omega$ é uma diferencial de Weil, uma vez que, se ω se anula em $\mathcal{A}_F(A) + F$, então $x\omega$ se anula em $\mathcal{A}_F(A + \langle x \rangle) + F$.

Proposição 2.59. *Ω_F tem dimensão 1, como espaço vetorial sobre F.*

Demonstração: Já vimos que $\Omega_F \neq 0$, e portanto, existe $0 \neq \omega_1 \in \Omega_F$. A demonstração desta proposição constituirá de mostrar que dado qualquer $\omega_2 \in \Omega_F$, existirá $z \in F$ tal que $\omega_2 = z\omega_1$, ou seja, $\{\omega_1\}$ será linearmente independente e gerador de Ω_F, e portanto base.

Seja $\omega_2 \in \Omega_F$ arbitrário e não nulo. Consider $A_1, A_2 \in \mathrm{Div}(F)$ tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$.

Para um divisor específico B, o qual será explicitado posteriormente, considere as aplicações

$$\varphi_i : \begin{cases} \mathcal{L}(A_i + B) & \longrightarrow & \Omega_F(-B), \\ x & \longmapsto & x\omega_i. \end{cases} \qquad (i = 1, 2)$$

Claramente φ_i está bem definida, é K-linear e injetiva, para $i = 1, 2$.

Afirmação: existe $B \in \mathrm{Div}(F)$ tal que

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

Usaremos o fato de que, se V é um espaco vetorial e U_1 e U_2 são subespaços de V, então

$$\dim(U_1 \cap U_2) \geq \dim(U_1) + \dim(U_2) - \dim(V).$$

Seja $B \in \mathrm{Div}(F)$ com $\deg(B)$ grande o suficiente para que $\ell(A_i + B) = \deg(A_i + B) + 1 - g$, $i = 1, 2$ (vide teorema 2.49).

Defina $U_i = \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Pelo lema 2.57,

$$\dim(\Omega_F(-B)) = i(-B) = \ell(-B) - \deg(-B) + g - 1 = \deg(B) + g - 1,$$

e assim,

$$\begin{aligned} \dim(U_1) + \dim(U_2) - \Omega_F(-B) &= \deg(A_1 + B) + 1 - g + \deg(A_2 + B) + 1 - g - (\deg(B) + g - 1) \\ &= \deg(A_1) + \deg(B) + 1 - g + \deg(A_2) + \deg(B) + 1 - g - \deg(B) + 1 - g \\ &= \deg(B) + (\deg(A_1) + \deg(A_2) + 3(1 - g)) > 0. \end{aligned}$$

Observe que a parcela entre parênteses não depende de B. Assim, $\dim(U_1) + \dim(U_2) - \Omega_F(-B) > 0$. Da afirmação feita acima, concluimos que

$$\dim(U_1 \cap U_2) \geq \dim(U_1) + \dim(U_2) - \Omega_F(-B) \geq 1,$$

ou seja $U_1 \cap U_2 \neq \{0\}$. Portanto,

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

Agora, usando esta afirmação, consideramos $x_1 \in \mathcal{L}(A_1 + B)$ e $x_2 \in \mathcal{L}(A_2 + B)$ com $\varphi_1(x_1) = \varphi_2(x_2)$.

Assim, $x_1\omega_1 = x_2\omega_2 \neq 0$, ou seja, $\omega_2 = (x_1 x_2^{-1})\omega_1$. Portanto, $\{\omega_1\}$ é base de Ω_F, e segue que $\dim(\Omega_F) = 1$.

■

Queremos agora relacionar cada divisor A com uma diferencial de Weil $\omega \neq 0$. Assim, dado $\omega \in \Omega_F$, consideramos o conjunto

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

Lema 2.60. *Seja $\omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$, para todo $A \in M(\omega)$.*

Demonstração: Pelo teorema 2.49, existe $c \in \mathbb{Z}$ dependendo somente de F/K tal que

$$i(A) = \ell(A) - \deg(A) + g - 1 = 0,$$

para todo $A \in \mathrm{Div}(F)$ com $\deg(A) \geq c$. Por outro lado, pelo teorema 2.54,

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

Assim, $\dim(\mathcal{A}_F(A)/(\mathcal{A}_F(A) + F)) = 0$, para todo $A \in \mathrm{Div}(F)$ com $\deg(A) \geq c$, ou seja, $\deg(A) < c$, para todo $A \in M(\omega)$. Desse modo, podemos escolher $W \in M(\omega)$ de grau máximo, já que temos uma limitação superior para o grau dos divisores de $M(\omega)$.

Suponhamos que W não possui a propriedade do lema. Assim, existe $A_0 \in W(\omega)$ com $A_0 \not\leq W$, ou seja, existe $Q \in \mathbb{P}_F$ tal que $v_Q(A_0) > v_Q(W)$.

Afirmamos que $W+Q \in M(\omega)$. De fato, considere uma adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W+Q)$. Escrevemos $\alpha = \alpha' + \alpha''$, onde

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

Então, $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in {}_{\mathcal{F}}(\mathcal{A}_{\prime})$ e segue que

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

Assim, ω se anula em $\mathcal{A}_F(W+Q) + F$, e portanto $W + Q \in M(\omega)$, o que é absurdo pela maximalidade da escolha de W. A unicidade de W é facilmente verificável do que fizemos agora.

■

Agora, com esse resultado, faz sentido a seguinte definição

Definição 2.61. *(a) O divisor $\langle\omega\rangle$ da diferencial de Weil $\omega \neq 0$ é o divisor unicamente determinado de F/K satisfazendo*

1. *ω se anula em $\mathcal{A}_F(\langle\omega\rangle) + F$,*

2. *se ω se anula em $\mathcal{A}_F(A) + F$, então $A \leq \langle\omega\rangle$.*

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

(c) Um lugar P é dito um zero (respectivamente polo) de ω se $v_P(\omega) > 0$ (respectivamente $v_P(\omega) > \omega$). A diferencial de Weil ω é chamada regular em P se $v_P(\omega) > 0$, e ω é dita simplesmente regular se é regular em todos os lugares $P \in \mathbb{P}_F$.

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

Observação 2.62. *Valem $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } \langle\omega\rangle \geq A\}$ e $\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ é regular }\}$.*

Proposição 2.63. *(a) Se $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$, então $\langle x\omega\rangle = \langle x\rangle + \langle\omega\rangle$*

(b) Quaisquer dois divisores canônicos são equivalentes.

Demonstração: (a) Se ω se anula em $\mathcal{A}_F(A)+F$, então $x\omega$ se anula em $\mathcal{A}_F(A\langle x\rangle)+F$, e segue que $\langle\omega\rangle+\langle x\rangle\leq\langle x\omega\rangle$.

Por esse memso argumento, segue que $\langle x\omega\rangle+\langle x^{-1}\rangle\leq\langle x^{-1}x\omega\rangle=\langle\omega\rangle$. Logo,

$$\langle x\rangle+\langle\omega\rangle\leq\langle x\omega\rangle\leq-\langle x^{-1}\rangle+\langle\omega\rangle=\langle x\rangle+\langle\omega\rangle,$$

e segue a igualdade desejada.

(b) Sejam $W_1=\langle\omega_1\rangle$ e $W_2=\langle\omega_2\rangle$ divisores canônicos, com $\omega_1,\omega_2\in\Omega_F$. Como $\dim_F(\Omega_F)=1$, existe $x\in F$ tal que $\omega_1=x\omega_2$. Portanto,

$$\langle\omega_1\rangle=\langle x\omega_2\rangle=\langle\omega_2\rangle+\langle x\rangle\Rightarrow W_1=\langle x\rangle+W_2\Rightarrow W_1\sim W_2.$$

■

Com essa proposição, podemos provar o teorema da Dualidade, que acarretará imediatamente no teorema de Riemann-Roch.

Teorema 2.64. *(da Dualidade) Sejam $A\in\mathrm{Div}(F)$ e $W=\langle\omega\rangle$ um divisor canônico de F/K. Então a aplicação*

$$\mu:\left\{\begin{array}{ccc}\mathcal{L}(W-A) & \longrightarrow & \Omega_F(A)\\ x & \longmapsto & x\omega\end{array}\right.$$

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

Demonstração: Note que, dado $x\in\mathcal{A}$, temos $\langle x\rangle\geq-(W-A)$. Agora,

$$\langle x\omega\rangle=\langle x\rangle+\langle\omega\rangle\geq-(W-A)+W=A\Rightarrow\langle x\omega\rangle\geq A.$$

Logo, $x\omega\in\Omega_F$, pela observação 2.62. Assim μ está bem definida. Temos ainda que:

(1) Se $x,y\in\mathcal{L}(W-A)$ e $\alpha\in K$, então $\mu(\alpha x+y)=(\alpha x+y)\omega=\alpha(x\omega)+y\omega=\alpha\mu(x)+\mu(y)$. Logo, μ é linear.

(2) μ é injetora. De fato,

$$\begin{aligned}\ker(\mu)=\{x\in\mathcal{L}(W-A)\mid\mu(x)=0\}=\{x\in\mathcal{L}(W-A)\mid\omega x=0\}=\\ =\{x\in\mathcal{L}(W-A)\mid x=0\}=\{0\}.\end{aligned}$$

(3) μ é sobrejetora. De fato, seja $\omega_1\in\Omega_F(A)$. Como $\Omega_F(A)$ tem dimensão 1 sobre F, então existe $x\in F$ tal que $\omega_1=x\omega$. Agora,

$$\langle x\rangle+W=\langle x\rangle+\langle\omega\rangle=\langle x\omega\rangle=\langle\omega_1\rangle\geq A\Rightarrow\langle x\rangle\geq-(W-A).$$

Logo, $x\in\mathcal{L}(W-A)$ e $\mu(x)=\omega x=\omega_1$.

Portanto, μ é isomorfismo, e segue que $\dim(\Omega_F(A))=\dim(\mathcal{L}(W-A))=\ell(W-A)$. Pelo lema 2.57, segue que $\ell(W-A)=i(A)$.

■

Teorema 2.65. *(de Riemann-Roch) Seja W um divisor canônico de F/K. Então, para cada divisor $A\in\mathrm{Div}(F)$,*

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

Demonstração: Segue imediatamente da definição de $i(A)$ e do teorema 2.64.

■

O teorema de Riemann-Roch nos dá uma forma de calcular a dimensão de um divisor de um corpo de funções F/K. Porém, nem sempre é fácil calcular a dimensão de $W - A$ onde W é um divisor canônico. Para isso, veremos no próximo resultado um caso particular em que a dimensão de um divisor pode ser facilmente calculada, sob certas hipóteses iniciais.

Teorema 2.66. *Considere A um divisor de F/K tal que* $\deg(A) \geq 2g - 1$. *Então*

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

Demonstração: Seja W um divisor canônico qualquer. Afirmamos que $\deg(W) = 2g-2$ e $\ell(W) = g$.

De fato, pelo teorema de Riemann-Roch, se considerarmos $A = 0$, obtemos

$$\ell(0) = \deg(0) + 1 - g + \ell(W) \Rightarrow 1 = 1 - g + \ell(W) \Rightarrow \ell(W) = g.$$

Por outro lado, se considerarmos $A = W$, obtemos

$$\ell(W) = \deg(W) + 1 - g + \ell(0) \Rightarrow g = \deg(W) + 1 - g + 1 \Rightarrow \deg(W) = 2g - 2.$$

Agora usando o fato de que $\deg(W) = 2g - 2$ e que por hipótese $\deg(A) \geq 2g - 1$, obtemos

$$\deg(W - A) = \deg(W) - \deg(A) \leq 2g - 2 - (2g - 1) = -1 \Rightarrow \ell(W - A) < 0,$$

e pelo corolário 2.46, temos $\ell(W - A) = 0$. Portanto $\ell(A) = \deg(A) + 1 - g$.

■

Observe que a cota $2g-1$ no teorema anterior é a melhor possível, pois se considerarmos W um divisor canônico, teremos

$$\deg(W) + 1 - g = 2g - 2 + 1 - g = g - 1 < g = \ell(W).$$

2.6 Consequências do teorema de Riemann-Roch

Nesta seção, apresentaremos alguns resultados importantes que decorrem do teorema de Riemann-Roch. Na seção anterior, encerramos com um resultado que nos dava exatamente a dimensão de um divisor cujo grau fosse $\geq 2g - 1$. Além disso, já sabemos o que acontece quando o grau é um número negativo. Nos resta analisar o que acontece com $\ell(A)$ quando $0 \leq \deg(A) \leq 2g - 2$. O teorema de Clifford nos dará uma cota superior para esta dimensão, que é de fato atingida.

Por agora, veremos alguns resultado envolvendo divisores canônicos, os quais serão utilizados na demonstração do teorema das lacunas de Weierstrass e de Clifford.

As primeiras duas proposições mostram que o divisor canônico é caracterizado pelo seu grau e sua dimensão.

Proposição 2.67. *Sejam $g_0 \in \mathbb{Z}$ e $W_0 \in \mathrm{Div}(F)$ satisfazendo $\ell(A) = \deg(A) + 1 - g_0 + \ell(W_0 - A)$, para todo $A \in \mathrm{Div}(F)$. Então $g = g_0$ e W_0 é um divisor canônico.*

Demonstração: Colocando $A = 0$, obtemos $\ell(W_0) = g_0$. Analogamente, se $A = W_0$, temos $\deg(W_0) = 2g_0 - 2$.

Seja W um divisor canônico de F/K. Escolha um divisor A com $\deg(A) > \max\{2g - 2, 2g_0 - 2\}$. Então

$$\ell(A) = \deg(A) + 1 - g, \text{ pelo teorema 2.66, e}$$
$$\ell(A) = \deg(A) + 1 - g_0, \text{ pela construção acima.}$$

Portanto, $g = g_0$. Agora, mostremos que $W \sim W_0$. Substituindo $A = W$ na equação da hipótese e usando que $g = g_0$, obtemos

$$\ell(W) = \deg(W)+1-g+\ell(W_0-W) \Rightarrow g = (2g-2)+1-g+\ell(W_0-W) \Rightarrow \ell(W_0-W) = 1.$$

Agora,

$$\ell(W_0 - w) = \deg(W_0 - W) + 1 - g + \ell(W_0 - (W_0 - W)) \Rightarrow$$
$$\Rightarrow 1 = \deg(W_0 - W) + 1 - g + g \Rightarrow \deg(W_0 - W) = 0.$$

Assim, pelo corolário 2.46, $W_0 - W$ é principal, e portanto $W_0 \sim W$, o garante que W_0 é divisor canônico.

■

Proposição 2.68. *Um divisor B é canônico se, e somente se,* $\deg(B) = 2g - 2$ *e* $\ell(B) \geq g$.

Demonstração: Se B é um divisor canônico, o resultado segue imediatamente. Reciprocamente, suponha que $\deg(B) = 2g - 2$ e $\ell(B) \geq g$ e seja W um divisor canônico. Mostremos que $B \sim W$. Pelo teorema de Riemann-Roch,

$$g \leq \ell(B) = \deg(B) + 1 - g + \ell(W - B) = 2g - 2 + 1 - g + \ell(W - B) =$$
$$g - 1 + \ell(W - B) \Rightarrow \ell(W - B) \geq 1.$$

Analogamente à proposição anterior, temos $\deg(W - B) = 0$. Pelo corolário 2.46, $W - B$ é principal, e portanto $W \sim B$, garantindo que B é canônico.

■

Proposição 2.69. *Seja F/K um corpo de funções algébricas. Então são equivalentes:*
(a) F/K é racional
(b) F/K tem gênero zero, e existe $A \in \mathrm{Div}(F)$ com $\deg(A) = 1$.

Demonstração: A implicação $(a) \Rightarrow (b)$ segue de maneira análoga ao exemplo 2.50.

Para a outra implicação, suponha $g = 0$ e $\deg(A) = 1$. Pelo teorema 2.66, como $\deg(A) = 1 \geq 2g - 1$, então $\ell(A) = \deg(A) + 1 - g = 2$. Assim $A \neq \{0\}$. Pela observação 2.39, existe $A' \geq 0$ com $A \sim A'$. Logo, $\ell(A') = 2$. Como $\ell(A') = 2 > 1$, então existe $x \in \mathcal{L}(A')\backslash K$.

Assim, $\langle x \rangle \neq 0$ e $\langle x \rangle + A' \geq 0$. Como $A' \geq 0$ e $\deg(A') = \deg(A) = 1$, isto só é possível se $A' = \langle x \rangle_\infty$.

Por fim, pelo teorema 2.45

$$[F : K(x)] = \deg(\langle x \rangle_\infty) = \deg(A') = 1 \Rightarrow F = K(x),$$

e segue que F/K é racional.

■

Veremos agora uma versão mais forte do teorema da aproximação fraca, visto nas seções passadas.

Teorema 2.70. *(da Aproximação Forte) Sejam $S \subsetneq \mathbb{P}_F$ e $P_1, \ldots, P_r \in S$. Suponha que sejam dados elementos $x_1, \ldots, x_r \in F$ e $n_1, \ldots n_r \in \mathbb{Z}$. Então, existe um elemento $x \in F$ tal que*

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

Demonstração: Considere a adele $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ onde

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

Escolhemos $Q \in \mathbb{P}_F \backslash S$. Para $m \in \mathbb{N}$ suficientemente grande, temos

$$\mathcal{A}_F = \mathcal{A}_F \left(mQ - \sum_{i=1}^{r} (n_i + 1) P_i \right) + F,$$

pelos teoremas 2.54 e 2.66, levando em conta a definição de índice de especialidade. Logo, existe $z \in F$ com $z - \alpha \in \mathcal{A}_F \left(mQ - \sum_{i=1}^{r} (n_i + 1) P_i \right)$. Isto significa que

$$v_{P_i}(z - x_i) > n_i, \text{ com } i = 1, \ldots, r \quad \text{e} \quad v_P(z) \geq 0, \text{ para todo } P \in S - \{P_1, \ldots, P_r\}.$$

Agora, escolha $y_1, \ldots y_r \in F$ com $v_{P_i}(y_i) = n_i$. Como foi feito na escolha de $z \in F$, podemos escolher $y \in F$ tal que

$$v_{P_i}(y - y_i) > n_i, \text{ com } i = 1, \ldots, r \quad \text{e} \quad v_P(y) \geq 0, \text{ para todo } P \in S - \{P_1, \ldots, P_r\}.$$

Assim, pela desigualdade triangular estrita,

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

Por fim, consideramos $x := y + z$, e obtemos

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = n_i.$$

O fato de que $v_P(x) \geq 0$, para todo $P \in S - \{P_1, \ldots, P_r\}$ segue do fato que $v_P(y), v_P(z) \geq 0$ nesse mesmo conjunto.

■

A próxima proposição será a motivação da definição de número polo e lacuna.

Proposição 2.71. *Seja $P \in \mathbb{P}_F$. Então, para cada $n \geq 2g$, existe $x \in F$ tal que $\langle x \rangle_\infty = nP$.*

Demonstração: Como $n \geq 2g$, então $n - 1 \geq 2g - 1$, e do teorema 2.66 segue que

$$\ell((n-1)P) = (n-1)\deg(P) + 1 - g \quad \text{e} \quad \ell(nP) = n\deg(P) + 1 - g.$$

Assim, $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Desse modo, todo elemento $x \in \mathcal{L}(nP) \backslash \mathcal{L}((n-1)P)$ tem um polo divisor nP.

■

Definição 2.72. *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado de número polo de P se existe $x \in F$ com $\langle x \rangle_\infty = nP$. Caso contrário, n é chamado de lacuna de P.*

O teorema a seguir, conhecido como teorema das lacunas de Weierstrass é um importante resultado que nos permite saber exatamente a quantidade de lacunas de um lugar P. Além disso, ele no garante que o inteiro 1 é uma lacuna e todas as outras lacunas são limitadas por um inteiro positivo dependendo do gênero.

Teorema 2.73. *(das lacunas de Weierstrass) Suponha que F/K tem gênero $g > 0$ e P é um lugar de grau 1. Então, existem exatamente g lacunas $i_1 < \cdots < i_g$ de P. Ainda,*

$$i_1 = 1 \quad e \quad i_g \leq 2g - 1.$$

Demonstração: Pela proposição 2.71, cada lacuna de P é $\leq 2g-1$, pois caso contrário, teríamos um número polo de P.

Ainda, da definição de número polo, segue que n é um número polo de P se, e somente se, $\ell(nP) > \ell((n-1)P)$, ou seja,

$$i \text{ é uma lacuna de } P \Leftrightarrow \ell(iP) = \ell((i-1)P).$$

Agora, consideramos a sequência de espaços vetoriais dada por

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

Pelo teorema 2.66, $\dim(\mathcal{L}(0)) = 1$ e $\dim(\mathcal{L}((2g-1)P)) = g$. Além disso, é fácil verificar que $\dim \mathcal{L}(iP) \leq \dim \mathcal{L}((i-1)P) + 1$.

Com isso, na sequência de espaços vetoriais construída, temos exatamente $g-1$ números $1 \leq i \leq 2g-1$ com $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Os outros g números restantes são lacunas de P. Obviamente todas as lacunas são $\leq 2g-1$. Resta mostrar que 1 é lacuna.

Suponhamos que 1 não é lacuna. Logo 1 seria um número polo de P. Como os números polos formam um semigrupo aditivo, então todo $n \in \mathbb{N}$ seria um número polo, o que contradiz o fato de termos $g > 0$ lacunas de P. Portanto, 1 é lacuna de P.

■

Definição 2.74. *Um divisor A é chamado não-especial se $i(A) = 0$. Caso contrário, A é chamado especial.*

Temos algumas consequências imediatas da definição acima e dos resultados até o momento vistos.

(a) A é não especial $\Leftrightarrow \ell(A) = \deg(A) + 1 - g$.

Esse fato segue diretamente da definição de índice de especialidade.

(b) Se $\deg(A) \geq 2g-2$, então A é não especial.

Segue diretamente do teorema 2.66.

(c) A propriedade de um divisor A ser especial ou não-especial depende unicamente da classe $\overline{A}$ de A no grupo de classe divisora.

Segue do fato que $\ell(A)$ e $\deg(A)$ dependem somente da classe de A.

(d) Todo divisor canônico é especial.

De fato, sendo W um divisor canônico, do teorema 2.64 segue que $i(W) = \ell(W-W) = \ell(0) = 1 \neq 0$. Portanto W é especial.

(e) Se A é um divisor tal que $\ell(A) > 0$ e $\deg(A) < g$, então A é especial.

De fato, se $\ell(A) > 0$, então $\ell(A) \geq 1$. Assim $1 \leq \ell(A) = \deg(A) + 1 - g + i(A)$. Logo, $i(A) \geq g - \deg(A) > 0$, e portanto, A é especial.

(f) Se A é não especial e $B \geq A$, então B é não-especial

De fato, como A é não-especial, então $i(A) = 0$. Pelo teorema 2.54, temos $\dim(\mathcal{A}_F/\mathcal{A}_F(A)+F) = 0$, ou seja, $\mathcal{A}_F = \mathcal{A}_F(A) + F$.

Como $B \geq A$, então $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$, e segue que B é não especial.

Proposição 2.75. *Suponha que $T \subseteq \mathbb{P}_F$ é um conjunto de lugares de grau 1 tal que $|T| \geq g$. Então, existe um divisor não-especial $B \geq 0$ tal que $\deg(B) = g$ e $\operatorname{supp}(B) \subseteq T$.*

Demonstração: Provaremos a seguinte afirmação: dados $P_1, \ldots, P_g \in T$ distintos e um divisor $A \geq 0$ com $\ell(A) = 1$ e $\deg(A) \leq g - 1$, existe $j \in \{1, \ldots, g\}$ tal que $\ell(A + P_j) = 1$.

Suponha que a afirmação seja falsa, ou seja, que para quaisquer $j = 1, \ldots, g$, temos $\ell(A + P_j) > 1$. Assim, como $\ell(A) = 1$, segue que existe $z_j \in \mathcal{L}(A + P_j)\backslash\mathcal{L}(A)$. Agora, como

$$v_{P_j}(z_j) = -v_{P_j}(A) - 1 \quad \text{e} \quad v_{P_i}(z_j) \geq -v_{P_i}(A) \quad \text{se } i \neq j,$$

pela desigualdade triangular estrita, os $g + 1$ elementos $1, z_1, \ldots, z_g$ são linearmente independentes sobre K. Escolha um divisor D com $D \geq A + P_1 + \cdots + P_g$ e $\deg(D) = 2g - 1$. Então, $1, z_1, \ldots, z_g \in \mathcal{L}(D)$. Da independência linear desses elementos, segue que $\ell(D) \geq g + 1$. Pelo teorema de Riemann-Roch, $\ell(D) = \deg(D) + 1 - g = 2g - 1 + 1 - g = g$. Portanto, chegamos em uma contradição, e a afirmação deve ser verdadeira. Agora, pela afirmação acima, podemos encontrar divisores

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

com $i_v \in \{1, \ldots, g\}$, não necessariamente distintos tais que $\ell(P_{i_1} + \cdots + P_{i_j}) = 1$, com $j = 1, \ldots, g$.

Defina $B := \sum_{j=1}^{g} P_{i_j}$. Então $\ell(B) = 1$. Claramente $B \geq 0$ e $\deg(B) = g$ pela afirmação provada. Resta mostrar que B é não-especial. Basta notar que

$$\ell(B) = 1 = 1 + g - g = \deg(B) + 1 - g \Rightarrow \ell(B) - \deg(B) + g - 1 = 0 \Rightarrow i(B) = 0.$$

■

Lema 2.76. *Sejam $A, B \in \operatorname{Div}(F)$ com $\ell(A), \ell(B) > 0$. Então $\ell(A) + \ell(B) \leq 1 + \ell(A + B)$.*

Demonstração: Por hipótese, existem $A_0, B_0 \geq 0$ tais que $A \sim A_0$ e $B \sim B_0$. Considere o conjunto

$$X := \{D \in \operatorname{Div}(F) \mid D \leq A_0 \text{ e } \mathcal{L}(A) = \mathcal{L}(A_0)\}.$$

Note que $X \neq \emptyset$, pois $A_0 \in X$. Como $D \geq 0$, para todo $D \in X$, pelo princípio da boa ordem, existe $D_0 \in X$ de grau mínimo, e segue que

$$\ell(D_0 - P) < \ell(D_0), \quad \forall P \in \mathbb{P}_F.$$

Queremos mostrar que $\ell(D_0) + \ell(B_0) \geq 1\ell(B_0 + D_0)$. Aqui assumimos que K é um corpo infinito.

Considere $\text{supp}(B_0) = \{P_1, \ldots, P_r\}$. Desse modo, $\mathcal{L}(D_0 - P_i) \subsetneq \mathcal{L}(D_0)$, para $i = 1, \ldots, r$. Agora, utilizando o fato de que todo espaço vetorial sobre um corpo infinito não é união finita de subespaços próprios, podemos considerar

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

Considere a aplicação

$$\varphi : \begin{cases} \mathcal{L}(B_0) \longrightarrow \mathcal{L}(D_0 + B_0)/\mathcal{L}(A_0) \\ x \longmapsto xz \bmod \mathcal{L}(A_0) \end{cases}.$$

φ é K-linear, pois dados $x, y \in \mathcal{L}(B_0)$ e $\alpha \in K$, segue que

$$\varphi(\alpha x + y) = (\alpha x + y)z \bmod \mathcal{L}(A_0) = \alpha(xz \bmod \mathcal{L}(A_0)) + (yz \bmod \mathcal{L}(A_0)) = \alpha\varphi(x) + \varphi(y).$$

Além disso, $\ker(\varphi) = K$. Pelo teorema do isomorfismo

$$\begin{gathered} \mathcal{L}(B_0)/\ker(\varphi) \simeq \text{Im}(\varphi) \leq \mathcal{L}(D_0 + B_0)/\mathcal{L}(A_0) \Rightarrow \dim(\mathcal{L}(B_0)) - \dim(K) \leq \\ \leq \dim(\mathcal{L}(D_0 + B_0)) - \dim(\mathcal{L}(A_0)) \Rightarrow \dim(\mathcal{L}(B_0)) + \dim(\mathcal{L}(A_0)) \leq \\ \leq \dim(\mathcal{L}(D_0 + B_0)) + 1 \Rightarrow \ell(B_0) + \ell(D_0) \leq \ell(B_0 + D_0) + 1. \end{gathered}$$

Usando este fato,

$$\begin{gathered} \ell(A) + \ell(B) = \ell(A_0) + \ell(B_0) = \ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0) \leq 1 + \ell(A_0 + B_0) = \\ = 1 + \ell(A + B). \end{gathered}$$

■

Encerramos essa seção com o teorema de Clifford, que nos dará uma cota superior para a dimensão de um divisor A tal que $0 \leq \deg(A) \leq 2g - 2$.

Teorema 2.77. *(de Clifford) Seja $A \in \text{Div}(F)$ tal que $0 \leq \deg(A) \leq 2g - 2$. Então $\ell(A) \leq 1 + \frac{1}{2} \cdot \deg A$.*

Demonstração: Já vimos que $\ell(A) = \deg(A) + 1 - g + \ell(W - A)$, onde W é um divisor canônico qualquer. Se $\ell(A) = 0$, a desigualdade segue trivialmente. Por outro lado, se $\ell(W - A) = 0$, então

$$\begin{gathered} \ell(A) = \deg(A) + 1 - g = \frac{1}{2}\deg(A) + 1 - \frac{1}{2}\deg(A) - g = \\ = 1 + \frac{1}{2}\deg(A) + \frac{1}{2}(\deg(A) - 2g) < 1 + \frac{1}{2}\deg(A). \end{gathered}$$

Agora, suponha $\ell(A) > 0$ e $\ell(W - A) > 0$. Pelo teorema de Riemann-Roch, segue que

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

Pelo lema 2.76,

$$\ell(A) + \ell(W - A) \leq 1 + \ell(A + W - A) = 1 + \ell(W) = 1 + g$$

Somando ambas, obtemos

$$2\ell(A) \leq \deg(A) + 2 \Rightarrow \ell(A) \leq 1 + \frac{1}{2}\deg(A).$$

■

2.7 Componentes locais das diferenciais de Weil

Na seção 2.5, consideramos as injeções da forma $F \hookrightarrow \mathcal{A}_F$ tais que a cada $x \in F$ é associada a sua adele principal. Lembramos que uma adele de F/K é uma aplicação

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{P}_F & \longrightarrow & F \\ P & \longmapsto & \alpha_P \end{array} \right.$$

tal que $\alpha_P \notin \mathcal{O}_P$ apenas para um núemro finito de $P \in \mathbb{P}_F$. Nosso objetivo nesta seção, é introduzir, para cada lugar $P \in \mathbb{P}_F$, uma injeção local, a qual denotaremos por $\iota_P : F \hookrightarrow \mathcal{A}_F$. Com isso, podemos mostrar que cada diferencial de Weil será a soma de suas componentes locais ligadas diretamente com ι_P.

Definição 2.78. *Seja $P \in \mathbb{P}_F$.*
(a) Dado $x \in F$, definimos $\iota_P(x) \in \mathcal{A}_F$ a adele cuja componente P é x e todas as outras são nulas.
(b) Dada uma diferencial de Weil $\omega \in \Omega_F$, definimos sua componente local pela aplicação $\omega_P : F \longrightarrow K$ tal que $\omega_P(x) := \omega(\iota_P(x))$.

É facil verificar que $\omega_P(x)$ é uma aplicação K-linear.

Proposição 2.79. *Sejam $\omega \in \Omega_F$ e $\alpha = (\alpha_P) \in \mathcal{A}_F$. Então $\omega_P(\alpha_P) \neq 0$ somente para um número finito 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: Assumimos que $\omega \neq 0$ e definimos $W := \langle \omega \rangle$ o divisor associado a ω.
Da definição de divisor, existe $S \subseteq \mathbb{P}_F$ finito tal que

$$v_P(W) = 0 \quad \text{e} \quad v_P(\alpha_P) \geq 0, \ \forall \ P \notin S.$$

Agora, defina $\beta = (\beta_P) \in \mathcal{A}_F$ por

$$\beta_P := \left\{ \begin{array}{ll} \alpha_P & \text{se} \quad P \notin S, \\ 0 & \text{se} \quad P \in S. \end{array} \right.$$

Logo, $\beta \in \mathcal{A}_F(W)$ e $\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P)$. Ainda, como $\beta \in \mathcal{A}_F(W)$, então ω se anula em β, ou seja,

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P).$$

Por fim, se $P \notin S$, temos $\iota_P(\alpha_P) \in \mathcal{A}_F(W)$ e assim, $\omega_P(\alpha_P) = 0$. Portanto,

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P).$$

Agora, note que $1 \notin P$, para todo $P \in \mathbb{P}_F$, pois P é ideal maximal. Logo, $\omega_P(1) = 0$, para todo P, e portanto, $\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0$.

■

O resultado seguinte nos diz que a diferencial de Weil é unicamente determinada por cada uma de suas componentes locais.

Proposição 2.80. *(a) Sejam $\omega \neq 0$ uma diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então*

$$v_P(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq -r\}.$$

Em particular, ω_P não é identicamente nulo.

(b) Se $\omega, \omega' \in \Omega_F$ são tais que $\omega_P = \omega'_P$, para algum lugar P, então $\omega = \omega'$.

Demonstração: (a) Por definição, $v_P(\omega) = v_P(W)$, onde $W = \langle\omega\rangle$. Seja $s = v_P(\omega)$. Dado $x \in F$ com $v_P(x) \geq -s$, temos $\iota_P(x) \in \mathcal{A}_F(W)$, e segue que $\omega_P(x) = \omega(\iota_P(x)) = 0$.

Resta mostrar a maximalidade. Suponha $v_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geq -s-1$ e seja $\alpha = (\alpha_Q)_{Q\in\mathbb{P}_F} \in \mathcal{A}_F(W+P)$.

Escrevendo $\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$, temos $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$ e $v_P(\alpha_P) \geq -s-1$. Logo,

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0,$$

ou seja, ω se anula em $\mathcal{A}_F(W+P)$, o que contradiz a definição de W, e isso conclui o item (a).

(b) Suponha que exista um lugar P tal que $\omega_P = \omega'_P$. Assim, $(\omega - \omega')_P = 0$ e pelo item (a), segue que $\omega - \omega' = 0$, ou seja, $\omega = \omega'$.

■

Para encerrar este capítulo, veremos o caso particular em que $F = K(x)$. Lembramos que P_∞ denota o polo divisor de x e P_a denota o zero divisor de $x-a$, onde $a \in K$.

Proposição 2.81. *Considere o corpo de funções racionais $K(x)/K$. Então*

(a) O divisor $-2P_\infty$ é canônico.

(b) Existe uma única diferencial de Weil $\eta \in \Omega_{K(x)}$ com $\langle\eta\rangle = -2P_\infty$ e $\eta_{P_\infty}(x^{-1}) = -1$.

(c) As componentes locais η_{P_∞} e η_{P_a} da diferencial de Weil acima saisfazem

$$\eta_{P_\infty}((x-a)^n) = \begin{cases} 0 & se \quad n \neq -1 \\ -1 & se \quad n = -1 \end{cases}$$

e

$$\eta_{P_a}((x-a)^n) = \begin{cases} 0 & se \quad n \neq -1 \\ 1 & se \quad n = -1 \end{cases}.$$

Demonstração: (a) Calculando o grau e a dimensão do divisor $-2P_\infty$, considerando $g = 0$, temos $\deg(-2P_\infty) = -2 = 2g-2$ e $\ell(-2P_\infty) = 0 = g$. Da proposição 2.68, $-2P_\infty$ é canônico.

(b) Primeiramente, escolha ω uma diferencial de Weil tal que $\langle\omega\rangle = -2P_\infty$. Assim, ω se anula em $\mathcal{A}_{K(x)}(-2P_\infty)$, mas não se anula em $\mathcal{A}_{K(x)}(-P_\infty)$. Agora, como

$$\dim\left(\mathcal{A}_{K(x)}(-P_\infty)/\mathcal{A}_{K(x)}(-2P_\infty)\right) = 1$$

e $\iota_{P_\infty}(x^{-1}) \in \mathcal{A}_{K(x)}(-P_\infty)\backslash\mathcal{A}_{K(x)}(-2P_\infty)$, segue que $c := \omega_{P_\infty}(x^{-1}) = \omega(\iota_{P_\infty}(x^{-1})) \neq 0$. Agora, defina $\eta = -c^{-1}\omega$. Assim, segue que $\langle\eta\rangle = -2P_\infty$ e $\eta_{P_\infty}(x^{-1}) = -1$.

Para a unicidade, suponha que exista η^* com as mesmas propriedades de η acima. Então $\eta - \eta^*$ se anula em $\mathcal{A}_{K(x)}(-P_\infty)$, ou seja $\eta - \eta^* = 0 \Rightarrow \eta = \eta^*$.

(c) Já sabemos que diferenciais de Weil se anulam em adeles principais. Assim, pela proposição 2.79, segue que

$$0 = \eta\left((x-a)^n\right) = \sum_{P \in \mathbb{P}_{K(x)}} \eta_P\left((x-a)^n\right).$$

Agora, se considerarmos lugares P distintos de P_∞ e P_a, temos $v_P((x-a)^n) = 0$, e utilizando a proposição 2.80, a diferencial η aplicada nesses elementos resulta em $\eta_P((x-a)^n) = 0$.

Desse modo, o somatório inicial se resume a $\eta_{P_\infty}\left((x-a)^n\right) + \eta_{P_a}\left((x-a)^n\right) = 0$. Vamos analisar três casos possíveis para n.

Caso 1: $n \leq -2$.

Neste caso, temos $v_{P_\infty}\left((x-a)^n\right) \geq 2$, e pela proposição 2.80, segue que $\eta_{P_\infty}\left((x-a)^n\right) = 0$. Assim, também devemos ter $\eta_{P_a}\left((x-a)^n\right) = 0$.

Caso 2: $n \geq 0$.

Analogamente, temos $v_{P_a}\left((x-a)^n\right) \geq 0$, e pela proposição 2.80, segue que $\eta_{P_a}\left((x-a)^n\right) = 0$, o que acarreta em $\eta_{P_\infty}\left((x-a)^n\right) = 0$.

Caso 3: $n = -1$.

Para resolver o problema quando $n = -1$, escrevemos

$$\frac{1}{x-a} = \frac{a}{x(x-a)} + \frac{1}{x}.$$

Agora, note que $\iota_{P_\infty}\left(\dfrac{a}{x(x-a)}\right) \in \mathcal{A}_{K(x)}(-2P_\infty)$. Assim, aplicando η_{P_∞}, obtemos pelo item (b) que

$$\eta_{P_\infty}\left((x-a)^{-1}\right) = \eta_{P_\infty}\left(x^{-1}\right) = -1.$$

Logo, também temos $\eta_{P_a}\left((x-a)^{-1}\right) = 1$, o que conclui a demonstração.

■

3 Códigos algébricos geométricos

Este capítulo é voltado para a aplicação dos resultados do capítulo anterior em códigos matemáticos. A teoria dos códigos lineares pode ser abordada através de diferentes ferramentas matemáticas. Aqui, vamos descrever a construção de códigos corretores de erros usando corpos de funções algébricas. Em 1981, V. D. Goppa introduziu os códigos geométricos utilizando ferramentas algébrico-geométricas. Para isso, começaremos um breve estudo dos conceitos da teoria de códigos, antes de introduzirmos os códigos AG (algébricos geométricos) de Goppa. O foco são os códigos de Goppa racionais.

3.1 Códigos

Introduziremos algumas notações básicas da teoria dos códigos. Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideramos o espaço vetorial $\mathbb{F}_q^n$, de dimensão n, cujos elementos são n-uplas $a = (a_1, \ldots, a_n)$, onde cada $a_i \in \mathbb{F}_q$.

Definição 3.1. *Dados $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, seja*

$$d(a, b) := |\{i; a_i \neq b_i\}| .$$

Essa função d é chamada distância de Hamming em $\mathbb{F}_q^n$. O peso de $a \in \mathbb{F}_q^n$ é definido por

$$\mathrm{wt}(a) := d(a, 0) = |\{i; a_i \neq 0\}| .$$

Note que $d(a, b) = wt(a-b, 0)$. Ainda, facilmente se prova que a distância de Hamming é uma métrica em $\mathbb{F}_q^n$.

Definição 3.2. *Um código C sobre o alfabeto $\mathbb{F}_q$ é um subespaço linear de $\mathbb{F}_q^n$, e os elementos de C são chamados palavras códigos.*

Chamamos de *comprimento* de C o natural n e *dimensão* de C a dimensão de C como $\mathbb{F}_q$-espaço vetorial. Um código $[n, k]$ é um código de comprimento n e dimensão k.

Definição 3.3. *Seja C um código não nulo. Definimos a distância mínima de C, e denotamos por $d = d(C)$ o inteiro*

$$d(C) := \min\{d(a, b) \mid a, b \in C \text{ e } a \neq b\} = \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}.$$

Um código $[n, k]$ com distância mínima d será denotado por $[n, k, d]$.

Observação 3.4. *Mais geralmente, podemos definir um código para um subconjunto $\emptyset \neq C \subseteq A^n$, onde $A \neq \emptyset$ é um conjunto finito. Se $A = \mathbb{F}_q$ e $C \subseteq \mathbb{F}_q^n$ é um subespaço lineaer, dizemos que C é um código linear. A maior parte dos códigos trabalhados na prática pertencem a esta categoria.*

Dado um código C com distância mínima $d = d(C)$, definimos $t := [(d-1)/2]$, onde $[x]$ denota a parte inteira do número real x. Nessas condições, C é dito um *corretor t-error*. Agora, dado $u \in \mathbb{F}_q^n$ e $d(u,c) \leq t$, para algum $c \in C$, então c é a única palavra código tal que $d(u,c) \leq t$.

Uma maneira simples para descrever um código C específico, é escrever uma base para C, como $\mathbb{F}_q$-espaço vetorial. Isso nos motiva a seguinte definição:

Definição 3.5. *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.*

Agora, podemos definir um produto interno em $\mathbb{F}_q^n$, o qual é análogo ao produto interno usual de $\mathbb{R}^n$.

Definição 3.6. *O produto interno canônico em $\mathbb{F}_q^n$ é definido por*

$$\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$

Observe que que este produto interno é uma forma bilinear simétrica não-degenerada em $\mathbb{F}_q^n$. A próxima definição vem de encontro com a definição de ortogonalidade de um conjunto da teoria de álgebra linear.

Definição 3.7. *Seja $C \subseteq \mathbb{F}_q^n$ um código. O conjunto*

$$C^{\perp} := \left\{ u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \text{ para todo } c \in C \right\}$$

é chamado de dual de C.

O código C é chamado *auto dual* se $C = C^{\perp}$ e chamado auto ortogonal se $C \subseteq C^{\perp}$. Segue também da álgebra linear que o dual de um código $[n,k]$ é um $[n, n-k]$ código, e que $\left(C^{\perp}\right)^{\perp} = C$. Em particular, a dimensão de um código auto dual de comprimento n, com n par, é $n/2$.

Definição 3.8. *Uma matriz geradora H de $C^{\perp}$ é chamada de matriz verificadora para C.*

Claramente, uma matriz verificadora H de um código C é uma matriz $(n-k) \times k$ de posto $n-k$, e temos

$$C = \left\{ u \in \mathbb{F}_q^n \mid H \cdot u^t = 0 \right\},$$

onde u^t é o transposto de u. Logo, a matriz verificadora serve para dizermos quando um vetor $u \in \mathbb{F}_q^n$ é ou não uma palavra código.

Um dos problemas básicos da teoria algébrica dos códigos é construir, sobre um alfabeto fixado $\mathbb{F}_q$, códigos cujas dimensões e distância mínima sejam grandes, quando comparadas com seu comprimento. Porém, há algumas restrições nesse processo. No caso da dimensão do código ser grande, com respeito ao seu comprimento, teremos sua distância mínima pequena. O próximo resultado nos assegura isto, fornecendo uma desigualdade envolvendo as três constantes.

