UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Marcos Henrique Silva Almeida

Corpos de funções algébricas: O Teorema de Riemann-Roch

Juiz de Fora
2020

Marcos Henrique Silva Almeida

Corpos de funções algébricas: O Teorema de Riemann-Roch

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de grau de bacharel em Matemática.

Orientadora: Dr[a] Joana Darc Antonia Santos da Cruz

Juiz de Fora

2020

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

Almeida, Marcos Henrique.
Corpos de funções algébricas : O Teorema de Riemann-Roch / Marcos Henrique Silva Almeida. – 2020.
95 f.

Orientadora: Joana Darc Antonia Santos da Cruz
Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Departamento de Matemática, 2020.

1. Corpos de Funções Algébricas. 2. Divisores. 3. Gênero. 4. Teorema de Riemann-Roch I. Cruz, Joana Darc Antonia Santos da, orient. II. Título.

Marcos Henrique Silva Almeida

Corpos de funções algébricas: O Teorema de Riemann-Roch

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de grau de bacharel em Matemática.

Aprovada em (dia) de (mês) de (ano)

BANCA EXAMINADORA

Drª Joana Darc Antonia Santos da Cruz - Orientadora
Universidade Federal de Juiz de Fora

Drª Flaviana Andrea Ribeiro
Universidade Federal de Juiz de Fora

Drª Tatiana Aparecida Gouveia
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

Agradeço primeiramente a Deus.

Agradeço a minha mãe, Maria Quitéria Silva Amaro, pelo imenso apoio e por sempre acreditar em mim.

Agradeço de forma incondicional a minha Vó Conceição e minha tia Bu (Ana Maria) por tudo que fazem por mim com relação ao meus estudos e minha vida como um todo. E minhas tias: Zana (Rosana), Tia Tina (Ana Cristina) e Paty (Ana Lúcia).

Agradeço a minha primeira orientadora, Beatriz Casulari da Motta Ribeiro, por despertar em mim a imensa paixão pela Álgebra.

Agradeço as minhas atuais orientadoras, Joana e Flaviana, por continuarem estimulando essa paixão pela Álgebra e despertarem em mim uma nova paixão: Geometria Algébrica.

Agradeço a todos meus colegas da graduação. De forma especial aos meus colegas que viraram amigos (família): Kaio Cruz e Silva, Rodrigo Pinto Leal, Raphael Cascelli dos Santos Souza e Tamires Loureiro.

Agradeço a minha família em Juiz de Fora (carinhosamente chamamos de família gay), Diego Azevedo Lopes, Jonathan Luís Hipolito Ferreira e Douglas Luiz J. Ribeiro, que foram o meu porto seguro no meio de tantas incertezas e medos.

Agradeço a todos os meus familiares. Em especial: minha vó Dalva, minha irmã Maria Fernanda e meu pai Fernando Cézar.

Por fim, agradeço a todos os professores que passei durante essa jornada e me ajudaram a traçar uma trajetória muito bonita.

"Bem, uma superfície de Riemann é um certo tipo de espaço Hausdorf. Você sabe o que é um espaço Hausdorf, não é? Também é compacto, ok. Eu acho que também é uma variedade. Certamente você sabe o que é uma variedade . Agora, deixe-me dizer-lhe um teorema não trivial, o teorema de Riemann-Roch.". (A lembrança de Gian-Carlo Rota das palestras de Lefschetz na década de 1940, citada em A Beautiful Mind por Sylvia Nasar)

RESUMO

O objetivo deste trabalho é apresentar um estudo sobre Corpos de Funções Algébricas. O foco principal do trabalho é apresentar a demonstração do Teorema de Riemann-Roch e algumas consequências. Este teorema é de grande importância nas áreas de Geometria Algébrica e Curvas Algébricas. Usaremos o Teorema de Riemann-Roch para apresentar algumas caracterizações importantes para o estudo de Corpos de Funções Algébricas através da análise do gênero destes corpos. Para o desenvolvimento do estudo serão apresentados conceitos tais como: Lugar, Valorização, Divisor, Gênero de um Corpo de Funções Algébricas.