Proposição 3.9. *(Cota de Singleton) Dado um código C com parâmetros $[n,k,d]$, a seguinte desigualdade é válida:*

$$k + d \leq n + 1.$$

Demonstração: Considere o subespaço $E \subseteq \mathbb{F}_q^n$ dado por

$$E := \left\{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid a_i = 0 \text{ para todo } i \geq d\right\}.$$

Assim, todo $a \in E$ tem peso $\leq d-1$, e portanto, $E \cap C = \{0\}$. Como $\dim E = d-1$, obtemos

$$k+(d-1) = \dim C + \dim E = \dim(C+E) + \dim(C \cap E) = \dim(C+E) \leq n \Rightarrow k+d \leq n+1.$$

■

Códigos tais que $k+d = n+1$ são ótimos códigos, e são chamados de códigos separáveis de distância máxima, ou códigos MDS. Mostraremos mais adiante que se $n \leq q+1$, então existem códigos MDS sobre $\mathbb{F}_q$ para todas as dimensões $k \leq n$.

3.2 Códigos algébricos geométricos (AG)

Os códigos algébricos geométricos (AG) foram introduzidos por V. D. Goppa, e por isso nos referimos a eles como códigos de Goppa. Com o intuito de motivar a construção desses códigos, vamos inicialmente considerar o que chamamos de códigos Reed-Solomon sobre $\mathbb{F}_q$, ou códigos RS. Os códigos AG são uma generalização dos códigos RS.

Seja $n = q-1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^* = \{\beta, \beta^2 \ldots, \beta^n = 1\}$. Dado um inteiro k com $1 \leq k \leq n$, consideramos o espaço vetorial de dimensão k dado por

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[x] \mid \deg f \leq k-1\}$$

e a aplicação *avaliação* $\text{ev} : \mathcal{L}_k \to \mathbb{F}_q^n$ dada por

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

Obviamente essa aplicação é $\mathbb{F}_q$-linear, uma vez que f é polinomial com coeficientes em $\mathbb{F}_q$. Além disso, é injetiva, uma vez que um polinômio não nulo $f \in \mathbb{F}_q[x]$ de grau $< n$ tem menos do que n raízes. Assim,

$$C_k := \left\{\left(f(\beta), f\left(\beta^2\right), \ldots, f\left(\beta^n\right)\right) \mid f \in \mathcal{L}_k\right\}$$

é um código $[n,k]$ em $\mathbb{F}_q$, chamado de *código RS* (código de Reed-Solomon).

O peso de uma palavra código $0 \neq c = \text{ev}(f) \in C_k$ é dado por

$$\text{wt}(c) = n - \left|\left\{i \in \{1, \ldots, n\}; f\left(\beta^i\right) = 0\right\}\right| \geq n - \deg f \geq n - (k-1).$$

Logo, a distância mínima d de C_k satisfaz $d \geq n-k+1$. Pela cota de Singleton, obtemos $d = n-k+1$, e segue que códigos RS são códigos MDS. Porém, é importante ressaltar que códigos RS são curtos em comparação com o tamanho do alfabeto $\mathbb{F}_q$, uma vez que $n = q-1$.

Antes de definirmos um outro tipo de código AG, vamos fixar algumas notações que serão úteis no decorrer desta seção:

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

Definição 3.10. *O código AG $C_{\mathcal{L}}(D,G)$ associado aos divisores D e G é definido por*

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

Essa definição faz sentido: dado $x \in \mathcal{L}(G)$, temos $v_{P_i}(x) \geq 0$, uma vez que $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$. Agora a classe residual $x(P_i)$ de x módulo P_i é um elemento do corpo de classe residual de P_i, e como $\deg P_i = 1$, sua classe residual é $\mathbb{F}_q$, e portanto, $x(P_i) \in \mathbb{F}_q$.

Como fizemos anteriormente, podemos definir a aplicação avaliação $\mathrm{ev}_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ por

$$\mathrm{ev}_D(x) := (x(P_1),\ldots,x(P_n)) \in \mathbb{F}_q^n.$$

Essa aplicação é $\mathbb{F}_q$-linear e $C_{\mathcal{L}}(D,G)$ é a imagem de $\mathcal{L}(G)$ sobre a aplicação ev_D.

O primeiro resultado desta seção é um teorema que nos fornece algumas relações entre os parâmetros de um código $C_{\mathcal{L}}(D,G)$

Teorema 3.11. *Seja $C_{\mathcal{L}}(D,G)$ um código com parâmetros $[n,k,d]$. Então*

$$k = \ell(G) - \ell(G-D) \quad e \quad d \geq n - \deg G.$$

Demonstração: Observe que a aplicação $\mathrm{ev}_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ é sobrejetiva. Agora, seu núcleo é dado por

$$\ker(\mathrm{ev}_D) = \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0 \text{ para } i = 1,\ldots,n\} = \mathcal{L}(G-D).$$

Logo, segue que

$$k = \dim C_{\mathcal{L}}(D,G) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D) = \ell(G) - \ell(G-D)$$

e isso prova a primeira afirmação do teorema. Agora, mostremos que $d \geq n - \deg G$. Assumimos que $C_{\mathcal{L}}(D,G) \neq 0$ e consideramos $x \in \mathcal{L}(G)$ tal que $\mathrm{wt}(\mathrm{ev}_D(x)) = d$.

Assim, $n-d$ lugares $P_{i_1},\ldots,P_{i_{n-d}} \in \operatorname{supp}(D)$ são zeros de x e assim,

$$0 \neq x \in \mathcal{L}\left(G - \left(P_{i_1} + \cdots + P_{i_{n-d}}\right)\right).$$

Do corolário 2.46, segue que

$$0 \leq \deg\left(G - \left(P_{i_1} + \cdots + P_{i_{n-d}}\right)\right) = \deg G - n + d$$

e portanto $d \geq n - \deg G$.

■

Como consequência imediata do teorema acima, temos o seguinte corolário:

Corolário 3.12. *Nas condições do teorema anterior, se $\deg G < n$, então a aplicação $\mathrm{ev}_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ é injetiva e ainda,*

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

$$d \geq n - \deg G \quad e \quad k = \ell(G) \geq \deg G + 1 - g.$$

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

(b) Se $2g - 2 < \deg G < n$, então $k = \deg G + 1 - g$.

(c) Se $\{x_1,\ldots,x_k\}$ é uma base de $\mathcal{L}(G)$, então a matriz

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \ldots & x_k(P_n) \end{pmatrix}$$

é uma matriz geradora de $C_{\mathcal{L}}(D,G)$.

Demonstração: Por hipótese $\deg G < n$, e como $\deg D = n$, segue que $\deg(G-D) < 0$. Assim, $\mathcal{L}(G-D) = 0$. Assim, $\mathrm{Ker}\,(\mathrm{ev}_D) = \mathcal{L}(G-D) = \{0\}$, e portanto, a aplicação é injetora.

(a) Segue diretamente do teorema 3.11 e do teorema de Riemann-Roch.

(b) Segue dos corolários do teorema de Riemann-Roch.

(c) Segue da definição de matriz geradora e do teorema 3.11.

■

Do corolário anterior, conseguimos uma cota inferior para a distância mínima d, dada por

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

Essa cota é bastante similar à cota de Singleton, que é dada por $d \geq n + 1 - k$. No caso em que $\deg G < n$,

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

Se F tem gênero zero, então $d + k = n + 1$, e obtemos que códigos AG construidos sobre corpos de funções racionais da forma $\mathbb{F}_q(z)$ são sempre códigos MDS. O fato de necessitarmos da hipótese $\deg G < n$ nos motiva a definição a seguir.

Definição 3.13. *O inteiro $d^* = n - \deg G$ é chamado de distância projetada do código $C_{\mathcal{L}}(D, G)$.*

O teorema 3.11 nos diz que a distância mínima de um código não pode ser menor do que a distância projetada. A observação a seguir nos diz quando $d^* = d$ ou $d^* < d$.

Observação 3.14. *Suponha $\ell(G) > 0$ e $d^* = n - \deg G > 0$. Então $d^* = d \Leftrightarrow \exists\, D' \in \mathrm{Div}(F)$ com $0 \leq D' \leq D$, tal que $\deg D' = \deg D$ e $\ell(G - D') > 0$.*

Demonstração: Suponha $d = d^*$. Logo, existe $0 \neq x \in \mathcal{L}(G)$ tal que a palavra código $(x(P_1), \ldots, x(P_n)) \in C_{\mathcal{L}}(D, G))$ tem exatamente $n - d = n - d^* = \deg G$ componentes nulas, ou seja,

$$x\left(P_{i_j}\right) = 0 \text{ para } j = 1, \ldots, \deg G.$$

Defina $D' := \sum_{j=1}^{\deg G} P_{i_j}$. Então

$$0 \leq D' \leq D,\ \deg D' = \deg G \text{ e } \ell(G - D') > 0, \text{ uma vez que } x \in \mathcal{L}(G - D').$$

Reciprocamente, seja D' satisfazendo as propriedades acima e escolha $0 \neq y \in \mathcal{L}(G - D')$. O peso da palavra código correspondente $(y(P_1), \ldots, y(P_n))$ é $n - \deg G = d^*$, ou seja, $d = d^*$.

■

Vamos introduzir agora um outro tipo de código, que também está associado aos divisores D e G, usando as componentes locais de Weil vistas na última seção do capítulo anterior. Lembramos que, dado $A \in \mathrm{Div}(F)$, denotamos por $\Omega_F(A)$ o espaço das diferenciais de Weil ω tais que $\langle\omega\rangle \geq A$. Este conjunto, é um $\mathbb{F}_q$-espaço vetorial de dimensão finita $i(A)$ (índice de especialidade de A). Ainda, dado $P \in \mathbb{P}_F$ e ω uma diferencial de Weil, a aplicação $\omega_P : F \longrightarrow F_q$ denota a componente local de ω em P. Com isso, podemos definir o outro tipo de código citado no início.

Definição 3.15. *Sejam D e G definidos como anteriormente. Definimos o código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ por*

$$C_\Omega(D,G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G-D)\}.$$

O código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ é também chamado de código algébrico geométrico. A relação entre os códigos $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ e $C_\mathcal{L}(D,G)$ será apresentada mais adiante. O próximo resultado é uma versão análoga do teorema 3.11, agora para o código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$.

Teorema 3.16. *Um código $C_\Omega(D,G) \subseteq \mathbb{F}_q^n$ com parâmetros $[n,k',d']$ satisfaz*

$$k' = i(G-D) - i(G) \quad e \quad d' \geq \deg G - (2g-2)$$

Ainda, se $\deg G > 2g-2$, então $k' = i(G-D) \geq n+g-1-\deg G$, e se $2g-2 < \deg G < n$, então $k' = n+g-1-\deg G$.

Demonstração: Seja $P \in \mathbb{P}_F$ um lugar de grau 1 e ω uma diferencial de Weil com $v_P(\omega) \geq -1$.

Afirmação 1: $\omega_P(1) = 0 \iff v_P(\omega) \geq 0$.

A proposição 2.80 afirma que, dado $r \in \mathbb{Z}$, tem-se

$$v_P(\omega) \geq r \iff \omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq -r.$$

Assim, se $v_P(\omega) \geq 0$, então $\omega_P(x) = 0$, para todo $x \in F$ tal que $v_P(x) \geq 0$. Agora, como $v_P(1) \geq 0$, segue que $\omega_P(1) = 0$. Por outro lado, suponha $\omega_P(1) = 0$ e considere $x \in F$ com $v_P(x) \geq 0$. Como $\deg P = 1$, escrevemos $x = a + y$, com $a \in \mathbb{F}_q$ e $v_P(y) \geq 1$. Então,

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = 0.$$

Aqui usamos o fato de que, se $v_P(\omega) \geq -1$ e $v_P(y) \geq 1$, então a proposição 2.80 garante que $\omega_P(y) = 0$. Com isso, a afirmação fica provada.

Consideramos agora a aplicação

$$\varrho_D : \begin{cases} \Omega_F(G-D) \longrightarrow C_\Omega(D,G), \\ \qquad\qquad \omega \longmapsto (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)). \end{cases}$$

Claramente ϱ_D é sobrejetiva, e ainda usando a *afirmação 1*, temos

$$\begin{aligned} \ker \varrho_D &= \{\omega \in \Omega_F(G-D) \mid \varrho_D(\omega) - 0\} = \{\omega \in \Omega_F(G-D) \mid \omega_{P_i}(1) = 0, i = 1, \ldots, n\} \\ &= \{\omega \in \Omega_F(G-D) \mid v_{P_i}(\omega) \geq 0, i = 1, \ldots, n\} = \Omega_F(G). \end{aligned}$$

Assim, do teorema do núcleo e da imagem, temos

$$k' = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G).$$

Agora, considere $\varrho_D(\omega) \in C_\Omega(D,G)$ uma palavra código de peso $m > 0$. Então, $\omega_{P_i}(1) = 0$, para índices $i = i_1, \ldots, i_{n-m}$, e assim,

$$\omega \in \Omega_F\left(G - \left(D - \sum_{j=1}^{n-m} P_{i_j}\right)\right).$$

Agora, como $i(A) = \Omega_F(A) \neq 0$, pelo teorema 2.66, segue que $\deg A \leq 2g-2$, e assim,

$$2g-2 \geq \deg G - (n-(n-m)) = \deg G - m \Rightarrow m \geq \deg G - (2g-2),$$

e portanto a distância mínima d' satisfaz $d' \geq \deg G - (2g-2)$.

Agora, vamos considerar o caso em que $\deg G > 2g-2$. Do teorema 2.66, obtemos $i(G) = 0$, e assim,

$$\begin{aligned} k' = i(G-D) &= \ell(G-D) - \deg(G-D) - 1 + g \\ &= \ell(G-D) + n + g - 1 - \deg G. \end{aligned}$$

Como $\ell(G-D) \geq 0$, então $k' \geq n + g - 1 - \deg G$.

Se tivermos $2g-2 < \deg G < n$, teremos $\ell(G-D) = 0$, e portanto, vale a igualdade no caso acima.

■

O inteiro $\deg G - (2g-2)$ é chamado de *distância projetada* do código $C_\Omega(D,G)$. Agora, veremos que existe uma relação bastante útil entre os dois códigos geométricos que trabalhamos até agora.

Teorema 3.17. *Os códigos $C_\mathcal{L}(D,G)$ e $C_\Omega(D,G)$ são duais entre si, isto é,*

$$C_\Omega(D,G) = C_\mathcal{L}(D,G)^\perp.$$

Demonstração: A ideia aqui será mostrar que $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$, e em seguida, verificar que ambos possuem a mesma dimensão como espaços vetoriais.

Sejam $P \in \mathbb{P}_F$ de grau um, ω uma diferencial de Weil com $v_P(\omega) \geq -1$ e $x \in F$ tal que $v_P(x) \geq 0$.

Afirmação 1: $\omega_P(x) = x(P) \cdot \omega_P(1)$.

De fato, como $x \in F$, podemos escrever $x = a + y$, com $a = x(P) \in \mathbb{F}_q$ e $v_P(y) > 0$. Assim, utilizando a proposição 2.80, temos

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = x(P) \cdot \omega_P(1).$$

Agora, vamos mostrar que $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$. Considere $\omega \in \Omega_F(G-D)$ e $x \in \mathcal{L}(G)$. Como as diferenciais de Weil se anulam em adeles principais, então $\omega(x) = 0$. Por outro lado, da proposição 2.79, podemos escrever cada diferencial de Weil como soma de suas componentes locais, ou seja,

$$\omega(x) = \sum_{P \in \mathbb{P}_F} \omega_P(x).$$

Agora, se considerarmos $P \in \mathbb{P}_F - \{P_1, \ldots, P_n\}$, temos $v_P(x) \geq -v_P(\omega)$, já que $x \in \mathcal{L}(G)$ e $\omega \in \Omega(G-D)$. E assim, pela proposição 2.80 temos $\omega_P(x) = 0$.

Logo, usando isto, e a *afirmação 1*, temos

$$\begin{aligned} 0 = \omega(x) &= \sum_{P \in \mathbb{P}_F} \omega_P(x) \\ &= \sum_{i=1}^{n} \omega_{P_i}(x) \\ &= \sum_{i=1}^{n} x\left(P_i\right) \cdot \omega_{P_i}(1) \\ &= \left\langle \left(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)\right), \left(x\left(P_1\right), \ldots, x\left(P_n\right)\right) \right\rangle. \end{aligned}$$

Logo, $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$. Resta verificarmos que ambos os códigos possuem mesma dimensão como espaços vetoriais. De fato,

$$\begin{aligned}\dim C_\Omega(D,G) &= i(G-D) - i(G)\\ &= \ell(G-D) - \deg(G-D) - 1 + g - (\ell(G) - \deg G - 1 + g)\\ &= \deg D + \ell(G-D) - \ell(G)\\ &= n - (\ell(G) - \ell(G-D))\\ &= n - \dim C_\mathcal{L}(D,G) = \dim C_\mathcal{L}(D,G)^\perp.\end{aligned}$$

Portanto, $C_\Omega(D,G) = C_\mathcal{L}(D,G)^\perp$.

■

O próximo resultado nos garante a existência de uma diferencial de Weil η com propriedades específicas, e esta, será útil para mostrarmos que todo código $C_\Omega(D,G)$ pode ser representado por $C_\mathcal{L}(D,H)$, onde H é um divisor dependendo de η.

Lema 3.18. *Existe uma diferencial de Weil η tal que*

$$v_{P_i}(\eta) = -1 \quad e \quad \eta_{P_i}(1) = 1 \quad \text{para } i = 1, \ldots, n.$$

Demonstração: Escolhemos inicialmente uma diferencial de Weil arbitrária $\omega_0 \neq 0$. Pelo teorema da aproximação, existe $z \in F$ tal que $v_{P_i}(z) = -v_{P_i}(\omega_0) - 1$, para $i = 1, \ldots, n$. Defina $\omega = z\omega_0$. Então, $v_{P_i}(\omega) = -1$. Colocando $a_i = \omega_{P_i}(1)$, temos $a_i \neq 0$, uma vez que $v_{P_i}(\omega) = 1 < 0$. Utilizando novamente o teorema da aproximação, podemos encontrar $y \in F$ tal que $v_{P_i}(y - a_i) > 0$. Assim, $y - a_i \in P_i$, e segue que $v_{P_i}(y) = 0$ e $y(P_i) = a_i$. Agora, basta definir $\eta = y^{-1}\omega$ e teremos

$$v_{P_i}(\eta) = v_{P_i}(\omega) = -1$$

e

$$\eta_{P_i}(1) = \omega_{P_i}\left(y^{-1}\right) = y^{-1}(P_i) \cdot \omega_{P_i}(1) = a_i^{-1} \cdot a_i = 1.$$

■

Proposição 3.19. *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,*

$$C_\mathcal{L}(D,G)^\perp = C_\Omega(D,G) = C_\mathcal{L}(D,H), \quad \text{onde} \quad H := D - G + \langle\eta\rangle.$$

Demonstração: O teorema 3.17 garante a primeira igualdade. Observe que o código $C_\mathcal{L}(D, D - G + \langle\eta\rangle)$ está bem definido, uma vez que $\operatorname{supp}(D - G + \langle\eta\rangle) \cap \operatorname{supp} D = \emptyset$, pois $v_{P_i}(\eta) = -1$.

Assim, do teorema da dualidade, existe um isomorfismo

$$\mu : \mathcal{L}(D - G + (\eta)) \to \Omega_F(G - D)$$

dado por $\mu(x) := x\eta$. Assim, para $x \in \mathcal{L}(D - G + \langle\eta\rangle)$

$$(x\eta)_{P_i}(1) = \eta_{P_i}(x) = x(P_i) \cdot \eta_{P_i}(1) = x(P_i),$$

e concluimos que $C_\Omega(D,G) = C_\mathcal{L}(D, D - G + \langle\eta\rangle)$.

■

Corolário 3.20. *Suponha η uma diferencial de Weil tal que*

$$2G - D \leq \langle \eta \rangle \quad e \quad \eta_{P_i}(1) = 1 \quad for \quad i = 1, \ldots, n.$$

Então, $C_{\mathcal{L}}(D, G)$ é auto-ortogonal. Ainda, se tivermos $2G - D = \langle \eta \rangle$ e $\eta_{P_i}(1) = 1$, para $i = 1 \ldots, n$, então o código $C_{\mathcal{L}}(D, G)$ é auto-dual.

Demonstração: Assuma $2G - D \leq \langle \eta \rangle$. Logo, $G \leq D - G + \langle \eta \rangle = H$, da proposição anterior. Da proposição 3.19, temos

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}(D, D - G + \langle \eta \rangle) \supseteq C_{\mathcal{L}}(D, G),$$

ou seja, $C_{\mathcal{L}}(D, G)$ é auto ortogonal. No caso de $2G - D = \langle \eta \rangle$, a igualdade segue de forma imediata.

■

Encerramos esta seção com a definição de códigos equivalentes.

Definição 3.21. *Dois códigos $C_1, C_2 \in \mathbb{F}_q^n$ são ditos equivalentes se existe $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^n)^*$ tal que $C_2 = aC_1$, ou seja,*

$$C_2 = \{(a_1 c_1, \ldots, a_n c_n) \mid (c_1, \ldots, c_n) \in C_1\}.$$

Claramente códigos equivalentes possuem a mesma dimensão e a mesma distância mínima. O resultado a seguir nos fornece condições necessária e suficiente para códigos serem equivalentes.

Proposição 3.22. *(a) Sejam G_1 e G_2 divisores equivalentes tais que $\operatorname{supp} G_1 \cap \operatorname{supp} D = \operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset$. Então os códigos $C_{\mathcal{L}}(D, G_1)$ e $C_{\mathcal{L}}(D, G_2)$ são equivalentes. O mesmo vale para os códigos $C_{\Omega}(D, G_1)$ e $C_{\Omega}(D, G_2)$.*

(b) Reciprocamente, se $C \subseteq \mathbb{F}_q^n$ é equivalente a $C_{\mathcal{L}}(D, G)$, então existe um divisor $G' \sim G$ tal que $\operatorname{supp} G' \cap \operatorname{supp} D = \emptyset$ e $C = C_{\mathcal{L}}(D, G')$. O mesmo vale para o código $C_{\Omega}(D, G)$.

Demonstração: (a) Da hipótese, existe $z \in F$ tal que $G_2 = G_1 - \langle z \rangle$, e ainda, $v_{P_i}(z) = 0$, para todo $i = 1, \ldots, n$.

Defina $a := (z(P_1), \ldots, z(P_n))$. Segue que $a \in (\mathbb{F}_q^n)^*$, ja que $z(P_i) \in \mathbb{F}_q$. Considere a aplicação

$$\varphi : \begin{cases} \mathcal{L}(G_1) \longrightarrow \mathcal{L}(G_2) \\ x \longmapsto xz \end{cases}.$$

Temos que φ é bijetora pelo lema 2.40. Assim, usando o fato de ser uma bijeção, dado $x \in \mathcal{L}(G_2)$, podemos encontrar $y \in \mathcal{L}(G_1)$ tal que $\varphi(y) = x$, e disso, segue facilmente da definição do código associado a um espaço de Riemann-Roch que $C_{\mathcal{L}}(D, G_2) = a \cdot C_{\mathcal{L}}(D, G_1)$, ou seja, os códigos são equivalentes. Para mostrar a equivalência entre $C_{\Omega}(D, G_1)$ e $C_{\Omega}(D, G_2)$, a demonstração é análoga, bastante definir um isomorfismo entre os códigos, usando o fato de $G_1 \sim G_2$.

(b) Para a recíproca, considere $C = aC_{\mathcal{L}}(D, G)$, onde $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^n)^*$. Defina $z(P_i) := a_i$ e considere $G' := G - \langle z \rangle$. Então, $G \sim G'$ e ainda, segue que $C = C_{\mathcal{L}}(D, G')$. No caso dos códigos envolvendo diferenciais de Weil, basta definir $a_i = \omega_{P_i}(1)$, e o resultado segue de maneira análoga.

■

3.3 Códigos AG racionais

Nesta seção, introduziremos os códigos AG associados a divisores de um corpo de funções racionais. Esses tipos de códigos serão explicitados a partir de matrizes geradoras e verificadoras, e são chamados de código de Reed-Solomon generalizados, ou códigos GRS. Dentre os exemplos que veremos estão os códigos BCH e os códigos de Goppa, que são os mais utilizados na prática.

Definição 3.23. *Um código algébrico geométrico $C_{\mathcal{L}}(D,G)$, onde D e G são divisores como na seção anterior de um corpo de funções $\mathbb{F}_q(z)/\mathbb{F}_q$ é dito racional.*

O comprimento de um código AG racional é limitado por $q+1$, uma vez que $\mathbb{F}_q(z)$ tem somente $q+1$ lugares de grau 1, a saber, o polo P_∞ de z e para cada $\alpha \in \mathbb{F}_q$, o zero P_α de $z-\alpha$, como já vimos no capítulo anterior.

O primeiro resultado desta seção nos fornece uma série de informações a respeito dos código AG racionais, envolvendo seus duais e os parâmetros n, k e d. Em seguida, veremos uma proposição que nos dará a forma da matriz geradora desse tipo de código.

Proposição 3.24. *Seja $C = C_{\mathcal{L}}(D,G)$ um código AG racional sobre $\mathbb{F}_q$ e n, k, d os seus parâmetros. Então*

(a) $n \leq q+1$.

(b) $k = 0 \Leftrightarrow \deg G < 0$ e $k = n \Leftrightarrow \deg G > n-2$.

(c) Se $0 \leq \deg G \leq n-2$, então $k = 1 + \deg G$ e $d = n = \deg G$. Em particular, C é um código MDS.

(d) $C^\perp$ é também um código AG racional.

Demonstração: (a) Segue da observação feita após a definição de código AG racional.

(b) Assuma que $k = 0$ e suponha por absurdo que $\deg G \geq 0$. Então, $\ell(G) = \deg G + 1 - g + \ell(W-G) \geq 1$, onde W é um divisor canônico. Assim, temos $\ell(G) > 0$, o que implica que $k > 0$, contradizendo a hipótese. Portanto, $\deg G < 0$.

Reciprocamente, se $\deg G < 0$, então $\deg G \leq -1$, e segue que $\ell(C) = 0$, ou seja, $k = 0$.

A outra equivalência segue do seguinte:

$$k = n \Leftrightarrow \ell(C) = \deg G + 1 - g + \ell(W-C) \Leftrightarrow n - 1 = \deg G + \ell(W-C) \Leftrightarrow \deg G > n-2.$$

(c) Segue do teorema 3.11.

(d) Segue imediatamente da definição de código AG racional.

■

Proposição 3.25. *Seja $C = C_{\mathcal{L}}(D,G)$ um código AG racional sobre $\mathbb{F}_q$ com parâmetros n, k, d.*

(a) Se $n \leq q$, então existem elementos distintos dois a dois $\alpha_1, \ldots \alpha_n \in \mathbb{F}_q$ e $v_1, \ldots, v_n \in \mathbb{F}_q^*$ (não necessariamente distintos) tais que

$$C = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \text{ and } \deg f \leq k-1\}$$

e a matriz

$$M = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \ldots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \ldots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \ldots & \alpha_n^{k-1} v_n \end{pmatrix}$$

é a matriz geradora de C (as linhas formam uma base para C).

(b) Se $n = q + 1$, então C tem a matriz geradora da forma

$$M = \begin{pmatrix} v_1 & v_2 & \dots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \dots & \alpha_{n-1} v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \dots & \alpha_{n-1}^2 v_{n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \dots & \alpha_{n-1}^{k-1} v_{n-1} & 1 \end{pmatrix},$$

onde $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_{n-1}\}$ e $v_1, \dots, v_{n-1} \in \mathbb{F}_q^*$.

Demonstração: (a) Seja $D = P_1 + \cdots P_n$. Como $n \leq q$, existe P um lugar de grau 1 tal que $P \notin \operatorname{supp} D$. Seja $Q \neq P$ de grau 1. Pelo teorema de Riemann-Roch, $\ell(Q - P) = 1$, e portanto $Q - P$ é principal, pelo corolário 2.46.

Seja $Q - P = \langle z \rangle$. Então, z é um gerador do corpo de funções sobre $\mathbb{F}_q$ e P é polo divisor de z, e escrevemos $P = P_\infty$. Pela proposição 3.24, podemos assumir $\deg G = k - 1 > 0$ (o caso $k = 0$ é trivial).

Considere o divisor $G' = (k-1)P_\infty - G$. Temos $\deg G' = 0$, e portanto, G' é principal, e assim, existe $u \in F$ não nulo tal que

$$\langle u \rangle = G' = (k-1)P_\infty - G.$$

Agora, os elementos $u, zu, \dots, z^{k-1}u \in \mathcal{L}(G)$ e são linearmente independentes sobre $\mathbb{F}_q$. Como $\ell(G) = k$, eles formam uma base para $\mathcal{L}(G)$, e assim,

$$\mathcal{L}(G) = \{uf(z) \mid f \in \mathbb{F}_q[z] \text{ and } \deg f \leq k-1\}.$$

Definindo $\alpha_i := z(P_i)$ e $v_i := u(P_i)$, obtemos

$$(uf(z))(P_i) = u(P_i)\, f(z(P_i)) = v_i f(\alpha_i),$$

e assim, $C = C_{\mathcal{L}}(D, G) = \{(v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) \mid \deg f \leq k-1\}$, como queríamos mostrar. Ainda, observe que a palavra código em C correspondendo a uz^j é $\left(v_1\alpha_1^j, v_2\alpha_2^j, \dots, v_n\alpha_n^j\right)$, e portanto a matriz M do enunciado é a matriz geradora de C.

(b) A prova desse item é semelhante ao caso em que $n \leq q$. Agora, como $n = q + 1$, escolhemos $z \in F$ tal que $P_n = P_\infty$ é o polo de z. Como no item (a), existe $u \in F$, $u \neq 0$ com $(k-1)P_\infty - G = \langle u \rangle$ e de modo que $\{u, uz, uz^2, \dots, uz^{k-1}\}$ seja base de $\mathcal{L}(G)$.

Para $i = 1, \dots, n-1 = q$, os elementos $\alpha_i := z(P_i) \in \mathbb{F}_q$ são dois a dois distintos, e assim, $\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_{n-1}\}$. Ainda, para $i = 1, \dots, n-1$, $v_i := u(P_i) \in \mathbb{F}_q^*$. Para o caso em que $1 \leq j \leq k-2$, temos

$$\left(\left(uz^j\right)(P_1), \dots, \left(uz^j\right)(P_n)\right) = \left(\alpha_1^j v_1, \dots, \alpha_{n-1}^j v_{n-1}, 0\right),$$

e se $j = k - 1$, tem-se

$$\left(\left(uz^{k-1}\right)(P_1), \dots, \left(uz^{k-1}\right)(P_n)\right) = \left(\alpha_1^{k-1} v_1, \dots, \alpha_{n-1}^{k-1} v_{n-1}, \gamma\right)$$

onde $0 \neq \gamma \in \mathbb{F}_q$. Substituindo u por $\gamma^{-1}u$, obtemos a matriz geradora do enunciado.

■

Isso motiva a seguinte definição:

Definição 3.26. *Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$, com α_i's elementos distintos de $\mathbb{F}_q$ e $v = (v_1, \ldots, v_n)$, com v_i's elementos não nulos, não necessariamente distintos de $\mathbb{F}_q$. Então o código de Reed-Solomon generalizado, denotado por $\mathrm{GRS}_k(\alpha, v)$ consiste de todos os vetores*

$$(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)),$$

com $f(z) \in \mathbb{F}_q[z]$ e $\deg f \leq k-1$, onde $k \leq n$ é um inteiro fixado.

No caso de termos $\alpha = (\beta, \beta^2, \ldots, \beta^n)$, com $n = q-1$, β uma raiz n-ésima primitiva da unidade e $v = (1, 1, \ldots, 1)$, o código $\mathrm{GRS}_k(\alpha, v)$ é um código de Reed-Solomon, como na seção anterior. Podemos mostrar agora uma recíproca da proposição 3.25.

Proposição 3.27. *Todo código $\mathrm{GRS}_k(\alpha, v)$ pode ser representado como um código AG racional.*

Demonstração: Sejam $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ e $v = (v_1, \ldots, v_n) \in (\mathbb{F}_q^n)^*$. Considere o corpo de funções racionais onde $F = \mathbb{F}_q(z)$. Denote por P_i o zero de $z - \alpha_i$ e por P_∞ o polo de z. Pelo teorema da aproximação, existe $u \in F$ tal que $u(P_i) = v_i$, para cada $i = 1, \ldots, n$. Desse modo, podemos definir $D = P_1 + \cdots + P_n$ e $G = (k-1)P_\infty - \langle u \rangle$, e o resultado segue da proposição 3.25, basta fazer o caminho inverso e teremos $\mathrm{GRS}_k(\alpha, v) = C_{\mathcal{L}}(D, G)$.

■

Para determinarmos o dual de um código AG racional $C = C_{\mathcal{L}}(D, G)$, precisamos de uma diferencial de Weil ω de $\mathbb{F}_q(z)$ tal que

$$v_{P_i}(\omega) = -1 \quad \text{e} \quad \omega_{P_i}(1) = 1, \quad \text{para} \quad i = 1, \ldots, n.$$

O próximo resultado garante a existência de tal diferencial de Weil

Lema 3.28. *Considere $F = \mathbb{F}_q(z)$ e n elementos distintos $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Sejam $P_i \in \mathbb{P}_F$ o zero de $z - \alpha_i$ e $h(z) = \prod_{i=1}^{n} (z - \alpha_i)$ e $y \in F$ tal que $y(P_i) = 1$, $i = 1, \ldots, n$. Então existe uma diferencial de Weil ω de $\mathbb{F}_q$ que satisfaz $v_{P_i}(\omega) = -1$ e $\omega_{P_i}(1) = 1$ e o divisor $\langle \omega \rangle$ satisfaz*

$$\langle \omega \rangle = \langle y \rangle + \langle h'(z) \rangle - \langle h(z) \rangle - 2P_\infty,$$

onde $h'(z)$ denota a derivada de $h(z)$.

Demonstração: Pela proposição 2.81, existe uma diferencial η de F com $\langle \eta \rangle = -2P_\infty$ e $\eta_{P_\infty}(z^{-1}) = -1$. Defina $\omega := y \cdot (h'(z)/h(z)) \cdot \eta$. Assim, o divisor $\langle \omega \rangle$ satisfaz

$$\langle \omega \rangle = \langle y \rangle + \langle h'(z) \rangle - \langle h(z) \rangle - 2P_\infty.$$

Em particular, $v_{P_i}(\omega) = -1$ para $i = 1, \ldots, n$. Precisamos agora verificar que $\omega_{P_i}(1) = 1$. Primeiramente, escreva $h(z) = (z - \alpha_i)\, g_i(z)$, onde $g_i(z) = \sum_{j \neq i} (z - \alpha_j)$, com $i = 1, \ldots, n$.

Então,

$$y \cdot \frac{h'(z)}{h(z)} = (1 + (y-1)) \cdot \left(\frac{g_i'(z)}{g_i(z)} + \frac{1}{z - \alpha_i} \right) = \frac{1}{z - \alpha_i} + u,$$

onde $u \in F$ e $v_{P_i}(u) \geq 0$, uma vez que $v_{P_i}(y-1) > 0$ e $v_{P_i}(g_i(z)) = 0$.

Agora, pelas proposições 2.80(a) e 2.81(c),

$$\eta_{P_i}\left((z-\alpha_i)^{-1}\right) = 1 \text{ and } \eta_{P_i}(u) = 0,$$

e assim,

$$\omega_{P_i}(1) = \eta_{P_i}\left(y \cdot \frac{h'(z)}{h(z)}\right) = \eta_{P_i}\left(\frac{1}{z-\alpha_i} + u\right) = 1.$$

■

Note que, o lema 3.28, combinado com o teorema 3.17 e as proposições 3.19 e 3.25, possibilita que especifiquemos uma matriz verificadora para o código $C_{\mathcal{L}}(D,G)$.

Nosso próximo objetivo é descrever dois códigos específicos: BCH e de Goppa, por meio de códigos AG racionais. Antes de definirmos códigos BCH, precisamos da seguinte definição:

Definição 3.29. *Considere uma extensão de corpos $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ e C um código sobre $\mathbb{F}_{q^m}$ de comprimento n. Então,*

$$C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^n$$

é a restrição de C em $\mathbb{F}_q$.

Segue diretamente da definição que $C|_{\mathbb{F}_q}$ é um código sobre $\mathbb{F}_q$, e sua distância mínima não pode ser menor do que a distância mínima de C, e podemos estimar a dimensão de $C|_{\mathbb{F}_q}$ por $\dim C|_{\mathbb{F}_q} \leq \dim C$. Com isso, vejamos a definição de códigos BCH.

Definição 3.30. *Suponha que $n \mid q^m - 1$ e seja $\beta \in \mathbb{F}_{q^m}$ uma raiz n-ésima primitiva da unidade. Considere ainda $l \in \mathbb{Z}$ e $\delta \geq 2$. Definimos o código $C(n,l,\delta)$ sobre $\mathbb{F}_{q^m}$ pela matriz geradora*

$$H := \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \dots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \dots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \dots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix}.$$

O código $C := C(n,l,\delta)^{\perp}\Big|_{\mathbb{F}_q}$ é chamado de código BCH de distância projetada δ. Em outra palavras,

$$C = \left\{c \in \mathbb{F}_q^n \mid H \cdot c^t = 0\right\}.$$

O resultado a seguir nos fornece uma relação entre código BCH e códigos associados a um espaço de Riemann-Roch.

Proposição 3.31. *Sejam $n \mid q^m - 1$ e $\beta \in \mathbb{F}_{q^m}$ uma raiz n-ésima primitiva da unidade. Considere $F = F_{q^m}(z)$ o corpo de funções racionais sobre $\mathbb{F}_{q^m}$ e P_0 (respectivamente P_∞) o zero (respectivamente polo) de z. Para $i = 1, \dots, n$, denote por P_i o zero de $z - \beta^{i-1}$ e defina $D_\beta := P_1 + \cdots + P_n$. Considere $a, b \in \mathbb{Z}$ com $0 \leq a, b \leq n-2$. Então,*

(a) $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty) = C(n,l,\delta)$, com $l = -a$ e $\delta = a + b + 2$.

(b) O dual de $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)$ é dado por

$$C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)^{\perp} = C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty),$$

com $r = -(a+1)$ e $s = n - b - 1$. Consequentemente, o código BCH $C(n,l,\delta)^{\perp}\Big|_{\mathbb{F}_q}$ é a restrição a $\mathbb{F}_q$ do código $C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)$, com $r = l - 1$ e $s = n + 1 - \delta - l$.

Demonstração: (a) Considere o código $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)$ com $0 \leq a+b \leq n-2$. Os elementos $z^{-a}z^j$, com $0 \leq j \leq a+b$ formam uma base para $\mathcal{L}(aP_0 + bP_\infty)$.

De fato, observe que $\dim(aP_0 + bP_\infty) = a+b+1$, uma vez que $\deg P_0 = \deg P_\infty = 1$. Ainda, se $0 \leq j \leq a+b$, temos

$$\langle z^{-a}z^j \rangle = -a\langle z \rangle + j\langle z \rangle \geq -(aP_0 - (-bP_\infty)) = -(aP_0 + bP_\infty),$$

ou seja, $z^{-a}z^j \in \mathcal{L}(aP_0 + bP_\infty)$. Ainda, esses elementos são linearmente independentes, e portanto formam uma base. Logo, a matriz

$$\begin{pmatrix} 1 & \beta^{-a} & \beta^{-2a} & \dots & (\beta^{n-1})^{-a} \\ 1 & \beta^{-a+1} & \beta^{-2a+2} & \dots & (\beta^{n-1})^{-a+1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{-a+(a+b)} & \beta^{-2a+2(a+b)} & \dots & (\beta^{n-1})^{-a+(a+b)} \end{pmatrix}$$

é uma matriz geradora do código $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)$. Se substituirmos $l = -a$ e $\delta = a+b+2$, obtemos a matriz da definição anterior, o que prova que $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty) = C(n, l, \delta)$.

(b) Usando a notação do lema 3.28, colocamos

$$y := z^{-n} \quad \text{e} \quad h(z) := \prod_{i=1}^{n} \left(z - \beta^{i-1}\right) = z^n - 1.$$

A proposição 3.19 nos diz que $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, B)$, onde

$$\begin{aligned} B =& D_\beta - (aP_0 + bP_\infty) + \langle z^{-n} \rangle + \langle h'(z) \rangle - \langle h(z) \rangle - 2P_\infty \\ =& D_\beta - (aP_0 + bP_\infty) + n(P_\infty - P_0) + (n-1)(P_0 - P_\infty) \\ & - (D_\beta - nP_\infty) - 2P_\infty \\ =& (-a-1)P_0 + (n-b-1)P_\infty. \end{aligned}$$

Como $l = -a$ e $\delta = a+b+2$, pelo item (a), podemos encontrar $C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)$, com $s = n-b-1 = n-(\delta-a-2)-1 = n+1-\delta-l$ e $r = -a-1 = l-1$.

■

Agora, introduzimos os códigos de Goppa, e em seguida, veremos uma versão análoga da proposição 3.31 para esse tipo de código.

Definição 3.32. *Sejam $L = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ com $|L| = n$ e $g(z) \in \mathbb{F}_{q^m}[z]$ um polinômio de grau t com $1 \leq t \leq n-1$ e $g(\alpha_i) \neq 0$, para todo $\alpha_i \in L$.*

(a) Definimos o código $C(L, g(z)) \subseteq (\mathbb{F}_{q^m})^n$ pela matriz geradora

$$H := \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \alpha_2 g(\alpha_2)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} g(\alpha_1)^{-1} & \alpha_2^{t-1} g(\alpha_2)^{-1} & \dots & \alpha_n^{t-1} g(\alpha_n)^{-1} \end{pmatrix}.$$

(b) O código $\Gamma(L, g(z)) := C(L, g(z))^\perp\big|_{\mathbb{F}_q}$ é chamado código de Goppa com polinômio de Goppa $g(z)$, ou seja,

$$\Gamma(L, g(z)) = \left\{ c \in \mathbb{F}_q^n \mid H \cdot c^t = 0 \right\}.$$

Note que a matriz H é um caso especial da matriz do item (a) da proposição 3.25, onde $v_i = g(\alpha_1)^{-1}$, e portanto $C(L, g(z))$ e $C(L, g(z))^{\perp}$ são códigos GRS.

Proposição 3.33. *Utilizando as notações da definição anterior, consideramos P_i o zero de $z - \alpha_i$, para todo $\alpha_i \in L$, P_∞ o polo divisor de z e $D_L = P_1 + \cdots + P_n$. Seja ainda G_0 o zero divisor de $g(z)$, do grupo divisor $F = \mathbb{F}_{q^m}(z)$. Então*

$$C(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty) = C_{\mathcal{L}}(D_L, A - G_0)^{\perp}$$

e

$$\Gamma(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty)^{\perp}\Big|_{\mathbb{F}_q} = C_{\mathcal{L}}(D_L, A - G_0)|_{\mathbb{F}_q},$$

onde A é determinado tomando $h(z) := \prod_{\alpha_i \in L} (z - \alpha_i)$ e definindo $A := \langle h'(z) \rangle + (n-1)P_\infty$.

Demonstração: Como $\Gamma(L, g(z)) := C(L, g(z))^{\perp}\Big|_{\mathbb{F}_q}$, basta provar a primeira igualdade. Para $1 \leq j \leq t-1$, o elemento $z^j g(z)^{-1} \in \mathcal{L}(G_0 - P_\infty)$, uma vez que

$$\left(z^j g(z)^{-1}\right) = j(P_0 - P_\infty) - (G_0 - tP_\infty) \geq -G_0 + P_\infty.$$

Agora,

$$\dim(G_0 - P_\infty) = \deg G_0 - \deg P_\infty + 1 - g = \deg G_0 = t.$$

Assim, os elementos $g(z)^{-1}, zg(z)^{-1}, \ldots, z^{t-1}g(z)^{-1}$ formam uma base para $\mathcal{L}(G_0 - P_\infty)$. Logo, a matriz H da definição de código de Goppa é uma matriz geradora para $C_{\mathcal{L}}(D_L, G_0 - P_\infty)$, e consequentemente

$$C(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty).$$

Ainda, pela proposição 3.19 e pelo lema 3.28, temos $C_{\mathcal{L}}(D_L, G_0 - P_\infty)^{\perp} = C_{\mathcal{L}}(D_L, B)$, onde

$$\begin{aligned} B &= D_L - (G_0 - P_\infty) + (h'(z)) - (h(z)) - 2P_\infty \\ &= D_L - G_0 + P_\infty + A - (n-1)P_\infty - (D_L - nP_\infty) - 2P_\infty \\ &= A - G_0, \end{aligned}$$

o que conclui a demonstração.

■

Encerramos este capítulo com uma consequência de ambas as proposições que demonstramos acima, a qual explicita cotas inferiores para a distância mínima de códigos BCH e de Goppa.

Corolário 3.34. *(a) (Cota de BCH) A distância mínima de um código BCH com distância projetada δ é pelo menos δ.*

(b) (Cota de Goppa) A distância mínima de um código de Goppa $\Gamma(L, g(z))$ é pelo menos $1 + \deg g(z)$.

Demonstração: (a) Usando a notação da proposição 3.31, representamos um código BCH da forma $C = C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)|_{\mathbb{F}_q}$. A distância mínima de um código $C_{\mathcal{L}}(D_\beta, rP_0 + sP_\infty)$ é dada por

$$d = n - \deg(rP_0 + sP_\infty) = n - ((l-1) + (n + 1 - \delta - l)) = \delta,$$

pelas proposições 3.24 e 3.31.

Agora, como a distância mínima da restrição de um código não pode ser menor que a distância mínima do código original, temos que a distância mínima de C é $\geq \delta$.

(b) Representamos $\Gamma(L, g(z))$ como $C\mathcal{L}\left(D_L, A - G_0\right)|_{\mathbb{F}_q}$, como na proposição 3.33, e assim, segue que

$$d = n - \deg\left(A - G_0\right) = n - \left((n-1) - \deg g(z)\right) = 1 + \deg g(z),$$

e a afirmação segue do fato de que a distância mínima de uma restrição não pode ser menor do que a distância mínima do código original.

■

4 Extensões de corpos de funções algébricas

Seja F/K um corpo de funções algébricas. Neste capítulo, estudaremos extensões F'/F de corpos de funções algébricas. Estaremos interessados em relacionar lugares, divisores, diferenciais de Weil e gênero de F e F'. Antes de iniciarmos, vamos fixar algumas notações que serão utilizadas ao longo do capítulo.

Durante este capítulo, F/K denota um corpo de funções algébricas de uma variável, cujo corpo completo das constantes é K. Por sua vez, K será considerado um corpo perfeito, ou seja, toda extensão é separável. Ainda, consideramos F'/K' um corpo de funções, com K' o corpo completo das constantes de F' tais que $F' \supseteq F$ é extensão algébrica e $K' \supseteq K$. Por conveniência, fixamos um corpo algbricamente fechado $\Phi \supseteq F$ e consideramos somente extensões F' de F tais que $F' \subseteq \Phi$.

4.1 Extensões algébricas de corpos de funções

Definição 4.1. *(a) Um corpo de funções algébricas F'/K' é chamado de extensão algébrica de F/K se $F \subseteq F'$ é uma extensão algébrica e $K \subseteq K'$.*

(b) A extensão algébrica F'/K' de F/K é chamada extensão de corpos constante se $F' = FK'$, o corpo compósito de F e K'.

(c) A extensão algébrica F'/K' de F/K é chamada extensão finita se $[F' : F] < \infty$.

O resultado a seguir nos fornece algumas consequências da definição anterior:

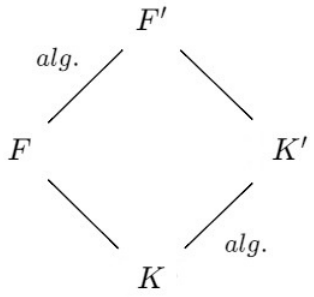
Lema 4.2. *Seja F'/K' uma extensão algébrica de F/K. Então*

(a) K'/K é algébrica e $K' \cap F = K$.

(b) F'/K' é uma extensão finita de $F/K \Leftrightarrow [K' : K] < \infty$.

(c) Seja $F_1 = FK'$. Então F_1/K' é uma extensão de corpos constante de F/K e F'/K' é uma extensão finita de F_1/K'.

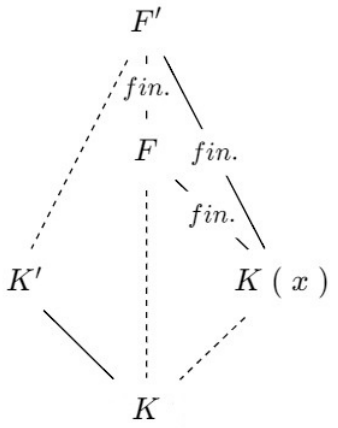
Demonstração: (a) Por hipótese, a extensão F'/F é algébrica, e como F/K tem grau de transcendência igual a 1 (pois K e o corpo completo das constantes de F), segue que a extensão F'/K também tem grau de transcendência igual a 1. Observe o diagrama abaixo:



Por outro lado, a extensão F'/K' também tem grau de transcendência igual a 1, já que K' é o corpo completo das constantes de F'. Assim, o grau de transcendência da extensão K'/K é zero, e ela é portanto algébrica.

Agora, obviamente $K \subseteq K' \cap F$. Resta mostrar a outra inclusão. Seja $\alpha \in F \cap K'$. Então, $\alpha \in K'$, e como K'/K é algébrica, segue que α é algébrico sobre K. Por outro lado, $\alpha \in F$, e como K é o corpo completo das constantes de F, segue $\alpha \in K$, e assim, temos a igualdade $K = K' \cap F$.

(b) Suponha F'/K' uma extensão finita de F/K, ou seja, $[F' : F] < \infty$. Assim, F' pode ser considerada como corpo de funções algébricas sobre K, com K' seu corpo completo das constantes. Veja o diagrama abaixo.



As linhas tracejadas representam extensões de corpos com grau de transcendência igual a 1. Pelo corolário 2.19, segue que $[K' : K] < \infty$.

Reciprocamente, assuma que $[K' : K] < \infty$ (portanto, algébrica) e $x \in F \backslash K$. Então $F'/K'(x)$ é uma extensão de corpos finita, uma vez que x é transcendente sobre K' (se fosse algébrico, x seria algébrico sobre K). Ainda, como $[K' : K]$ é finito, então existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Além disso, da teoria de corpos, segue que α é raiz de algum polinômio $\varphi(t) \in K[t]$, irredutível, com $\deg \varphi(t) = [K' : K]$. Portanto, $K'(x) = K(x)(\alpha)$. Portanto,

$$[K'(x) : K(x)] = [K(x)(\alpha) : K(x)] \leq \deg \varphi(t) = [K' : K].$$

Logo, $[F' : K(x)] = [F' : K'(x)] \cdot [K'(x) : K(x)] < \infty$, e como $K(x) \subseteq F \subseteq F'$, segue que $[F' : F] < \infty$.

(c) Se $F_1 = FK'$, então K' é corpo de constantes de F_1. Como F' é extensão algébrica de F, então FK' também o é. Segue que F_1/K' é extensão algébrica de F/K, e portanto F_1/K' é extensão constante. Agora, como $[K' : K] = 1$, segue do item (b) que $[F' : F_1] \leq \infty$, e isso conclui a demonstração.

■

Nosso objetivo agora é relacionar os lugares de F' com os lugares de F. Para isso, temos a seguinte definição:

Definição 4.3. *Considere F'/K' uma extensão algébrica de F/K. Dizemos que um lugar P' de F'/K' é uma extensão de $P \in \mathbb{P}_F$ se $P \subseteq P'$, e escrevemos $P'|P$.*

Veremos agora como se comportam os lugares de F'/K' em relação aos lugares de F/K, bem como seus anéis de valorização. Além disso, o próximo resultado nos motiva a definição de índice de ramificação, o qual será bastante utilizado no decorrer do capítulo.

Proposição 4.4. *Sejam F'/K' uma extensão algébrica de F/K, P um lugar de F/K, P' um lugar de F'/K', e $\mathcal{O}_P$ e $\mathcal{O}_{P'}$ seus respectivos anéis de valorização. Considere ainda v_P e $v_{P'}$ as respectivas valorizações discretas associadas aos lugares P e P'. Então, são equivalentes:*

(a) $P'|P$;

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

(c) Existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = ev_P(x)$, para todo $x \in F$.

Além disso, se $P'|P$, então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Por essa razão, P também é chamado de restrição de P' para F.

Demonstração: $(a) \Rightarrow (b)$: Suponha $P'|P$ e que $\mathcal{O}_P \nsubseteq \mathcal{O}_{P'}$. Logo, existe $u \in \mathcal{O}_P$ tal que $u \notin \mathcal{O}_{P'}$. Assim, $v_P(u) \geq 0$ e $v_{P'}(u) < 0$. Assim, devemos ter $v_P(u) = 0$, já que $P'|P$.

Escolha $t \in F$ tal que $v_P(t) = 1 > 0$. Assim, $t \in P \subseteq P'$. Defina $r := v_{P'}(t) > 0$. Assim,

$$v_P\left(u^r t\right) = r \cdot v_P(u) + v_P(t) = 1,$$

e

$$v_{P'}\left(u^r t\right) = r \cdot v_{P'}(u) + v_{P'}(t) \leq -r + r = 0,$$

e assim, concluimos que $u^r t \in P \backslash P'$, o que contradiz o fato de P' ser uma extensão de P.

$(b) \Rightarrow (a)$: Provamoes inicialmente a seguinte afirmação.

Afirmação 1: Se $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, então $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$.

Claramente $F \cap \mathcal{O}_{P'}$ é subanel de F, com $\mathcal{O}_P \subseteq F \cap \mathcal{O}_{P'}$. Assim, pelo teorema 2.16, segue que $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$ ou $F \cap \mathcal{O}_{P'} = F$.

Suponha que $F \cap \mathcal{O}_{P'} = F$, ou seja, $F \subseteq \mathcal{O}_{P'}$ e considere $z \in F' \backslash \mathcal{O}_{P'}$. Como a extensão F'/F é algébrica, existem $c_0, c_1, \ldots, c_{n-1} \in F$ tal que

$$z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 = 0.$$

Note que $v_{P'}\left(z^n\right) = n \cdot v_{P'}(z) < 0$ já que $z \notin \mathcal{O}_{P'}$. Logo,

$$v_{P'}\left(z^n\right) < v_{P'}\left(c_\nu z^\nu\right) \quad \text{para} \quad \nu = 0, \cdots, n-1.$$

Agora, pela desigualdade triangular estrita, tem-se

$$v_{P'}\left(z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0\right) = n \cdot v_{P'}(z) \neq v_{P'}(0),$$

o que contradiz o fato de $v_{P'}(z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0) = 0$. Portanto, $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$.

Agora, podemos mostrar a implicação $(b) \Rightarrow (a)$. Seja $a \in P$. Então, pela proposição 2.6, $a^{-1} \notin \mathcal{O}_P = \mathcal{O}_{P'} \cap F$, pela *afirmação 1.* Assim, como $a^{-1} \in F$, segue que $a^{-1} \notin \mathcal{O}_{P'}$, e novamente pela proposição 2.6, segue que $a \in P'$, e portanto, $P'|P$.

$(b) \Rightarrow (c)$: Seja $u \in F$ tal que $v_P(u) = 0$. Logo, como $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, segue que $u, u^{-1} \in \mathcal{O}_{P'}$, e assim, $v_{P'}(u) = 0$.

Escolha agora $t \in F$ tal que $v_P(t) = 1$ e defina $e := v_{P'}(t)$. Como $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, segue que $P \subseteq P'$ pelo que fizemos anteriormente, e assim, $e \geq 1$, pois caso contrário, teríamos $v_{P'}(t) < v_P(t)$, o que não ocorre.

Agora, considere $0 \neq x \in F$ e defina $v_P(x) := r \in \mathbb{Z}$. Então,

$$v_P(xt^{-r}) = v_P(x) - rv_P(t) = 0,$$

e assim,

$$v_{P'}(x) = v_{P'}(xt^{-r}t^r) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + rv_{P'}(t) = e \cdot v_P(x).$$

$(c) \Rightarrow (b)$ Nesse caso, supondo a existência de e, para cada $x \in F$,

$$x \in \mathcal{O}_P \Rightarrow v_P(x) \geq 0 \Rightarrow v_{P'}(x) = e \cdot v_P(x) \geq 0 \Rightarrow v_{P'}(x) \geq 0 \Rightarrow x \in \mathcal{O}_{P'}.$$

Portanto, $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

Provadas as equivalências, observe que, na demonstração de $(b) \Rightarrow (a)$, mostramos ainda que $\mathcal{O} \subseteq F \cap \mathcal{O}_{P'}$. Agora, supondo válida qualquer uma das hipóteses $(a), (b)$ e (c), vamos mostrar que $P = P' \cap F$. Como $P \subset F$ e $P \subseteq P'$, então $P \subseteq P' \cap F$.

De (c), segue que $P' \cap F \subset P$, pois dado $z \in P' \cap F$, temos

$$v_{P'}(z) > 0 \Rightarrow v_{P'}(z) = e \cdot v_P(z) > 0 \Rightarrow z \in P,$$

e assim, vale a igualdade desejada.

■

Uma consequência da proposição anterior é que, se $P'|P$, então existe uma injeção canônica

$$\varphi : \begin{cases} F_P \longrightarrow F_{P'} \\ x(P) \longmapsto x(P') \end{cases},$$

onde $x \in \mathcal{O}_P$. A aplicação φ está bem definida e é injetora, pois dado $x \in \mathcal{O}_P$ tal que $\varphi(x(P)) = 0$,

$$x\,(P') = \varphi(x(P)) = 0 \Rightarrow x \in P' \Rightarrow x \in P' \cap F = P \Rightarrow x(P) = 0.$$

Assim, F_P pode ser visto como subcorpo de $F'_{P'}$.

Agora, podemos definir dois conceitos importantes para a teoria que será desenvolvida neste capítulo: o índice de ramificação e o grau relativo de $P'|P$.

Definição 4.5. *Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ tal que $P'|P$, onde $P \in \mathbb{P}_F$.*

(a) O inteiro $e := e(P'|P)$ tal que $v_{P'}(x) = e \cdot v_P(x)$, para todo $x \in F$ é chamado de índice de ramificação de P' sobre P. Ainda, dizemos que $P'|P$ é ramificada se $e > 1$ e não ramificada se $e = 1$.

(b) $f\,(P' \mid P) := [F'_{P'} : F_P]$ é chamado de grau relativo de P' sobre P.

Proposição 4.6. *Sejam F'/K' uma extensão algébrica de F/K e $P'|P$, onde $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$. Então*

(a) $f\,(P' \mid P) < \infty \Longleftrightarrow [F' : F] < \infty$.

(b) Se considerarmos uma outra extensão, F''/K'' de F'/K', valem as igualdades:

$$e\left(P'' \mid P\right) = e\left(P'' \mid P'\right) \cdot e\left(P' \mid P\right)$$

e

$$f\left(P'' \mid P\right) = f\left(P'' \mid P'\right) \cdot f\left(P' \mid P\right).$$

Demonstração: (a) Pelo lema 4.2, temos que $[F' : F]$ é finito se, e somente se, $[K' : K]$ também o é. Ainda, temos $[F'_{P'} : K'] = \deg\left(P'\right) < \infty$ e $[F_P : K] = \deg(P) < \infty$.

Agora, consideramos as extensões $K \subseteq F_P \subseteq F'_{P'}$ e $K \subseteq K' \subseteq F'_{P'}$. Assim, temos

$$\deg P' \cdot [K' : K] = \deg P \cdot f(P'|P),$$

e o resultado segue imediatamente.

(b) Ambas as igualdade seguem diretamente da definição anterior, bastando aplicá-las duas vezes, uma para cada extensão.

■

Na próxima proposição, veremos a relação entre os lugares de F e F'.

Proposição 4.7. *Seja F'/K' uma extensão algébrica de F/K. Então:*

(a) Para cada lugar P' de F'/K', existe exatamente um lugar P de F/K tal que $P'|P$, com $P = P' \cap F$.

(b) Reciprocamente, todo lugar $P \in \mathbb{P}_F$ tem pelo menos uma, e no máximo um número finito de extensões $P' \in \mathbb{P}_{F'}$.

Demonstração: Antes de provarmos cada um dos itens, vamos provar a seguinte afirmação:

Afirmação 1: Existe $z \in F$ não nulo tal que $v_{P'}(z) \neq 0$.

Suponha que a afirmação seja falsa, ou seja, $v_{P'}(z) = 0$, para todo $z \in F$ e escolha $t \in F'$ uma parâmetro local, isto é, $v'_P(t) > 0$.

Como F'/F é algébrica, existem $c_i \in F$, com $i = 0, 1, \ldots n-1$ tais que

$$t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 = 0,$$

onde $c_0 \neq 0$ e n de grau mínimo. Por hipótese, $v_{P'}(c_i) = 0$, para todo $i = 0, \ldots, n-1$. Agora,

$$v_{P'}\left(t^n\right) > v_{P'}\left(c_i t^i\right) > v_{P'}\left(c_j t^j\right), \quad 0 \leq j < i \leq n-1.$$

Por outro lado, pela desigualdade triangular estrita, temos

$$v_{P'}(0) = v_{P'}\left(t^n + c_{n-1}t^{n-1} + \cdots + c_0\right) = v_{P'}\left(c_0\right) = 0,$$

o que contradiz o que fizemos acima. Logo, a afirmação é válida.

(a) Defina $\mathcal{O} := \mathcal{O}_{P'} \cap F$ e $P := P' \cap F$. Pela *afirmação 1*, $\mathcal{O}$ é um anel de valorização de F/K, pois $K \subsetneqq \mathcal{O} \subsetneqq F$, e dado $z \in F$, podemos ter $z \in \mathcal{O}_{P'}$ ou $z \notin \mathcal{O}_{P'}$.

Se $z \in \mathcal{O}_{P'}$, então $z \in \mathcal{O}_{P'} \cap F = \mathcal{O}$. Por outro lado, se $z \notin \mathcal{O}_{P'}$, então $z^{-1} \in \mathcal{O}_{P'}$. Assim, $z^{-1} \in F \cap \mathcal{O}_{P'} = \mathcal{O}$.

Concluimos que $\mathcal{O}$ é de valorização e o lugar correspondente é $P = P' \cap F$. A unicidade segue do fato de P ser maximal.

(b) Seja P um lugar de F/K. Pela proposição 2.71, podemos escolher $x \in F/K$ tal que o único zero é P.

Afirmação: Dado $P' \in \mathbb{P}_{F'}$, temos $P'|P \Leftrightarrow v_{P'}(x) > 0$.

Se $P'|P$, então $v_{P'}(x) = e(P'|P) \cdot v_P(x) > 0$. Reciprocamente, se $v_{P'}(x) > 0$, denote por Q o lugar de F/K tal que $Q \subseteq P'$, o qual existe pelo item (a). Então $v_Q(x) > 0$, ou seja, $P = Q$, uma vez que tomamos P como o único zero de x em F/K, e assim, $P'|P$.

Assim, como x tem no mínimo um, mas no máximo um número finito de zeros em F'/K', o item (b) segue como consequência da afirmação acima.

■

Definição 4.8. *Seja F'/K' uma extensão algébrica de F/K. Dado $P \in \mathbb{P}_F$, definimos sua conorma em relação a F'/F por*

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e\left(P' \mid P\right) \cdot P'.$$

Pela proposição 4.7, podemos definir um homomorfismo entre os grupos divisores $\mathrm{Div}(F)$ e $\mathrm{Div}(F')$. Com isso, a definição de conorma pode ser estendida a um homomorfismo como citado acima, da forma:

$$\mathrm{Con}_{F'/F}\left(\sum n_P \cdot P\right) := \sum n_P \cdot \mathrm{Con}_{F'/F}(P).$$

Agora, pela proposição 4.6, se tivermos extensões $F \subseteq F' \subseteq F''$, vale a fórmula

$$\mathrm{Con}_{F''/F}(A) = \mathrm{Con}_{F''/F'}\left(\mathrm{Con}_{F'/F}(A)\right), \quad \forall A \in \mathrm{Div}(F).$$

O primeiro resultado envolvendo a conorma de um lugar P, nos garante que ela leva divisores principais de F em divisores principais de F', via homomorfismo.

Proposição 4.9. *Seja F'/K' uma extensão algébrica de F/K. Dado $0 \neq x \in F$, denote por $\langle x\rangle_0^F$, $\langle x\rangle_\infty^F$ e $\langle x\rangle^F$ o divisor zero, polo e principal de x em $\mathrm{Div}(F)$, respectivamente, e $\langle x\rangle_0^{F'}$, $\langle x\rangle_\infty^{F'}$ e $\langle x\rangle^{F'}$ o divisor zero, polo e principal de x em $\mathrm{Div}(F')$, respectivamente. Então,*

$$\mathrm{Con}_{F'/F}\left(\langle x\rangle_0^F\right) = \langle x\rangle_0^{F'}, \mathrm{Con}_{F'/F}\left(\langle x\rangle_\infty^F\right) = \langle x\rangle_\infty^{F'}, \text{ e } \mathrm{Con}_{F'/F}\left(\langle x\rangle^F\right) = \langle x\rangle^{F'}.$$

Demonstração: Vamos mostrar somente a igualdade envolvendo o divisor principal pois as igualdades envolvendo o divisor zero e o divisor polo podem ser demonstradas analogamente, considerando-se somente a parte positiva e a parte negativa, respectivamente.

Pela definição de divisor principal, temos

$$\begin{aligned}
\langle x\rangle^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x) \cdot P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e\left(P' \mid P\right) \cdot v_P(x) \cdot P' \\
&= \sum_{P \in \mathbb{P}_F} v_P(x) \cdot \mathrm{Con}_{F'/F}(P) = \mathrm{Con}_{F'/F}\left(\sum_{P \in \mathbb{P}_F} v_P(x) \cdot P\right) \\
&= \mathrm{Con}_{F'/F}\left(\langle x\rangle^F\right).
\end{aligned}$$

■

Pela proposição anterior, a conorma induz um homomorfismo dado por

$$\mathrm{Con}_{F'/F} : \begin{cases} \mathrm{Cl}(F) \longrightarrow \mathrm{Cl}(F) \\ [D] \longmapsto [\mathrm{Con}_{F'/F}(D)] \end{cases}.$$

Essa aplicação está bem definida, uma vez que, dados divisores A e B com $[A] = [B]$, existe $0 \neq x \in F$ tal que $A = B + \langle x \rangle^F$. Assim, pela proposição 4.9,

$$\begin{aligned}\mathrm{Con}_{F'/F}([A]) &= \left[\mathrm{Con}_{F'/F}(A)\right] = \left[\mathrm{Con}_{F'/F}\left(B + \langle x \rangle^F\right)\right] = \\ &= \left[\mathrm{Con}_{F'/F}(B) + \langle x \rangle^{F'}\right] = \left[\mathrm{Con}_{F'/F}(B)\right] = \mathrm{Con}_{F'/F}([B]).\end{aligned}$$

Em geral, essa aplicação não é injetora nem sobrejetora, enquanto a aplicação $\mathrm{Con}_{F'/F} : \mathrm{Div}(F) \to \mathrm{Div}\,(F')$ é injetora.

Lema 4.10. *Sejam K'/K uma extensão de corpos finita e x transcendente sobre K. Então,*

$$[K'(x) : K(x)] = [K' : K]\,.$$

Demonstração: Já mostramos no lema 4.2 que $[K'(x) : K(x)] \leq [K' : K]$. Mostremos agora a outra desigualdade.

Como K'/K é finita, então existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Vamos mostrar que o polinômio minimal $\varphi(t) \in K[t]$ de α sobre K continua irredutível sobre $K(x)$. Suponha que isso não é válido e escreva $\varphi(t) = g(t) \cdot h(t)$, com $g(t), h(t) \in K(x)[t]$ polinômios mônicos com grau $< \deg \varphi$.

Como $\varphi(\alpha) = 0$, podemos supor sem perda de generalidade que $g(\alpha) = 0$. Escreva

$$g(t) = t^r + c_{r-1}(x)t^{r-1} + \cdots + c_1(x)t + c_0(x),\ c_i(x) \in K(x) \text{ e } r < \deg \varphi.$$

Então $\alpha^r + c_{r-1}(x)\alpha^{r-1} + \cdots + c_0(x) = 0$. Multiplicando por um denominador comum, obtemos

$$g_r(x)\alpha^r + g_{r-1}(x)\alpha^{r-1} + \cdots + g_0(x) = 0,$$

para certos $g_i(x) \in K[x]$, e podemos assumir que nem todos os $g_i(x)$'s são divisíveis por x. Colocando $x = 0$ na última igualdade, obtemos uma equação não trivial para α sobre K de grau $< \deg \varphi$, o que contradiz o fato de φ ser o minimal de α sobre K. Portanto, $[K' : K] \leq [K'(x) : K(x)]$, e segue a igualdade.

■

O seguinte teorema irá relacionar o grau da extensão F'/F com o índice de ramificação e o grau relativo de um lugar P' sobre P.

Teorema 4.11. *(Igualdade fundamental) Sejam F'/K' uma extensão finita de F/K, $P \in \mathbb{P}_F$ e $P_1, \ldots, P_m$ todos os lugares de F'/K' que estendem P. Sejam ainda $e_i := e(P_i|P)$ e $f_i := f(P_i|P)$. Então*

$$\sum_{i=1}^{m} e_i f_i = [F' : F]\,.$$

Demonstração: Escolha $x \in F$ tal que P é o único zero de x em F/K e defina $v_P(x) := r > 0$. Assim, os lugares $P_1, \ldots, P_m$ são exatamente os zeros de x em F'/K', uma vez que $P'|P \Leftrightarrow v_{P'}(x) > 0$.

Observe que $[F' : K(x)] = [F' : K'(x)] \cdot [K'(x) : K(x)]$. Agora, do lema 4.10, temos $[K'(x) : K(x)] = [K' : K]$, e assim,

$$[F' : K(x)] = [F' : K'(x)] \cdot [K' : K].$$

Por outro lado,

$$[F' : K'(x)] = \sum_{i=1}^{m} v_{P_i}(x) \cdot \deg P_i = \sum_{i=1}^{m} (e_i \cdot v_P(x)) \cdot \left[F'_{P_i} : K'\right].$$

Logo,

$$\begin{aligned}[F' : K(x)] &= \sum_{i=1}^{m} (e_i \cdot v_P(x)) \cdot \left(\left[F'_{P_i} : K'\right] \cdot [K' : K]\right) \\ &= r \cdot \sum_{i=1}^{m} e_i \cdot \left[F'_{P_i} : F_P\right] \cdot [F_P : K] \\ &= r \cdot \deg P \cdot \sum_{i=1}^{m} e_i f_i.\end{aligned}$$

Como rP é o zero divisor de x em F/K, segue que $[F : K(x)] = r \deg P$, e

$$[F' : K(x)] = [F' : F] \cdot [F : K(x)] = [F' : F] \cdot r \cdot \deg P.$$

Comparando as duas igualdade, obtemos a igualdade fundamental desejada.

■

Definição 4.12. *Sejam F'/K' uma extensão finita de F/K com $[F' : F] = n$ e $P \in \mathbb{P}_F$.*

(a) Dizemos que P se decompõe completamente em F'/F se existem exatamente n lugares distintos $P' \in F'/K'$ tais que $P'|P$.

(b) Dizemos que P é totalmente ramificado em F'/F se existe $P' \in \mathbb{P}_{F'}$ com $P'|P$ e $e(P'|P) = n$.

Segue diretamente do teorema 4.11 que P se decompõe completamente em F'/F se, e somente se, $e\,(P' \mid P) = f\,(P' \mid P) = 1$, para toda extensão P' de P. Ainda, se P é totalmente ramificado, então existe um único lugar P' de F'/K' que estende P.

Uma outra consequência da igualdade fundamental é o corolário a seguir, o qual nos fornece uma relação entre o grau de um divisor A e o grau da sua conorma.

Corolário 4.13. *Sejam F'/K' uma extensão finita de F/K e $A \in \mathrm{Div}(F)$. Então,*

$$\deg \mathrm{Con}_{F'/F}(A) = \frac{[F' : F]}{[K' : K]} \cdot \deg A.$$

Demonstração: Vamos mostrar inicialmente para o caso em que A é um divisor primo

P. Segue que

$$\begin{aligned}
\deg \mathrm{Con}_{F'/F}(P) &= \deg\left(\sum_{P'|P} e\left(P' \mid P\right)\cdot P'\right)\\
&= \sum_{P'|P} e\left(P' \mid P\right)\cdot [F'_{P'} : K']\\
&= \sum_{P'|P} e\left(P' \mid P\right)\cdot \frac{[F'_{P'} : K]}{[K' : K]}\\
&= \frac{1}{[K' : K]}\cdot \sum_{P'|P} e\left(P' \mid P\right)\cdot [F'_{P'} : F_P]\cdot [F_P : K]\\
&= \frac{1}{[K' : K]}\cdot \left(\sum_{P'|P} e\left(P' \mid P\right)\cdot f\left(P' \mid P\right)\right)\cdot \deg P\\
&= \frac{[F' : F]}{[K' : K]}\cdot \deg P \quad \text{(pelo teorema 4.11).}
\end{aligned}$$

No caso em que A é um divisor qualquer, escrevermos $A = \sum n_P P$. Agora, como

$$\mathrm{Con}_{F'/F}\left(\sum n_P P\right) = \sum n_P \,\mathrm{Con}_{F'/F}(P)$$

e

$$\deg\left(\sum n_P P\right) = \sum n_P \deg(P),$$

podemos aplicar o caso particular feito anteriormente, e o resultado segue.

■

4.2 Subanéis de corpos de funções

Como na seção anterior, F/K denota um corpo de funções com corpo constante K. Vamos agora introduzir a definição de subanel de um corpo de funções, o qual será importante para definirmos posteriormente anel holomórfico.

Definição 4.14. *Um subanel de F/K é um anel R tal que $K \subseteq R \subseteq F$ e R não é corpo.*

Em particular, se R é um subanel de F/K, então $K \subsetneqq R \subsetneqq F$. Apresentamos dois exemplos clássicos de subanéis de corpos de funções.

(a) $R = \mathcal{O}_P$, com $P \in \mathbb{P}_F$.

(b) $R = K[x_1, \ldots, x_n]$, com $x_1, \ldots, x_n \in F \backslash K$.

Claramente o exemplo do item (a) é um subanel, pela definição de $\mathcal{O}_P$. Para vermos que $K[x_1, \ldots, x_n]$ é subanel de F/K, basta verificar que não é corpo.

Escolha $P \in \mathbb{P}_F$ tal que $v_P\left(x_1\right) \geq 0, \ldots, v_P\left(x_n\right) \geq 0$. Seja $x = x_1$ e $d := \deg P = [F_P : K]$. Assim, as classes residuais $1, x(P), \ldots, x^d(P) \in \mathcal{O}_P/P$ são linearmente dependentes, e existirão $\alpha_0, \ldots, \alpha_d \in K$ tais que $z = \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d$ e $v_P(z) > 0$.

Como $x \notin K$, então x é transcendente sobre K. Obviamente $z \in K[x_1, \ldots, x_n]$ mas $z^{-1} \notin K[x_1, \ldots, x_n]$, uma vez que $v_P(y) \geq 0$, para todo $y \in K[x_1, \ldots, x_n]$ e $v_P(z^{-1}) < 0$. Portanto $K[x_1, \ldots x_n]$ não é corpo.

Definição 4.15. *Dado $\emptyset \neq S \subseteq \mathbb{P}_F$, seja $\mathcal{O}_S := \{z \in F \mid v_P(z) \geq 0$ para todo $P \in S\}$ a interseção de todos os anéis de valorizações $\mathcal{O}_P$ com $P \in S$. Um anel $R \subseteq F$ da forma $R = \mathcal{O}_S$ para $\emptyset \neq S \subsetneqq \mathbb{P}_F$ é chamado anel holomórfico.*

Por hora, consideramos que o anel $K[x]$ é um anel holomórfico do corpo de funções racional $K(x)/K$, basta verificarmos que

$$K[x] = \bigcap_{P \neq P_\infty} \mathcal{O}_P,$$

onde P_∞ denota o único polo de x em $K(x)$.

O próximo resultado é um lema que nos fornece algumas propriedades desses anéis e será usado nas demonstrações futuras. Uma delas, é que esses anéis são unicamente determinados pelo conjunto S.

Lema 4.16. *(a) Todo anel de valorização $\mathcal{O}_P$ é um anel holomórfico, onde $\mathcal{O}_P = \mathcal{O}_S$, com $S = \{P\}$.*

(b) Todo anel holomórfico $\mathcal{O}_S$ é um subanel de F/K.

(c) Para $P \in \mathbb{P}_F$ e $\emptyset \neq S \subsetneqq \mathbb{P}_F$, tem-se

$$\mathcal{O}_S \subseteq \mathcal{O}_P \Longleftrightarrow P \in S.$$

Consequentemente, $\mathcal{O}_S = \mathcal{O}_T \Longleftrightarrow S = T$.

Demonstração: (a) imediato da definição.

(b) Como $K \subseteq \mathcal{O}_S \subseteq F$, basta verificar que $\mathcal{O}_S$ não é corpo. Seja $P_1 \in S$. Do teorema da aproximação forte, existe $0 \neq x \in F$ tal que

$$v_{P_1}(x) > 0 \quad \text{e} \quad v_P(x) \geq 0 \quad \text{para todo} \quad P \in S.$$

Assim, $x \in \mathcal{O}_S$ pois $v_P(x) \geq 0$, para todo $P \in S$, mas $x^{-1} \in \mathcal{O}_S$, pois $v_{P_1}(x^{-1}) = -v_{P_1}(x) < 0$. Logo, $\mathcal{O}_S$ não é corpo.

(c) Suponha $P \notin S$. Novamente, pelo teorema da aproximação forte, existe $z \in F$ com

$$v_P(z) < 0 \quad \text{e} \quad v_Q(z) \geq 0 \quad \text{para todo} \quad Q \in S.$$

Se $S \cup \{P\} \neq \mathbb{P}_F$, isso é sempre válido. Se $S \cup \{P\} = \mathbb{P}_F$, basta tomar $z \in \mathcal{O}_S$ com pelo menos um zero em S, e como z deve ter algum polo, segue que $v_P(z) < 0$.

Agora, cada elemento z satisfazendo $v_Q(z) \geq 0$ está em $\mathcal{O}_S$, mas não está em $\mathcal{O}_P$, o que é absurdo da hipótese. Logo, $P \in S$.

Reciprocamente, suponha que $P \in S$ e seja $z \in \mathcal{O}_S$. Então $v_P(z) \geq 0$. Logo, $z \in \mathcal{O}_P$, e segue que $\mathcal{O}_S \subseteq \mathcal{O}_P$.

■

Definição 4.17. *Seja R um subanel de F/K.*

(a) Um elemento $z \in F$ é dito inteiro ou integral sobre R se $f(z) = 0$ para algum polinômio mônico $f(x) \in R[x]$. Isto é, existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0.$$

Essa equação é chamada de equação integral ou equação inteira para z sobe R.

(b) O conjunto $\mathrm{ic}_F(R) := \{z \in F \mid z$ é inteiro sobre $R\}$ é chamado fecho integral de R em F.

(c) Seja $F_0 \subseteq F$ o corpo de frações de R. O anel R é dito integralmente fechado se $\mathrm{ic}_F(R) = R$.

O próximo resultado relaciona os conceitos de anel holomórfico e ser integralmente fechado.

Proposição 4.18. *Seja $\mathcal{O}_S$ um anel holomórfico de F/K. Então*
(a) F é o corpo de frações de $\mathcal{O}_S$.
(b) $\mathcal{O}_\mathcal{S}$ é integralmente fechado.

Demonstração: (a) Sejam $0 \neq x \in F$ e P_0 um lugar. Pelo teorema da aproximação forte, existe $z \in F$ tal que $v_{P_0}(z) = \max\{0, v_{P_0}(x^{-1})\}$ e $v_P(z) \geq \max\{0, v_P(x^{-1})\}$ para todo $P \in S$.

Claramente $z \in \mathcal{O}_S$, uma vez que $v_P(z) \geq 0$, para todo $P \in S$. Além disso, como $z \neq 0$, defina $y := zx$, e assim, $y \in \mathcal{O}_S$, visto que $v_P(y) = v_P(x) + v_P(z) \geq 0$.

Logo, $x = yz^{-1}$ pertence ao corpo de frações de $\mathcal{O}_S$, o que prova o item (a).

(b) Seja $u \in F$ inteiro sobre $\mathcal{O}_S$ e escreva $u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$, com $a_i \in \mathcal{O}_S$. Precisamos mostrar que $v_P(u) \geq 0$, para todo $P \in S$, e teremos $u \in \mathcal{O}_S$.

Suponha que isto seja falso, ou seja, que exista $P \in S$ com $v_P(u) < 0$. Como $a_i \in \mathcal{O}_S$, para todo i, então $v_P(a_i) \geq 0$. Logo,

$$v_P(u^n) = nv_P(u) < iv_P(u) \leq iv_P(u) + v_P(a_i) = v_P(a_i u^i), \text{ para todo } i = 0, \ldots, n-1.$$

Assim, pela desigualdade triangular estrita, segue que $v_P(u) = 0$, o que contradiz a suposição de $v_P(u) < 0$. Portanto, $\mathcal{O}_S$ é integralmente fechado.

■

Teorema 4.19. *Seja R um subanel de F/K e $S(R) := \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$. Então,*
(a) $\emptyset \neq S(R) \subsetneqq \mathbb{P}_F$.
(b) O fecho integral de R em F é $\mathrm{ic}_F(R) = \mathcal{O}_{S(R)}$. Em particular, $\mathrm{ic}_F(R)$ é um anel integralmente fechado de F/K com corpo de frações F.

Demonstração: (a) Como R não é corpo, existe um ideal $I \subsetneqq R$ próprio, e pelo teorema 2.22, existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Então, $S(R) \neq \emptyset$.

Agora, seja $x \in R$ transcendente. Cada lugar $Q \in \mathbb{P}_F$ que é polo de x, não pertence a $S(R)$, logo $S(R) \neq \mathbb{P}_F$.

(b) Note que $R \subseteq \mathcal{O}_{S(R)}$ e $\mathcal{O}_{S(R)}$ é integralmente fechado pela proposição 4.18, e segue que $\mathrm{ic}_F(R) \subseteq \mathcal{O}_{S(R)}$.

Agora, seja $z \in \mathcal{O}_{S(R)}$. Afirmamos que $z^{-1} \cdot R[z^{-1}] = R[z^{-1}]$. Suponhamos que isso não é valido. Assim, pelo teorema 2.22, existe $Q \in \mathbb{P}_F$ tal que $R[z^{-1}] \subset \mathcal{O}_Q$ e $z^{-1} \in Q$. Logo, $Q \in S(R)$ e $z \notin \mathcal{O}_Q$, o que contradiz o fato de $z \in \mathcal{O}_{S(R)}$.

Logo $1 - z^{-1}\sum_{i=0}^{s} a_i(z^{-1})^i = 0$, $a_0, \ldots, a_s \in R$. Multiplicando por z^{s+1},

$$z^{s+1} - \sum_{i=0}^{s} a_i z^{s-i} = 0.$$

Logo, z é integral sobre R, o que implica que $\mathcal{O}_{S(\mathcal{R})} \subseteq \mathrm{ic}_F(R)$, e disso segue o item (b).

■

Como consequência desse teorema, o seguinte corolário segue de forma imediata, e este relaciona os conceitos de ser integralmente fechado e ser um anel holomórfico.

Corolário 4.20. *Um subanel R de F/K com corpo de frações F é integralmente fechado se, e somente se, R é um anel holomórfico.*

O próximo resultado nos garante a existência de uma injeção entre o conjunto S e o conjunto dos ideais maximais de $\mathcal{O}_S$.

Proposição 4.21. *Seja $\mathcal{O}_S$ um anel holomórfico. Então existe uma injeção entre S e o conjunto dos ideais maximais de $\mathcal{O}_S$ dado por $P \longmapsto M_P := P \cap \mathcal{O}_S$, $P \in S$.*

Mais ainda, a aplicação

$$\varphi : \begin{cases} \mathcal{O}_S/M_P \longrightarrow F_P = \mathcal{O}_P/P \\ x + M_P \longmapsto x + P \end{cases}$$

é um isomorfismo.

Demonstração: Seja $P \in S$ e considere o homomorfismo de anéis

$$\phi : \begin{cases} \mathcal{O}_S & \longrightarrow F_P \\ x & \longmapsto x + P \end{cases}.$$

Afirmamos que ϕ é sobrejetora. Seja $z + P \in F_P$, com $z \in \mathcal{O}_P$. Pelo teorema da aproximação forte, existe $x \in F$ com $v_P(x - z) > 0$ e $v_Q(x) \geq 0$, para todo $Q \in S \backslash \{P\}$. Assim, $x \in \mathcal{O}_S$ e $\phi(x) = x + P = z + P$, uma vez que $x - z \in P$, e isso prova a sobrejetividade. É fácil ver que $\ker \phi = \mathcal{O}_S \cap P$.

Defina $M_P := \mathcal{O}_S \cap P$. Assim, ϕ induz um isomorfismo $\varphi : \mathcal{O}_S/M_P \to F_P$. Como F_P é corpo, segue que M_P é maximal. Se $P \neq Q$, o teorema da aproximação fraca garante que $M_P \neq M_Q$.

Resta mostrar que todo ideal maximal de $\mathcal{O}_S$ pode ser escrito como $P \cap \mathcal{O}_S$, com $P \in S$. Seja $M \subseteq \mathcal{O}_S$ um ideal maximal. Pelo teorema 2.22, existe $P \in \mathbb{P}_F$ com $M \subseteq P$ e $\mathcal{O}_S \subseteq \mathcal{O}_P$. Agora, pelo lema 4.16, item (c), segue que $P \in S$. Como $M \subseteq P \cap \mathcal{O}_\mathcal{S}$ e M é ideal maximal de $\mathcal{O}_S$, obtemos $M = P \cap \mathcal{O}_S$.

■

Terminamos essa seção mostrando que o anel $\mathcal{O}_S$ é um domínio principal, em um caso específico.

Proposição 4.22. *Se $S \subseteq \mathbb{P}_F$ é um conjunto finito e não vazio de lugares de F/K, então $\mathcal{O}_S$ é um domínio principal.*

Demonstração: Seja $S = \{P_1, \ldots, P_s\}$ e considere $\{0\} \neq I \subseteq \mathcal{O}_S$ um ideal de $\mathcal{O}_S$. Para $i = 1, \ldots, s$, escolha $x_i \in I$ tal que

$$v_{P_i}(x_i) =: n_i \leq v_{P_i}(u) \quad \text{para todo} \quad u \in I,$$

o que é possível uma vez que $v_{P_i}(u) \geq 0$, para todo $u \in I$. Pelo teorema da aproximação forte, existe $z_i \in F$ tal que

$$v_{P_i}(z_i) = 0 \quad \text{e} \quad v_{P_j}(z_i) > n_j \quad \text{para} \quad j \neq i.$$

Como $z_i \in \mathcal{O}_S$, então $x := \sum_{i=1}^{s} x_i z_i \in I$. Pela desigualdade triangular estrita, temos $v_{P_i}(x) = n_i$, para $i = 1, \ldots, s$.

Nosso objetivo é mostrar que $I \subseteq \mathcal{O}_S$, ou seja, teremos I principal. Seja $z \in I$ e defina $y := x^{-1}z$. Então

$$v_{P_i}(y) = v_{P_i}(x^{-1}z) = v_{P_i}(z) - v_{P_i}(x) = v_{P_i}(z) - n_i \geq 0, \quad i = 1, \ldots, s.$$

Portanto, $y \in \mathcal{O}_S$, e $z = xy \in x\mathcal{O}_S$, o que conclui a demonstração.

■

4.3 Bases integrais locais

Nesta seção investigaremos o fecho integral de um subanel de F/K. Sempre F/K denotará novamente um corpo de funções algébricas com corpo das constantes K, $F' \supseteq F$ uma extensão de corpos finita, e o corpo das constantes é K'.

O primeiro resultado nos fornece uma condição necessária e suficiente para que um elemento seja inteiro sobre um anel R.

Proposição 4.23. *Seja R um subanel integralmente fechado de F/K tal que F é o corpo de funções de R. Dado $z \in F'$ considere $\varphi(t) \in F[t]$ seu polinômio minimal sobre F. Então*

$$z \text{ é inteiro sobre } R \Leftrightarrow \varphi(t) \in R[t].$$

Demonstração: Suponhamos primeiramente que $\varphi(t) \in R[t]$. Por definição $\varphi(t)$ é o único polinômio mônico irredutível com coeficientes em F tal que $\varphi(z) = 0$. Como $\varphi(t) \in R[t]$, então claramente z é inteiro sobre R.