Palavras-chave: Corpos de Funções Algébricas. Divisores. Gênero. Teorema de Riemann-Roch.

ABSTRACT

In this work we study algebraic function fields. The main purpose here is to present the demonstration of the Riemann-Roch Theorem and some of its consequences. This theorem is a very important result in Algebraic Geometry and Algebraic Curves. For example, we use the Riemann-Roch Theorem to present an important characterization of the genus of the algebraic function fields. For the development of the study it will be presented, concepts such as places, valuation, divisors and genus of algebraic functions fields.

Keywords: Algebraic function field. Divisor. Genus. Riemann-Roch Theorem.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem como principal foco a demonstração do Teorema de Riemann-Roch através do estudo no Corpo de Funções Algébricas. Os corpos de funções algébricas sobre o corpo K são extensões de corpos $F \supseteq K$, tal que F é uma extensão algébrica finita de $K(x)$, para algum elemento $x \in F$ que é transcendente sobre K. Para o estudo destes elementos algébricos serão apresentados conceitos importantes: Lugar, Valorização, Polos e Zeros. No decorrer dos estudos introduzimos o conceito de Divisores, Gênero de Corpos de Funções Algébricas e os Adeles são apresentado com intuito de auxiliar na compreensão e demonstração do Teorema de Riemann-Roch.

O teorema de Riemann-Roch foi apresentado primeiramente como a desigualdade de Riemann, ou como Teorema de Riemann: "Para todo $A \in Div(F)$, $l(A) \geq gr(A) + 1 - g$". Posteriormente, em seus estudos , Gustav Roch (1965) apresentou correções e conseguiu a igualdade.

O capítulo Preliminares apresenta as noções básicas de Álgebra e Álgebra Linear necessários para a compreensão do texto.

O terceiro capítulo apresenta o conceitos: Corpos de Funções Algébricas, Lugar e Valorizações. O principal resultado do capítulo é o Teorema da Aproximação Fraca que além de nos mostrar a independência das valorizações tem como consequência o corolário de suma importância para o nosso estudo: " Todo Corpo de Funções Algébrica tem um número infinito de lugares.".

O quarto capítulo apresenta o conceito de divisores e um estudo sobre eles. Ao decorrer do capítulo apresentamos o espaço de Riemann-Roch, $\mathcal{L}(A)$ de um divisor A, estudamos a dimensão deste espaço e definimos o gênero de um Corpo de Funções F/K. Por fim, é apresentado e demonstrado o Teorema de Riemann.

O quinto capítulo exibe os conceitos de índice de especialidade de um divisor, o adele de um corpo de funções e divisor principal. O estudo destes conceitos nos guiam a demonstração do Teorema da Dualidade e o Teorema de Riemann-Roch.

No sexto capítulo vamos caracterizar: divisores canônicos de um Corpo de Funções Algébricas F/Ke o corpo de funções racionais através do estudo do gênero.

Por fim, vamos definir Lacuna e demonstrar o Teorema das Lacunas de Weiestrass.

2 PRELIMINARES

Começaremos o presente trabalho, apresentando algumas definições, resultados e exemplos de Álgebra e Álgebra Linear imprescindíveis para o entendimento do texto. Grande parte das demonstrações serão omitidas, no entanto, estão referenciadas para possíveis consultas.

2.1 ANÉIS, SUBANÉIS, IDEAIS E HOMOMORFISMOS

Definição 2.1.1. *Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de soma e produto em A e denotaremos por $+$ e $\cdot$, respectivamente. Assim, temos que*

$$+ : \begin{cases} A \times A & \longrightarrow & A \\ (x,y) & \longmapsto & x+y \end{cases} \qquad e \qquad \cdot : \begin{cases} A \times A & \longrightarrow & A \\ (x,y) & \longmapsto & x \cdot y \end{cases}.$$

Dizemos que $(A, +, \cdot)$ é um anel (ou simplesmente A é um anel) se as seguintes propriedades são verificadas para quaisquer x, y, $z \in A$.