Para a recíproca, utilizaremos o fato de que R é integralmente fechado. Seja $z \in F'$ inteiro sobre R e considere $f(t) \in R[t]$ seu polinômio minimal. Como $\varphi(t)$ é seu polinômio minimal sobre F, então claramente $\varphi \mid f$, ou seja, existe $\psi(t) \in F[t]$ tal que $\varphi(t)\psi(t) = f(t)$.

Agora, considere $F'' \supseteq F'$ uma extensão finita de F contendo todas as raízes de φ e $R'' = \mathrm{ic}_{F''}(R)$ o fecho integral de R sobre F''. Como toda raiz de φ é também uma raiz de f, essas raízes estão em R''. Agora, os coeficientes de $\varphi(t)$ são expressões polinomiais das raízes de φ, e portanto $\varphi(t) \in R''[t]$. Por outro lado, temos $\varphi(t) \in F[t]$ e $F \cap R'' = R$, já que R é integralmente fechado. Logo, $\varphi(t) \in R[t]$.

■

Vamos agora recordar a definição e algumas propriedades da aplicação traço. Considere inicialmente uma extensão finita M/L de grau n. Se M/L não for separável, a aplicação traço $\mathrm{Tr}_{M/L} : M \to L$ será a aplicação nula. Para isso, assumimos que a extensão é separável. Escolha agora, um corpo algebricamente fechado $\Psi \supseteq L$. Uma injeção de M/L em Ψ é um homomorfismo de corpos $\sigma : M \to \Psi$ tal que $\sigma(a) = a$, para todo $a \in L$. Como M/L é separável, existem exatamente n injeções distintas $\sigma_1, \ldots, \sigma_n$ de M/L em Ψ. Assim, dado $x \in M$ definimos

$$\mathrm{Tr}_{M/L}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

Se $\varphi(t) = t^r + a_{r-1}t^{r-1} + \cdots + a_0 \in L[t]$ for o minimal de x sobre L, então $\mathrm{Tr}_{M/L}(x) = -sa_{r-1}$, onde $s := [M : L(x)]$.

Além disso, a aplicação traço funciona bem quando temos uma cadeia de extensões, isto é, dadas extensões de corpos $L \subseteq M \subseteq H$, vale a igualdade

$$\mathrm{Tr}_{H/L}(x) = \mathrm{Tr}_{M/L}\left(\mathrm{Tr}_{H/M}(x)\right).$$

Como consequência da construção acima e da proposição 4.23, temos o corolário a seguir.

Corolário 4.24. *Nas mesmas notações da proposição 4.23, considere a aplicação* $\mathrm{Tr}_{F'/F}$ *e* $x \in F'$ *inteiro sobre* R. *Então* $\mathrm{Tr}_{F'/F}(x) \in R$.

Proposição 4.25. *Sejam* M/L *um extensão finita e separável e* $\{z_1, \ldots, z_n\}$ *base de* M/L. *Então existem elementos* $z_1^*, \ldots, z_n^* \in M$ *unicamente determinados, tais que*

$$\mathrm{Tr}_{M/L}\left(z_i z_j^*\right) = \delta_{ij},$$

onde δ_{ij} *denota o símbolo de Kronecker. Nesse caso* $\{z_1^*, \ldots, z_n^*\}$ *é uma base de* M/L, *que é dual a* $\{z_1, \ldots, z_n\}$.

Demonstração: Considere $M^\wedge$ o espaço dual de M, ou seja, $M^\wedge = \{\lambda : M \to L \mid \lambda \text{ é } L - \text{linear}\}$. Da álgebra linear, sabemos que $M^\wedge$ tem dimensão n como L-espaço vetorial. Agora, dados $z \in M$ e $\lambda \in M^\wedge$, defina $z \cdot \lambda \in M^\wedge$ por $(z \cdot \lambda)(w) := \lambda(zw)$. Assim, temos uma ação de M em $M^\wedge$. Desse modo, $M^\wedge$ é um espaço unidimensional sobre M, já que

$$n = \dim_L M^\wedge = [M : L] \cdot \dim_M M^\wedge = n \dim_M M^\wedge.$$

Agora, $\mathrm{Tr}_{M/L}$ não é a aplicação nula, já que M/L é separável, e disso segue que, dado $\lambda \in M^\wedge$, existe uma única representação da forma $\lambda = z \cdot \mathrm{Tr}_{M/L}$.

Em particular, funcionais lineares $\lambda_j \in M^\wedge$ dados por $\lambda_j(z_i) := \delta_{ij}$, com $i = 1, \ldots, n$ podem ser escritos como $\lambda_j = z_j^* \cdot \mathrm{Tr}_{M/L}$ com $z_j^* \in M$. Assim,

$$\mathrm{Tr}_{M/L}\left(z_i z_j^*\right) = \left(z_j^* \cdot \mathrm{Tr}_{M/L}\right)(z_i) = \lambda_j(z_i) = \delta_{ij}.$$

Assim, como $\lambda_1, \ldots, \lambda_n$ são linearmente independentes sobre L, o mesmo vale para $z_1^*, \ldots, z_n^*$, e assim, $\{z_1^*, \ldots, z_n^*\}$ forma uma base de M/L.

■

Teorema 4.26. *Sejam* R *um subanel integralmente fechado de* F/K *com corpo de frações* F *e* F'/F *uma extensão separável e finita de grau* n. *Considere* $R' = \mathrm{ic}_{F'}(R)$ *o fecho integral de* R *em* F'. *Então*

(a) Dada uma base $\{x_1, \ldots, x_n\}$ *de* F'/F, *existem* $a_i \in R \backslash \{0\}$ *tais que* $a_1 x_1, \ldots a_n x_n \in R'$. *Consequentemente, existem bases de* F'/F *que estão contidas em* R'.

(b) Se $\{z_1, \ldots, z_n\} \subseteq R'$ *é uma base de* F'/F *e* $\{z_1^*, \ldots, z_n^*\}$ *é sua base dual com respeito a aplicação traço, então*

$$\sum_{i=1}^{n} R z_i \subseteq R' \subseteq \sum_{i=1}^{n} R z_i^*.$$

(c) Se, no item acima tivermos a hipótese de R *ser um domínio principal, então existe uma base* $\{u_1, \ldots, u_n\}$ *de* F'/F *que satisfaz*

$$R' = \sum_{i=1}^{n} R u_i.$$

Demonstração: (a) Queremos mostrar que, dado $x \in F'$, existe $0 \neq a \in R$ tal que ax satisfaz uma equação integral sobre R.

Por hipótese, F'/F é finita, e portanto algébrica. Considere $x \in F'$. Como a extensão é algébrica e F é o corpo de frações de R, existem elementos $a_i, b_i \in R$, com $a_i \neq 0$ tais que

$$x^r + \frac{b_{r-1}}{a_{r-1}}x^{r-1} + \cdots + \frac{b_1}{a_1}x + \frac{b_0}{a_0} = 0.$$

Multiplicando a equação por a^r, com $a := a_0 \cdot a_1 \cdot \cdots \cdot a_{r-1}$, obtemos

$$(ax)^r + c_{r-1}(ax)^{r-1} + \cdots + c_1(ax) + c_0 = 0,$$

com $c_i \in R$ e logo, $ax \in R'$.

(b) Seja agora $\{z_1, \ldots, z_n\}$ uma base de F'/F tal que $z_i \in R'$ e $\{z_1^*, \ldots, z_n^*\}$ sua base dual. Em particular, cada $z \in F'$ pode ser representado da forma

$$z = e_1 z_1^* + \ldots + e_n z_n^* \quad \text{com} \quad e_i \in F.$$

Se $z \in R'$ então $zz_j \in R'$, com $j = 1, \ldots, n$, e do corolário 4.24, segue que $\mathrm{Tr}_{F'/F}(zz_j) \in R$. Assim, como

$$\mathrm{Tr}_{F'/F}(zz_j) = \mathrm{Tr}_{F'/F}\left(\sum_{i=1}^{n} e_i z_j z_i^*\right) = \sum_{i=1}^{n} e_i \cdot \mathrm{Tr}_{F'/F}(z_j z_i^*) = e_j,$$

segue que $e_j \in R$, e portanto, $R' \subseteq \sum_{i=1}^{n} Rz_i^*$

(c) Escolha $\{w_1, \ldots, w_n\}$ uma base de F'/F com $R' \subseteq \sum_{i=1}^{n} Rw_i$, o que é possível pelo item (b). Agora, para $1 \leq k \leq n$, defina

$$R_k := R' \cap \sum_{i=1}^{k} Rw_i.$$

Vamos construir recursivamente $u_1, \ldots, u_n$ tais que $R_k = \sum_{i=1}^{k} Ru_i$.

Para $k = 1$, $R_1 = R' \cap Rw_1$. Consideramos o conjunto $I_1 := \{a \in F \mid aw_1 \in R'\}$. Note que $I_1 \subseteq R$, uma vez que $R' \subseteq \sum_{i=1}^{n} Rw_i$. Mais ainda, I_1 é um ideal de R. De fato, dados $a \in I_1$ e $r \in R$, temos $aw_1 \in R'$, e desse modo, $(ar)w_1 \in R'$, já que $R \subseteq R'$. Portanto, $ar \in I_1$.

Da hipótese, R é principal, e segue que $I_1 = a_1 R$, para algum $a_1 \in R$. Defina $u_1 = a_1 w_1$. Mostremos que $R_1 = u_1 R$.

Se $x \in R_1 = R' \cap Rw_1$, então $x = aw_1$, com $a \in R$. Agora, $a \in I_1$, e portanto $a = a_1 u$ com $u \in R$. Assim, $x = a_1 w_1 u$, ou seja, $x \in u_1 R$.

Agora, se $x \in u_1 R$, então $x = a_1 w_1 u$, com $u \in R$. Assim, claramente $x \in Rw_1$. Agora, como $a_1 \in I_1$, então $a_1 w_1 \in R'$, e como $u \in R \subseteq R'$, segue também que $x \in R'$. Portanto, $x \in Rw_1 \cap R'$ e temos $R_1 = Ru_1$.

Suponhamos agora que, para $k \geq 2$, encontramos $u_1, \ldots, u_{k-1}$ tais que $R_{k-1} = \sum_{i=1}^{k-1} Ru_i$. Seja

$$I_k := \{a \in F \mid \text{ existem } b_1, \ldots, b_{k-1} \in R \text{ tais que } b_1 w_1 + \cdots + b_{k-1} w_{k-1} + aw_k \in R'\}.$$

Novamente, I_k um ideal de R, e escrevemos $I_k = a_k R$. Escolha agora $u_k \in R'$ com

$$u_k = c_1 w_1 + \cdots + c_{k-1} w_{k-1} + a_k w_k.$$

Como fizemos no caso $k = 1$, é fácil ver que $R_k \supseteq \sum_{i=1}^{k} Ru_i$. Vamos mostrar a outra inclusão.

Considere $w \in R_k$ e escreva $w = d_1 w_1 + \cdots + d_k w_k$, com $d_i \in R$. Então $d_k \in I_k$, ou seja, $d_k = da_k$, com $d \in R$, e temos

$$w - du_k \in R' \cap \sum_{i=1}^{k-1} Rw_i = R_{k-1} = \sum_{i=1}^{k-1} Ru_i,$$

ou seja, $w \in \sum_{i=1}^{k} Ru_i$.

Com essa construção, provamos que $R' = R_n = \sum_{i=1}^{n} Ru_i$. Pelo item (a), R' contém alguma base de F'/F, e segue que $u_1, \ldots, u_n$ são linearmente independentes sobre F, e portanto é base de F'/F.

■

A seguir, temos um corolário que relaciona o teorema anterior com os anéis de valorizações de um lugar P, juntamente com suas extensões.

Corolário 4.27. *Seja F'/F uma extensão finita e separável do corpo de funções F/K e considere $P \in \mathbb{P}_F$. Então o fecho integral $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F' é*

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

Além disso, existe uma base $\{u_1, \ldots, u_n\}$ de F'/F tal que $\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot u_i$

Demonstração: A primeira igualdade decorre do teorema 4.19 (b), visto que $\mathrm{ic}_F(R) = \mathcal{O}_{S(R)}$, onde $S(R) = \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$. A existência da base com a propriedade da segunda igualdade segue diretamente do teorema anterior e do fato de $\mathcal{O}_P$ ser principal.

■

Uma base como descrita no corolário 4.27 é chamada **base integral** de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$ ou **base integral local** de F'/F para P.

Antes de demonstrarmos o principal teorema desta seção, veremos a seguir um teorema a respeito da existência de bases integrais locais.

Teorema 4.28. *Sejam F/K um corpo de funções e F'/F uma extensão finita e separável. Então toda base $\{z_1, \ldots z_n\}$ de F'/F é uma base integral para quase todo $P \in \mathbb{P}_F$, exceto um número finito de lugares.*

Demonstração: Seja $\{z_1, \dots z_n\}$ base de F'/F e considere $\{z_1^*, \dots, z_n^*\}$ sua base dual. O polinômio minimal de $z_1, \dots, z_n, z_1^*, \dots, z_n^*$ sobre F envolvem um número finito de coeficientes apenas.

Seja $S \subseteq \mathbb{P}_F$ o conjunto de todos os polos destes coeficientes. Logo, S é finito. Ainda, se $P \notin S$, então

$$z_1, \dots, z_n, z_1^*, \dots, z_n^* \in \mathcal{O}'_P$$

onde $\mathcal{O}'_P = \mathrm{ic}_{F'}(\mathcal{O}_P)$, uma vez que não há polos nesses pontos. Note que, pela construção, temos $\sum \mathcal{O}_P \cdot z_i \subseteq \mathcal{O}'_P$ e $\sum \mathcal{O}_P \cdot z_i^* \subseteq \mathcal{O}'_P$.

Por outro lado, pelo teorema 4.26 (b), segue que $\mathcal{O}'_P \subseteq \sum \mathcal{O}_P \cdot z_i^*$. Agora, se olharmos para $\{z_1, \dots, z_n\}$ como base dual de $\{z_1^*, \dots, z_n^*\}$, novamente pelo teorema 4.26 (b), obtemos $\mathcal{O}'_P \subseteq \sum \mathcal{O}_P \cdot z_i$. Combinando todas as inclusões, obtemos

$$\sum \mathcal{O}_P \cdot z_i \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P \cdot z_i^* \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P \cdot z_i.$$

Portanto, $\{z_1, \dots, z_n\}$ é base integral para todo $P \notin S$.

■

Nosso próximo passo é estudar o teorema de Kummer, o qual busca descrever um método para determinar as extensões de um lugar fixado P em F'. Para isso, primeiramente vamos fixar algumas notações que serão utilizadas daqui em diante.

Denotaremos $\bar{F} := F_P$ o corpo de classe residual de P e $\bar{a} := a(P) = a + P \in \bar{F}$ a classe residual de a em $\mathcal{O}_P$. Dado um polinômio $\psi(t) = \sum c_i t^i$ com coeficientes $c_i \in \mathcal{O}_P$, definimos $\bar{\psi}(t) := \sum \bar{c}_i t^i \in \bar{F}[t]$.

Obviamente, todo polinômio $\gamma(t) \in \bar{F}[t]$ pode ser representado como $\gamma(t) = \bar{\psi}(t)$, onde $\psi(t) \in \mathcal{O}_P[t]$ e $\deg \psi(t) = \deg \gamma(t)$. Fixadas tais notações, podemos demonstrar o teorema de Kummer.

Teorema 4.29. *(de Kummer) Suponha $F' = F(y)$, com y integral sobre $\mathcal{O}_P$ e considere $\varphi(t) \in \mathcal{O}_P[t]$ o polinômio minimal de y sobre F. Seja*

$$\bar{\varphi}(t) = \prod_{i=1}^{r} \gamma_i(t)^{\varepsilon_i}$$

a decomposição de $\bar{\varphi}(t)$ em polinômios irredutíveis sobre $\bar{F}$ (os polinômios $\gamma_i(t)$ são irredutíveis, mônicos, dois a dois distintos, e $\varepsilon_i \geq 1$). Escolhemos polinômio mônicos $\varphi_i(t) \in \mathcal{O}_P[t]$ com

$$\bar{\varphi}_i(T) = \gamma_i(T) \quad e \quad \deg \varphi_i(T) = \deg \gamma_i(T).$$

Então, para $1 \leq i \leq r$, existem lugares $P_i \in \mathbb{P}_{F'}$ que satisfazem

$$P_i \mid P, \quad \varphi_i(y) \in P_i \quad e \quad f(P_i \mid P) \geq \deg \gamma_i(T).$$

Mais ainda, se $i \neq j$, então $P_i \neq P_j$.

Sob algumas hipóteses adicionais, podemos provar ainda mais. Suponha que ao menos uma das condições a seguir é satisfeita:

($\star$) $\varepsilon_i = 1, i = 1, \dots, r$;

($\star\star$) $\{1, y, \dots, y^{n-1}\}$ *é base integral de P.*

Então, para cada $1 \leq i \leq r$*, existe exatamente um lugar* $P_i \in \mathbb{P}_{F'}$ com $P_i \mid P$ *e* $\varphi_i(y) \in P_i$*. Os lugares* $P_1, \ldots, P_r$ *são todos os lugares de* F' *que estendem* P *e temos*

$$\mathrm{Con}_{F'/F}(P) = \sum_{i=1}^{r} \varepsilon_i P_i,$$

isto é, $\varepsilon_i = e(P_i \mid P)$*. Ainda, o corpo de classe residual* $F'_{P_i} = O_{P_i}/P_i$ *é isomorfo a* $\bar{F}[t]/\langle \gamma_i(t) \rangle$*, logo* $f(P_i \mid P) = \deg \gamma_i(t)$*.*

Demonstração: Inicialmente, defina $\overline{F_i} = \overline{F}[T]/\langle \gamma_i(T) \rangle$. Da hipótese, $\gamma_i(t)$ é irredutível, e portanto, $\overline{F_i}$ é uma extensão de $\overline{F}$ com $[\overline{F_i} : \overline{F}] = \deg \gamma_i(t)$. Considere o anel $\mathcal{O}_P[y] = \sum_{j=0}^{n-1} \mathcal{O}_P y^j$, onde $n = [F' : F] = \deg \varphi(t)$.

Considere as aplicações

$$\rho : \begin{cases} \mathcal{O}_P[T] & \longrightarrow & \mathcal{O}_P[y] \\ \sum c_j T^j & \longmapsto & \sum c_j y^j \end{cases}$$

e

$$\pi_i : \begin{cases} \mathcal{O}_P[T] & \longrightarrow & \bar{F}_i, \\ \sum c_j T^j & \longmapsto & \sum \bar{c}_j T^j \bmod \gamma_i(T). \end{cases}$$

Mostremos agora que $\ker \rho = \langle \varphi(t) \rangle$ e $\ker \rho \subseteq \ker \pi_i$.

De fato, seja $p(t) \in \langle \varphi(t) \rangle$. Então, existe $\lambda(t) \in \mathcal{O}_P[t]$ tal que $p(t) = \lambda(t)\varphi(t)$. Portanto

$$\rho(p(t)) = \rho(\lambda(t))\rho(\varphi(t)) = \rho(\lambda(t))\varphi(y) = 0,$$

ou $p(t) \in \ker \rho$. Agora, considere $p(t) \in \ker \rho$. Assim, $p(y) = 0$, e como φ é o polinômio minimal de y, segue que $\varphi(t) \mid p(t)$, ou seja, $p(t) \in \langle \varphi(t) \rangle$, e segue a primeira igualdade desejada.

Agora, vamos mostrar a segunda inclusão. Considere $p(t) = \ker \rho = \langle \varphi(t) \rangle$. Assim, existe $\lambda(t) \in \mathcal{O}_P[t]$ tal que $p(t) = \varphi(t)\lambda(t)$. Então

$$\pi_i(p(t)) = \pi_i(\lambda(t))\pi_i(\varphi(t)) = \pi_i(\lambda(t))\bar{\varphi}(t)(\mathrm{mod}\gamma_i(T)),$$

ou seja, $\ker \rho \subseteq \ker \pi_i$.

Assim, existe um único homomorfismo $\sigma_i : \mathcal{O}_P[y] \longrightarrow \overline{F_i}$ tal que $\pi_i = \sigma_i \circ \rho$. Da construção que fizemos anteriormente, segue que σ é um epimorfismo, e dado $\sum_{j=0}^{n-1} c_j y^j \in \mathcal{O}_P[y]$, sua imagem pela aplicação σ_i é $\sum_{j=0}^{n-1} \overline{c_j} t^j \bmod \gamma_i(t)$.

Afirmação 1: $\ker \sigma_i = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$.

Considere $z \in P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$. Então, existem $p \in P$ e $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in \mathcal{O}_P$ tais que

$$\begin{aligned} z &= p\left(a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}\right) + \varphi_i(y)\left(b_0 + b_1 y + \cdots + b_{n-1} y^{n-1}\right) \\ \Rightarrow \sigma_i(z) &= \sigma_i\left(p\left(a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}\right) + \varphi_i(y)\left(b_0 + b_1 y + \cdots + b_{n-1} y^{n-1}\right)\right) \\ &= \sigma_i(p)\left(\sum_{j=0}^{n-1} \overline{a_j} T^j\right) \bmod \gamma_i(T) = 0, \end{aligned}$$

ou seja, $P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y] \subseteq \ker(\sigma_i)$.

Para a outra inclusão, considere $\sum_{j=0}^{n-1} c_j y^j \in \ker(\sigma_i)$, ou seja, $\sigma_i\left(\sum_{j=0}^{n-1} c_j y^j\right) = 0$ em $\overline{F_i}$.

Logo, $\sum_{j=0}^{n-1} \overline{c_j} t^j \in \langle \gamma_i(t) \rangle = \langle \overline{\varphi_i}(t) \rangle$, e assim, existe $\psi(t) \in \mathcal{O}_P[t]$ tal que $\sum_{j=0}^{n-1} \overline{c_j} t^j = \overline{\varphi_i}(t)\psi(t)$.

Assim, $\sum_{j=0}^{n-1} c_j t^j - \varphi_i(t)\psi(t) \in P \cdot \mathcal{O}_P[t]$. Substituindo $t = y$, obtemos

$$\sum_{j=0}^{n-1} c_j y^j - \varphi_i(y)\psi(y) \in P \cdot \mathcal{O}_P[y] \Rightarrow \sum_{j=0}^{n-1} c_j y^j \in P \cdot \mathcal{O}_P[t] + \varphi_i(y) \cdot \mathcal{O}_P[y],$$

e segue a afirmação.

Pelo teorema 2.22 existe P_i um lugar de F' tal que $\ker \sigma_i \subseteq P_i$ e $\mathcal{O}_P[y] \subseteq \mathcal{O}_{P_i}$, e assim, $P \in \ker(\sigma_i) \subseteq P_i$, ou seja, $P_i | P$ e $\varphi_i(y) \in P_i$.

Agora, o corpo de classe residual $\mathcal{O}_{P_i}/P_i$ contém $\mathcal{O}_P[y]/\ker \sigma_i$, o qual é isomorfo a $\overline{F_i}$, via σ_i. Em particular, $\ker \sigma_i$ é um ideal maximal. Logo $[\overline{F_i} : \overline{F}] = \deg \gamma_i(t)$, e temos $\left[F'_{P_i} : F_P\right] \geq \left[F_i : \overline{F}\right] = \deg \gamma_i(t)$.

Resta mostrar que, dados $i \neq j$, temos $P_i \neq P_j$. Considere índices i, j distintos $\gamma_i(t)$ e $\gamma_j(t)$ primos entre si em $\overline{F}[t]$. Logo, existem $\lambda_i(t), \lambda_j(t) \in O_P[t]$ tais que

$$1 = \overline{\lambda_i}(t)\gamma_i(t) + \overline{\lambda_j}(t)\gamma_j(t).$$

Assim,

$$\begin{gathered}
\overline{\varphi_i}(t)\overline{\lambda_i}(t) + \overline{\varphi_j}(t)\overline{\lambda_j}(t) - 1 = 0 \\
\Rightarrow \varphi_i(t)\lambda_i(t) + \varphi_j(t)\lambda_j(t) - 1 \in P\mathcal{O}_P[t] \\
\Rightarrow \varphi_i(y)\lambda_i(y) + \varphi_j(y)\lambda_j(y) - 1 \in P\mathcal{O}_P[y] \\
\Rightarrow 1 \in P \cdot \mathcal{O}_P[y] + \varphi_i(y)\mathcal{O}_P[y] + \varphi_j(y)O_{\mathcal{O}}[y] = \ker \sigma_i + \ker \sigma_j.
\end{gathered}$$

Agora, se $1 \in \ker \sigma_i + \ker \sigma_j$, então, existe $z_i \in P_i$ tal que $1 - z_i \in P_j$, uma vez que $\ker \sigma_j$ e $\ker \sigma_i$ são ideais maximais.

Se $P_i = P_j$, então teríamos $1 \in P_j$, o que contraria o fato de P_j ser maximal. Portanto $P_i \neq P_j$.

Agora vamos supor válida a condição $(\star)$. Nesse caso, temos $\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(t)$. Utilizando a primeira parte da demonstração e o teorema 4.11,

$$\begin{aligned}
[F' : F] = \deg \varphi(T) &= \sum_{i=1}^{r} \deg \varphi_i(T) \\
&\leq \sum_{i=1}^{r} f(P_i \mid P) \leq \sum_{i=1}^{r} e(P_i \mid P) \cdot f(P_i \mid P) \\
&\leq \sum_{P'|P} e(P' \mid P) \cdot f(P' \mid P) = [F' : F],
\end{aligned}$$

Assim, em todas as passagens acima, vale a igualdade, e então:

(a) $\sum_{i=1}^{r} f(P_i \mid P) = \sum_{i=1}^{r} e(P_i \mid P) f(P_i \mid P) \Rightarrow e(P_i \mid P) = 1$;

(b) $\sum_{i=1}^{r} \deg \varphi_i(t) = \sum_{i=1}^{r} f(P_i \mid P)$ e $\deg \varphi_i(t) \leq f(P_i \mid P), \forall i \Rightarrow \deg \varphi_i(t) = f(P_i \mid P), \forall i$;

e

(c) $\sum_{i=1}^{r} e(P_i \mid P) f(P_i \mid P) = \sum_{P'|P} e(P' \mid P) f(P' \mid P) \Rightarrow P_1, \ldots, P_r$ são exatamente os lugares de F' que estendem P.

Por fim, vamos supor válida a condição ($\star\star$). Escolhemos novamente $P_i \in \mathbb{P}_{F'}$ tal que $P_i|P$ e $\varphi_i(y) \in P_i$.

Afirmação 2: $P_1, \ldots, P_r$ são os únicos lugares de F' que estendem P.

De fato, considere uma extensão qualquer P' de P em F'. Sabemos que

$$0 = \varphi(y) = \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \bmod P \cdot \mathcal{O}_P[y].$$

Logo,

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in P', \quad \text{pois } P \subseteq P'.$$

Como P' é um ideal primo em $\mathcal{O}_{P'}$, segue que $\varphi_i(y) \in P'$, para algum $i = 1, \ldots, r$ e ainda,

$$P \cdot \mathcal{O}_P[y] + \varphi_i(y)\mathcal{O}_P[y] \subseteq P' \cap \mathcal{O}_P[y].$$

Pela afirmação 1, $\ker \sigma_i = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$. Pela maximalidade do núcleo, temos a igualdade

$$P \cdot \mathcal{O}_P[y] + \varphi_i(y)\mathcal{O}_P[y] = P' \cap \mathcal{O}_P[y].$$

Além disso, como $\ker \sigma_i \subseteq P_i \Rightarrow P \cdot \mathcal{O}_P[y] + \varphi_i(y)\mathcal{O}_P[y] \subseteq P_i \cap \mathcal{O}_P[y]$, segue novamente pela maximalidade do núcleo que $P \cdot \mathcal{O}_P[y] + \varphi_i(y)\mathcal{O}_P[y] = P_i \cap \mathcal{O}_P[y]$, e assim, $P_i \cap \mathcal{O}_P[y] = P' \cap \mathcal{O}_P[y]$.

Pela hipótese adicional $\{1, y, \ldots, y^{n-1}\}$ é base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$. Logo, a proposição 4.21 garante que $P' = P_i$, o que prova a afirmação. Pela afirmação 2 e o corolário 4.27, segue que

$$\mathcal{O}_P[y] = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}.$$

Pelo teorema da aproximação forte, existem $t_1, \ldots, t_r \in F'$ tais que $v_{P_i}(t_i) = 1$ e $v_{P_j}(t_i) = 0$, se $i \neq j$.

Escolhemos $t \in F$ um parâmetro local para P. Então,

$$t_i \in \mathcal{O}_P[y] cap P_i = \varphi_i(y)\mathcal{O}_P[y] + t\mathcal{O}_P[y],$$

pelas construções já feitas. Escrevemos cada t_i como $t_i = \varphi_i(y)a_i(y) + tb_i(y)$, onde $a_i(y), b_i(y) \in \mathcal{O}_P[y]$. Logo,

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = \prod_{i=1}^{r} (\varphi_i(y)a_i(y) + tb_i(y))^{\varepsilon_i} = a(y) \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + tb(y),$$

com $a(y), b(y) \in \mathcal{O}_P[y]$. Como $\varphi(y) = 0$ e $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \equiv \varphi(y) \bmod tO_P[y]$, segue que $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in tO_P[y]$. Assim, $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} = tu(y)$, onde $u(y) \in \mathcal{O}_P[y]$. Por outro lado,

$$\varepsilon_i = v_{P_i}\left(\prod_{i=1}^{r} t_i^{\varepsilon_i}\right) = v_{P_i}(a(y)tu(y)+tb(y)) = v_{P_i}(a(y)u(y)+b(y))+v_{P_i}(t) \geq v_{P_i}(t) = e(P_i \mid P).$$

Resta mostrar que $f(P_i \mid P) = \deg \gamma_i(t)$. Já vimos que $[\overline{F_i} : \overline{F}] = \deg \gamma_i(t)$ e que $\ker \sigma_i = P_i \cap \mathcal{O}_P[y]$. Pela proposição 4.21,

$$\frac{\mathcal{O}_P[y]}{P_i \cap \mathcal{O}_P[y]} \cong \frac{\mathcal{O}_{P_i}}{P_i}.$$

Assim,

$$\deg(\gamma_i(T)) = \left[\overline{F_i} : \overline{F}\right] = \left[\frac{\mathcal{O}_P[y]}{\ker(\sigma_i)} : \overline{F}\right] = \left[\frac{\mathcal{O}_{P_i}}{P_i} : \bar{F}\right] = f(P_i \mid P).$$

Concluimos então que $\deg \gamma_i(t) = f(P_i \mid P)$, e pela igualdade fundamental, devemos ter $e(P_i \mid P) = \varepsilon_i$, o que conclui a demonstração.

■

Encerramos esta seção com um caso particular do teorema de Kummer.

Corolário 4.30. *Seja $\varphi(t) = t^n + f_{n-1}(x)t^{n-1} + \cdots + f_0(x) \in K(x)[t]$ irredutível. Consideramos o corpo de funções $K(x,y)/K$, onde y satisfaz $\varphi(y) = 0$ e $\alpha \in K$ tal que $f_j(\alpha) \neq \infty$, para todo $j = 1, \ldots, n-1$. Denote por $P_\infty \in \mathbb{P}_{K(x)}$ o zero de $x - \alpha$ em $K(x)$. Suponha que o polinômio*

$$\varphi_\alpha(t) := t^n + f_{n-1}(\alpha)t^{n-1} + \cdots + f_0(\alpha) \in K[t]$$

tem a seguinte decomposição em $K[t]$:

$$\varphi_\alpha(t) = \prod_{i=1}^{r} \psi_i(t)$$

onde $\psi_i(t)$ são mônicos, irredutíveis e distintos dois a dois. Então:

(a) Para cada $i = 1, \ldots, r$, existe um lugar $P_i \in \mathbb{P}_{K(x,y)}$ unicamente determinado tal que $x - \alpha \in P_i$ e $\psi_i(x) \in P_i$. O elemento $x - \alpha$ é tal que $e(P_i \mid P_\alpha) = 1$ e o corpo de classe residual de P_i é K-isomorfo a $K[t]/\langle \psi_i(t) \rangle$. Portanto, $f(P_i \mid P_\alpha) = \deg \psi_i(t)$.

(b) Se existe $i = 1, \ldots, r$ tal que $\deg \psi_i(T) = 1$, então K é o corpo completo das constantes de $K(x,y)$.

(c) Se $\varphi_\alpha(t)$ tem $n = \deg \varphi(t)$ raízes distintas β em K, então para cada β, com $\varphi_\alpha(\beta) = 0$, existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)}$ tal que

$$x - \alpha \in P_{\alpha,\beta} \quad e \quad y - \beta \in P_{\alpha,\beta}.$$

Nesse caso, $P_{\alpha,\beta}$ é um lugar de $K(x,y)$ de grau 1.

Demonstração: Definimos $F := K(x)$ e $F' := K(x)(y) = K(x,y)$. Pela hipótese $f_j(\alpha) \neq \infty$, então y é integral sobre o anel de valorização associado ao lugar P_α. Ainda, seguindo as notações do teorema de Kummer, o polinômio $\varphi_\alpha(t)$ é exatamente o polinômio $\overline{\varphi}(t)$. Assim, estamos nas hipóteses do teorema de Kummer, com a hipótese $(\star)$ sendo válida. Assim, os itens $(a), (b)$ e (c) seguem imediatamente.

■

4.4 Cotraço da diferencial de Weil e a fórmula do gênero de Hurwitz

Nesta seção, novamente, F/K denota um corpo de funções algébricas, com corpo das constantes K, e F'/K' é uma extensão algébrica do corpo de funções F/K, onde K' é corpo das constantes de F'. Ainda, consideramos o caso em que as extensões F'/F e K'/K são finitas e separáveis.

O objetivo desta seção é associar cada diferencial de Weil de F/K com uma diferencial de Weil de F'/K'. Esta associação culminará em uma fórmula útil para o cálculo do gênero de F', chamada fórmula do gênero de Hurwitz. Como estaremos sempre considerando a extensão F'/F sendo separável, então a aplicação traço é não nula. Introduzimos agora a definição de módulo complementar.

Definição 4.31. *Sejam $P \in \mathbb{P}_F$ e $\mathcal{O}'_P := \mathrm{ic}_{F'}(\mathcal{O}_P)$ o fecho integral de $\mathcal{O}_P$ em F'. O conjunto*

$$\mathcal{C}_P := \left\{ z \in F' \mid \mathrm{Tr}_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P \right\}$$

é chamado de módulo complementar sobre $\mathcal{O}_P$.

Usando as notações da definição acima temos o seguinte resultado:

Proposição 4.32. *(a) $\mathcal{C}_P$ é um $\mathcal{O}'_P$-módulo e $\mathcal{O}'_P \subseteq \mathcal{C}_P$.*
(b) Se $\{z_1, \ldots, z_n\}$ é uma base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$, então

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot z_i^*,$$

onde $\{z_1^*, \ldots, z_n^*\}$ é a base dual de $\{z_1, \ldots, z_n\}$.
(c) Existe $t \in F'$, dependendo de P tal que $\mathcal{C}_P = t \cdot \mathcal{O}'_P$. Mais ainda, $v_{P'}(t) \leq 0$, para todo $P'|P$, e para todo $t' \in F'$,

$$\mathcal{C}_P = t'\mathcal{O}'_P \Leftrightarrow v_{P'}(t') = v_{P'}(t), \forall P'|P.$$

(d) $\mathcal{C}_P = \mathcal{O}'_P$, para quase todo $P \in \mathbb{P}_F$.

Demonstração: (a) Considere $z \in \mathcal{C}_P$ e $\alpha, \beta \in O'_P$. Então $\mathrm{Tr}_{F'/F}(z\alpha\beta) = \mathrm{Tr}_{F'/F}(z\alpha)\,\mathrm{Tr}_{F'/F}(\beta) \in \mathcal{O}_P$. Portanto, $\mathcal{C}_P$ é um $\mathcal{O}'_P$-módulo.

Mostremos que $\mathcal{O}'_P \subseteq \mathcal{C}_P$. Seja $y \in \mathcal{O}'_P$. Então, y é inteiro sobre $\mathcal{O}_P$. Pelo corolário 4.24, segue que $\mathrm{Tr}_{F'/F}(y) \in \mathcal{O}_P$. Portanto, $\mathrm{Tr}_{F'/F}(y\mathcal{O}'_P) \in \mathcal{O}_P$, ou seja, $y \in \mathcal{C}_P$.

(b) Seja $z \in \mathcal{C}_P$. Como $\{z_1^*, \ldots, z_n^*\}$ é base de F'/F, existem $x_1, \ldots, x_n \in F$ tais que

$$z = x_1 z_1^* + x_2 z_2^* + \cdots + x_n z_n^*.$$

Como $z \in \mathcal{C}_P$ e $z_1, \ldots, z_n \in \mathcal{O}'_P$, segue que

$$\mathrm{Tr}_{F'/F}(zz_j) \in \mathcal{O}_P, \quad j = 1, \ldots, n.$$

Pelas propriedades de base dual,

$$\begin{aligned} \mathrm{Tr}_{F'/F}(zz_j) &= \mathrm{Tr}_{F'/F}\left(\sum_{i=1}^{n} x_i z_i^* z_j\right) \\ &= \sum_{i=1}^{n} x_i \cdot \mathrm{Tr}_{F'/F}(z_i^* z_j) = x_j. \end{aligned}$$

Assim, $x_j \in \mathcal{O}_P$ e $z \in \sum \mathcal{O}_P z_i^*$, e segue que $\mathcal{C}_P \subseteq \sum \mathcal{O}_P z_i^*$.

Considere $z \in \sum \mathcal{O}_P z_i^*$ e $u \in \mathcal{O}'_P$. Escreva $z = \sum x_i z_i^*$ e $u = \sum y_j z_j$, onde $x_i, y_j \in \mathcal{O}_P$. Então,

$$\begin{aligned}\mathrm{Tr}_{F'/F}(zu) &= \mathrm{Tr}_{F'/F}\left(\sum x_i y_j z_i^* z_j\right) \\ &= \sum x_i y_j \cdot \mathrm{Tr}_{F'/F}\left(z_i^* z_j\right) = \sum x_i y_i \in \mathcal{O}_P,\end{aligned}$$

e portanto, $z \in \mathcal{C}_P$, o que garante a igualdade desejada.

(c) Pelo item (b), sabemos que $\mathcal{C}_P = \sum \mathcal{O}_P u_i$, onde $\{u_1, \ldots, u_n\}$ é uma base apropriada de F'/F. Seja $x \in F$ tal que

$$v_P(x) \geq -v_{P'}(u_i), \quad \forall P'|P \quad \text{e} \quad i = 1, \ldots, n.$$

Então, $v_{P'}\left(xu_i\right) = e\left(P' \mid P\right) \cdot v_P(x) + v_{P'}\left(u_i\right) \geq 0,$, para todo $P'|P$ e $i = 1, \ldots, n$. Pelo corolário 4.27, segue que $x\mathcal{C}_P \subseteq \mathcal{O}'_P$. Além disso, $x\mathcal{C}_P$ é um ideal de $\mathcal{O}'_P$, pois dados $a \in \mathcal{C}_P$ e $y \in \mathcal{O}'_P$,

$$\mathrm{Tr}_{F'/F}((xa)y) = x\,\mathrm{Tr}_{F'/F}(ay) \in \mathcal{O}_P.$$

Logo, $(xa)y \in x\mathcal{C}_P$, e segue que $x\mathcal{C}_P$ é ideal. Como $\mathcal{O}'_P$ é principal, então existe $y \in \mathcal{O}'_P$ tal que $x\mathcal{C}_P = y\mathcal{O}'_P$, pela proposição 4.22.

Definindo $t := x^{-1}y$, temos $\mathcal{C}_P = t\mathcal{O}'_P$, onde $t \in F'$. Agora, seja $z \in \mathcal{O}'_P$ tal que $1 = zt$. Então, $v_{P'}(t) = -v_{P'}(z) \leq 0, \forall P'|P$.

Por fim, dado $t' \in F'$,

$$\begin{aligned}tO'_P = t'O'_P \Leftrightarrow tt'^{-1}, t^{-1}t' \in O'_P &\Leftrightarrow v_{P'}\left(tt'^{-1}\right) = 0, \forall P' \mid P \\ &\Leftrightarrow v_{P'}(t) = v_{P'}\left(t'\right), \forall P' \mid P.\end{aligned}$$

(d) Seja $\{z_1, \ldots, z_n\}$ base de F'/F. . Pelo teorema 4.28, $\{z_1, \ldots, z_n\}$ é base integral para quase todo $P \in \mathbb{P}_F$ e $\{z_1^*, \ldots, z_n^*\}$ é base integral para quase todo $P \in \mathbb{P}_F$. Pelo item (b), $\mathcal{C}_P = \mathcal{O}'_P$ para quase todo $P \in \mathbb{P}_F$.

■

Com esse resultado, podemo definir o expoente do diferente de uma extensão P' de P.

Definição 4.33. *Sejam $P \in \mathbb{P}_F$ e $\mathcal{O}'_P = \mathrm{ic}_{F'}(\mathcal{O}_P)$. Considere $\mathcal{C}_P = t\mathcal{O}'_P$ o módulo complementar sobre $\mathcal{O}_P$. Dado $P'|P$, definimos o expoente do diferente de P' sobre P por $d\left(P' \mid P\right) = -v_{P'}(t)$.*

Note que, da proposição 4.32, $d(P'|P)$ está bem definido e é não negativo. Mais ainda, $d(P'|P) = 0$ para quase todo $P \in \mathbb{P}_F$ e $P'|P$, uma vez que $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$, para quase todo P. Isso nos motiva a definição do diferente da extensão F'/F.

Definição 4.34. *O divisor* $\mathrm{Diff}\left(F'/F\right) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d\left(P' \mid P\right) P'$ *é chamado de diferente de F'/F.*

Da definição de diferente, segue que $\mathrm{Diff}(F'/F) \geq 0$. A observação a seguir nos fornece uma condição necessária e suficiente para que um elemento z pertença a $\mathcal{C}_P$, envolvendo o expoente do diferente.

Observação 4.35. *Dado $z \in F'$, temos $z \in \mathcal{C}_P \Leftrightarrow v_{P'}(z) \geq -d(P'|P)$, para todo $P'|P$.*

A observação segue de maneira imediata uma vez que

$$v_{P'}(z) \geq -d(P'|P) \Leftrightarrow v_{P'}(z) \geq v_{P'}(t) \Leftrightarrow v_{P'}(zt^{-1}) \geq 0 \Leftrightarrow zt^{-1} \in \mathcal{O}'_P \Leftrightarrow z \in t\mathcal{O}'_P \Leftrightarrow z \in \mathcal{C}_P.$$

A partir de agora, utilizaremos algumas notações já vistas no primeiro capítulo, na seção em que estudamos as diferenciais de Weil.

Definição 4.36. *Definimos o conjunto $\mathcal{A}_{F'/F}$ por*

$$\mathcal{A}_{F'/F} := \{\alpha \in \mathcal{A}_{F'} | \alpha_{P'} = \alpha_{Q'} \text{ sempre que } P' \cap F = Q' \cap F\}.$$

Claramente o $\mathcal{A}_{F'/F}$ é um F'-subsepaço de $\mathcal{A}_{F'}$. A aplicação traço Tr:$F' \longrightarrow F$ pode ser estendida para uma aplicação F-linear da $\mathcal{A}_{F'/F}$ para $\mathcal{A}_F$, definindo

$$\left(\mathrm{Tr}_{F'/F}(\alpha)\right)_P := \mathrm{Tr}_{F'/F}(\alpha_{P'}),$$

onde P' é um lugar de F' que estende P e $\alpha \in \mathcal{A}_{F'/F}$. Note que $\alpha_{P'} \in \mathcal{O}'_P$ para quase todo $P' \in \mathbb{P}_F$, e assim, pelo corolário 4.24, $\mathrm{Tr}_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$, para quase todo $P \in \mathbb{P}_F$. Portanto, $\mathrm{Tr}_{F'/F}(\alpha)$ é uma adele de F/K.

Ainda, o traço de uma adele principal $z \in F'$ é a adele principal de $\mathrm{Tr}_{F'/F}(z)$. Por fim, dado $A' \in$ F', definimos

$$\mathcal{A}_{F'/F}(A') := \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}.$$

O teorema principal deste seção irá relacionar uma diferencial de Weil de F/K com uma diferencial de Weil de F'/K'. Antes de enunciarmos este resultado, veremos dois lemas que auxiliarão na sua demonstração.

O primeiro lema nos fornece uma escrita para os elementos do conjunto $\mathcal{A}_{F'}$.

Lema 4.37. *Dado $C' \in \mathrm{Div}(F')$, $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$.*

Demonstração: Seja $\alpha = (\alpha_{P'})_{P' \in \mathbb{P}_{F'}}$ uma adele de F'. Para todo $P \in \mathbb{P}_F$, pelo teorema da aproximação forte, existe $x_P \in F'$ com

$$v_{P'}(\alpha_{P'} - x_P) \geq -v_{P'}(C'), \forall P' \mid P.$$

Definimos agora $\beta = (\beta_{P'})_{P' \in \mathbb{P}_{F'}}$, onde $\beta_{P'} = x_P$, se $P'|P$.

Assim, $\beta \in \mathcal{A}_{F'/F}$ e $\alpha - \beta \in \mathcal{A}_{F'}(C')$. Como $\alpha = \beta + (\alpha - \beta)$, segue a igualdade desejadas.

■

O segundo lema nos fornece uma espécie de extensão de uma aplicação M-linear para uma aplicação L-linear, onde M/L é uma extensão de corpos. Além disso, essa função estendida é única, e fazendo a composição do traço com esta aplicação, voltamos na inicial.

Lema 4.38. *Sejam M/L uma extensão de corpos finita e separável, V um espaço vetorial sobre M e $\mu : V \longrightarrow L$ uma aplicação L-linear. Então, existe uma única aplicação M-linear $\mu' : V \longrightarrow M$ tal que*

$$\mathrm{Tr}_{M/L} \circ \mu' = \mu.$$

Demonstração: Considere $\hat{M} := \{\lambda : M \to L \mid \lambda \text{ é } L-\text{ linear }\}$. Já vimos que $\hat{M}$ é um espaço vetorial sobre M se definirmos

$$(z\lambda)(w) = \lambda(zw),$$

onde $\lambda \in \hat{M}$ e $z, w \in M$. Ainda, $\dim_M \hat{M} = 1$ e todo $\lambda \in \hat{M}$ tem um única representação $\lambda = z \operatorname{Tr}_{M/L}$, com $z \in M$.

Dado $v \in V$, defina $\lambda_v : M \longrightarrow L$, $\lambda_v(a) := \mu(av)$. Facilmente verifica-se que λ_v é linear. Como fizemos anteriormente, existe um único $z_v \in M$ tal que $\lambda_v = z_v \operatorname{Tr}_{M/L}$. Defina agora $\mu' : V \longrightarrow M$ por $\mu'(v) = z_v$. Assim para todo $a \in M$ e $v \in V$

$$\mu(av) = \lambda_v(a) = \left(z_v \operatorname{Tr}_{M/L}\right)(a) = \left(\mu'(v) \operatorname{Tr}_{M/L}\right)(a) = \operatorname{Tr}_{M/L}\left(a\mu'(v)\right),$$

Tomando $a = 1$, obtemos $\mu = \operatorname{Tr}_{M/L} \circ \mu'$. Ainda, μ' é M-linear. De fato, dados $u, v \in V$ e $\alpha \in M$, temos $\mu'(\alpha v + u) = z_{\alpha v+u}$, onde $z_{\alpha v+u}$ é tal que $\lambda_{\alpha v+u} = z_{\alpha v+u} \operatorname{Tr}_{M/L}$. Assim,

$$\begin{aligned}\lambda_{\alpha v+u}(a) = \mu((\alpha v + u)(a)) = \alpha\mu(va) + \mu(ua) = \lambda_{\alpha v}(a) + \lambda_u(a) = \\ = z_{\alpha v} \operatorname{Tr}_{M/L}(a) + z_u \operatorname{Tr}_{M/L}(a),\end{aligned}$$

e disso segue que $\mu'(\alpha v + u) = \alpha\mu'(v) + \mu'(u)$.

Por fim, resta mostrar a unicidade de μ'. Suponha que exista $\mu^* : V \longrightarrow M$ tal que $\mu = \operatorname{Tr}_{M/L} \circ \mu' = \operatorname{Tr}_{M/L} \circ \mu^*$ e $\mu' \neq \mu^*$. Então, $\mu' - \mu^*$ é M-linear, e ainda,

$$\operatorname{Tr}_{M/L} \circ \mu' - \operatorname{Tr}_{M/L} \circ \mu^* = 0 \Rightarrow \operatorname{Tr}_{M/L} \circ (\mu' - \mu^*) = 0,$$

e segue que $\operatorname{Tr}_{M/L}$ deveria ser a aplicação nula, o que contradiz o fato da extensão ser separável.

■

Com esses dois lemas, podemos enunciar e demonstrar o teorema principal desta seção.

Teorema 4.39. *Dada uma diferencial de Weil ω de F/K, existe uma única diferencial de Weil ω' de F'/K' tal que*

$$\operatorname{Tr}_{K'/K}\left(\omega'(\alpha)\right) = \omega\left(\operatorname{Tr}_{F'/F}(\alpha)\right), \quad \forall \alpha \in \mathcal{A}_{F'/F}.$$

Essa diferencial de Weil é chamada de cotraço de ω em F'/F e é denotada por $\operatorname{Cotr}_{F'/F}(\omega)$. Se $\omega \neq 0$, então

$$\langle \operatorname{Cotr}_{F'/F}(\omega) \rangle = \operatorname{Con}_{F'/F}(\langle \omega \rangle) + \operatorname{Diff}\left(F'/F\right).$$

Demonstração: Vamos mostrar para o caso não trivial em que $\omega \neq 0$ (se $\omega = 0$, basta considerarmos $\omega' = 0$).

Defina $W' := \operatorname{Con}_{F'/F}(\langle\omega\rangle) + \operatorname{Diff}(F'/F)$. A demonstração será dividida em três etapas.

Etapa 1: A aplicação K-linear $\omega_1 : \mathcal{A}_{F'/F} \to K$ definida por $\omega_1 := \omega \circ \operatorname{Tr}_{F'/F}$ tem as seguintes propriedades:

(a_1) $\omega_1(\alpha) = 0$, para todo $\alpha \in \mathcal{A}_{F'/F}(W') + F'$.

(b_1) Se $B' \in \operatorname{Div}(F')$ é tal que $B' \nleq W'$, então existe $\beta \in \mathcal{A}_{F'/F}(B')$ com $\omega_1(\beta) \neq 0$.

Demonstração: (a_1) Primeiramente, note que ω_1 é linear sobre K, pois é composta de aplicações K-lineares. Ainda, como ω se anula em F, então ω_1 se anula em F', pois

$$\omega_1(F') = \omega \circ \operatorname{Tr}_{F'/F}(F') = \omega\left(\operatorname{Tr}_{F'/F}(F')\right) \subseteq \omega(F) = 0.$$

Agora, seja $\alpha \in \mathcal{A}_{F'/F}(W')$. Queremos mostrar que $\omega_1(\alpha) = 0$. Vamos mostrar que para todo $P \in \mathbb{P}_F$ e $P'|P$, vale que $v_P\left(\mathrm{Tr}_{F'/F}(\alpha_{P'})\right) \geq -v_P(\omega)$, e seguirá da definição do divisor canônico $\langle\omega\rangle$ que $\omega_1(\alpha) = 0$. Seja $x \in F$ com $v_P(x) = v_P(\omega)$. Então,

$$\begin{aligned} v_{P'}(x\alpha_{P'}) &= v_{P'}(x) + v_{P'}(\alpha_{P'}) \geq e(P' \mid P) \cdot v_P(\omega) - v_{P'}(W') \\ &= v_{P'}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) - W'\right) = -v_{P'}(\mathrm{Diff}(F'/F)) = -d(P' \mid P). \end{aligned}$$

Assim, pela observação 4.35, segue que $x\alpha_{P'} \in \mathcal{C}_P$, e logo, $v_P\left(\mathrm{Tr}_{F'/F}(x\alpha_{P'})\right) \geq 0$. Agora, como $\mathrm{Tr}_{F'/F}(x\alpha_{P'}) = x \cdot \mathrm{Tr}_{F'/F}(\alpha_{P'})$ e $v_P(x) = v_P(\omega)$, segue que

$$v_P\left(\mathrm{Tr}_{F'/F}(x\alpha_{P'})\right) \geq 0 \Rightarrow v_P(x) + v_P\left(\mathrm{Tr}_{F'/F}(\alpha_{P'})\right) \geq 0 \Rightarrow v_P\left(\mathrm{Tr}_{F'/F}(\alpha_{P'})\right) \geq -v_P(\omega),$$

e isso conclui o item (a_1)

(b_1) Seja B' tal que $B' \nleq W'$. Então, existe $P_0 \in \mathbb{P}_F$ tal que

$$v_{P^*}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) - B'\right) < -d(P^* \mid P_0),$$

onde $P^*|P$ e $v_{P^*}(B') > v_{P^*}(W')$.

Sejam $\mathcal{O}'_{P_0}$ o fecho integral de $\mathcal{O}_{P_0}$ em F' e $\mathcal{C}_{P_0}$ o módulo complementar sobre $\mathcal{O}_{P_0}$ e considere o conjunto

$$J := \left\{z \in F' \mid v_{P^*}(z) \geq v_{P^*}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) - B'\right), \forall P^* \mid P_0\right\}.$$

Pelo teorema da aproximação forte, existe $u \in J$ tal que $v_{P^*}(u) = v_{P^*}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) - B'\right)$, para todo $P^*|P_0$. Assim, pela observação 4.35 e pela escolha de P_0, temos $J \nsubseteq \mathcal{C}_{P_0}$. Agora, como $J \cdot \mathcal{O}'_{P_0} \subseteq J$, segue que $\mathrm{Tr}_{F'/F}(J)$ não está contido em $\mathcal{O}_{P_0}$.

Considere t um parâmetro local para P_0. Da definição de J, existe $r \geq 0$ grande o suficiente tal que $t^r \cdot J \subseteq \mathcal{O}'_{P_0}$. Logo, $t^r\,\mathrm{Tr}_{F'/F}(J) \subseteq \mathcal{O}_{P_0}$. Mais ainda, $t^r\,\mathrm{Tr}_{F'/F}(J)$ é um ideal de $\mathcal{O}_P$, e como estamos em um domínio principal, existe $s \geq 0$ tal que $t^r\,\mathrm{Tr}_{F'/F}(J) = t^s\mathcal{O}_{P_0}$. Assim, $\mathrm{Tr}_{F'/F}(J) = t^m\mathcal{O}_{P_0}$, onde $m = s - r$. Por outro lado, como $\mathrm{Tr}_{F'/F}(J) \notin \mathcal{O}_{P_0}$, segue que $m \leq -1$, e

$$t^{-1} \cdot \mathcal{O}_{P_0} \subseteq \mathrm{Tr}_{F'/F}(J).$$

Pela proposição 2.80 item (a), $v_P(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P(x) = 0, \forall x \in F \,\mathrm{com}\, v_P(x) \geq -r\}$. Logo, podemos tomar $x \in F$ tal que

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \text{ e } \omega_{P_0}(x) \neq 0.$$

Seja agora $y \in F$ tal que $v_{P_0}(y) = v_{P_0}(\omega)$. Então,

$$v_{P_0}(xy) = -1 \Rightarrow xy \in t^{-1}\mathcal{O}_{P_0},$$

e portanto, existe $z \in J$ tal que $\mathrm{Tr}_{F'/F}(z) = xy$, uma vez que $t^{-1}\mathcal{O}_{P_0} \subseteq \mathrm{Tr}_{F'/F}(J)$. Definimos $\beta \in \mathcal{A}_{F'/F}$ por

$$\beta_{P'} := \begin{cases} 0 & \text{se } P' \nmid P_0, \\ y^{-1}z & \text{se } P' \mid P_0. \end{cases}$$

Então, para $P'|P_0$,

$$\begin{aligned} v_{P'}(\beta) &= -v_{P'}(y) + v_{P'}(z) \\ &\geq -v_{P'}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle)\right) + v_{P'}\left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) - B'\right) \\ &= -v_{P'}(B'), \end{aligned}$$

ou seja, $\beta \in \mathcal{A}_{F'/F}(B')$. Por fim, basta notar que $\omega_1(\beta) \neq 0$, como queríamos mostrar, concluindo a etapa 1 da demonstração.

Etapa 2: Definimos agora $\omega_2 : \mathcal{A}_{F'} \longrightarrow K'$ da seguinte forma: considere $\alpha \in \mathcal{A}_{F'}$. Pelo lema 4.37, existem adeles $\beta \in \mathcal{A}_{F'/F}$ e $\gamma \in \mathcal{A}_{F'}(W')$ tais que $\alpha = \beta + \gamma$. Colocamos então $\omega_2(\alpha) := \omega_1(\beta)$.

Essa aplicação está bem definida. De fato, suponha $\alpha = \beta + \gamma = \beta_1 + \gamma_1$, onde $\beta, \beta_1 \in \mathcal{A}_{F'/F}$ e $\gamma, \gamma_1 \in \mathcal{A}_{F'}(W')$. Então,

$$\beta - \beta_1 = \gamma_1 - \gamma \in \mathcal{A}_{F'/F} \cap \mathcal{A}_{F'}(W') = \mathcal{A}_{F'/F}(W').$$

Assim, $\omega_1(\beta) - \omega(\beta_1) = \omega(\beta - \beta_1) = 0$, por (a_1). Logo, $\omega_2(\beta + \gamma) = \omega_2(\beta_1 + \gamma_1)$. Além disso, ω_2 é K-linear, uma vez que ω_1 o é. Do que fizemos nos itens (a_1) e (b_1) da etapa 1, segue que

(a_2) $\omega_2(\alpha) = 0$, para todo $\alpha \in \mathcal{A}_{F'}(W') + F'$;

(b_2) Se B' é um divisor de F' tal que $B' \nleq W'$, então existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\omega_2(\beta) \neq 0$.

Portanto, ω_2 é uma aplicação K-linear que se anula em $\mathcal{A}_{F'}(W') + F'$. O que não podemos garantir é que ω_2 é uma diferencial de Weil de F'/K', pois podemos ter $K \subsetneqq K'$.

Etapa 3: Nosso objetivo nesta etapa é estender a aplicação ω_2 da etapa 2, de modo a obtermos uma aplicação K'-linear.

Pelo lema 4.38, existe $\omega' : \mathcal{A}_{F'} \longrightarrow K$ uma aplicação K'-linear tal que $\mathrm{Tr}_{K'/K} \circ \omega' = \omega_2$. Se $\alpha \in \mathcal{A}_{F'/F}$, então

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right).$$

Para concluir a demonstração, devemos mostrar:

(a_3) $\omega'(\alpha) = 0$, para todo $\alpha \in \mathcal{A}_{F'}(W') + F'$:

(b_3) Se B' é um divisor de F' tal que $B' \nleq W'$, então existe $\beta \in \mathcal{A}_{F'}(B')$ com $\omega'(\beta) \neq 0$

Demonstração: (a_3) Como ω' é K'-linear, a imagem de $\mathcal{A}_{F'}(W') + F'$ por ω' é 0 ou K'. Se $\omega'\left(\mathcal{A}_{F'}\left(W'\right) + F'\right) = K'$, como $\mathrm{Tr}_{K'/K}$ é não nula, então existe $\alpha \in \mathcal{A}_{F'}(W') + F'$ tal que $0 \neq \mathrm{Tr}_{K'/K}(\omega(\alpha)) = \omega_2(\alpha)$, o que contraria o item (a_2), provando o item (a_3).

(b_3) Por (b_2), existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\omega_2(\beta) \neq 0$. Logo, $\mathrm{Tr}_{K'/K}(\omega(\beta)) \neq 0 \Rightarrow \omega'(\beta) \neq 0$.

Assim, mostramos a existência de uma diferencial de Weil ω' de F'/K' tal que

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right),$$

onde ω é uma diferencial de Weil de F/K. Vamos mostrar agora que $\langle\omega'\rangle = W'$. Seja $A \in M\left(\omega'\right) = \{A \in \mathrm{Div}(F) \mid \omega' \text{ se anula em } \mathcal{A}_F(A) + F\}$.

Se não tivermos $A \leq W'$, então existe $\alpha \in \mathcal{A}_{F'}(A)$ tal que $\omega'(\alpha) \neq 0$, logo $A \notin M\left(\omega'\right)$. Portanto, para todo $A \in M(\omega')$, temos $A \leq W'$. Disto, segue que $\langle\omega'\rangle = W'$. Para concluir a demonstração, precisamos apenas mostrar a unicidade. Suponha $\omega^* \in \Omega_{F'}$ tal que $\mathrm{Tr}_{K'/K}\left(\omega^*(\alpha)\right) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right)$, para todo $\alpha \in \mathcal{A}_{F'/F}$.

Defina $\eta := \omega^* - \omega'$. Então $\mathrm{Tr}_{K'/K}(\eta(\alpha)) = 0, \forall \alpha \in \mathcal{A}_{F'/F}$. Além disso, como η é uma diferencial de Weil de F'/K', segue que η se anula $\mathcal{A}_{F'}(C')$, para algum divisor C'. Pelo lema 4.37 e pela construção acima, segue que $\mathrm{Tr}_{K'/K}(\eta(\alpha)) = 0$, para todo $\alpha \in \mathcal{A}_{F'}$. Portanto, $\eta \equiv 0$, e segue que $\omega' = \omega^*$.

■

Observe que, usando as notações das componentes locais de Weierstrass, pela proposição 2.79, para todo $P \in \mathbb{P}_F$ e $y \in F'$,

$$\omega_P\left(\mathrm{Tr}_{F'/F}(y)\right) = \mathrm{Tr}_{K'/K}\left(\sum_{P'|P} \omega'_{P'}(y)\right).$$

A próxima proposição será útil para demonstrar a transitividade do diferente, ou seja, como o diferente se comporta quando trabalhamos com extensões de corpos $F \subseteq F' \subseteq F''$.

Proposição 4.40. *(a) Sejam ω, ω_1 e ω_2 diferenciais de Weil de F/K e $x \in F$. Então,*

$$\mathrm{Cotr}_{F'/F}(\omega_1 + \omega_2) = \mathrm{Cotr}_{F'/F}(\omega_1) + \mathrm{Cotr}_{F'/F}(\omega_2)$$

e

$$\mathrm{Cotr}_{F'/F}(x\omega) = x \cdot \mathrm{Cotr}_{F'/F}(\omega).$$

(b) Se F''/F' é também uma extensão finita e separável, então

$$\mathrm{Cotr}_{F''/F}(\omega) = \mathrm{Cotr}_{F''/F'}\left(\mathrm{Cotr}_{F'/F}(\omega)\right).$$

Demonstração: (a) Note que, pelo teorema 4.39 e pela linearidade do traço, temos

$$\begin{aligned}
&\mathrm{Tr}_{K'/K}\left(\left(\mathrm{Cotr}_{F'/F}(\omega_1) + \mathrm{Cotr}_{F'/F}(\omega_2)\right)(\alpha)\right) \\
&= \mathrm{Tr}_{K'/K}\left(\mathrm{Cotr}_{F'/F}(\omega_1)\right)(\alpha) + \mathrm{Tr}_{K'/K}\left(\mathrm{Cotr}_{F'/F}(\omega_2)\right)(\alpha) \\
&= \omega_1\left(\mathrm{Tr}_{F'/F}(\alpha)\right) + \omega_2\left(\mathrm{Tr}_{F'/F}(\alpha)\right) = (\omega_1 + \omega_2)\left(\mathrm{Tr}_{F'/F}(\alpha)\right).
\end{aligned}$$

A unicidade no teorema 4.39 garante que $\mathrm{Cotr}_{F'/F}(\omega_1 + \omega_2) = \mathrm{Cotr}_{F'/F}(\omega_1) + \mathrm{Cotr}_{F'/F}(\omega_2)$. Analogamente, prova-se que $\mathrm{Cotr}_{F'/F}(x\omega) = x \cdot \mathrm{Cotr}_{F'/F}(\omega)$.

(b) Vamos prosseguir de modo análogo ao que fizemos no item (a). Observe que

$$\mathrm{Tr}_{K'/K}\left(\mathrm{Cotr}_{F''/F}(\omega)(\alpha)\right) = \omega\left(\mathrm{Tr}_{F''/F}(\alpha)\right) = \omega\left(\mathrm{Tr}_{F''/F'}\left(\mathrm{Tr}_{F'/F}(\alpha)\right)\right),$$

e novamente da unicidade, segue que $\mathrm{Cotr}_{F''/F}(\omega) = \mathrm{Cotr}_{F''/F'}\left(\mathrm{Cotr}_{F'/F}(\omega)\right)$.

■

Corolário 4.41. *(Transitividade do diferente) Se $F \subseteq F' \subseteq F''$ são extensões finitas e separáveis, então:*

(a) $\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F')$ *e*

(b) $d(P'' \mid P) = e(P'' \mid P') \cdot d(P' \mid P) + d(P'' \mid P')$*, onde $P'' \in \mathbb{P}_{F''}$, $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ e $P \subseteq P' \subseteq P''$.*

Demonstração: Note que $(a) \Rightarrow (b)$. Mostremos o item (a). Seja $\omega \neq 0$ uma diferencial de Weil de F/K. Então, pelo teorema 4.39, o divisor do $\mathrm{Cotr}_{F''/F}(\omega)$ é

$$\left\langle \mathrm{Cotr}_{F''/F}(\omega) \right\rangle = \mathrm{Con}_{F''/F}(\langle\omega\rangle) + \mathrm{Diff}(F''/F).$$

Pela proposição 4.40,

$$\begin{aligned}
\left\langle \mathrm{Cotr}_{F''/F}(\omega) \right\rangle &= \left\langle \mathrm{Cotr}_{F''/F'} \left(\mathrm{Cotr}_{F'/F}(\omega) \right) \right\rangle \\
&= \mathrm{Con}_{F''/F'} \left(\left\langle \mathrm{Cotr}_{F'/F}(\omega) \right\rangle \right) + \mathrm{Diff}\,(F''/F') \\
&= \mathrm{Con}_{F''/F'} \left(\mathrm{Con}_{F'/F}(\langle\omega\rangle) + \mathrm{Diff}\,(F'/F) \right) + \mathrm{Diff}\,(F''/F') \\
&= \mathrm{Con}_{F''/F}(\langle\omega\rangle) + \mathrm{Con}_{F''/F'}\left(\mathrm{Diff}\,(F'/F)\right) + \mathrm{Diff}\,(F''/F')
\end{aligned}$$

Comparando ambas as expressões, temos o resultado.

■

Encerramos esta seção com um teorema que fornece uma fórmula para o cálculo do gênero de um corpo de funções, a fórmula do gênero de Hurwitz. Em seguida, temos um corolário de um caso particular deste resultado, em que trabalhamos com corpo de funções racionais.

Teorema 4.42. *(Fórmula do gênero de Hurwitz) Sejam F/K um corpo de funções algébricas de gênero g e F'/F uma extensão finita e separável. Denote por K' o corpo das constantes de F' e g' o gênero de F'/K'. Então*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg\left(\mathrm{Diff}\,(F'/F)\right).$$

Demonstração: Seja $\omega \neq 0$ uma diferencial de Weil de F/K. Do teorema 4.39, segue que

$$\left\langle \mathrm{Cotr}_{F''/F}(\omega) \right\rangle = \mathrm{Con}_{F''/F}(\langle\omega\rangle) + \mathrm{Diff}(F''/F).$$

Agora, lembramos que o grau de um divisor canônico de um corpo de funções de gênero g é $2g - 2$. Assim, da equação acima e do corolário 4.13, temos

$$\begin{aligned}
\deg \left\langle \mathrm{Cotr}_{F''/F}(\omega) \right\rangle &= \deg \left(\mathrm{Con}_{F''/F}(\langle\omega\rangle) + \mathrm{Diff}(F''/F) \right) \Rightarrow \\
\deg \left\langle \mathrm{Cotr}_{F''/F}(\omega) \right\rangle &= \deg \mathrm{Con}_{F''/F}(\langle\omega\rangle) + \deg \mathrm{Diff}(F''/F) \Rightarrow \\
2g' - 2 &= \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg\left(\mathrm{Diff}\,(F'/F)\right).
\end{aligned}$$

■

Corolário 4.43. *Seja F/K um corpo de funções algébricas de gênero g e considere $x \in F \backslash K$ tal que $F/K(x)$ é separável. Então*

$$2g - 2 = -2[F : K(x)] + \deg \mathrm{Diff}(F/K(x))$$

Demonstração: Segue diretamente do teorema 4.42, bastando lembrar que $g = 0$ para $K(x)|K$.

■

4.5 O diferente

No fim da seção anterior, explicitamos uma fórmula útil para determinarmos o gênero de um corpo de funções. Porém, aparece nesta fórmula o grau do diferente, o qual ainda não sabemos como calculá-lo. Nesta seção, estudaremos mais a fundo o diferente e propriedades que serão úteis para este cálculo um pouco mais explícito.

Consideramos novamente uma extensão finita e separável F'/F, onde F/K e F'/K' são corpos de funções algébricas com corpos das constantes K e K' respectivamente. Além disso, consideramos os casos em que K e K' são perfeitos.

O primeiro passo é encontrar uma relação entre o índice de ramificação e o expoente do diferente.

Lema 4.44. *Sejam F^*/F um corpo de funções algébricas, $P \in \mathbb{P}_F$ e $P^* \in \mathbb{P}_{F^*}$ com $P^*|P$. Considere também σ um automorfismo de F^*/F. Então*

$$\sigma\left(P^*\right) := \{\sigma(z) \mid z \in P^*\}$$

é um lugar de F^* e

(a) $v_{\sigma(P^*)}(y) = v_{P^*}\left(\sigma^{-1}(y)\right), \forall y \in F^*$.

(b) $\sigma\left(P^*\right)|P$.

(c) $e\left(\sigma\left(P^*\right)|P\right) = e\left(P'|P\right)$ e $f\left(\sigma\left(P^*\right)|P\right) = f\left(P'|P\right)$.

Demonstração: Mostremos inicialmente que $\sigma\left(\mathcal{O}_{P^*}\right)$ é uma anel de valorização de F^*, onde σ é uma automorfismo. Como $\mathcal{O}_{P^*} \subsetneqq F^*$, então $\sigma\left(\mathcal{O}_{P^*}\right) \subsetneqq F^*$. Ainda, $K^* \subsetneqq \mathcal{O}_{P^*}$, e segue também que $\sigma\left(\mathcal{O}_{P^*}\right)$ contém K^* via isomorfismo.

Seja $z \in F^*$ e suponha $\sigma(z) \notin \sigma\left(\mathcal{O}_{P^*}\right)$. Então, $z \notin \mathcal{O}_{P^*}$, e assim, $z^{-1} \in \mathcal{O}_{P^*}$, e segue que $\sigma(z^{-1}) \in \sigma\left(\mathcal{O}_{P^*}\right)$. Ainda, como P^* é ideal maximal de $\mathcal{O}_{P^*}$, então $\sigma(P^*)$ é um ideal maximal de $\sigma\left(\mathcal{O}_{P^*}\right)$. É facilmente verificável ainda que se t^* é um parâmetro local de P^*, então $\sigma(t^*)$ é um parâmetro local de $\sigma(P^*)$.

(a) Seja $0 \neq y \in F^*$. Logo, existe $z \in F^*$ tal que $y = \sigma(z)$. Escreva $z = (t^*)^r u$, com $r = v_{P^*}(z)$ e $u \in \mathcal{O}_{P^*} \backslash P^*$.

Assim, $y = \sigma(z) = \sigma(t^*)^r \sigma(u)$, e segue que $v_{\sigma(P^*)}(y) = r = v_{P^*}(z) = v_{P^*}\left(\sigma^{-1}(y)\right)$.

(b) Segue diretamente do fato de que $P \subseteq \sigma(P) \subseteq \sigma(P^*)$, uma vez que σ é um automorfismo de F^*/F e $P \subseteq F$.

(c) Seja x uma parâmetro local de P sobre F. Então, do item (a),

$$v_P(x)e(\sigma(P^*)|P) = v_{\sigma(P^*)}(x) = v_{P^*}\left(\sigma^{-1}(x)\right) = v_{P^*}(x) = v_P(x)e(P^*|P) = e(P^* \mid P).$$

Agora, o automorfismo σ de F^*/F induz um isomorfismo $\overline{\sigma}$ de $F^*_{P^*}$ em $F^*_{\sigma(P^*)}$, dado por

$$\overline{\sigma}\left(z + P^*\right) := \sigma(z) + \sigma(P^*).$$

Agora, quando restringimos $\overline{\sigma}$ a F_P, temos a identidade, uma vez que se $z \in F$ e $P \in \mathbb{P}_F$, tem-se

$$\overline{\sigma}(z + P) = \sigma(z) + \sigma(P) = z + P.$$

Portanto, $f(P^*|P) = f(\sigma(P^*)|P)$.

■

Lema 4.45. *Sejam $P \in \mathbb{P}_F$ e $P_1, \ldots, P_r \in \mathbb{P}_F$ todas as extensões de P em F'/F. Considere $k := \mathcal{O}_P/P$ e $k_i := \mathcal{O}_{P_i}/P_i \supseteq k$ os corpos de classes residuais e $\pi : \mathcal{O}_P \longrightarrow k$ e $\pi_i : \mathcal{O}_{P_i} \longrightarrow k_i$ as aplicações de classes residuais, $i = 1, \ldots, r$. Então, para todo $u \in \mathcal{O}'_P = \mathrm{ic}_{F'}(\mathcal{O}_P)$, tem-se*

$$\pi\left(\mathrm{Tr}_{F'/F}(u)\right) = \sum_{i=1}^{r} e\left(P_i \mid P\right) \cdot \mathrm{Tr}_{k_i/k}\left(\pi_i(u)\right).$$

Demonstração: Aqui usaremos a propriedade de que $\mathrm{Tr}_{F'/F}(u)$ pode ser avaliado como o traço da aplicação F-linear $\mu : F' \longrightarrow F$ dada por $\mu(z) = uz$.

Primeiramente, vamos mostrar que $\pi\left(\mathrm{Tr}_{F'/F}(u)\right)$ pode ser interpretada como o traço de uma certa aplicação k-linear $\mu : V \longrightarrow V$, onde V é uma k-espaço vetorial que definiremos adiante. Por fim, iremos decompor V em soma de subespaços invariantes e teremos a igualdade desejada.

Seja t um parâmetro local de P sobre F. Defina $V := \mathcal{O}'_P/t\mathcal{O}'_P$. Esse conjunto tem estrutura de k-espaço vetorial se considerarmos a multiplicação por escalar definida por $(x + P)\left(z + tO'_P\right) := xz + (tO'_P)$.

Seja $\{z_1, \ldots, z_n\}$ uma base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_{P'}$, onde $n = [F' : F]$. O conjunto $\{z_1 + t\mathcal{O}'_P, \ldots, z_n + t\mathcal{O}'_P\}$ forma uma base para V sobre k

De fato, basta mostrarmos que os elementos são linearmente independentes. Considere $\alpha_1, \ldots, \alpha_n \in k$, onde $\alpha_i = x_i + P$, tais que $\sum_{i=1}^{n} \alpha_i(z_i + t\mathcal{O}'_P) = 0$. Então

$$\sum_{i=1}^{n} \alpha_i(z_i + t\mathcal{O}'_P) = 0 \Rightarrow \sum_{i=1}^{n}(x_i + P)(z_i + t\mathcal{O}'_P) = 0 = \sum_{i=1}^{n} x_i z_i + t\mathcal{O}'_P = 0 \Rightarrow$$
$$\sum_{i=1}^{n} x_i z_i = 0 \Rightarrow x_i = 0 \Rightarrow \alpha_i \in P.$$

Logo, os elementos constituem uma base. Em particular, $\dim_k V = n$. Definimos agora a aplicação k -linear $\overline{\mu} : V \longrightarrow V$ por $\overline{\mu}(z + t\mathcal{O}'_P) = uz + t\mathcal{O}'_P$.

Seja $A = (a_{ij})_{1 \leq i,j \leq n}$ a matriz de μ com relação a base $\{z_1, \ldots, z_n\}$. Como essa base é integral e $u \in \mathcal{O}'_P$, então $a_{ij} \in \mathcal{O}_P$, para todo i, j. Ainda, $\overline{A} := (\pi(a_{ij}))_{1 \leq i,j \leq n}$ é a matriz de $\overline{\mu}$ com relação a base $\{z_1 + t\mathcal{O}'_P, \ldots, z_n + \mathcal{O}'_P\}$. Assim,

$$\pi\left(\mathrm{Tr}_{F'/F}(u)\right) = \pi(\mathrm{Tr}(A)) = \mathrm{Tr}(\bar{A}) = \mathrm{Tr}(\bar{\mu}). \quad (I)$$

Agora, para cada $i = 1, \ldots, r$, definimos os quocientes $V_i := \mathcal{O}_{P_i}/P_i^{e_i}$. Note que esses conjuntos estão bem definidos umas vez que se P_i é ideal, então $P_i^{e_i}$ também é. Assim, definimos as aplicações $\mu_i : V_i \longrightarrow V_i$ por

$$\mu_i\left(z + P_i^{e_i}\right) := uz + P_i^{e_i}.$$

Analogamente ao que provamos anteriormente, segue que V_i também é um k-espaço vetorial e consequentemente, μ_i é uma aplicação k-linear. Nesse caso, podemos construir o isomorfismo

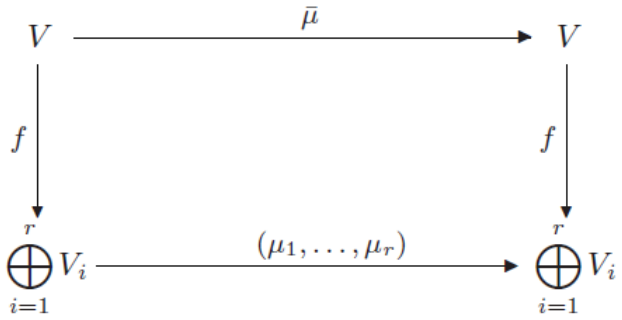
$$f : V \to \bigoplus_{i=1}^{r} V_i$$

dado por $f\left(z + t\mathcal{O}'_P\right) := (z + P_1^{e_1}, \ldots, z + P_r^{e_r})$.

A aplicação f é de fato um isomorfismo. Para verificarmos a injetividade, consideramos $f(z + t\mathcal{O}'_P) = 0$. Então, $z + P_i^{e_i} = 0$, para todo i. Assim,

$$z \in P_i \Rightarrow v_{P_i}(z) \geq e_i \Rightarrow v_{P_i}(z) \geq v_{P_i}(t) \Rightarrow v_{P_i}(zt^{-1}) \geq 0 \Rightarrow zt^{-1} \in \mathcal{O}'_P \Rightarrow z \in t\mathcal{O}'_P.$$

Agora, a sobrejetividade segue do teorema da aproximação forte. Temos então o seguinte diagrama:



onde $(\mu_1, \ldots, \mu_r)(v_1, \ldots, v_r) = (\mu_1(v_1), \ldots, \mu_r(v_r)), v_i \in V_i$. Como f é isomorfismo, então $\mathrm{Tr}(\bar{\mu}) = \mathrm{Tr}((\mu_1, \ldots, \mu_r)) = \sum_{i=1}^{n} \mathrm{Tr}(\mu_i)$.

Logo, por (I), segue que $\pi\left(\mathrm{Tr}_{F'/F}(u)\right) = \sum_{i=1}^{r} \mathrm{Tr}(\mu_i)$. Agora, restar mostrar que, podemos escrever cada parcela $\mathrm{Tr}(\mu_i)$ como $e_i \,\mathrm{Tr}_{k_i/k}(\pi_i(u))$.

Para isso, consideramos a cadeia de k-subespaços $V_i = V_i^{(0)} \supseteq V_i^{(1)} \supseteq \cdots \supseteq V_i^{(e_i)} = \{0\}$, onde $V_i^{(j)} := P_i^j / P_i^{e_i} \subseteq V_i$. Com uma rápida manipulação, é possível mostrarmos que esses espaços são invariantes sobre μ_i, ou seja, $\mu\left(V_i^{(j)}\right) \subseteq V_i^{(j)}$.

Assim, μ_i induz aplicações lineares da forma

$$\sigma_{ij} : \begin{cases} V_i^{(j)}/V_i^{(j+1)} & \longrightarrow & V_i^{(j)}/V_i^{(j+1)}, \\ [z + P_i^{e_i}] & \longmapsto & [u \cdot z + P_i^{e_i}] \end{cases}$$

com $j = 0, \ldots, e_i - 1$. Aqui, $[z + P_i^{e_i}]$ denota a classe residual de $z + P_i^{e_i}$ em $V_i^{(j)}/V_i^{(j+1)}$. Então $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i-1} \mathrm{Tr}(\sigma_{ij})$.

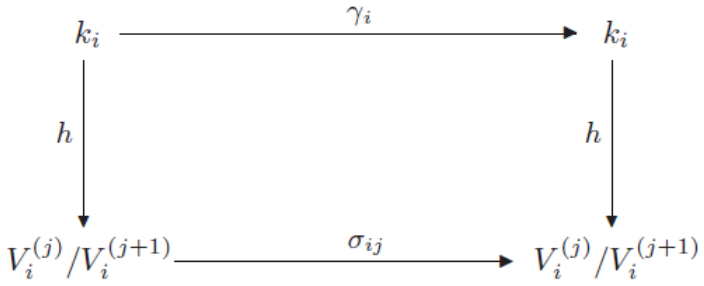
Sabemos ainda que, $\mathrm{Tr}_{k_i/k}(\pi_i(u)) = \mathrm{Tr}(\gamma_i)$, com $\gamma_i : k_i \to k_i$ uma aplicação k-linear dada por $\gamma_i(z + P_i) = uz + P_i$.

Agora, consideramos, para cada $j = 0, \ldots, e_i - 1$, um isomorfismo $h : k_i \to V_i^j / V_i^{j+1}$ de k-espaços vetoriais de tal forma que o diagrama a seguir comuta.

Como h é isomorfismo, segue que $\mathrm{Tr}(\gamma_i) = \mathrm{Tr}(\sigma_{ij})$. Agora, temos $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i-1} \mathrm{Tr}(\sigma_{ij})$ e $\mathrm{Tr}_{k_i/k}(\pi_i(u)) = \mathrm{Tr}(\gamma_i) = \mathrm{Tr}(\sigma_{ij})$. Logo, $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i-1} \mathrm{Tr}_{k_i/k}(\mu_i(u))$, e segue que $\mathrm{Tr}(\mu_i) = e_i \,\mathrm{Tr}_{k_i/k}(\pi_i(u))$, o que conclui a demonstração do lema.

■

Com esses dois lemas, podemos enunciar e demonstrar o teorema do diferente de Dedekind, o qual relaciona o expoente do diferente e o índice de ramificação.



Teorema 4.46. *(Diferente de Dedekind) Utilizando as notações já vistas durante esta seção, para todo $P'|P$,*

(a) $d(P'|P) \geq e(P'|P) - 1$.

(b) $d(P'|P) = e(P'|P) - 1 \Leftrightarrow \operatorname{char} K \nmid e(P'|P)$. Em particular, se $\operatorname{char} K = 0$, então $d(P'|P) = e(P'|P) - 1$.

Demonstração: (a) Seja $\mathcal{O}'_P = \mathrm{ic}_{F'}\,\mathcal{O}_P$ e $\mathcal{C}_P$ o módulo complementar sobre $\mathcal{O}_P$. Queremos mostrar que $\mathrm{Tr}_{F'/F}(t\mathcal{O}'_P) \subseteq \mathcal{O}_P$, para todo $t \in F'$ tal que $v_P(t) = 1 - e(P'|P)$, para todo $P'|P$.

Considere F^*/F uma extensão de Galois finita tal que $F \subseteq F' \subseteq F^*$ e escolha $n = [F' : F]$ automorfismos $\sigma_1, \ldots, \sigma_n$ de F^*/F cujas restrições a F' sejam distintos dois a dois. Dado $z \in \mathcal{O}'_P$, temos

$$\mathrm{Tr}_{F'/F}(tz) = \sum_{i=1}^{n} \sigma_i(tz). \quad (I)$$

Para P^* fixado tal que $P^*|P$, defina $P_i^* := \sigma_i^{-1}(P^*)$ e $P'_i = P^* \cap F'$. Agora, como $z \in \mathcal{O}'_P$, temos que $\sigma_i(z)$ é integral sobre $\mathcal{O}_P$. e portanto, $v_{P^*}(\sigma_i(z)) \geq 0$. Assim, usando o lema 4.44 e o fato de que $v_{P'}(t) = 1 - e(P'|P)$, temos

$$\begin{aligned} v_{P^*}(\sigma_i(t \cdot z)) &= v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z)) \\ &\geq v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) \\ &= e(P_i^*|P'_i)(1 - e(P'_i|P)) \\ &> -e(P_i^*|P'_i) \cdot e(P'_i|P) \\ &= -e(P_i^*|P) = -e(P^*|P) \end{aligned}$$

Então

$$-e(P^*|P) < v_{P^*}\left(\mathrm{Tr}_{F'/F}(tz)\right) = e(P^*|P) v_P\left(\mathrm{Tr}_{F'/F}(tz)\right),$$

ou seja,

$$v_P\left(\mathrm{Tr}_{F'/F}(tz)\right) > -1 \Rightarrow v_P\left(\mathrm{Tr}_{F'/F}(tz)\right) \geq 0 \Rightarrow \mathrm{Tr}_{F'/F}(tz) \in \mathcal{O}_P.$$

Agora, como $\mathrm{Tr}_{F'/F}(t\mathcal{O}'_P) \subseteq \mathcal{O}_P$, segue que $t \in \mathcal{C}_P$, e pela observação 3.4, temos

$$v'_P(t) \geq -d(P'|P) \Rightarrow 1 - e(P'|P) \geq -d(P'|P) \Rightarrow d(P'|P) \geq e(P'|P) - 1.$$

(b) Usaremos as mesmas notações do lema 4.45 e escrevemos $e_i := e(P_i|P)$. Seja $P' = P_1$ e $e = e(P'|P)$. Queremos mostrar que

$$d(P'|P) = e - 1 \Leftrightarrow \operatorname{char} K \nmid e.$$

($\Leftarrow$): Suponha que $\operatorname{char} K \nmid e$ e que $d(P'|P) \geq e$. Então, existe $w \in F'$ tal que

$$v_{P'}(w) \leq -e \quad \text{e} \quad \operatorname{Tr}_{F'/F}(w\mathcal{O}'_P) \subseteq \mathcal{O}_P.$$

Como K é perfeito, a extensão k_1/k é separável, e então existe $y_0 \in \mathcal{O}'_P$ tal que $\operatorname{Tr}(\pi_1(y_0)) \neq 0$.

Pelo teorema da aproximação forte, existe $y \in F'$ tal que $v_{P'}(y - y_0) > 0$ e $v_{P_i}(y) \geq \max\{1, e_i + v_{P_i}(w)\}$, com $2 \leq i \leq r$. Assim, $y \in \mathcal{O}'_P$, e pelo lema 4.45,

$$\pi\left(\operatorname{Tr}_{F'/F}(y)\right) = e \operatorname{Tr}_{k_1/k}(\pi_1(y)) + \sum_{i=2}^{r} e_i \operatorname{Tr}_{k_i/k}(\pi_i(y)).$$

Agora, como y foi tomado de forma que $y \in P_i$, para $i = 2, \ldots, r$, temos $\operatorname{Tr}_{k_i/k}(\pi_i(y)) = 0$. Para o caso $i = 1$, temos $\pi_1(y) = \pi_1(y_0)$.

Assim, $\pi\left(\operatorname{Tr}_{F'/F}(y)\right) = e \operatorname{Tr}_{k_1/k}(\pi_1(y_0)) \neq 0$, pois $\operatorname{char} K \nmid e$. Escolhemos $x \in F$ um parâmetro local para P. Então, como $v_P(x^{-1}) < 0$, $\operatorname{Tr}_{F'/F}(x^{-1}y) \notin O_P$.

Por outro lado, $x^{-1}yw^{-1} \in \mathcal{O}'_P$, pois

$$v_{P'}(x^{-1}yw^{-1}) = -v_{P'}(x) + v_{P'}(y) - v_{P'}(w) = -e + v_{P'}(y) - v_{P'}(w) \geq 0,$$

pois $v_{P'}(w) \leq -e$. Ainda,

$$v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P_i}(w)) \geq 0 \quad i = 2, \ldots, r.$$

Logo, $x^{-1}y \in w\mathcal{O}'_P$ e $\operatorname{Tr}_{F'/F}(x^{-1}y) \in \mathcal{O}'_P$, pois $\operatorname{Tr}_{F'/F}(w\mathcal{O}'_P) \subseteq \mathcal{O}_P$, o que contradiz o que fizemos anteriormente. Portanto, $d(P'|P) \leq e \Rightarrow d(P'|P) = e(P'|P) - 1$.

($\Rightarrow$): Suponha agora que $\operatorname{char} K | e$, e mostremos que obrigatoriamente teremos $d(P'|P) \geq e$.

Seja $u \in F'$ tal que $v_{P'}(u)$ e $v_{P_i}(u) \geq -e_i + 1$, para $i = 2, \ldots, r$. Novamente, tomamos x uma parâmetro local de P, e dado $z \in \mathcal{O}'_P$,

$$v_{P'}(xuz) = v_{P'}(x) + v_{P'}(u) + v_{P'}(z) = v_{P'}(z) \geq 0$$

e

$$v_{P_i}(xuz) = v_{P_i}(x) + v_{P_i}(u) + v_{P_i}(z) \geq e_i - e_i + 1 + v_{P_i}(z) > 0.$$

Logo, $xuz \in \mathcal{O}'_P$. Pelo lema 4.45,

$$\pi\left(\operatorname{Tr}_{F'/F}(xuz)\right) = e \operatorname{Tr}_{k_1/k}(\pi_1(xuz)) = 0.$$

Então

$$\operatorname{Tr}_{F'/F}(xuz) = x \operatorname{Tr}_{F'/F}(uz) \in P = x\mathcal{O}_P \Rightarrow \operatorname{Tr}_{F'/F}(uz) \in \mathcal{O}_P, \forall z \in \mathcal{O}'_P.$$

Assim, $u \in \mathcal{C}_P$ e pela observação 4.35, $-e = v_{P'}(u) \geq -d(P'|P)$, o que contraria a hipótese de que $(P'|P) = e - 1$. Portanto, $\operatorname{char} K \nmid e$.

■

Definição 4.47. *Sejam F'/F uma extensão algébrica de corpos de funções e $P \in \mathbb{P}_F$.*

(a) Uma extensão P' de P em F' é dita mansamente ramificada se $e(P'|P) > 1$ e $\operatorname{char} K \nmid e(P'|P)$ e é dita selvagemente ramificada se $e(P'|P) > 1$ e $\operatorname{char} K \mid e(P'|P)$.

(b) Dizemos que P é ramificado em F'/F se existe pelo menos um $P' \in \mathbb{P}_{F'}$ tal que P' estende P e $P'|P$ é ramificada. Se para todo $P' \in \mathbb{P}_{F'}$ tal que $P'|P$ tivermos $P'|P$ não ramificada, então P é dito não ramificado.

(c) P é dito mansamente ramificado em F'/F se for ramificado e toda extensão P' de P for mansamente ramificada. Em contrapartida, se existe P' uma extensão de P tal que P' é selvagemente ramificado, então P é dito selvagemente ramificado.

(d) P é dito totalmente ramificado em F'/F se existe apenas uma extensão P' de P em F', e $e(P'|P) = [F' : F]$.

(e) A extensão F/F' é dita ramificada se pelo menos um de seus lugares o for. Caso contrário, é dita não ramificada.

(f) F'/F é dita ser mansa se nenhum $P \in \mathcal{O}_P$ for selvagemente ramificado em F'/F.

Com essa definição, temos dois corolários cujas demonstrações seguem de maneira imediata utilizando o teorema de Dedekind.

Corolário 4.48. *Seja F'/F uma extensão finita e separável de corpos de funções algébricas.*

(a) Se $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ são tais que P' estende P, então $P'|P$ é ramificada se, e somente se, $P' \leq \operatorname{Diff}(F'/F)$.

No caso em que $P'|P$ for ramificada, valem ainda as seguintes equivalências:

$$d(P'|P) = e(P'|P) - 1 \Leftrightarrow P'|P \text{ é mansamente ramificada; e}$$
$$d(P'|P) \geq e(P'|P) \Leftrightarrow P'|P \text{ é selvagemente ramificada.}$$

(b) Quase todos os lugares $P \in \mathbb{P}_F$ são não ramificados em F'/F.

Corolário 4.49. *Sejam F'/F uma extensão finita e separável de corpos de funções com mesmo corpo de constante K. Então F/K e F'/K' possuem o mesmo gênero.*

O próximo resultado é uma versão do teorema do elemento primitivo para corpos de funções.

Teorema 4.50. *(Lüroth) Todo subcorpo de um corpo de funções racionais é racional, isto é, se $K \subsetneq F_0 \subseteq K(x)$, então $F_0 = K(y)$, para algum $y \in F_0$.*

Demonstração: Vamos dividir a demonstração em dois casos.

Caso 1: $K(x)/F_0$ separável. Podemos então usar a fórmula do gênero de Hurwitz. Seja g_0 o gênero de F_0/K. Então,

$$2g - 2 = \frac{[K(x) : F_0]}{[K : K]}(2g_0 - 2) + \deg \operatorname{Diff}(K(x)/F_0) \Rightarrow$$
$$\Rightarrow -2 = [K(x) : F_0](2g_0 - 2) + \deg \operatorname{Diff}(K(x)/F_0)$$

Para a igualdade ser satisfeita, devemos ter $2g_0 - 2 < 0$, ou seja, $g_0 < 0 \Rightarrow g_0 = 0$. Agora, seja $P \in \mathbb{P}_{K(x)}$ de grau 1. Então $P_0 = P \cap F_0 \in \mathbb{P}_{F_0}$ e tem grau 1 também. Pela proposição 2.69, F_0/K é racional.

Caso 2: $K(x)/F_0$ não separável. Existe então um subcorpo F_1 com $F_0 \subseteq F_1 \subseteq K(x)$ e F_1/F_0 é separável e $K(x)/F_1$ é puramente inseparável.

Se provarmos que F_1/K é racional, cairemos no caso 1 e o resultado seguirá. Observe que, como $K(x)/F_1$ é puramente inseparável, então $[K(x) : F_1] = q = p^n$, onde $p = \operatorname{char} K > 0$ e $z^q \in F_1$, para todo $z \in K(z)$. Em particular,

$$K(x^q) \subseteq F_1 \subseteq K(x).$$

Agora, pelo teorema 2.45, $[K(x) : K(x^q)] = q$. Pela multiplicidade dos graus segue que $[F_1 : K(x^q)] = 1$, ou seja, F_1 é racional, e segue o resultado.

■

Teorema 4.51. *Seja $F' = F(y)$ uma extensão finita e separável de um corpo de funções F de grau $[F' : F] = n$. Sejam $P \in \mathbb{P}_F$ tal que o polinômio minimal $\varphi(t)$ de y sobre $F(t)$ tenha coeficientes em $\mathcal{O}_P$, ou seja, y é integral sobre $\mathcal{O}_P$, e $P_1, \ldots, P_r \in \mathbb{P}_F$ todas as extensões de P em F'. Então,*

(a) $d(P_i \mid P) \leq v_{P_i}(\varphi'(y)), i = 1, \ldots, r$.

(b) $\{1, y, \ldots, y^{n-1}\}$ é uma base integral de F'/F em $P \Leftrightarrow v_{P_i}(\varphi'(y)) = d(P_i \mid P)$, $i = 1, \ldots, r$, onde $\varphi'(t)$ é a derivada de $\varphi(t)$.

Demonstração: Primeiramente, mostremos algumas afirmações que nos serão úteis na demonstração dos itens (a) e (b).

Pela proposição 4.32, a base dual de $\{1, y, \ldots, y^{n-1}\}$ está fortemente relacionada com os expoentes dos diferentes $d(P_i|P)$. Por isso, vamos determinar essa base dual. Como $\varphi(y) = 0$, podemos escrever $\varphi(t)$ em $F'[t]$ da forma

$$\varphi(t) = (t - y)\left(c_{n-1}t^{n-1} + \cdots + c_1 t + c_0\right) \text{ com } c_0, \ldots, c_{n-1} \in F' \text{ e } c_{n-1} = 1.$$

Afirmação 1: $B = \left\{\dfrac{c_0}{\varphi'(y)}, \ldots, \dfrac{c_{n-1}}{\varphi'(y)}\right\}$ é base dual de $\{1, y, \ldots, y^{n-1}\}$.

Note que $\varphi'(y) \neq 0$, já que y é separável sobre F. Para mostrarmos a afirmação, é suficiente mostrar que

$$\operatorname{Tr}_{F'/F}\left(\frac{c_i}{\varphi'(y)} \cdot y^l\right) = \delta_{il} \quad \text{para } 0 \leq i, l \leq n-1,$$

onde δ_{il} denota o símbolo de Kronecker.

Considere $\sigma_1, \ldots, \sigma_n$ injeções distintas de F'/F em Φ, onde Φ denota uma extensão algebricamente fechada de F. Defina $y_j := \sigma_j(y)$. Assim,

$$\varphi(t) = \prod_{j=1}^{n}(t - y_j).$$

Derivando a equação e substituindo $t = y_\nu$,

$$\varphi'(y_\nu) = \prod_{i \neq \nu}(y_\nu - y_i).$$

Agora, para cada $0 \leq l \leq n-1$, consideramos o polinômio

$$\varphi_l(t) := \left(\sum_{j=1}^{n} \frac{\varphi(t)}{t - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)}\right) - t^l \in \Phi[t].$$

Seu grau é, no máximo $n-1$ e para $1 \leq \nu \leq n$,

$$\varphi_l(y_\nu) = \left(\prod_{i \neq \nu}(y_\nu - y_i)\right) \cdot \frac{y_\nu^l}{\varphi'(y_\nu)} - y_\nu^l = 0.$$

Assim, φ_l tem grau no máximo $n-1$ e n raízes, e segue que $\varphi_l = 0$, ou seja,

$$t^l = \sum_{j=1}^{n} \frac{\varphi(t)}{t-y_j} \cdot \frac{y_j^l}{\varphi'(y_j)}, \quad 0 \leq l \leq n-1.$$

As injeções $\sigma_i : F' \longrightarrow \Phi$ podem ser estendidas em injeções $\sigma_i : F'[t] \longrightarrow \Phi[t]$, colocando $\sigma_i(t) = t$. Assim obtemos

$$\begin{aligned} t^l &= \sum_{j=1}^{n} \sigma_j \left(\frac{\varphi(t)}{t-y} \cdot \frac{y^l}{\varphi'(y)}\right) \\ &= \sum_{j=1}^{n} \sigma_j \left(\sum_{i=0}^{n-1} c_i t^i \cdot \frac{y^l}{\varphi'(y)}\right) \\ &= \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n} \sigma_j \left(\frac{c_i}{\varphi'(y)} \cdot y^l\right)\right) t^i \\ &= \sum_{i=0}^{n-1} \mathrm{Tr}_{F'/F} \left(\frac{c_i}{\varphi'(y)} \cdot y^l\right) t^i. \end{aligned}$$

Comparando os coeficientes, $\mathrm{Tr}_{F'/F}\left(c_i \frac{y^l}{\varphi'(y)}\right) = \delta_{il}, 0 \leq i, l \leq n-1$, como queríamos mostrar, e segue a afirmação 1.

Afirmação 2: $c_j \in \sum_{i=1}^{n-1} \mathcal{O}_P \cdot y^i$, para $j = 0, \ldots, n-1$.

Observe que o polinômio minimal $\varphi(t)$ de y sobre F é da forma $\varphi(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$, com $a_i \in \mathcal{O}_P$. Por outro lado, sabemos que

$$\varphi(t) = (t-y)(c_{n-1}t^{n-1} + \cdots + c_1 t + c_0) = c^{n-1}t^n + (-yc_{n-1}c_{n-2})t^{n-1} + \cdots + (-yc_1 + c_0)t + (-yc_0).$$

Comparando os coeficientes, obtemos

$$c_{n-1} = 1,\ c_0 y = -a_0 \text{ e } c_i y = c_{i-1} - a_i, \text{ para } 1 \leq i \leq n-1.$$

Para $j = n-1$, $c_{n-1} = 1 \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$. Suponha que exista $j \in \{0, \ldots, n-1\}$ tal que

$$c_j = \sum_{i=0}^{n-1} s_i y^i, \text{ com } s_i \in \mathcal{O}_P.$$

Pelo que fizemos acima,

$$\begin{aligned} c_{j-1} &= a_j + c_j y = a_j + \sum_{i=0}^{n-2} s_i y^{i+1} + s_{n-1} y^n \\ &= a_j + \sum_{i=0}^{n-2} s_i y^{i+1} - s_{n-1} \sum_{i=0}^{n-1} a_i y^i \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i, \end{aligned}$$

e isso prova a afirmação. Analogamente, podemos mostrar a seguinte afirmação:

Afirmação 3: $y^j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i$, para $j = \ldots, n-1$.

Para $j = 0$, temos $y^0 = 1 \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i$. Agora, se existe $j \geq 0$ tal que $y^j = \sum_{i=0}^{n-1} r_i c_i$, com $r_i \in \mathcal{O}_P$, pelo mesmo argumento que fizemos anteriormente,

$$\begin{aligned} y^{j+1} &= \sum_{i=0}^{n-1} r_i c_i y = \sum_{i=1}^{n-1} r_i \left(c_{i-1} - a_i\right) - r_0 a_0 \\ &= \sum_{i=0}^{n-2} r_{i+1} c_i - \left(\sum_{i=0}^{n-1} r_i a_i\right) \cdot c_{n-1} \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i. \end{aligned}$$

Agora, podemos mostrar o item (a) do teorema. Consideramos o módulo complementar $\mathcal{C}_P$ e $\mathcal{O}'_P = \mathrm{ic}_{F'}(\mathcal{O}_P)$. Queremos mostrar que $d(P_i|P) \leq v_{P_i}\left(\varphi'(y)\right)$, o que é equivalente a mostrar que $z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geq -v_{P_i}\left(\varphi'(y)\right)$, pars $i = 1, \ldots, r$.

Seja $z \in \mathcal{C}_P$ e escreva $z = \sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)}$, com $r_i \in F$. , uma vez que pela afirmação 1, o conjunto B forma uma base de F'/F. Como y^l é integral sobre $\mathcal{O}_P$ e $z \in \mathcal{C}_P$, então

$$\mathrm{Tr}_{F'/F}\left(zy^l\right) \in O_P, \quad l = 0, \ldots, n-1.$$

Agora, pela afirmação 1,

$$\mathrm{Tr}_{F'/F}\left(z \cdot y^l\right) = \mathrm{Tr}_{F'/F}\left(\sum_{i=0}^{n-1} r_i \cdot \frac{c_i}{\varphi'(y)} \cdot y^l\right) = r_l.$$

Logo, $r_l \in \mathcal{O}_P$. Da afirmação 2,

$$z \in \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} \mathcal{O}_P y^i \subseteq \frac{1}{\varphi'(y)} \mathcal{O}'_P.$$

Portanto, $z\varphi'(y) \in \mathcal{O}'_P$, e segue que $v_{P_i}(z\varphi'(y)) \geq 0$, logo $v_{P_i}(z) \geq -v_{P_i}(\varphi'(y))$, para todo $i = 0, \ldots, n-1$, e segue o item (a).

(b) Pelas afirmações 2 e 3, segue que $\sum_{i=0}^{n-1} \mathcal{O}_P y^i = \sum_{j=0}^{n-1} \mathcal{O}_P c_j$.

($\Rightarrow$) Seja $\{1, y, \ldots, y^{n-1}\}$ uma base integral de P. Pela afirmação 1 e a proposição 4.32,

$$\begin{aligned} \mathcal{C}_P &= \sum_{i=0}^{n-1} \mathcal{O}_P \cdot \frac{c_i}{\varphi'(y)} = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i \\ &= \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P. \end{aligned}$$

Por outro lado, $\mathcal{C}_P = t\mathcal{O}'_P$, onde $d\left(P_i|P\right) = -v_{P_i}(t)$, $\forall P_i|P$. Então,

$$d\left(P_i|P\right) = -v_{P_i}\left(\frac{1}{\varphi'(y)}\right) = v_{P_i}\left(\varphi'(y)\right), \quad i = 0, \ldots, n-1.$$

($\Leftarrow$): Reciprocamente, suponha $d\left(P_i|P\right) = v_{P_i}\left(\varphi'(y)\right)$. Queremos mostrar que $\mathcal{O}'_P \subseteq \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$, pois a outra inclusão é trivial.

Seja $z \in \mathcal{O}'_P$ e escreva $z = \sum_{i=0}^{n-1} t_i y^i$, $t_i \in F$. Pela afirmação 2, segue que $c_j \in \mathcal{O}'_P$. Ainda, da hipótese e da proposição 4.32, segue que $\mathcal{C}_P = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P$. Logo,

$$\mathrm{Tr}_{F'/F}\left(\frac{1}{\varphi'(y)} \cdot c_j \cdot z\right) \in \mathcal{O}_P.$$

Portanto, como

$$\mathrm{Tr}_{F'/F}\left(\frac{1}{\varphi'(y)} \cdot c_j \cdot z\right) = \mathrm{Tr}_{F'/F}\left(\sum_{i=0}^{n-1} t_i \cdot \frac{c_j}{\varphi'(y)} \cdot y^i\right) = t_j,$$

concluimos que $t_j \in \mathcal{O}_P$, o que conclui a demonstração.

■

Corolário 4.52. *Sejam $F' = F(y)$ uma extensão finita e separável de corpos de funções de grau n e $\varphi(t) \in F[t]$ o minimal de y sobre F. Suponha ainda, que $P \in \mathbb{P}_F$ é tal que*

$$\varphi(T) \in \mathcal{O}_P[T] \text{ e } v_{P'}\left(\varphi'(y)\right) = 0.$$

Então P é não ramificado em F'/F e $\{1, y, \ldots, y^{n-1}\}$ é base integral de F'/F em P.

Demonstração: Pelo teorema 4.51 (a),

$$0 \leq d(P'|P) \leq v_{P'}\left(\varphi'(y)\right), \ \forall P'|P \Rightarrow d(P'|P) = v_{P'}\left(\varphi'(y)\right) = 0,$$

e do item (b) do mesmo teorema, segue que $\{1, y, \ldots, y^{n-1}\}$ é base integral de F'/F em P. Agora, o teorema 4.46 garante que $e(P'|P) = 1$, para todo P' que estende P, e portanto, P é não ramificado em F'/F.

■

Encerramos esta seção com uma condição suficiente para que as potências de um elemento de F' formem uma base integral para um lugar P.

Proposição 4.53. *Sejam F'/F uma extensão finita e separável de corpos de funções, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$, com $P'|P$. Suponha que $P'|P$ é totalmente ramificado, ou seja, $e(P'|P) = [F' : F] = n$. Considere $t \in F'$ um parâmetro local de P' e φ o polinômio minimal de t sobre F. Então $d(P'|P) = v_{P'}\left(\varphi'(t)\right)$ e $\{1, t, \ldots, t^{n-1}\}$ é base integral e F'/F em P.*

Demonstração: Queremos mostrar que $B = \{1, t, \ldots, t^{n-1}\}$ é base integral de F'/F em P. Primeiro mostremos que B é linearmente independente. Assuma que não, ou seja, existem $r_i \in F$ não todos nulos tais que

$$\sum_{i=0}^{n-1} r_i t^i = 0.$$

Para os índices i tais que $r_i \neq 0$,

$$v_{P'}(r_i t^i) - v_{P'}(r_i) + i v_{P'}(t) = v_{P'}(r_i) + 1 = n v_P(r_i) + i \equiv i \pmod{n}.$$

Portanto, se i, j são tais que $i \neq j$ e $r_i \neq r_j$, segue que $v_{P'}\left(r_i t^i\right) \neq v_{P'}\left(r_j t^j\right)$. Assim, da desigualdade triangular estrita,

$$v_{P'}\left(\sum_{i=0}^{n-1} r_i t^i\right) = \min\left\{v_{P'}\left(r_i t^i\right); r_i \neq 0\right\} < \infty,$$

o que é absurdo. Logo, B é linearmente independente sobre F, e segue que B é base de F'/F. Do teorema 4.11 sabemos que $\sum e_i f_i = n$. Como $e(P'|P) = n$, então P' é o único lugar de F' que estende P, e portanto, $\mathcal{O}_{P'} = \mathrm{ic}_F(\mathcal{O}_P)$. Então, precisamos mostrar que

$$\mathcal{O}_{P'} = \sum_{i=0}^{n-1} \mathcal{O}_P \cdot t^i.$$

Seja $z \in \mathcal{O}_{P'}$ não nulo. Então, como B é base de F'/F, existem x_i's em F tais que $z = \sum_{i=0}^{n-1} x_i t^i$. Pelo mesmo argumento feito anteriormente, segue que

$$0 \leq v_{P'}(z) = \min\left\{n v_P\left(x_i\right) + i; 0 \leq i \leq n-1, \text{ com } x_i \neq 0\right\}.$$

Assim, $v_P(x_i) \geq 0$, e segue que $x_i \in \mathcal{O}_P$, e portanto, $z \in \sum_{i=1}^{n-1} \mathcal{O}_P \cdot t^i$. Como a outra inclusão é imediata, segue que $1, t, \ldots, t^{n-1}$ é base integral. Do teorema 4.51, item (b), segue que $d(P'|P) = v_{P'}\left(\varphi'(t)\right)$.

■

4.6 Extensões de corpos constantes

Aqui, continuamos com as notações da seção anterior e ressaltamos que K é um corpo perfeito, e este fato será essencial na demonstração dos resultados desta seção. Também fixamos $\Phi \supseteq F$ um corpo algebricamente fechado.

Consideramos $K' \supseteq K$ uma extensão algébrica tal que $K' \subseteq \Phi$. Estaremos interessados em estudar o corpo de funções F'/K', onde $F' = FK'$ é o compósito de F e K', e seu corpo das constantes é uma extensão finita de K'.

A princípio, não sabemos se K' é o corpo das constantes de F'/K'. Para provarmos que K' é de fato esse corpo das constantes, precisamos do lema a seguir, o qual generaliza o lema 4.10.

Lema 4.54. *Seja $\alpha \in \Phi$ algébrico sobre K. Então $[K(\alpha) : K] = [F(\alpha) : F]$.*

Demonstração: Sejam $[K(\alpha) : K] = n = \deg\left(\min_K \alpha\right)$ e $[F(\alpha) : F] = m = \deg\left(\min_F \alpha\right)$. Como $K \subseteq F$, então $n \geq m$. Resta mostrar que $\min_K \alpha$ se mantém irredutível sobre F.

Seja $\varphi(t) \in K[t]$ o polinômio minimal de α sobre K, e escrevemos $\varphi(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$, com $a_i \in K$. Suponha que $\varphi(t)$ é irredutível sobre F, ou seja, existem $g(t), h(t) \in F[t]$ com $\deg g(t), \deg h(t) \geq 1$, tais que $\varphi(t) = g(t) \cdot h(t)$.

Como $g(t), h(t) \in F[t]$ e $F \subseteq \Phi$, então todas as raízes de $g(t)$ e $h(t)$ estão em Φ, e portanto, toda raiz de $\varphi(t)$ também está. Assim, todas as raízes de $\varphi(t)$ são algébricas sobre K, ou seja, os coeficientes de $g(t)$ e $h(t)$ são algébricos sobre K.

Por outro lado, esses elementos estão em F, e como K é o corpo das constantes de F, eles também estão em K, o que implica que $g(t), h(t) \in K[t]$, o que é absurdo pela irredutibilidade de $\varphi(t)$ sobre K.

■

Podemos então demonstrar o seguinte resultado:

Proposição 4.55. *Seja $F' = FK'$ uma extensão algébrica constante de F/K, podendo ser finita ou infinita. Então*

(a) K' é o corpo das constantes de F'.

(b) Se $S \subseteq F$ é linearmente independente sobre K, então também o é sobre K'

(c) $[F : K(x)] = [F' : K'(x)]$, para todo $x \in F \backslash K$.

Demonstração: (a) Considere $\gamma \in F'$ algébrico sobre K'. Como K'/K é algébrica, então γ é algébrico sobre K.

Como $F' = FK'$, então existem $\alpha_1, \ldots, \alpha_r \in K'$ tais que $\gamma \in F(\alpha_1, \ldots, \alpha_r)$. Considere a extensão finita separável $K(\alpha_1, \ldots, \alpha_r)/K$. Pelo teorema do elemento primitivo, existe $\alpha \in K'$ tal que $K(\alpha_1, \ldots, \alpha_r) = K(\alpha)$.

Agora, como γ é algébrico sobre K, existe $\beta \in F'$ tal que $K(\alpha, \gamma) = K(\beta)$. Logo,

$$F(\beta) = F(\alpha, \gamma) = F(\alpha), \text{ pois } \gamma \in F(\alpha_1, \ldots, \alpha_r).$$

Pelo lema 4.54, $[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K], \text{com } K(\alpha) \subseteq K(\beta)$. Como $K(\alpha) \subseteq \mathbb{K}(\alpha, \gamma) = K(\beta)$, então vale a igualdade. Logo, $\gamma \in K(\beta) = K(\alpha) \subseteq K'$, e segue que K' é o corpo completo das constantes de F'.

■

(b) Sejam $y_1, \ldots, y_r \in F$ linearmente independentes sobre F e

$$\sum_{i=1}^{r} \gamma_i y_i = 0, \text{ com } \gamma_i \in K'.$$

Uma vez que K é perfeito, existe $\alpha \in K'$ tal que $\gamma_1, \ldots, \gamma_r \in K(\gamma_1, \ldots, \gamma_r) = K(\alpha)$. Então, escrevemos

$$\gamma_i = \sum_{j=0}^{n-1} c_{ij}\alpha^j, \text{ com } c_{ij} \in K \text{ e } n = [K(\alpha) : K].$$

Assim,

$$\sum_{j=0}^{n-1} \left(\sum_{i=1}^{r} c_{ij} y_i \right) \alpha^j = 0,$$

onde $\sum_{i=1}^{r} c_{ij} y_i \in F$. Pelo lema 4.54, $[F(\alpha) : F] = [K(\alpha) : K] = n$, portanto os elementos $1, \alpha, \ldots, \alpha^{n-1}$ são linearmente independentes sobre F, e assim, $\sum_{i=1}^{r} c_{ij} y_i = 0$, para $j = 0, \ldots, n-1$. Agora, usando o fato de que $y_1, \ldots, y_r$ são linearmente independentes sobre K, segue que $c_{ij} = 0$, ou seja, $\gamma_i = 0$, para todo i.

(c) Como $[F' : K'(x)] \leq [F : K(x)]$, basta mostrarmos a outra desigualdade. Para isso mostraremos que se $z_1, \ldots, z_s \in F$ são linearmente independentes sobre $K(x)$, então esses elementos continuam independentes sobre $K(x)$.

Suponha que existam $f_i(x) \in K'(x)$, não todos nulos tais que

$$\sum_{i=1}^{s} f_i(x) z_i = 0.$$

Multiplicando por um denominador comum, podemos assumir que todo $f_i(x) \in K'[x]$. Assim, a relação acima nos fornece uma dependência linear do conjunto $\{x^j z_i \mid 1 \leq i \leq s \text{ e } j \geq 0\}$ sobre K.

Do item (b), obtemos que esse conjunto é linearmente dependente sobre K, e portanto, teríamos $z_1, \ldots, z_n$ dependentes sobre $K(x)$, o que é absurdo. Portanto, fica demonstrada a igualdade.

■

Encerramos esta seção com um teorema que relaciona o grau de um divisor com o grau de sua conorma para casos em que temos extensões de corpos constante, e um corolário que fornece uma fórmula para o cálculo do grau da conorma no caso geral. Ainda, é possível mostrar que ambos possuem a mesma dimensão, como espaços vetoriais.

Teorema 4.56. *Seja $F' = FK'$ uma extensão de corpos algébrica constante de F/K. Então:*

(a) $\deg \mathrm{Con}_{F'/F}(A) = \deg A$, *para todo* $A \in \mathrm{Div}(F)$.

(b) F'/F é não ramificado.

(c) Se K'/K é finita, toda base de K'/K é uma base integral de F'/F, para todo $P \in \mathbb{P}_F$.

(d) F'/K' e F/K possuem o mesmo gênero.

Demonstração: (a) Basta mostrarmos para o caso em que $P \in \mathbb{P}_F$ é um divisor primo. Seja $x \in F$ tal que P é o único zero de x em $\mathbb{P}_F$. Esse elemento existe pela proposição 2.71. Então, o divisor zero $\langle x \rangle_0^F$ de x em $\mathrm{Div}(F)$ é da forma $\langle r \rangle_o^F = rP$, com $r > 0$. Assim, da proposição 4.9,

$$\langle x \rangle_0^{F'} = \mathrm{Con}_{F'/F}\left(\langle x \rangle_0^F\right) = r \cdot \mathrm{Con}_{F'/F}(P).$$

Como pelo teorema 2.45, $[F' : K'(x)] = \deg\left(\langle x \rangle_0^{F'}\right)$, segue que

$$\begin{aligned} r \cdot \deg \mathrm{Con}_{F'/F}(P) &= [F' : K'(x)] \\ &= [F : K(x)] \\ &= \deg\left((x)_0^F\right) = r \cdot \deg P, \end{aligned}$$

Como P é um divisor primo qualquer, então a afirmação é válida para todo $A \in \mathrm{Div}(F)$.

(b) Consideramos primeiramente o caso em que temos uma extensão de corpos constante finita. Logo, como K é perfeito, existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Nesse caso, como $K \subseteq F$, segue que $F' = FK' = FK(\alpha) = F(\alpha)$. Considere $\varphi(t)$ o polinômio minimal de α sobre K. Então pelo lema 4.54, $\varphi(t)$ é irredutível sobre F. Considere $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$.

Pelo teorema 4.51 o expoente do diferente satisfaz

$$0 \leq d(P'|P) \leq v_{P'}\left(\varphi'(\alpha)\right).$$

Agora, α é separável sobre K, e segue que $\varphi'(\alpha) \neq 0$. Assim, como $\varphi'(\alpha) \in K'$, temos $v_{P'}\left(\varphi'(\alpha)\right) = 0$. Pelo teorema de Dedekind, $d(P'|P) = 0$, e portanto $P'|P$ é não ramificado (esse caso será importante para provarmos o item (c)).

Agora, para o caso geral, consideramos $P' \in \mathbb{P}_F$ tal que $P'|P$ e $t \in F'$ um parâmetro local de P'. Então $P' = t\mathcal{O}_{P'}$. Considere a extensão K'/K. Então existe K_1 corpo tal que $K \subseteq K_1 \subseteq K'$ tal que $[K_1 : K] < \infty$ e $t \in F_1 = FK'$. Seja $P_1 := P' \cap F_1$. Então

$$1 = v_{P'}(t) = e(P'|P)v_{P_1}(t) \Rightarrow e(P'|P_1) = 1.$$

Já vimos que $e(P_1|P) = 1$, pelo caso finito, e da proposição 4.6, segue que $e(P'|P) = 1$, isto é, $P'|P$ é não ramificado.

(c) Como K é perfeito, então existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Defina $n = [K' : K]$. Nesse caso, pelo item (a), temos $d(P'|P) = v_{P'}(\varphi'(\alpha))$. Logo, pelo teorema 4.51, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base integral de F'/F, para todo $P \in \mathbb{P}_F$.

Agora, se considerarmos $\{\gamma_1, \ldots, \gamma_n\}$ uma outra base qualquer de K'/K,

$$\sum_{i=0}^{n-1} \mathcal{O}_P \cdot \alpha^i = \sum_{j=1}^{n} \mathcal{O}_P \cdot \gamma_j.$$

Assim $\{\gamma_1, \ldots, \gamma_n\}$ é também base integral de F'/F.

(d) Sejam g o gênero de F/K e F'/K'. No caso finito, podemos aplicar a fórmula do gênero de Hurwitz. Já vimos no item (a) que $d(P'|P) = 0$, e segue que $\mathrm{Diff}(F'/F) = 0$, e portanto seu grau é zero.

Pelo lema 4.54 temos $[F' : F] = [F(\alpha) : F] = [K(\alpha) : K] = [K' : K]$. Logo, pela fórmula do gênero de Hurwitz, $g' = g$.

Provemos agora o caso geral, onde podemos ter uma extensão de grau infinito.

Afirmação 1: $\ell(A) \leq \ell(\mathrm{Con}_{F'/F}(A))$, para todo $A \in \mathrm{Div}\, F$.

Seja $\{x_1, \ldots, x_r\}$ uma base de $\mathcal{L}(A)$. Assim, da proposição 4.9, temos $x_i \in \mathcal{L}(\mathrm{Con}_{F'/F}(A))$. Agora, pela proposição 4.55, $\{x_1, \ldots, x_r\}$ é linearmente independente sobre K', o que prova a afirmação.

Escolha $C \in \mathrm{Div}(F)$ tal que $\deg C \geq \max\{2g - 1, 2g' - 1\}$. Do teorema de Riemann-Roch, segue que $\ell(C) = \deg C + 1 - g$ e, usando o item (c), temos tambem $\ell(\mathrm{Con}_{F'/F}(C)) = \deg C + 1 - g'$.

Da afirmação 1, segue que $g' \leq g$. Agora, considere $\{u_1, \ldots, u_s\}$ uma base de $\mathcal{L}(\mathrm{Con}_{F'/F}(C))$. Existe K_0 um corpo tal que $K \subseteq K_0 \subseteq K'$, tal que $[K_0 : K] < \infty$ e $u_1, \ldots, u_s \in F_0 = FK_0$. Obviamente $u_1, \ldots, u_s \in \mathcal{L}(\mathrm{Con}_{F_0/F}(C))$ e então

$$\ell(\mathrm{Con}_{F_0/F}(C)) \geq \ell(\mathrm{Con}_{F'/F}(C)).$$

Pelo que fizemos no caso finito, F_0/K_0 tem gênero g, e do teorema de Riemann-Roch,

$$\ell(\mathrm{Con}_{F'/F}(C)) = \deg C + 1 - g,$$

ou seja, $-g \geq -g'$, logo $g' \geq g$, e segue o item (d).

■

Corolário 4.57. *Seja F'/K' uma extensão algébrica de F/K. Então para cada $A \in \mathrm{Div}(F)$,*

$$\deg \mathrm{Con}_{F'/F}(A) = [F' : FK'] \cdot \deg A.$$

Demonstração: Se F'/K' for uma extensão de corpos constante, o resultado segue diretamente do teorema 4.56.

Para o caso geral, o lema 4.2 garante que $[F' : FK'] < \infty$, e FK'/K' é uma extensão de corpos constante de F/K. Agora, como

$$\mathrm{Con}_{F'/F}(A) = \mathrm{Con}_{F'/FK'}\left(\mathrm{Con}_{FK'/F}(A)\right),$$

segue do corolário 4.13 e do teorema 4.56 que

$$\deg \mathrm{Con}_{F'/F}(A) = [F' : FK'] \cdot \deg \mathrm{Con}_{FK'/F}(A) = [F' : FK'] \cdot \deg A.$$

■

4.7 Extensões de Galois

Vamos investigar nesta seção, como se comportam as extensões de Galois de um corpo de funções. Esses tipos de extensões possuem muitas propriedades que outras extensões arbitrárias não possuem. Veremos também dois tipos especiais de extensões de Galois: as extensões de Kummer e as extensões de Artin-Schreier.

Lembramos que, uma extensão de corpos finita M/L é dita ser de Galois se o grupo de automorfismos

$$\mathrm{Aut}(M/L) = \{\sigma : M \to M; \sigma \text{ é isomorfismo com } \sigma(a) = a, \forall a \in L\}$$

tem ordem $[M : L]$. Nesse Caso, chamamos $\mathrm{Aut}(M/L)$ de grupo de Galois da extensão M/L e escrevemos $\mathrm{Gal}(M/L) := \mathrm{Aut}(M/L)$.

Uma extensão F'/K' de um corpo de funções F/K é dita Galoisiana ou de Galois se F'/F é extensão de Galois de grau finito. Considere $P \in \mathbb{P}_F$.

Então $\mathrm{Gal}(F'/F)$ age no conjunto $\{P' \in \mathbb{P}_{F'} \mid P'|P\}$ via $\sigma(P') = \{\sigma(x) \mid x \in P'\}$, e ainda, pelo lema 4.44, vimos que

$$v_{\sigma(P')}(y) = v_{P'}\left(\sigma^{-1}(y)\right), \text{ para } y \in F'.$$

Teorema 4.58. *Sejam F'/K' uma extensão de Galois de F/K e $P_1, P_2 \in \mathbb{P}_{F'}$ extensões de $P \in \mathbb{P}_F$. Então existe $\sigma \in \mathrm{Gal}\,(F'/F)$ tal que $\sigma(P_1) = P_2$.*

Demonstração: Faremos a demonstração por absurdo. Suponha que $\sigma(P_1) \neq P_2$, para todo $\sigma \in \mathrm{Gal}\,(F'/F) =: G$. Pelo teorema da aproximação existe $z \in F'$ tal que $v_{P_2}(z) > 0$ e $v_Q(z) = 0$, para todo $Q \in \mathbb{P}_{F'}$, com $Q|P$ e $Q \neq P_2$. Em particular, $v_{P_1}(z) = 0$.

Considere $N_{F'/F} : F' \longrightarrow F$ a aplicação norma, a qual pode ser definida de maneira análoga ao traço, porém neste caso, considerando-se o produto dos automorfismos de G. Então,

$$v_{P_1}\left(\mathrm{N}_{F'/F}(z)\right) = v_{P_1}\left(\prod_{\sigma\in G}\sigma(z)\right) = \sum_{\sigma\in G} v_{P_1}(\sigma(z)) =$$
$$= \sum_{\sigma\in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma\in G} v_{\sigma(P_1)}(z) = 0, \quad (\star)$$

pois estamos supondo que $P_2 \neq \sigma(P_1)$. Por outro lado,

$$v_{P_2}\left(\mathrm{N}_{F'/F}(z)\right) = \sum_{\sigma\in G} v_{\sigma(P_2)}(z) = v_{P_2}(z) > 0. \quad (\star\star)$$

Agora, como $N_{F'/F}(z) \in F$, segue que

$$v_{P_1}\Big(\mathrm{N}_{F'/F}(z)\Big) = 0 \Leftrightarrow v_P\Big(\mathrm{N}_{F'/F}(z)\Big) = 0 \Leftrightarrow v_{P_2}\Big(\mathrm{N}_{F'/F}(z)\Big) = 0,$$

o que contradiz $(\star)$ e $(\star\star)$. Portanto, existe σ automorfismo tal que $\sigma(P_1) = P_2$.

■

Corolário 4.59. *Nas mesmas condições do teorema 4.58, considere $P_1, \ldots, P_r$ todos os lugares de F' que estendem P. Então:*

(a) $e(P_i|P) = e(P_j|P)$ e $f(P_i|P) = f(P_j|P)$, e portanto, escrevemos apenas $e(P)$ e $f(P)$.

(b) $e(P) \cdot f(P) \cdot r = [F' : F]$.

(c) Os expoentes do diferente $d(P_i|P)$ e $d(P_j|P)$ são iguais para todo i e j.

Demonstração: (a) Segue direto do teorema 4.58 e do lema 4.44.

(b) Da igualdade fundamental e do teorema 4.58, segue que $[F' : F] = \sum_{i=1}^{r} e(P_i|P)f(P_i|P) = e(P) \cdot f(P) \cdot r$.

(c) Considere o fecho integral

$$\mathcal{O}'_P = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}$$

de $\mathcal{O}_P$ em F' e o módulo complementar

$$\mathcal{C}_P = \left\{ z \in F'; \mathrm{Tr}_{F'/F}\left(z\mathcal{O}'_P\right) \subseteq \mathcal{O}_P \right\}.$$

Note que, dado $u \in F'$, $\mathrm{Tr}_{F'/F}(u) = \mathrm{Tr}_{F'/F}(\sigma(u)), \forall \sigma \in G$. Mostremos inicialmente que $\sigma\left(\mathcal{O}'_P\right) = \mathcal{O}'_P$ e $\sigma\left(\mathcal{C}_P\right) = \mathcal{C}_P, \forall \sigma \in G$.

Seja $z \in \mathcal{O}'_P$. Então $v_{P_i}(z) \geq 0$, para todo $i = 1, \ldots, r$. Para cada $1 \leq j \leq r$, existe i tal que $v_{P_j}(\sigma(z)) = v_{\sigma^{-1}(P_j)}(z) = v_{P_i}(z) \geq 0$. Logo, $\sigma(z) \in \mathcal{O}'_P$, e assim, $\sigma(\mathcal{O}'_P) \subseteq \mathcal{O}'_P$.

Queremos mostrar que $\mathcal{O}'_P \subseteq \sigma(\mathcal{O}'_P)$. Note que $\sigma_{P_j}(\sigma^{-1}(z)) = v_{\sigma(P_j)}(z) = v_{P_i}(z) \geq 0$. Logo, $\sigma^{-1}(z) \in \mathcal{O}'_P \Rightarrow z \in \sigma(\mathcal{O}'_P) \Rightarrow \mathcal{O}'_P \subseteq \sigma(\mathcal{O}'_P)$, e isso prova a igualdade.

Vamos mostrar que $\sigma(\mathcal{C}_P) = \mathcal{C}_P$. Seja $z \in \mathcal{C}_P$. Então $\mathrm{Tr}_{F'/F}\left(z\mathcal{O}'_P\right) \subseteq \mathcal{O}_P$. Observe $\mathrm{Tr}_{F'/F}(\sigma(z)u) = \mathrm{Tr}_{F'/F}\left(z\sigma^{-1}(u)\right) \in \mathcal{O}_P$, $\forall u \in \mathcal{O}'_P$. Então $\sigma\left(\mathcal{C}_P\right) \subseteq \mathcal{C}_P$. Como fizemos antes, $\mathcal{C}_P = \sigma\left(\mathcal{C}_P\right)$.

Escrevemos $\mathcal{C}_P = t\mathcal{O}'_P$ (podemos fazer isso pela proposição 4.32), e

$$\sigma(t)\mathcal{O}'_P = \sigma\left(t\mathcal{O}'_P\right) = \sigma\left(\mathcal{C}_P\right) = \mathcal{C}_P = t\mathcal{O}'_P.$$

Novamente, pela proposição 4.32 e da definição do expoente do diferente,

$$v_{P_i}(\sigma(t)) = v_{P_i}(t), i = 1, \ldots, r \Rightarrow -d\left(P_i \mid P\right) = v_{P_i}(\sigma(t)), \forall i \text{ e } \forall \sigma \in G.$$

Por fim, considerando P_i e P_j distintos tais que $P_i = \sigma(P_j)$, segue que

$$-d\left(P_i \mid P\right) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d\left(P_j \mid P\right) \Rightarrow d(P_i|P) = d(P_j|P).$$

■

Como foi dito no início da seção, estaremos interessados em dois casos particulares de extensões de Galois: as de Kummer e as de Artin-Schreier. O próximo resultado define as extensões de Kummer e nos fornece algumas de suas propriedades.

Proposição 4.60. *(Extensões de Kummer) Seja F/K um corpo de funções algébricas tal que K contém uma raiz n-ésima primitiva da unidade, $n > 1$ e $\mathrm{mdc}(\mathrm{char}\, K, n) = 1$. Seja $u \in F$ tal que*

$$u \neq w^d, \forall w \in F \text{ e } d \mid n, d > 1.$$

Defina $F' = F(y)$, onde $y^n = u$. A exntesão F'/F é chamada de extensão de Kummer, e valem as seguintes propriedades:

(a) O polinômio $\Phi(t) = t^n - u$ é o minimal de y sobre F. Além disso, a extensão F'/F é de Galois com $[F' : F] = n$, seu grupo de Galois é cíclico, e os automorfismos de F'/F são dado por $\sigma(y) = \zeta y$, onde $\zeta \in K$ é uma raiz n-ésima da unidade.

(b) Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ tal que $P'|P$. Então

$$e(P'|P) = \frac{n}{r_P} \text{ e } d(P'|P) = \frac{n}{r_P} - 1,$$

onde $r_P := \mathrm{mdc}(n, v_P(u)) > 0$.

(c) Sejam K' o corpo das constantes de F', g o gênero de F/K e g' o gênero de F'/K'. Então

$$g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg(P) \right).$$

Demonstração: (a) Observe que y se anula em $\Phi(t)$ e $\Phi(t)$ é irredutível sobre F (caso não fosse, teríamos $u = w^d$, o que é absurdo por hipótese). Então, $\Phi(t)$ é o minimal de y sobre F.

Pela hipótese K contém uma raiz n-ésima primitiva da unidade, então contém todas. As raízes de $\Phi(t)$ são exatamente os elementos do conjunto $\{y, \zeta y, \zeta^2 y, \ldots, \zeta^{n-1} y\}$, então a extensão F'/F é o corpo de raízes do polinômio $\Phi(t)$, e portanto é normal. Além disso, a extensão F'/F é separável, pois K é perfeito. Assim, por um resultado da teoria de corpos, F'/F é de Galois, ou seja, $\mathrm{o}(\mathrm{Aut}(F'/F)) = n$. Agora, segue imediatamente que o automorfismo $\sigma(y) = \zeta y$ gera os automorfismos do grupo de Galois, ou seja, a extensão é cíclica.

(b) Vamos dividir em 3 casos:

Caso 1: $r_P = 1$.

Como $y^n = u$, então $n v_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P'|P)\, v_P(u)$. Agora, como $1 = r_P$, segue que $n \mid e(P'|P)$ e $v_P(u) \mid v_{P'}(y)$. Pelo item (a), $[F' : F] = n$, e assim, do corolário 4.59, item (b), temos que $e(P'|P) \mid n$, ou seja $n = e(P'|P)$, como queríamos mostrar. Por fim, pelo teorema do diferente de Dedekind, como $n \nmid \mathrm{char}\, K$, segue que $d(P'|P) = e(P'|P) - 1 = n/r_P - 1$.

Caso 2: $r_P = n$.

Observe que nesse caso, $n \mid v_P(u)$, e então existe $l \in \mathbb{Z}$ tal que $nl = v_P(u)$. Assim, $v_P(u) = n v_P(y) \Rightarrow v_P(y) = l$. Escolha $t \in F$ tal que $v_P(t) = l$ e defina $y_1 := t^{-1} y$ e $u_1 = t^{-n} u$. Então $y_1^n = (t^{-1})^n y^n = t^{-n} u = u_1$, e ainda

$$v_{P'}(y_1) = v_{P'}(t^{-1} y) = -v_{P'}(t) + v_{P'}(y) = -v_P(t) + v_P(y) = -l + l = 0$$

e

$$v_P(u_1) = v_P(t^{-n} u) = -n v_P(t) + v_P(u) = -nl + nl = 0.$$

Agora, o polinômio minimal de y_1 sobe F é $\psi(t) = t^n - u_1$, uma vez que y_1 se anula em $\psi(t)$ e $\psi(t)$ é irredutível sobre F. Então, y é integral sobre $\mathcal{O}_P$ e pelo teorema 4.51, segue que

$$0 \leq d\left(P' \mid P\right) \leq v_{P'}\left(\psi'\left(y_1\right)\right).$$

Agora, note que $\psi'(y_1) = ny_1^{n-1}$, ou seja, $v_{P'}(\psi'(y_1)) = (n-1)v_{P'}(y_1) = 0$, e segue que $d(P'|P) = 0$, e assim, pelo teorema do diferente de Dedekind, $e(P'|P) = 1$, e fica provado para o caso $r_P = n$.

Caso 3: $1 < r_P < n$.

Considere o corpo intermediário $F_0 = F(y_0)$, onde $y_0 = y^{\frac{n}{r_P}}$. Neste caso, $\psi(t) = t^{r_P} - u$ é o polinômio minimal de y_0 sobre F.

Logo, $[F_0 : F] = r_P$ e $[F' : F_0] = \dfrac{[F' : F]}{[F_0 : F]} = \dfrac{n}{r_P}$. Defina $P_0 := P' \cap F_0$. Podemos então aplicar o caso 2 para a extensão F_0/F, uma vez que $[F_0 : F] = r_P$. Assim, temos $e(P_0|P) = 1$. Ainda, como $y_0^{r_P} = u$, segue que

$$v_{P_0}\left(y_0^{r_P}\right) = v_{P_0}(u) \Rightarrow v_{P_0}\left(y_0\right) = \frac{v_P(u)}{r_P}.$$

Assim, temos $\operatorname{mdc}\left(\dfrac{n}{r_P}, v_{P_0}\left(y_0\right)\right) = 1$ e podemos aplicar o caso 1 para $F' = F_0(y)$, e obtemos

$$e\left(P'|P_0\right) = \frac{n}{r_P} \Rightarrow e\left(P'|P\right) = e\left(P'|P_0\right) e\left(P_0|P\right) = \frac{n}{r_P}.$$

Ainda, do corolário 4.41, como $P \subseteq P_0 \subseteq P'$,

$$d\left(P'|P\right) = e\left(P'|P_0\right) d\left(P_0|P\right) + d\left(P_0|P\right) = \frac{n}{r_P} - 1.$$

(c) Para mostrarmos esse item, a ideia será aplicar a fórmula do gênero de Hurwitz. Inicialmente, calculamos o grau do diferente de F'/F. Pelo item (b),

$$\deg\left(\operatorname{Diff}\left(F'/F\right)\right) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d\left(P'|P\right) \deg\left(P'\right) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} \left(\frac{n}{r_P} - 1\right) \deg\left(P'\right).$$

Agora, fixamos $P \in \mathbb{P}_F$. Pelo corolário 4.59 o índice de ramificação $e(P) = e(P'|P)$ independente de P', segue do item (b) e do corolário 4.13 que

$$\sum_{P'|P} \deg\left(P'\right) = \frac{1}{e(P)} \left(\sum_{P'|P} e\left(P'|P\right) \deg\left(P'\right)\right) = \frac{1}{e(P)} \deg\left(\sum_{P'|P} e\left(P'|P\right) P'\right) =$$
$$= \frac{1}{e(P)} \deg\left(\operatorname{Con}_{F'/F}(P)\right) = \frac{r_P}{n} \frac{[F' : F]}{[K' : K]} \deg(P) = \frac{r_P}{[K' : K]} \deg\left(P\right).$$

Então

$$\deg\left(\operatorname{Diff}\left(F'/F\right)\right) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} \left(\frac{n}{r_P} - 1\right) \deg\left(P'\right) =$$
$$= \sum_{P \in \mathbb{P}_F} \left(\left(\frac{n}{r_P} - 1\right) \sum_{P'|P} \deg\left(P'\right)\right) =$$
$$= \sum_{P \in \mathbb{P}_F} \left(\frac{n}{r_P} - 1\right) \frac{r_P}{[K' : K]} \deg(P) = \frac{n}{[K' : K]} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg(P).$$

Substituindo na fórmula do gênero de Hurwitz,

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'/F) \Rightarrow$$
$$\Rightarrow g' - 1 = \frac{n}{[K' : K]}(g - 1) + \frac{1}{2}.\frac{n}{[K' : K]} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg P \Rightarrow$$
$$\Rightarrow g' = 1 + \frac{n}{[K' : K]} \left(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg P\right).$$

■

Corolário 4.61. *Sejam F/K um corpo de funções de $F' = F(y)$ com $y^n = u \in F$, onde* $\mathrm{char}\, K \nmid n$, *e K contendo uma raiz n-ésima primitiva da unidade. Suponha que existe $Q \in \mathbb{P}_F$ tal que* $\mathrm{mdc}(v_Q(u), n) = 1$. *Então K é o corpo completo das constantes de F', a extensão F'/F é cíclica de grau n e*

$$g' = 1 + n(g - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \deg(P).$$

Demonstração: Suponha inicialmente que existe $w \in F$ tal que $u = w^d$, com $d \mid n$, $d > 1$. Então $v_Q(u) = dv_Q(w) \Rightarrow d \mid v_Q(u)$. Como $d \mid n$, então teríamos $\mathrm{mdc}(v_Q(u), n) = d > 1$, o que contradiz a hipótese. Logo, $u \neq w^d$, para todo $w \in F$, $d \mid n$, $d > 1$.

Assim, estamos nas hipóteses da proposição 4.60. Vamos mostrar que $[K' : K] = 1$. Seja Q' tal que $Q'|Q$ em F'. Pelo item (b) da proposição 4.60,

$$e(Q'|Q) = \frac{n}{r_P} = n = [F' : F]. \quad (\star)$$

Suponha por absurdo que $[K' : K] > 1$ e considere o corpo intermediário $F_1 := FK' \supsetneq F$ e o lugar $Q_1 := Q' \cap F_1$. Por $(\star)$, $e(Q'|Q_1) = [F' : F_1]$, já que

$$v(u) = e(Q_1|Q) \cdot v_Q(u) = v_Q(u),$$

pelo teorema 4.56, item (a).

Então $1 = e(Q_1|Q) = [F_1 : F] > 1$, o que é absurdo, e assim, $[K' : K] = 1$. Portanto, colocando $[K' : K] = 1$ no item (c) da proposição 4.60, e segue a igualdade desejada.

■

Observação 4.62. *Nas demonstrações anteriores, não utilizamos o fato de que K possui uma raiz n-ésima primitiva da unidade. As afirmações da proposição 4.60 itens (b) e (c) e do corolário 4.61 são válidas em geral, com uma única exceção: $F(y)/F$ não é de Galois caso K não contenha uma raiz n-ésima da unidade.*

Exemplo 4.63. *Sejam K um corpo com* $\mathrm{char}\, K \neq 2$ *e $F = K(x, y)$, com $y^2 = f(x) = p_1(x)p_2(x) \dots p_s(x) \in K[x]$, onde os $p_i(x)$'s são polinômios mônicos, irredutíveis e $s \geq 1$. Então K é o corpo completo das constantes de F e F/K tem gênero g, onde*

$$g = \frac{m - 1}{2} \text{ se } m \equiv 1 \bmod 2 \text{ ou}$$
$$g = \frac{m - 2}{2} \text{ se } m \equiv 0 \bmod 2,$$

e $m = \deg f(x)$.

De fato, note que $F = F_0(y)$, onde $F_0 = K(x)$. Sejam $P_i \in \mathbb{P}_{K(x)}$ o zero correspondente a $p_i(x)$ e P_∞ o polo de x em $K(x)$. Então $v_{P_i}(f(x)) = 1$ e $v_{P_\infty}(f(x)) = -m$. Assim, do corolário 4.61, $F/F_0 = K(x,y)/K(x)$ cíclica de grau 2 e K o corpo completo das constantes de F.

Agora, vamos verificar as informações a respeito de r_P, onde r_P é definido como nos resultados anteriores. Observe que:

(i) Para $1 \leq i \leq s$, $r_{P_i} = \text{mdc}(n, v_{P_i}(u)) = \text{mdc}(2, v_{P_i}(f(x))) = \text{mdc}(2,1) = 1$.

(ii) $r_{P_\infty} = \text{mdc}(n, v_{P_\infty}) = \text{mdc}(2, v_{P_\infty}(f(x))) = \text{mdc}(2,-m) = 2$, se $2 \mid m$, ou 1, se $2 \nmid m$.

(iii) Para $P \in \mathbb{P}_{K(x)} \backslash \{P_1, \ldots, P_s, P_\infty\}$, $r_P = \text{mdc}(n, v_P(u)) = \text{mdc}(2, v_P(y^2)) = 2$.

Agora, substituindo na fórmula do corolário 4.61,

$$g' = 1+2(0-1) + \frac{1}{2}\sum_{i=1}^{s} \deg(P_i) + \frac{1}{2}(2 - r_{P_\infty}) =$$
$$= \frac{m}{2} - 1 + \frac{2 - r_{P_\infty}}{2} = \frac{m - r_{P_\infty}}{2},$$

e segue a igualdade desejada.

Para finalizar esta seção, um outro tipo especial de extensões de Galois são as extensões de Artin-Schreier. Nesse caso, trabalharemos com corpos de característica $p > 0$. Antes de introduzirmos este tipo de extensão, precisamos do lema a seguir.

Lema 4.64. *Sejam F/K um corpo de funções algébricas de característica $p > 0$, $u \in F$ e $P \in \mathbb{P}_F$. Então,*

(a) ou existe $z \in F$ tal que $v_P(u - (z^p - z)) > 0$,

(b) ou existe $z \in F$ tal que $v_P(u - (z^p - z)) = -m$, onde $\text{mdc}(m,p) = 1$.

No caso da validade do item (b), o inteiro m é unicamente determinado por u e P, como

$$-m = \max\{v_P(u - (w^p - w)) \,; w \in F\}.$$

Demonstração: Mostremos primeiramente a seguinte afirmação:

Afirmação 1: Sejam $x_1, x_2 \in F - \{0\}$ tais que $v_P(x_1) = v_P(x_2)$. Então existe $y \in F$ tal que

$$v_P(y) = 0 \text{ e } v_P(x_1 - y^p x_2) > v_P(x_1).$$

De fato, como $v_P(x_1) = v_P(x_2)$, então $v_P\left(\frac{x_1}{x_2}\right) = 0 \Rightarrow \frac{x_1}{x_2} \in \mathcal{O}_P \backslash P \Rightarrow \left(\frac{x_1}{x_2}\right)(P) \neq 0$.

Como $\mathcal{O}_P/P$ é perfeito e $\text{char}\, K = p > 0$, existe $y \in \mathcal{O}_P/P$ tal que $\left(\frac{x_1}{x_2}\right)(P) = (y(P))^p$. Logo, $v_P(y) = 0$ e $v_P\left(\frac{x_1}{x_2} - y^p\right) > 0$, e assim

$$v_P\left(\frac{x_1}{x_2} - y^p\right) > 0 \Rightarrow v_P\left(\frac{1}{x_2}(x_1 - y^p x_2)\right) > 0 \Rightarrow$$
$$\Rightarrow v_P(x_1 - y^p x_2) > v_P(x_2) = v_P(x_1).$$

Agora, queremos mostrar o seguinte: se $v_P(u - (z_1^p - z_1)) = -lp < 0$, então existe $z_2 \in F$ tal que

$$v_P(u - (z_2^p - z_2)) > -lp.$$

Seja $t \in F$ tal que $v_P(t) = -l$. Então $v_P\left(u - (z_1^p - z_1)\right) = -lp = v_P(t) \cdot p = v_P\left(t^p\right)$. Pela *afirmação 1*, existe $y \in F$ com $v_P(y) = 0$ e

$$v_P\left(u - \left(z_1^P - z_1\right) - (yt)^p\right) > -lp.$$

Agora, como $v_P(y) = 0$, então $v_P(yt) = v_P(t) = -l > -lp$ e assim,

$$v_P\left(u - (z_1^p - z_1) - ((yt)^p - yt)\right) > -lp.$$

Definimos $z_2 := z_1 + yt$, e então

$$v_P\left(u - (z_2^p - z^2)\right) = v_P\left(u - ((z_1 + yt)^p - (z_1 + yt))\right) = v_P\left(u - z_1^p - (yt)^p + z_1 + yt\right) = v_P\left(u - (z_1^p - z_1) - ((yt)^p - yt)\right) > -lp$$

Da forma como construímos, ou o item (a) ou o item (b) devem ser satisfeitos. Agora, para o caso em que (b) é verdadeiro, precisamos determinar m. Neste caso, estamos supondo a existência de $z \in F$ tal que $v_P\left(u - (z^p - z)\right) = -m < 0$ com $\text{mdc}(m, p) = 1$.

Seja $w \in F$. Então $p \cdot v_P(w - z) = v_P(z^p - w^p) \neq -m$. Dividimos em dois casos:

Caso 1: $pv_P(w - z) > -m$.

Nesse caso,

$$pv_P(w - z) > -m \Rightarrow v_P\left((w - z)^p\right) > -m \text{ e } v_P(w - z) > \frac{-m}{p} > -m.$$

Logo, pela desigualdade triangular, segue que

$$v_P\left((w - z)^p - (w - z)\right) > -m.$$

Ainda, pela desigualdade triangular estrita, temos

$$\begin{aligned} v_P\left(u - (w^p - w)\right) &= v_P\left(u - (z^p - z) - ((w^p - w) - (z^p - z))\right) \\ &= v_P\left(u - (z^p - z) - ((w^p - z^p) - (w - z))\right) \\ &= v_P\left(u - (z^p - z) - ((w - z)^p - (w - z))\right) = -m. \end{aligned}$$

Caso 2: $p \cdot v_P(w - z) < -m$.

Nesse caso, se procedemos como anteriormente,

$$v_P\left(u - (w^p - w)\right) = v_P\left(u - (z^p - z) - ((w - z)^p - (w - z))\right) < -m.$$

Logo, sempre $v_P\left(u - (w^p - w)\right) \leq -m$, e segue que

$$-m = \max\left\{v_P\left(u - (w^p - w)\right); w \in F\right\},$$

como queríamos mostrar.

■

Proposição 4.65. *(Extensões de Artin-Schreier) Seja F/K um corpo de funções algébricas de característica $p > 0$. Considere $u \in F$ satisfazendo*

$$u \neq w^p - w, \forall w \in F.$$

Defina $F' = F(y)$ onde $y^p - y = u$. A extensão F'/F é chamada de extensão de Artin-Schreier de F. Para $P \in \mathbb{P}_F$, definimos

$$m_P := \begin{cases} m & \text{se existe } z \in F \text{ tal que } v_P(u - (z^p - z)) = -m < 0 \\ & \text{e } m \not\equiv 0 \bmod p, \\ -1 & \text{se } v_P(u - (z^p - z)) \geq 0 \quad \text{para algum } z \in F. \end{cases}$$

Então,

(a) F'/F é uma extensão de Galois, cíclica de grau p, e os automorfismos de F'/F são dados por $\sigma(y) = y + \nu$, com $\nu = 0, 1, \ldots, p-1$.

(b) P é não ramificado em F'/F se, e somente se, $m_P = -1$.

(c) P é totalmente ramificado em F'/F se, e somente se $m_P > 0$. Neste caso, se denotarmos por P' a única extensão de P em F', temos

$$d(P'|P) = (p-1)(m_P + 1).$$

(d) Se pelo menos um lugar Q de F satisfaz $m_Q > 0$, então K é algebricamente fechado em F' e

$$g' = pg + \frac{p-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_p + 1)\deg(P)\right),$$

onde g' denota o gênero de F'/K' e g denota o gênero de F/K.

Demonstração: (a) Considere o polinômio $\varphi(t) = t^p - t - u$. Claramente y é raiz de $\varphi(t)$, e ainda, para todo $i = 1, \ldots, p-1$,

$$\varphi(y+i) = (y+i)^p - (y+i) - u = (y^p - y - u) + (i^p - i) = 0.$$

Logo, $\varphi(t)$ tem p raízes distintas. Se uma delas está em F, então todas estão. Como $[F' : F] = [F(y) : F]$, basta mostrarmos que $\varphi(t)$ é irredutível sobre F, e assim, teremos $[F(y) : F] = \deg \min_F y = \deg \varphi(t) = p$.

Suponha por absurdo que $\varphi(t) = g(t)h(t)$, com $g(t), h(t) \in F[t]$ e $1 \leq \deg g(t), \deg h(t)$. Como as raízes de $\varphi(t)$ são $y + i$, com $i = 0, 1 \ldots, p-1$, então podemos escrever

$$\varphi(t) \prod_{i=1}^{p-1} (t - (y+i)).$$

Assim, $g(t)$ pode ser escrito como produto de $t - (y + j)$, para alguns j's. Sem perda de generalidade, podemos considerar

$$g(t) = \prod_{i=o}^{d-1} (t - (y+i)) \quad \text{e} \quad h(t) = \prod_{i=d}^{p-1} (t - (y+i)).$$

O coeficiente de t^{d-1} em $g(t)$ é a soma dos termos $-(y+i)$ dos d inteiros i que aparecem em sua decomposição. Logo, esse coeficiente é igual a $-dy + j$, para algum inteiro j. Mas, $d \neq 0$ em F e $y \in F$, pois os coeficientes de $g(t)$ estão em F, o que nos gera uma contradição. Logo, $\varphi(t)$ é irredutível. Além disso, todas as suas raízes estão em $F(y)$, e portanto, $F(y)/F$ é normal. Por fim, como $\varphi(t)$ não tem raízes múltiplas, segue que $F(y)/F$ é separável. De um resultado da teoria de Galois, segue que $F(y)/F$ é uma extensão Galoisiana.

Agora, como $y+1$ é raiz de $\varphi(t)$, segue que existe um automorfismo de $F(y)/F$ tal que $\sigma(y) = y+1$. Logo, as potências σ^i de σ também são automorfismos tais que $\sigma(y) = y+i$, para $i = 0, \ldots, p-1$, e são todos distintos.

Assim, como a extensão é de Galois,

$$p = [F(y) : F] = \mathrm{o}\left(\mathrm{Aut}(F(y)/F)\right),$$

e segue que o grupo de Galois de $F(y)/F$ consiste desses automorfismos, gerados por $\sigma(y) = y+1$, e portanto, a extensão é cíclica de grau p.

(b) e (c): Faremos ambos os itens de forma simultânea, e vamos dividir em casos.

Caso 1: $m_P = -1$.

Da definição, existe $z \in F$ tal que $v_P\left(u - (z^p - z)\right) \geq 0$. Sejam $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Então $F' = F(y_1)$, pois $z \in F$ e $\varphi_1(t) = t^p - t - u_1$ é o polinômio minimal de y_1 sobre F, já que anula y_1 e é irredutível em F.

Como $v_P\left(u_1\right) = v_P\left(u - (z^p - z)\right) \geq 0$, então $u_1 \in \mathcal{O}_P$. Assim, pela proposição 4.23, segue que y_1 é integral sobre $\mathcal{O}_P$. Além disso, derivando $\varphi_1(t)$, obtemos

$$\varphi_1'(t) = pt^{p-1} - 1 = -1.$$

Considere P' uma extensão de P em F'. Então $v_{P'}\left(\varphi_1'\left(y_1\right)\right) = 0$, e pelo teorema 4.51,

$$0 \leq d\left(P'|P\right) \leq v_{P'}\left(\varphi_1'\left(y_1\right)\right) = 0 \Rightarrow d\left(P'|P\right) = 0.$$

Pelo teorema do diferente de Dedekind, $e(P'|P) = 1$, ou seja $P'|P$ é não ramificada, e logo, P é não ramificado em F'/F, e isso prova uma implicação do item (b).

Agora, assumimos $m_P > 0$. Da definição, existe $z \in F$ tal que

$$v_P(u - (z_p - z)) = -m_P.$$

Novamente, consideramos os elementos y_1 e u_1 definidos como acima, e temos $F' = F(y_1)$ e $\varphi_1(t) = t^p - t - u_1$ o minimal de y_1 sobre F. Seja P' uma extensão de P em F'. Como $y_1^p - y_1 = u_1$,

$$v_{P'}\left(u_1\right) = e\left(P'|P\right) v_P\left(u_1\right) = -m_P \cdot e\left(P'|P\right)$$

e

$$v_{P'}\left(u_1\right) = v_{P'}\left(y_1^p - y_1\right) = p v_{P'}\left(y_1\right).$$

Ou seja, $-m_P e(P'|P) = p v_{P'}(y_1)$. Como $\mathrm{mdc}(m, p) = 1$, então $p \mid e(P'|P)$. Por outro lado, $e(P'|P) \leq [F' : F] = p$, e segue que $p = e(P'|P)$ (consequentemente, $-m_P = v_{P'}(y_1)$). Portanto, P é totalmente ramificado em F'/F, o que prova uma implicação do item (c)

Para as outras implicações dos itens (b) e (c), consideramos $x \in F$ um parâmetro local do lugar totalmente ramificado P ($e(P'|P) = p$) e P' uma extensão de P em F'. Como $\mathrm{mdc}(-m_P, p) = 1$, existem $i, j \in \mathbb{Z}$ tais que $1 = ip - jm_P$. Assim, o elemento $t = x^i y_1^j$ é um parâmetro local de P', pois

$$v_{P'}(t) = v_{P'}\left(x^i y_1^j\right) = i v_{P'}(x) + j v_{P'}\left(y_1\right) = 1.$$

Pela proposição 4.53, $d(P'|P) = v_{P'}(\psi(T))$, onde $\psi(T)$ é o polinômio minimal de t sobre F. Seja $G := \mathrm{Gal}(F'/F)$ e considere o polinômio $\prod_{\sigma \in G} (T - \sigma(t))$. Como $\psi(T)$ é o minimal de t sobre F e F'/F é de Galois, então

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t)h(T), \text{ onde } h(T) = \prod_{\sigma \neq id} (T - \sigma(t)) \in F'[T].$$

Assim, $\psi'(T) = h(T) + (T-t)h'(T)$, e segue que $\psi'(t) = h(t)$. Logo,

$$d\left(P' \mid P\right) = v_{P'}\left(\prod_{\sigma \neq id}\left(t - \sigma(t)\right)\right) = \sum_{\sigma \neq id} v_{P'}(t - \sigma(t)).$$

Dado $\sigma \in G - \{\mathrm{id}\}$, temos $\sigma(y_1) = \sigma(y - z) = y + \mu - z = y_1 + \mu$, onde $\mu \in \{1, \ldots, p-1\}$, e assim,

$$t - \sigma(t) = x^i y_1^j - x^i\left(y_1 + \mu\right)^j = -x^i\left(\left(y_1 + \mu\right)^j - y_1^j\right) =$$
$$= -x^i\left(\sum_{l=0}^{j}\left(\begin{array}{c} j \\ l \end{array}\right) y_1^{j-l}\mu^l - y_1^l\right) = -x^i\left(\sum_{l=1}^{j}\left(\begin{array}{c} j \\ l \end{array}\right) y_1^{j-l}\mu^l\right).$$

Agora, note que

$$v_{P'}(y_1^{l-1}) = (l-1)v_{P'}(y_1) = (l-1)(-m_P) = -lm_P + m_P \text{ e}$$
$$v_{P'}(y_1^{l-2}) = (l-2)v_{P'}(y_1) = (l-2)(-m_P) = -lm_P + 2m_P.$$

Como $m_P < 2m_P$, então $v_{P'}(y_1^{l-1}) < v_{P'}(y_1^{l-2})$, e pela desigualdade triangular estrita,

$$v_{P'}(t - \sigma(t)) = v_{P'}\left(-x^i\left(\sum_{l=0}^{j}\left(\begin{array}{c} j \\ l \end{array}\right) y_1^{j-l}\mu^l\right)\right) =$$
$$= v_{P'}\left(-x^i\right) + v_{P'}\left(\sum_{l=0}^{j}\left(\begin{array}{c} j \\ l \end{array}\right) y_1^{j-l}\mu^l\right) = ip + v_{P'}\left(\left(\begin{array}{c} j \\ 1 \end{array}\right)\mu y_1^{j-1}\right) = ip + v_{P'}\left(j\mu y_1^{j-1}\right) =$$
$$= ip + (j-1)\left(-m_P\right) = ip - jm_P + m_P = 1 + m_P.$$

Portanto, $d\left(P'|P\right) = \sum_{\sigma \neq \mathrm{id}} v_{P'}(t - \sigma(t)) = (p-1)\left(1 + m_P\right)$. Assim,

$$P \text{ não ramificado } \Rightarrow e(P'|P) = 1 \Rightarrow d(P'|P) = (1 + m_P))(p-1) = 0 \Rightarrow m_P = -1,$$

e

$$P \text{ totalmente ramificado} \Rightarrow e(P'|P) = p \Rightarrow d(P'|P) \geq p - 1$$
$$\Rightarrow (1 + m_P)(p-1) \geq (p-1) \Rightarrow 1 + mp > 1 \Rightarrow m_P > 0,$$

o que conclui a demonstração dos itens (b) e (c).

(d) Assumimos que existe $Q \in \mathbb{P}_F$ tal que $m_Q > 0$. Pelo item (c), segue que Q é totalmente ramificado em F'/F. Agora, a demonstração do fato de K ser o corpo completo das constantes segue da mesma maneira que fizemos no corolário 4.61.

Pela fórmula do gênero de Hurwitz,

$$2g' - 2 = p(2g-2) + \sum_{P\in\mathbb{P}_F}\sum_{P'|P} d\left(P'|P\right)\deg\left(P'\right) =$$
$$= p(2g-2) + \sum_{P\in\mathbb{P}_F}\sum_{P'|P} \left(m_P+1\right)\left(p-1\right)\deg\left(P'\right) =$$
$$= p(2g-2) + (p-1)\sum_{P\in\mathbb{P}_F} \frac{(m_P+1)}{e(P)}\deg\left(\sum_{P'|P} e\left(P'|P\right)P'\right) =$$
$$= p(2g-2) + (p-1)\sum_{P\in\mathbb{P}_F} \frac{(m_P+1)}{e(P)}\deg\left(\mathrm{Con}_{F'/F}(P)\right) =$$
$$= 2pg - 2p + (p-1)\sum_{P\in\mathbb{P}_F}(m_P+1)\deg(P)$$
$$\Rightarrow g' = pg + \frac{(p-1)}{2}\left(-2 + \sum_{P\in\mathbb{P}_F}(m_P+1)\deg(P)\right).$$

■

Observação 4.66. *Nas notações da proposição anterior, suponha que exista um lugar $Q \in \mathbb{P}_F$ tal que $v_Q(z) < 0$ e $p \nmid v_Q(u)$. Então para todo $k \in K$, $v_Q(k^p - k) = 0$ ou $v_Q(k^p - k) = \infty$, logo não existe $k \in K$ tal que $k^p - k = u$. Isso vale também para todo $k \in \mathcal{O}_Q$.*

Seja agora $w \in F\backslash\mathcal{O}_Q$. Se tivermos $w^p - w = u$, então necessariamente $v_Q(w^p - w) < 0$, e portanto, $v_Q(w^p) < v_Q(w) < 0$. Segue então que $v_Q(u) = pv_Q(w)$, ou seja, $p \mid v_Q(u)$, o que contradiz a hipótese. Logo, não existe $w \in F$ tal que $u = w^p - w$, e portanto, u satisfaz as condições da proposição anterior, e podemos aplicá-la neste caso.

Ambas as extensões definidas nesta seção, são casos particulares de extensões de Galois muito utilizadas para construção de curvas maximais específicas. Utilizando o 90º teorema de Hilbert, é possível mostrar que toda extensão cíclica de grau p, com p primo, pode ser vista como uma extensão de Artin-Schreier. Alguns exemplos das construções de extensões utilizando esses dois tipos específicos, as de Kummer e de Artin-Shcreier, podem ser encontradas em [12] e [13].

5 Corpos de funções algébricas sobre corpos finitos

Até o momento, estudamos a teoria de corpos de funções algébricas sobre um corpo de constantes perfeito K. Estudaremos agora o caso particular em que $K = \mathbb{F}_q$, onde q é uma potência de primo. Estaremos interessados em lugares de grau um de um corpo de funções sobre um corpo finito. O número desses lugares é finito, e pode ser estimado pela cota de Hasse-Weil.

Ao longo deste capítulo, F denota um corpo de funções algébricas de gênero g cujo corpo das constantes é um corpo finito $\mathbb{F}_q$.

5.1 A função de Zeta de um corpo de funções

Denote por $\mathrm{Div}(F)$ o grupo divisor do corpo de funções $F/\mathbb{F}_q$. Um divisor $A = \sum_{P \in \mathbb{P}_F} a_P P$ é positivo (efetivo) se $a_P \geq 0$ para todo P e escrevemos $A \geq 0$.

O primeiro resultado desta seção nos garante a existência de um número finito de divisores positivos de um determinado grau.

Lema 5.1. *Dado $n \geq 0$, existe somente um número finito de divisores positivos de grau n.*

Demonstração: Seja $D_0 \in \mathrm{Div}(F)$. Lembramos que D_0 é primo se $D_0 = P$, com $P \in \mathbb{P}_F$. Assim, um divisor $D \geq 0$ é a soma de divisores primos, não necessariamente distintos.

Considere o conjunto $S = \{P \in \mathbb{P}_F \mid \deg(P) \leq n\}$. Provaremos que $|S| < \infty$, e portanto, só existirão finitos divisores positivos de grau n. Seja $x \in F/\mathbb{F}_q$ e considere $S_0 = \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} | \deg(P_0) \leq n\}$, onde

$$\mathbb{F}_q(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}_q[x] \text{ e } g \neq 0 \right\}.$$

Pelas proposições 4.6 e 4.7, $P \cap \mathbb{F}_q(x) \in S_0$, para todo $P \in S$ e cada $P_0 \in S$ tem somente um número finito de extensões de F. Assim, resta ver que S_0 é finito. Como os lugares de $\mathbb{F}_q(x)$ correspondem a polinômios irredutíveis e mônicos $p(x) \in \mathbb{F}_q(x)$, então S_0 é finito é segue o resultado.

■

Definição 5.2. *O conjunto* $\mathrm{Div}^0(F) := \{A \in \mathrm{Div}(F) \mid \deg(A) = 0\}$ *é chamado grupo de divisores de grau zero, o qual é claramente subgrupo de* $\mathrm{Div}(F)$ *e o conjunto* $\mathrm{Cl}^0(F) := \{[A] \in \mathrm{Cl}(F) \mid \deg(A) = 0\}$ *é chamado grupo das classes divisores de grau zero.*

Proposição 5.3. $\mathrm{Cl}^0(F)$ *é um grupo finito.*

Demonstração: Seja $B \in \mathrm{Div}(F)$ com $\deg(B) = n \geq g$ e considere o conjunto $\mathrm{Cl}^n(F) = \{[C] \in \mathrm{Cl}(F) \mid \deg(C) = n\}$. Defina a aplicação

$$\varphi : \begin{cases} \mathrm{Cl}^0(F) & \longrightarrow & \mathrm{Cl}^n(F), \\ [A] & \longmapsto & [A+B] \end{cases}$$

A função φ está bem definida e é bijetora. Assim, basta mostrarmos que $\mathrm{Cl}^n(F)$ é finito, e o resultado segue pois φ é bijetora. Afirmamos que dado $[C] \in \mathrm{Cl}^n(F)$, existe $A \in [C]$ com $A \geq 0$.

De fato, considere $[C] \in \mathrm{Cl}^n(F)$. Então $\deg(C) = n \geq g$. Pelo teorema de Riemann-Roch, $\ell(C) \geq n + 1 - g \geq 1$. Assim, $\mathcal{L}(C) \neq \{0\}$, e existe $A \geq 0$ com $A \sim C \Rightarrow A \in [C]$.

Agora, pelo lema 5.1, existe somente um número finito de divisores $A \geq 0$ de grau n, e portanto, $\mathrm{Cl}^n(F)$ é finito, e segue que $\mathrm{Cl}^0(F)$ é finito.

■

A ordem de $\mathrm{Cl}^0(F)$ é chamada *número de classe* de $F/\mathbb{F}_q$, e é denotada por $h = h_F = \mathrm{ord}(\mathrm{Cl}^0(F))$. Definimos o inteiro $\partial := \min\{\deg(A) \mid A \in \mathrm{Div}(F) \text{ e } \deg(A) > 0\}$. Considere a aplicação grau dada por $\varphi : \mathrm{Div}(F) \longrightarrow \mathbb{Z}$ com $\varphi(A) = \deg(A)$. É fácl ver que φ está bem definida, $\mathrm{Im}(\varphi) \leq \mathbb{Z}$ e $\mathrm{Im}(\varphi) = \langle \partial \rangle$, ou seja, o grau de cada divisor de $F/\mathbb{F}_q$ é múltiplo de ∂.

Estaremos interessados em calcular os números

$$A_n := \mid \{A \in \mathrm{Div}(F) \mid A \geq 0 \text{ e } \deg A = n\} \mid .$$

Claramente A_1 é o número de lugares $P \in \mathbb{P}_F$ de grau 1 e por convenção $A_0 := 1$.

Proposição 5.4. *a) Se* $\partial \nmid n$, *então* $A_n = 0$.

b) Se $[C] \in \mathrm{Cl}(F)$, *então* $|\{A \in [C] \mid A \geq 0\}| = \dfrac{1}{q-1}\left(q^{\ell([C])} - 1\right)$.

c) Se $n > 2g - 2$ *e* $\partial \mid n$, *então* $A_n = \dfrac{h}{q-1}\left(q^{n+1-g} - 1\right)$.

Demonstração: a) Segue do fato de que a imagem da aplicação grau (φ citada acima) é gerada por ∂ e do fato de que todo divisor de $F/\mathbb{F}_q$ é múltiplo de ∂.

b) Note que se $A \in [C]$ e $A \geq 0$, então existe $0 \neq x \in F$ tal $A = \langle x \rangle + C$ e $\langle x \rangle \geq -C$, ou seja, $\mathcal{L}(C) \neq \{0\}$.

Agora, note que $\mid \mathcal{L}(C) \backslash \{0\} \mid = q^{\ell([C])} - 1$. Ainda, dois elementos geram o mesmo divisor, se, e somente se, eles diferem por um constante $0 \neq \alpha \in \mathbb{F}_q$. Por isso, dividindo por $q - 1$, obtemos

$$\mid \{A \in [C] \mid A \geq 0\} \mid = \frac{1}{q-1}\left(q^{\ell([C])} - 1\right).$$

c) Sabemos que existem h classe divisoras de grau n, as quais denotaremos por $[C_1], \ldots, [C_h]$. Pelo item b) e o teorema de Riemann-Roch,

$$|\{A \in [C_j] \mid A \geq 0\}| = \frac{1}{q-1}\left(q^{\ell(C_j)} - 1\right) = \frac{1}{q-1}\left(q^{n+1-g} - 1\right), \quad j = 1, \ldots, h.$$

Agora, dado $A \in \mathrm{Div}(F)$ com $\deg(A) = n$, existe um único $j = 1, \ldots, h$ tal que $A \in [C_j]$. Portanto,

$$A_n = \sum_{j=1}^{h} |\{A \in [C_j] \mid A \geq 0\}| = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

■

Definição 5.5. *A série de potências* $Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$ *é chamada função de Zeta de* $F/\mathbb{F}_q$.

Mostraremos agora que essa série converge em uma vizinhança do zero.

Proposição 5.6. *A série de potências* $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ *converge para* $|t| < q^{-1}$. *Além disso, se* $|t| < q^{-1}$, *então*

(a) Se $F/\mathbb{F}_q$ *tem gênero* $g = 0$, *então* $Z(t) = \dfrac{1}{q-1}\left(\dfrac{q}{1-(qt)^{\partial}} - \dfrac{1}{1-t^{\partial}}\right)$.

(b) Se $g \geq 1$, *então* $Z(t) = F(t) + G(t)$, *onde*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} \cdot t^{\deg C}$$

e

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

Demonstração: (a) Suponha $g = 0$. Mostremos que $h = \mathrm{ord}(\mathrm{Cl}^0(\mathrm{F})) = 1$, ou seja, todo divisor de grau zero é principal. Seja $A \in \mathrm{Div}(F)$ com $\deg(A) = 0$. Como $g = 0$, então pelo teorema de Riemann-Roch, $\ell(A) = \deg(A) + 1 - g = 1$.

Assim, $\mathcal{L}(A) \neq \{0\}$, ou seja, existe $0 \neq x \in F$ tal que $\langle x \rangle \geq -A$. Como ambos os divisores são de grau zero, segue que

$$\langle x \rangle \geq -A \Rightarrow A = -\langle x \rangle = \langle x^{-1} \rangle \Rightarrow A \text{ é principal.}$$

Portanto, $h = 1$. Pelo lema 5.4,

$$\begin{aligned}
\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} \\
&= \sum_{n=0}^{\infty} \frac{1}{q-1}\left(q^{\partial n+1} - 1\right) t^{\partial n} \\
&= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\right) \\
&= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right),
\end{aligned}$$

para $|t| < q^{-1}$.

(b) Suponha agora $g \geq 1$. Então

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{\deg C \geq 0} |\{A \in [C]; A \geq 0\}| \cdot t^{\deg C} = \sum_{\deg C \geq 0} \frac{q^{\ell(C)} - 1}{q-1} \cdot t^{\deg C}$$
$$= \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} \cdot t^{\deg C} + \frac{1}{q-1} \sum_{\deg C > 2g-2} q^{\deg C + 1 - g} \cdot t^{\deg C}$$
$$- \frac{1}{q-1} \sum_{\deg C \geq 0} t^{\deg C} = F(t) + G(t),$$

onde

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg C \leq 2g-2} q^{\ell(C)} \cdot t^{\deg C}$$

e

$$(q-1)G(t) = \sum_{n=((2g-2)/\partial)+1}^{\infty} h q^{n\partial + 1 - g} \cdot t^{n\partial} - \sum_{n=0}^{\infty} h t^{n\partial}$$
$$= h q^{1-g} (qt)^{2g-2+\partial} \frac{1}{1-(qt)^{\partial}} - h \frac{1}{1-t^{\partial}}.$$

■

Corolário 5.7. *A série $Z(t)$ pode ser estendida a uma função racional em $\mathbb{C}$, e tem um polo simples em $t = 1$.*

Demonstração: Segue direto da proposição 5.6, uma vez que $\dfrac{1}{1-t^{\partial}}$ tem um polo simples em $t = 1$.

■

Para o estudo de função Zeta de $F/\mathbb{F}_q$ sobre extensões de corpos finitos, é conveniente que tenhamos uma segunda representação de $Z(t)$ como um produto infinito. Lembramos que um produto infinito da forma

$$\prod_{i=1}^{\infty} (1 + a_i), \quad a_i \in \mathbb{C}, \ a_i \neq -1.$$

é dito ser convergente com limite $a \in \mathbb{C}$ se

$$\lim_{n \to \infty} \prod_{i=1}^{n} (1 + a_i) = a \neq 0.$$

O produto é dito absolutamente convergente se

$$\sum_{i=1}^{\infty} |a_i| < \infty.$$

Sabemos que absolutamente convergente implica em convergente, e o limite de um produto absolutamente convergente independe da ordem dos fatores. Ainda,

$\prod_{i=1}^{\infty} (1 + a_i) = a$ converge absolutamente $\Rightarrow \prod_{i=1}^{\infty} (1 + a_i)^{-1}$ converge aboslutamente para a^{-1}.

O próximo resultado nos fornece uma função geradora de $Z(t)$, a qual nos auxiliará em estudar como essa função se comporta.

Proposição 5.8. *(Produto de Euler) Se $|t| < q^{-1}$, a função Zeta pode ser representada como um produto absolutamente convergente da forma*

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

Em particular, $Z(t) \neq 0$ se $|t| < q^{-1}$.

Demonstração: Note que o lado direito da igualdade converge absolutamente para $|t| < q^{-1}$, pois

$$\sum_{P \in \mathbb{P}_F} |t|^{\deg P} \leq \sum_{n=0}^{\infty} A_n |t|^n < \infty,$$

pela proposição 5.6. Cada fator do produtório acima pode ser escrito como uma série geométrica, e portanto

$$\prod_{P \in \mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1} = \prod_{P \in \mathbb{P}_F} \sum_{n=0}^{\infty} t^{\deg(nP)} = \sum_{A \in \mathrm{Div}(F); A \geq 0} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t),$$

o que conclui a demonstração.

■

Agora, consideramos $\overline{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$ e a extensão $\overline{F} = F\overline{\mathbb{F}}_q$ de $F/\mathbb{F}_q$. Da teoria de corpos, para cada $r \geq 1$, existe exatamente uma extensão $\mathbb{F}_{q^r}/\mathbb{F}_q$ de grau r com $\mathbb{F}_{q^r} \subseteq \overline{\mathbb{F}_q}$ e definimos

$$F_r := F\mathbb{F}_{q^r} \subseteq \overline{F}.$$

Para o que veremos adiante, precisamos de uma igualdade polinomial apropriada. Dados inteiros $m, r \geq 1$ e $d = \mathrm{mcd}(m, r)$, vale a igualdade

$$\left(x^{r/d} - 1\right)^d = \prod_{\zeta^r = 1} (x - \zeta^m),$$

onde ζ varia entre todas as raízes r-ésimas da unidade em $\mathbb{C}$. Substituímos $x = t^{-m}$ e multiplicamos ambos os lados por $t^{mr} = t^{\frac{mr}{d} d}$, obtemos

$$\left(1 - t^{mr/d}\right)^d = \prod_{\zeta^r = 1} (1 - (\zeta t)^m).$$

Com isso, podemos demonstrar o próximo resultado.

Proposição 5.9. *Seja $Z(t)$ (respectivamente $Z_r(t)$) a função de Zeta de F (respectivamente $F_r = F\mathbb{F}_{q^r}$). Então, para todo $t \in \mathbb{C}$,*

$$Z_r(t^r) = \prod_{\zeta^r = 1} Z(\zeta t).$$

Demonstração: É suficiente mostrarmos que essa igualdade é válida em uma vizinhança do zero, ou seja, quando $|t| < q^{-1}$. Pela proposição 5.8,

$$Z_r(t^r) = \prod_{P \in \mathbb{P}_F} \prod_{P' | P} \left(1 - t^{r \cdot \deg P'}\right)^{-1}.$$

Fixando $P \in \mathbb{P}_F$, colocamos $m := \deg(P)$ e $d = \mathrm{mdc}(r, m)$. Então,

$$\prod_{P' | P} \left(1 - t^{r \cdot \deg P'}\right) = \left(1 - t^{rm/d}\right)^d = \prod_{\zeta^r = 1} (1 - (\zeta t)^m) = \prod_{\zeta^r = 1} \left(1 - (\zeta t)^{\deg P}\right).$$

Juntando ambas as igualdades,

$$Z_r\left(t^r\right) = \prod_{\zeta^r=1} \prod_{P\in\mathbb{P}_F} \left(1-(\zeta t)^{\deg P}\right)^{-1} = \prod_{\zeta^r=1} Z(\zeta t).$$

■

Temos a seguir dois corolários que seguem imediatamente da proposição anterior.

Corolário 5.10. *(F. K. Schmidt)* $\partial = \min\{\deg(A) \mid A \in \mathrm{Div}(F) \text{ e } \deg(A) > 0\} = 1$.

Demonstração: Para $\zeta^\partial = 1$,

$$Z(\zeta t) = \prod_{P\in\mathbb{P}_F} \left(1-(\zeta t)^{\deg P}\right)^{-1} = \prod_{P\in\mathbb{P}_F} \left(1-t^{\deg P}\right)^{-1} = Z(t).$$

Logo, pela proposição 5.9, $Z_\partial(t^\partial)$ tem um polo de ordem ∂ em $t=1$. Portanto, $\partial = 1$.

■

Corolário 5.11. *(a) Todo corpo de funções $F/\mathbb{F}_q$ de gênero zero é racional, e sua função de zeta é dada por*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

(b) Se $F/\mathbb{F}_q$ tem gênero $g \geq 1$, então sua função de Zeta pode ser escrita na forma $Z(t) = F(t) + G(t)$, onde

$$F(t) = \frac{1}{q-1} \sum_{0\leq \deg C \leq 2g-2} q^{\ell(C)} \cdot t^{\deg C}$$

e

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

Demonstração: Se $g=0$, pela proposição 2.69, segue que $F/\mathbb{F}_q$ é racional. As igualdades tanto do item (a) quanto do item (b) seguem diretamente da proposição 5.6 e do fato de que $\partial = 1$.

■

Agora, veremos um resultado que nos fornece uma igualdade para a função de Zeta avaliada em t, envolvendo a função de Zeta avaliada em $1/qt$. Essa igualdade é chamada de equação funcional da função de Zeta, e será importante para a definição de L-polinômio de um corpo de funções.

Proposição 5.12. *(Equação Funcional da Função de Zeta) A função de Zeta de $F/\mathbb{F}_q$ satisfaz a equação*

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

Demonstração: Suponhamos inicialmente que $g=0$. Então, pelo corolário 5.11, segue que

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

Suponhamos agora que $g \geq 1$ e escreva $Z(t) = F(t) + G(t)$ como no corolário 5.11. Seja W um divisor canônico de F. Logo, para qualquer $C \in \mathrm{Div}(F)$, tem-se $\ell(C) = \deg(C)+1-g+\ell(W-C)$ e $\deg(W) = 2g-2$. Ainda, se $[C]$ é tal que $0 \leq \deg(C) \leq 2g-2$, então o mesmo vale para $[W-C]$. Então

$$\begin{aligned}
(q-1)F(t) &= \sum_{0\leq \deg C\leq 2g-2} q^{\ell(C)}\cdot t^{\deg C} \\
&= \sum_{0\leq \deg C\leq 2g-2} q^{\deg C+1-g+\ell([W-C])}\cdot t^{\deg C} \\
&= q^{g-1}t^{2g-2}\sum_{0\leq \deg C\leq 2g-2} q^{\deg C-(2g-2)+\ell([W-C])}\cdot t^{\deg C-(2g-2)} \\
&= q^{g-1}t^{2g-2}\sum_{0\leq \deg C\leq 2g-2} q^{\ell([W-C])}\cdot \left(\frac{1}{qt}\right)^{\deg[W-C]} \\
&= q^{g-1}t^{2g-2}(q-1)F\left(\frac{1}{qt}\right),
\end{aligned}$$

e

$$\begin{aligned}
q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right) &= \frac{h}{q-1}q^{g-1}t^{2g-2}\left(q^g\left(\frac{1}{qt}\right)^{2g-1}\frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}}\right) \\
&= \frac{h}{q-1}\left(\frac{1}{t}\frac{1}{1-\frac{1}{t}} - \frac{q^gt^{2g-1}}{qt\left(1-\frac{1}{qt}\right)}\right) = G(t).
\end{aligned}$$

Logo, $F(t) = q^{g-1}t^{2g-2}F\left(\frac{1}{qt}\right)$ e $G(t) = q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right)$. Somando ambas as igualdades,

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

■

Definição 5.13. *O polinômio $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ é chamado de L-polinômio de $F/\mathbb{F}_q$.*

Segue diretamente do corolário 5.11 que $\deg(L(t)) \leq 2g$. Observe ainda que, conhecendo o polinômio $L(t)$, conheceremos todos os A_n's da definição de função de Zeta, uma vez que

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_nt^n.$$

Teorema 5.14. *(a) $L(t) \in \mathbb{Z}(t)$ e $\deg(L(t)) = 2g$*
(b) A equação funcional de $L(t)$ é dada por $L(t) = q^gt^{2g}L(1/qt)$
(c) $L(1) = h$, onde h é o número de classe de $F/\mathbb{F}_q$.
(d) Escrevendo $L(t) = a_0 + a_1t + \cdots + a_{2g}t^{2g}$, segue que

(i) $a_0 = 1$ *e* $a_{2g} = q^g$
(ii) $a_{2g-i} = q^{g-i}a_i$, *com* $0 \leq g \leq g$
(iii) $a_1 = N - (q+1)$, *onde* N *é o número de lugares de grau* 1.
(e) $L(t)$ *se fatora em* $\mathbb{C}[t]$ *da forma*

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Além disso, os números complexos $\alpha_1, \ldots, \alpha_{2g}$ *são inteiros algébricos e podem ser reordenados de forma a obter que* $\alpha_i\alpha_{g+i} = q$, *com* $i = 1, \ldots, g$.
(f) Se $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ *é o L-polinômio de* F_r, *então*

$$L_r(t) = \prod_{i=1}^{2g}\left(1 - \alpha_i^r t\right),$$

onde os α_i*'s são os mesmos do item (e).*

Demonstração: (a) Se $g = 0$, então pelo corolário 5.11 segue que $L(t) = 1$, e o resultado segue. Suponhamos $g \geq 1$. Por um lado, $L(t) = (1-t)(1-qt)Z(t)$, ou seja, $L(t)$ é um polinômio, uma vez que a função de Zeta $Z(t)$ é racional. Por outro lado, $L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$, ou seja, os coeficientes são inteiros uma vez que $A_n \in \mathbb{Z}$. Assim, segue que $L(t) \in \mathbb{Z}[t]$. O fato de $\deg(L(t)) = 2g$ será mostrado no item d).

(b) Para qualquer $g \geq 0$,

$$\begin{aligned} L\left(\frac{1}{qt}\right) &= \left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)Z\left(\frac{1}{qt}\right) = \left(\frac{1}{qt^2}\right)(qt-1)(t-1)Z\left(\frac{1}{qt}\right) \\ &= (1-qt)(1-t)Z(t)\left(\frac{1}{q^{g-1}t^{2g-2}}qt^2\right) = \frac{L(t)}{q^g t^{2g}}, \end{aligned}$$

e portanto, $L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right)$.

(c) Se $g = 0$, o resultado decorre diretamente do item a). Suponhamos $g \geq 1$, pelo corolário 5.11, temos substituindo os valores na equação, obtemos $L(1) = h$.

(d) Já sabemos que $\deg(L(t)) \leq 2g$. Então, escrevemos $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$. Do item (b), segue que

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \cdots + q^g a_0 t^{2g}.$$

Assim, já obtemos que $a_{2g-i} - q^{g-i}a_i$, com $0 \leq i \leq g$. Por outro lado, sabemos que $L(t) = (1 - qt - t + qt^2)\sum_{n=0}^{\infty} A_n t^n$. Nessa expressão, o coeficiente de t^0 é dado por A_0 e o coeficiente de t é dado por $A_1 - (q+1)A_0$. Logo, $a_0 = A_0$ e $a_1 = A_1 - (q+1)A_0$. Como por definição $A_0 = 1$ e $A_1 = N$, segue que $a_0 = 1$ e $a_1 = N - (q+1)$. Por fim, $a_{2g} = a_0 q^g = q^g \neq 0$, e portanto $\deg(L(t)) = 2g$.

(e) Vamos considerar o polinômio recíproco de $L(t)$ dado por

$$L^{\perp}(t) := t^{2g}L\left(\frac{1}{t}\right) = a_0 t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g} = t^{2g} + a_1 t^{2g-1} + \cdots + q^g.$$

Como $L^{\perp}(t)$ é mônico em $\mathbb{Z}[t]$, segue que suas raízes são inteiros algébricos. Escrevemos então

$$L^{\perp}(t) = \prod_{i=1}^{2g} (t - \alpha_i) \qquad \text{com} \qquad \alpha_i \in \mathbb{C}.$$

Note que

$$L(t) = t^{2g} L^{\perp}\left(\frac{1}{t}\right) = \prod_{i=1}^{2g} (1 - \alpha_i t)\,.$$

Para cada $j = 1, \ldots, 2g$, vale $L(\alpha_j^{-1}) = (1 - \alpha_j \alpha_j^{-1}) \prod_{i \neq j} (1 - \alpha_i t) = 0$ e $\prod_{i=1}^{2g} \alpha_i = a_{2g} = q^g$. Substituindo $t = qu$ e usando a equação funcional do item (b),

$$\begin{aligned}
\prod_{i=1}^{2g} (t - \alpha_i) = L^{\perp}(t) &= t^{2g} L\left(\frac{1}{t}\right) \\
&= q^{2g} u^{2g} L\left(\frac{1}{qu}\right) = q^g L(u) = q^g \cdot \prod_{j=1}^{2g} (1 - \alpha_j u) \\
&= q^g \cdot \prod_{j=1}^{2g} \left(1 - \frac{\alpha_j}{q} t\right) = q^g \cdot \prod_{j=1}^{2g} \frac{\alpha_j}{q} \cdot \prod_{j=1}^{2g} \left(t - \frac{q}{\alpha_j}\right) \\
&= \prod_{j=1}^{2g} \left(t - \frac{q}{\alpha_j}\right).
\end{aligned}$$

Reagrupando as raízes, uma vez que a fatoração dos polinômio é única, $\alpha_i \alpha_{g+i} = q$, para $i = 1, \ldots, g$.

(f) Da proposição 5.9,

$$\begin{aligned}
L_r\left(t^r\right) = \left(1 - t^r\right)\left(1 - q^r t^r\right) Z_r\left(t^r\right) &= \left(1 - t^r\right)\left(1 - q^r t^r\right) \prod_{\zeta^r = 1} Z(\zeta t) \\
&= \left(1 - t^r\right)\left(1 - q^r t^r\right) \prod_{\zeta^r = 1} \frac{L(\zeta t)}{(1 - \zeta t)(1 - q\zeta t)} = \prod_{\zeta^r = 1} L(\zeta t) \\
&= \prod_{i=1}^{2g} \prod_{\zeta^r = 1} (1 - \alpha_i \zeta t) = \prod_{i=1}^{2g} \left(1 - \alpha_i^r t^r\right).
\end{aligned}$$

Portanto, $L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t)$.

■

O teorema anterior nos mostra que o número

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

pode ser calculado se o polinômio $L(t)$ for conhecido. Mais geralmente, consideramos o caso em que $r \geq 1$, e definimos o número

$$N_r := N\left(F_r\right) = \left|\{P \in \mathbb{P}_{F_r} \mid \deg P = 1\}\right|,$$

com F_r de grau r.

Corolário 5.15. *Para todo $r \geq 1$, vale a igualdade*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

onde $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ são os inversos das raízes de $L(t)$.

Demonstração: Pelo teorema 5.14, se considerarmos o L-polinômio de $L_r(t)$, o coeficiente que multiplica t é dado por $N_r - (q^r + 1)$. Por outro lado,

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t),$$

e assim o coeficiente que multiplica t é dado por $-\sum_{i=1}^{2g} \alpha_i^r$. Portanto,

$$N_r - (q^r) + 1 = -\sum_{i=1}^{2g} \alpha_i \Rightarrow N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i.$$

■

O corolário a seguir encerra esta seção, nos mostrando que é possível calcularmos o L-polinômio de um corpo de funções, quando se conhece os números N_r's definidos anteriormente.

Corolário 5.16. *Sejam $L(t) = \sum_{i=0}^{2g} a_i t^i$ o L-polinômio de $F/\mathbb{F}_q$ e $S_r := N_r - (q^r + 1)$. Então*

(a) $\dfrac{L'(t)}{L(t)} = \sum_{r=1}^{\infty} S_r t^{r-1}$ *e*

(b) $a_0 = 1$ e $a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}$, com $i = 1, \ldots, g$. Assim, dados $N_1, \ldots, N_g$, podemos determinar $L(t)$ pela equação acima e por $a_{2g-i} = q^{g-i} a_i$.

Demonstração: (a) Primeiramente escrevemos $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$, como no teorema 5.14. Por indução, podemos mostrar que

$$\frac{L'(t)}{L(t)} = \sum_{i=1}^{2g} \frac{-\alpha_i}{(1 - \alpha_i t)}.$$

Assim, do corolário 5.15 e da definição de S_r, obtemos

$$\frac{L'(t)}{L(t)} = \sum_{i=1}^{2g} \frac{-\alpha_i}{(1 - \alpha_i t)} = \sum_{i=1}^{2g} (-\alpha_i) \cdot \sum_{r=0}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} -\alpha_i^r \right) t^{r-1} = \sum_{r=1}^{\infty} S_r t^{r-1},$$

como queríamos mostrar.

(b) Pelo teorema 5.14, já sabemos que $a_0 = 1$. Agora, como $L(t) = \sum_{i=0}^{2g} a_i t^i$, então

$$L'(t) = a_1 + 2a_2 t + 3a_3 t^2 + \cdots + 2g a_{2g} t^{2g-1}.$$

Do item (a), temos

$$a_1 + 2a_2t + \cdots + 2ga_{2g}t^{2g-1} = \left(a_0 + a_1t + \cdots + a_{2g}t^{2g}\right) \cdot \sum_{r=1}^{\infty} S_r t^{r-1},$$

e comparando os coeficientes,

$$\begin{cases} a_1 = a_0S_1 \\ 2a_2 = a_0S_2 + a_1S_1 \\ \vdots \\ ga_g = a_0S_g + a_1S_{g-1} + \cdots + a_{g-1}S_1 \end{cases},$$

e portanto vale a igualdade do enunciado.

■

5.2 O teorema de Hasse-Weil

Nesta seção, iremos manter todas as notações da seção anterior. Nosso objetivo será estudar o teorema de Hasse-Weil, o qual afirma que os inversos das raízes de $L_F(t)$ satisfazem

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

O teorema de Hasse-Weil é geralmente referido como hipótese de Riemann para corpos de funções. Mais adiante veremos essa comparação com mais detalhes. Ao decorrer desta seção teremos vários resultados que nos auxiliarão na demonstração do teorema principal.

Lema 5.17. *Seja $m \geq 1$. Então o teorema de Hasse-Weil é válido para $F/\mathbb{F}_q$ se, e somente se, é válido para a extensão de corpo constante $F_m/\mathbb{F}_{q^m}$.*

Demonstração: Denote por α_i, $i = 1, 2, \ldots, 2g$ os inversos das raízes de $L_F(t)$. Pelo teorema 5.14, denotando por $L_m(t)$ o L-polinômio de F_m, segue que os inversos das raízes de $L_m(t)$ são $\alpha_1^m, \ldots, \alpha_{2g}^m$.

Assim,

$$|\alpha_i| = q^{1/2} \Leftrightarrow |\alpha_i|^m = \left(q^{1/2}\right)^m \Leftrightarrow |\alpha_i^m| = \left(q^m\right)^{1/2},$$

e portanto segue o resultado.

■

O próximo lema nos dará uma ideia de como será feita a demonstração do teorema de Hasse-Weil.

Lema 5.18. *Suponha que exista $c \in \mathbb{R}$ tal que, para todo $r \geq 1$, vale a desigualdade*

$$|N_r - (q^r + 1)| \leq cq^{r/2}.$$

Então, o teorema de Hasse-Weil é válido para $F/\mathbb{F}_q$.

Demonstração: Pelo corolário 5.15, para todo $r \geq 1$, tem-se

$$N_r - (q^r + 1) = -\sum_{i=1}^{2g} \alpha_i^r.$$

Logo,

$$|N_r - (q^r + 1)| \leq cq^{r/2} \Rightarrow \left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq cq^{r/2}.$$

Considere agora a função meromorfa $H(t) := \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}$ e $\varrho := \min\left\{ \left| \alpha_i^{-1} \right| ; 1 \leq i \leq 2g \right\}$. Além disso, considere a expansão em série de potências de $H(t)$. Note que, como as únicas singularidades de $H(t)$ são os α_i^{-1}'s, então o raio de convergência desse série em torno de $t = 0$ é exatamente ϱ.

Por outro lado, para $|t| < \varrho$,

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^r \right) t^r.$$

Como $\left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq cq^{r/2}$, então $H(t)$ converge para $|t| < q^{-1/2}$, ou seja $q^{-1/2} \leq \varrho$. Assim, $|\alpha_i| \leq q^{1/2}$, para todo $i = 1, \ldots, 2g$. Por outro lado, pelo teorema 5.14, $\prod_{i=1}^{2g} \alpha_i = q^g$, e portanto

$$q^g = \left(q^{1/2} \right)^{2g} \geq \prod_{i=1}^{2g} |\alpha_i| \geq \prod_{i=1}^{2g} \alpha_i = q^g \Rightarrow q^{1/2} = |\alpha_i|.$$

■

Note que a desigualdade $|N_r - (q^r + 1)| \leq cq^{r/2}$ é equivalente a existirem cotas superiores e inferiores para N_r, ou seja, existem $c_1, c_2 > 0$ tais que

$$N_r \leq q^r + 1 + c_1 q^{r/2} \quad \text{e} \quad N_r \geq q^r + 1 + c_2 q^{r/2},$$

para todo $r \geq 1$. Pelo lema 5.17 o teorema de Hasse-Weil é válido para $F/\mathbb{F}_q$ se ele for válido para alguma extensão de corpo constante de F. Logo, é suficiente provarmos as desigualdade acima com algumas hipóteses adicionais, as quais pode ser vistas em alguma extensão finita apropriada.

Proposição 5.19. *Suponha que $F/\mathbb{F}_q$ é um corpo de funções tal que q é um quadrado perfeito e $q > (g+1)^4$. Então, o número $N = N(F)$ de lugares de grau 1 pode ser estimado por*

$$N < (q + 1) + (2g + 1)q^{1/2}.$$

Demonstração: Se $N = 0$, a proposição é trivial. Suponhamos $N > 0$, ou seja, existe $Q \in \mathbb{P}_F$ com $\deg(Q) = 1$. Defina

$$q_0 := q^{1/2}, \quad m := q_0 - 1 \quad \text{e} \quad n := 2g + q_0.$$

Se $r := q - 1 + (2g + 1)q^{1/2}$, então $r = m + nq_0$. Seja

$$T := \{i \mid 0 \leq i \leq m, \text{ e } i \text{ e um número polo de } Q\}.$$

Lembramos que $i \geq 0$ é número polo de Q se existe $x \in F$ tal que $\langle x \rangle_\infty = iQ$.

Agora, dado $i \in T$, existe $u_i \in F$ tal que seu polo divisor é dado por iQ. Logo, o conjunto $\{u_i \mid i \in T\}$ é uma base pra $\mathcal{L}(mQ)$. Considere o conjunto

$$\mathcal{L} := \mathcal{L}(mQ) \cdot \mathcal{L}(nQ)^{q_0} \subseteq \mathcal{L}(rQ).$$

Por definição, $\mathcal{L}$ é formado por somas finitas da forma $\sum_{\text{finita}} x_\nu y_\nu^{q_0}$, com $x_\nu \in \mathcal{L}(mQ)$ e $y_\nu \in \mathcal{L}(nQ)$. Assim $\mathcal{L}$ é um espaço vetorial sobre $\mathbb{F}_q$, e a inclusão $\mathcal{L} \subseteq \mathcal{L}(rQ)$ segue da forma com que r foi definido. Dividiremos a demonstração em três afirmações.

Afirmação 1: Dado $y \in \mathcal{L}$, y pode ser escrito de maneira única da forma $y = \sum_{i \in T} u_i z_i^{q_0}$, com $z_i \in \mathcal{L}(nQ)$.

De fato, como $y \in \mathcal{L}$, então $y = \sum_{\text{finita}} x_\nu y_\nu^{q_0}$. Agora, como $x_\nu \in \mathcal{L}(mQ)$ e $\{u_i \mid i \in T\}$ é base de $\mathcal{L}(mQ)$, então x_ν pode ser escrito como combinação linear dos u_i's. Reajustando os índices,

$$y = \sum_{i \in T} u_i z_i^{q_0}, \quad \text{com } z_i \in \mathcal{L}(nQ).$$

Para a unicidade, suponhamos que exista uma igualdade da forma $\sum_{i \in T} u_i x_i^{q_0} = 0$, com $x_i \in \mathcal{L}(nQ)$, onde nem todos os x_i's são nulos. Assim, para cada $i \in T$ tal que $x_i \neq 0$,

$$v_Q\left(u_i x_i^{q_0}\right) \equiv v_Q\left(u_i\right) \equiv -i \bmod q_0.$$

Agora, como $m = q_0 - 1$, os números $i \in T$ são dois a dois distintos módulo q_0. Logo, pela desigualdade triangular estrita, segue que

$$v_Q\left(\sum_{i \in T} u_i x_i^{q_0}\right) = \min\left\{v_Q\left(u_i x_i^{q_0}\right) \mid i \in T\right\} \neq \infty,$$

e isso prova a afirmação 1.

Agora, consideramos a aplicação $\lambda : \mathcal{L} \to \mathcal{L}\left(\left(q_0 m + n\right) Q\right)$ dada por

$$\lambda\left(\sum_{i \in T} u_i z_i^{q_0}\right) := \sum_{i \in T} u_i^{q_0} z_i.$$

Pela afirmação 1, λ está bem definida, porém não é $\mathbb{F}_q$-linear. Em contrapartida, λ é um homomorfismo do grupo aditivo de $\mathcal{L}$ em $\mathcal{L}((q_0 m + n)Q)$.

Afirmação 2: $\ker \lambda \neq \{0\}$.

É suficiente mostrarmos que $\dim \mathcal{L} > \dim \mathcal{L}\left(\left(q_0 m + n\right) Q\right)$. Pelo teorema de Riemann-Roch,

$$\dim \mathcal{L} = \ell(mQ) \cdot \ell(nQ) \geq (m + 1 - g)(n + 1 - g).$$

Por outro lado,

$$q_0 m + n = q_0(q_0 - 1) + (2g + q_0) = q + 2g$$

e logo obtemos $\dim \mathcal{L}((q_0 m + n)Q) = (2g + q) + 1 - g = g + q + 1$. Queremos mostrar que $(m + 1 - g)(n + 1 - g) > g + q + 1$. Por hipótese $q > (g + 1)^4$, e logo,

$$q > (g+1)^4 \Leftrightarrow q_0 > (g+1)^2 \Leftrightarrow q_0 + q > g^2 + 2g + 1 + q \Leftrightarrow (q_0 - g)(2g + q_0 + 1 - g) > g + 1 + q \Leftrightarrow$$
$$\Leftrightarrow (m + 1 - g)(n + 1 - g) > g + 1 + q.$$

Portanto, $\dim \mathcal{L} > \dim \mathcal{L}((q_0 m + n)Q)$, o que prova a afirmação 2.

Afirmação 3: Sejam $0 \neq x \in \mathcal{L}$ tal que $x \in \ker \lambda$ e $P \neq Q$ um lugar de grau 1. Então $x(P) = 0$.

Primeiramente, note que $y(P) \neq \infty$ para todo $y \in \mathcal{L}$, uma vez que Q é o único polo de y. Agora, como $\mathbb{F}_q$ é o corpo de classe residual de P, temos $y(P)^q = y(P)$. Agora, da hipótese, $x \in \ker \lambda$ e $x \neq 0$. Escreva $x = \sum_{i \in T} u_i z_i^{q_0}$. Assim,

$$\begin{aligned} x(P)^{q_0} &= \left(\sum_{i \in T} u_i(P) \cdot z_i(P)^{q_0} \right)^{q_0} \\ &= \sum_{i \in T} u_i^{q_0}(P) \cdot z_i(P)^q \\ &= \left(\sum_{i \in T} u_i^{q_0} z_i \right)(P) = \lambda(x)(P) = 0 \end{aligned}$$

Logo, $x(P) = 0$.

Agora, vamos combinar todas essa afirmações para concluir a demonstração da proposição. Da *afirmação 3*, existe $0 \neq x \in \mathcal{L}$ tal que $x(P) = 0$, para todo $P \in \mathbb{P}_F$ com $\deg P = 1$ e $P \neq Q$. Logo, todos os lugares de grau 1, com exceção de Q são zeros de x, e o divisor zero $\langle x \rangle_0$ é tal que $\deg \langle x \rangle \geq N - 1$.

Como $x \in \mathcal{L} \subseteq \mathcal{L}(rQ)$, segue que

$$\deg \langle x \rangle_0 = \deg \langle x \rangle_\infty \leq r = q - 1 + (2g+1)q^{1/2}.$$

Combinando as duas desigualdades, obtemos $N \leq q + (2g+1)q^{1/2}$, o que conclui a demonstração.

■

Com essa proposição, mostramos a existência de uma cota superior para N_r, bastando escolher uma extensão de corpo constante apropriada. Para a demonstração da existência de uma cota inferior, uma série de resultados da teoria de grupos é necessária, e podem ser encontrados em [1] e em [2]. Com isso, é válido o teorema de Hasse-Weil, o qual enunciaremos a seguir.

Teorema 5.20. *(Hasse-Weil) Os inversos das raízes de $L_F(t)$ satisfazem $|\alpha_i| = q^{1/2}$, com $i = 1, 2, \ldots, 2g$.*

Observação 5.21. *Como citamos anteriormente, o teorema de Hasse-Weil muitas vezes é referido como a hipótese de Riemann para corpos de funções. Muitos matemáticos consideram a função de Zeta $Z_F(t)$ do corpo de funções $F/\mathbb{F}_q$ como uma função análoga a clássica função ζ de Riemann*

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$$

onde $s \in \mathbb{C}$ e $\mathrm{Re}(s) > 1$, no seguinte sentido:

Definimos a norma absoluta de $A \in \mathrm{Div}(F)$ por $\mathcal{N}(A) := q^{\deg A}$. Aqui, a norma absoluta $\mathcal{N}(P)$ de um divisor primo $P \in \mathbb{P}_F$ é a cardinalidade de sua classe residual no corpo F_P, onde $F_P = \mathcal{O}_P/P$ e $\mathcal{O}_P$ é o anel de valorização associado a P. Então, a função $\zeta_F(s) := Z_F(q^{-s})$ pode ser escrita como

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathrm{Div}(F), A \geq 0} \mathcal{N}(A)^{-s}$$

Da teoria dos números, sabemos que a ζ-função de Riemann tem uma continuação analítica como uma função meromorfa em $\mathbb{C}$. A clássica Hipótese de Riemann afirma que, a menos dos zeros triviais $s = -2, -4, \ldots$, todos os zeros de $\zeta(s)$ pertencem a reta $\mathrm{Re}(s) = \dfrac{1}{2}$. No caso de corpos de funções, o teorema de Hasse-Weil nos assegura que

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}$$

e como $|q^{-s}| = q^{-\mathrm{Re}(s)}$, isso nos diz que

$$\zeta_F(s) = 0 \Rightarrow \mathrm{Re}(s) = \frac{1}{2}.$$

Logo, o teorema 5.20 pode ser visto como uma forma análoga da Hipótese de Riemann.

Teorema 5.22. *(Cota de Hasse-Weil) O número $N = N(F)$ de lugares de $F/\mathbb{F}_q$ de grau 1 satisfaz a desigualdade*

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

Demonstração: Pelo corolário 5.15, $N - (q+1) = -\sum_{i=1}^{2g} \alpha_i$, e pelo teorema 5.20, $|\alpha_i| = q^{1/2}$, para $i = 1, \ldots, 2g$. Portanto,

$$|N - (q+1)| = \left| -\sum_{i=1}^{2g} \alpha_i \right| \leq \sum_{i=1}^{2g} |\alpha_i| = \sum_{i=1}^{2g} q^{1/2} = 2gq^{1/2}.$$

■

Usando a cota de Hasse-Weil, podemos calcular uma estimativa para o número de lugares de um grau fixado r. Dado $F/\mathbb{F}_q$ de gênero g, definimos

$$B_r := B_r(F) := |\{P \in \mathbb{P}_F; \deg P = r\}|.$$

Observe que $B_1 = N(F)$. Existe ainda uma relação entre os números B_r e N_s, em que N_s denota o número de lugares de grau um da extensão de corpos constantes $F_s = F\mathbb{F}_q$ dada por

$$N_r = \sum_{d|r} d \cdot B_d.$$

Essa fórmula segue do fato de que todo lugar $P \in \mathbb{P}_F$ de grau d, com $d \mid r$ se decompõe em d lugares de grau um em $\mathbb{P}_F$, e as extensões P' de P em F_r/F possuem grau $\deg P' > 1$ se $\deg P \nmid r$.

Considere agora a função de Mobius $\mu : \mathbb{N} \to \{0, -1, 1\}$ dada por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{existe um inteiro } k > 1 \text{ tal que } k^2 \mid n, \\ (-1)^l & \text{se } n \text{ é o produto de } l \text{ primos distintos.} \end{cases}$$

A fórmula da inversão de Mobuis transforma a relação anterior em

$$r \cdot B_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot N_d.$$

Definimos agora $S_r := -\sum_{i=1}^{2g} \alpha_i^r$ onde os α's são os inversos das raízes de $L_F(t)$. No caso em que o gênero é nulo, convenciona-se que $g = 0$. Assim, pelo corolário 5.15, temos $N_r = q^r + 1 + S_r$.

Agora, substituindo na equação transformada por μ, obtemos

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) N_d = \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d + 1 + S_d) = \sum_{d|r} \mu\left(\frac{r}{d}\right) q^d + \sum_{d|r} \mu\left(\frac{r}{d}\right) + \sum_{d|r} \mu\left(\frac{r}{d}\right) S_d.$$

Portanto $rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d + S_d)$. Com isso, temos provado o seguinte resultado:

Proposição 5.23. *Para quaisquer $r \geq 2$, tem-se* $B_r = \frac{1}{r} \cdot \sum_{d|r} \mu\left(\frac{r}{d}\right)\left(q^d + S_d\right)$.

Corolário 5.24. *(a) A desigualdade*

$$\left|B_r - \frac{q^r}{r}\right| \leq \left(\frac{q}{q-1} + 2g\frac{q^{1/2}}{q^{1/2}-1}\right) \cdot \frac{q^{r/2}-1}{r} < (2+7g) \cdot \frac{q^{r/2}}{r}$$

é válida para todo $r \geq 1$.

(b) Se $g = 0$, então $B_r > 0$, para todo $r \geq 1$.

(c) Seja r tal que $2g + 1 \leq q^{(r-1)/2}\left(q^{1/2} - 1\right)$. Então existe pelo menos um lugar de grau r. Em particular, se $r \geq 4g + 3$, então $B_r \geq 1$.

Demonstração: (a) Para $r = 1$, a desigualdade segue diretamente da cota de Hasse-Weil. Vamos mostrar para o caso em que $r \geq 2$. Pela proposição 5.23, temos que

$$B_r - \frac{q^r}{r} = \frac{1}{r} \sum_{d|r, d<r} \mu\left(\frac{r}{d}\right) q^d + \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right) S_d.$$

Defina $l := [r/2]$ (parte inteira de $r/2$). Agora, observando que

$$|S_d| = \left|\sum_{i=1}^{2g} \alpha_i^d\right| \leq 2gq^{d/2},$$

obtemos

$$\begin{aligned}
\left|B_r - \frac{q^r}{r}\right| &\leq \frac{1}{r}\sum_{d=1}^{l} q^d + \frac{2g}{r}\sum_{d=1}^{r} q^{d/2} \\
&= \frac{q}{r} \cdot \frac{q^l - 1}{q-1} + \frac{2gq^{1/2}}{r} \cdot \frac{q^{r/2}-1}{q^{1/2}-1} \\
&\leq \left(\frac{q}{q-1} + 2g\frac{q^{1/2}}{q^{1/2}-1}\right) \cdot \frac{q^{r/2}-1}{r} \\
&< (2+7g) \cdot \frac{q^{r/2}}{r}.
\end{aligned}$$

(b) e (c): Observe que do item (a), segue que $B_r > 0$ sempre que

$$\frac{q^r}{r} > \left(\frac{q}{q-1} + 2g\frac{q^{1/2}}{q^{1/2}-1}\right) \cdot \frac{q^{r/2}-1}{r}. \quad (\star)$$

Agora, quando $g = 0$, a equação acima é válida para todo $r \geq 1$, o que prova o item (b), e vamos supor agora $g \geq 1$. A equação $(\star)$ pode ser reescrita da forma

$$2g + \frac{1}{1 + q^{-1/2}} < \frac{q^r \left(q^{1/2} - 1\right)}{q^{1/2} \left(q^{r/2} - 1\right)}.$$

Valem então as desigualdades

$$2g + \frac{1}{1 + q^{-1/2}} < 2g + 1 \quad \text{e} \quad q^{(r-1)/2} \left(q^{1/2} - 1\right) < \frac{q^r \left(q^{1/2} - 1\right)}{q^{1/2} \left(q^{r/2} - 1\right)}.$$

Como estamos supondo $2g+1 \leq q^{(r-1)/2} \left(q^{1/2} - 1\right)$, temos $B_r > 0$. Por fim, se $r \geq 4g+3$, segue que

$$2g + 1 < 2^{2g+1} \left(2^{1/2} - 1\right) \leq 2^{(r-1)/2} \left(2^{1/2} - 1\right) \leq q^{(r-1)/2} \left(q^{1/2} - 1\right),$$

o que conclui a prova do item (c).

■

5.3 Melhorias da cota de Hasse-Weil

Em geral, a cota de Hasse-Weil $|N - (q+1)| \leq 2gq^{1/2}$ é a melhor possível, pois existem exemplos de corpos de funções $F/\mathbb{F}_q$ tais que $N = q + 1 + 2gq^{1/2}$ ou $N = q + 1 - 2gq^{1/2}$.

Definição 5.25. *Um corpo de funções $F/\mathbb{F}_q$ de gênero g é dito maximal se $N = q + 1 + 2gq^{1/2}$.*

Como $n \in \mathbb{Z}$, o corpo de funções maximais existe somente se q for um quadrado perfeito. Contudo, sob certas condições, essa cota pode ser melhorada. Se q não é um quadrado perfeito, então claramente

$$|N - (q + 1)| \leq \left[2gq^{1/2}\right],$$

onde $[a]$ denota a parte inteira do número a. Temos inicialmente a cota de Serre.

Teorema 5.26. *(Cota de Serre) Se $F/\mathbb{F}_q$ é um corpo de funções de gênero g, então o número de lugares de grau 1 é limitado por*

$$|N - (q + 1)| \leq g \left[2q^{1/2}\right].$$

Demonstração: Seja $\mathbb{A} \subseteq \mathbb{C}$ o conjunto dos inteiros algébricos, ou seja, $\alpha \in \mathbb{A}$ se, e somente se, existe $p(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ tal que $p(\alpha) = 0$. Da teoria algébrica dos números, temos que $\mathbb{A}$ é um subanel de $\mathbb{C}$ e $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. Assumimos $g > 0$ e consideramos o L-polinômio de $F/\mathbb{F}_q$ dado por

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t).$$

Os números $\alpha_1, \ldots, \alpha_{2g}$ são inteiros algébricos com $|\alpha_i| = q^{1/2}$, e podem ser reordenados de forma a obter $\alpha_i \alpha_{g+i} = q$. Como $|\alpha_i| = q^{1/2}$ e $\alpha_i \alpha_{g+i} = q$, segue que $\overline{\alpha_i} = \alpha_{g+1} = \dfrac{q}{\alpha_i}$, para $i = 1, \ldots, g$. Defina

$$\gamma_i := \alpha_i + \bar{\alpha}_i + \left[2q^{1/2}\right] + 1$$
$$\delta_i := -(\alpha_i + \bar{\alpha}_i) + \left[2q^{1/2}\right] + 1$$

Pelo que construimos, γ_i e α_i são inteiros algébricos e como $|\alpha_i| = q^{1/2}$, segue que $\gamma_i, \delta_i > 0$. Cada injeção da forma $\sigma : \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g}) \longrightarrow \mathbb{C}$ permuta $\alpha_1, \ldots, \alpha_{2g}$, uma vez que

$$\prod_{i=1}^{2g} (t - \alpha_i) = L^{\perp}(t) \in \mathbb{Z}[t],$$

pelo teorema 5.14. Mais ainda, $\sigma(\alpha_i) = \alpha_j$, e então

$$\sigma(\bar{\alpha}_i) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = \overline{\sigma(\alpha_i)} = \bar{\alpha}_j.$$

Logo, σ é uma permutação dos conjuntos $\{\gamma_1, \ldots \gamma_g\}$ e $\{\delta_1, \ldots, \delta_g\}$. Defina

$$\gamma := \prod_{i=1}^{g} \gamma_i \quad \text{e} \quad \delta := \prod_{i=1}^{g} \delta_i.$$

Os números γ e δ são inteiros algébricos, os quais são invariantes sob todas as injeções de $\mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ em $\mathbb{C}$. Logo, $\gamma, \delta \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. Como $\gamma_i, \delta_i > 0$ então $\delta, \gamma > 0$, e logo

$$\prod_{i=1}^{g} \gamma_i \geq 1 \quad \text{e} \quad \prod_{i=1}^{g} \delta_i \geq 1.$$

Sabemos da aritmética básica que a média aritmética é sempre maior ou igual a média geométrica, e portanto,

$$\frac{1}{g} \sum_{i=1}^{g} \gamma_i \geq \left(\prod_{i=1}^{g} \gamma_i \right)^{1/g} \geq 1.$$

Agora,

$$\frac{1}{g} \sum_{i=1}^{g} \gamma_i = \frac{1}{g} \sum_{i=1}^{g} \left(\alpha_i + \overline{\alpha_i} + [2q^{1/2}] + 1 \right) \geq 1 \Rightarrow \left(\sum_{i=1}^{g} (\alpha_i + \overline{\alpha_i}) \right) + g[2q^{1/2}] + g \geq g \Rightarrow$$
$$\Rightarrow g \leq \sum_{i=1}^{2g} \alpha_i + g\left[2q^{1/2}\right] + g$$

Pelo corolário 5.15, $\displaystyle\sum_{i=1}^{2g} \alpha_i = (q+1) - N$. Logo,

$$g \leq -N + (q+1) + g[2q^{1/2}] + g \Rightarrow N \leq (q+1) + g[2q^{1/2}].$$

Agora, fazendo o mesmo processo para os δ_i's, obtemos

$$\frac{1}{g} \sum_{i=1}^{g} \delta_i \geq \left(\prod_{i=1}^{g} \delta_i \right)^{1/g} \geq 1.$$

Consequentemente

$$N \geq q + 1 - g\left[2q^{1/2}\right],$$

e portanto $|N - (q+1)| \leq g[2q^{1/2}]$.

■

O próximo resultado, e último deste capítulo, nos diz que $F/\mathbb{F}_q$ não pode ser maximal se g for grande em relação a q.

Proposição 5.27. *(Ihara) Seja $F/\mathbb{F}_q$ um corpo de funções maximal. Então $g \leq \dfrac{q-q^{1/2}}{2}$.*

Demonstração: Sejam $\alpha_1, \ldots, \alpha_{2g}$ os inversos das raízes de $L(t)$. Sabemos que

$$N = q + 1 - \sum_{i=1}^{2g} \alpha_i \quad \text{e} \quad |\alpha_i| = q^{1/2}.$$

Além dsso, da hipótese, $N = q + 1 + 2gq^{1/2}$. Logo,

$$2gq^{1/2} = -\sum_{i=1}^{2g} \alpha_i \Rightarrow \alpha_i = -q^{1/2}, \quad i = 1, \ldots, 2g.$$

Agora, consideramos o número N_2 de lugares de grau um da extensão $F\mathbb{F}_{q^2}/\mathbb{F}_{q^2}$. Temos $N_2 \geq N$, e

$$N_2 = q^2 + 1 - \sum_{i=1}^{2g} \alpha_i^2 = q^2 + 1 - 2gq.$$

Logo,

$$q + 1 + 2gq^{1/2} \leq q^2 + 1 - 2gq \Rightarrow 2g(q^{1/2} + q) \leq (q - q^{1/2})(q + q^{1/2}) \Rightarrow g \leq \frac{q - q^{1/2}}{2}.$$

■

Encerramos este capítulo com a seguinte observação, a qual pode ser encontrada detalhadamente em [1], no exemplo 6.3.6.

Observação 5.28. *Considere o corpo de funções $H := \mathbb{F}_{q^2}(x, y)$ sobre $\mathbb{F}_{q^2}$, onde $x^{q+1} + y^{q+1} = 1$. Neste caso H é chamado de corpo de funções Hermitiano sobre $\mathbb{F}_{q^2}$.*

Neste caso, é possível mostrar que H é um corpo de funções maximal com $g = q(q-1)/2$, o que garante que a desigualdade proposta na proposição 5.27 não pode ser melhorada.

Referências

[1] STITCHTENOTH, H. *Algebraic Function Fields and Codes*. [S.l.]: Springer-Verlag, 1993.

[2] NIEDERREITER, H.; XING, C. *Rational Poits on Curves over Finite Fields Theory and Applications*. [S.l.]: London Mathematical Society Lecture Note Series 285, 2001.

[3] CHEVALLEY, C. *Introduction to the Theory of Algebraic Function of One Variable*. [S.l.]: AMS Math. Surveys, 1951. v. 6.

[4] EISENBUD, D. *Commutative Algebra, with a View Toward Algebraic Geometry*. [S.l.]: Springer-Verlag, 1999.

[5] ENGE, A. *Elliptic Curves and Their Applications to Cryptography: An Introduction*. [S.l.]: Kluwer, 1999.

[6] FULTON, W. *Algebraic Curves*. [S.l.]: Benjamin Cummings, 1969.

[7] MORENO, C. *Algebraic Curves over Finite Fields*. [S.l.]: Cambridge Tracts in Mathematics (97), Cambridge University Press, 1991.

[8] MENEZES, A. J. *Elliptic Curve Public Key Cryptosystems*. [S.l.]: Kluwer, 1993.

[9] LORENZINI, D. *An Invitation to Arithmetic Geometry*. [S.l.]: American Mathematical Society, 1996. v. 9.

[10] BLAKE, I. F.; SEROUSSI, G.; SMART, N. P. *Elliptic Curves in Cryptography*. Cambridge: London Math. Soc. Lecture Note Series, 1999.

[11] CLARK, G. C. J.; CAIN, J. B. *Error-Correction Coding for Digital Communications*. [S.l.]: Plenum Press, 1981.

[12] GARCIA, A.; STICHTENOTH, H. *A Tower of Artin-Schreier Extensions of Function Fields attaining the Drinfeld-Vladut Bound*. [S.l.]: Springer-Verlag, 1995.

[13] GARCIA, A.; STICHTENOTH, H. *On the asymptotic behaviour of some towers of function fields over finite fields*. [S.l.]: Journal of Number Theory, 1996. 248-273 p.