A1) $(x+y)+z = x+(y+z)$;

A2) Existe $0 \in A$ *tal que* $x+0 = 0+x = x$;

A3) Para todo $x \in A$ *existe* $-x \in A$ *tal que* $x+(-x) = (-x)+x = 0$;

A4) $x+y = y+x$;

A5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

A6) $x \cdot (y+z) = x \cdot y + x \cdot z$;

A7) $(x+y) \cdot z = x \cdot z + y \cdot z$.

Definição 2.1.2. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

A8) Existe $1 \in A$, $1 \neq 0$, *tal que* $1 \cdot x = x \cdot 1 = x$ *para todo* $x \in A$,

dizemos que $(A, +, \cdot)$ é um anel com unidade.

Definição 2.1.3. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

A9) Para todo x, $y \in A$, $x \cdot y = y \cdot x$,

dizemos que $(A, +, \cdot)$ é um anel comutativo.

Definição 2.1.4. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

A10) Dados x e $y \in A$ tal que $x \cdot y = 0$ então $x = 0$ ou $y = 0$,

dizemos que $(A, +, \cdot)$ é um anel sem divisores de zero.

Definição 2.1.5. *Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um domínio de integridade.*

Definição 2.1.6. *Se $(A, +, \cdot)$ é um anel comutativo com unidade e satisfaz a propriedade:*

A11) Para todo $x \in A$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$,

dizemos que $(A, +, \cdot)$ é um corpo.

Observação 2.1.7. *Um corpo $(A, +, \cdot)$ será denotado apenas por K.*

Definição 2.1.8. *Sejam A um anel e B um subconjunto não vazio de A. Se B for fechado para as operações $+$ e $\cdot$ de A e B for um anel com essas operações, dizemos que B é um subanel de A.*

Se B é um subanel de um corpo K e B também é um corpo, dizemos que B é um subcorpo de K.

Proposição 2.1.9. *Sejam A um anel e B um subconjunto de A. Então B é um subanel de A se e somente, se:*

i) $0_A \in B$ (o elemento neutro de A pertence a B);

ii) x, $y \in B$, então $x - y \in B$;

iii) $x, y \in B$, *então* $x \cdot y \in B$;

Demonstração. Ver em [5], Capítulo III, Proposição 1. □

Definição 2.1.10. *Sejam* A *um anel e* I *um subanel de* A. *Dizemos que* I *é um ideal à esquerda de* A *se,* $a \cdot x \in I$, $\forall x \in I$ *e* $\forall a \in A$. *Ou seja, se* $A \cdot I \subset I$.

Sejam A *um anel e* J *um subanel de* A. *Dizemos que* J *é um ideal à direita de* A *se,* $x \cdot a \in J$, $\forall x \in J$ *e* $\forall a \in A$. *Ou seja, se* $J \cdot A \subset J$.

Se I *é um ideal simultaneamente à direita e à esquerda de um anel* A, *dizemos que* I *é um ideal de* A, *ou seja, se* $A \cdot I \subset I$ *e* $I \cdot A \subset I$.

Observemos que se A é um anel comutativo, um ideal à esquerda de A ou à direita de A é um ideal de A. Esta afirmação segue pois todo subanel de um anel comutativo é também comutativo.

Teorema 2.1.11. *Um subconjunto não vazio* I *de um anel* A *é um ideal se e somente se:*

(i) $a - b \in I$, *para todo* $a, b \in I$;

(ii) $x \cdot a$ *e* $a \cdot x$ *pertencem a* I, *se* $a \in A$ *e* $x \in I$.

Demonstração. A demostração decorre diretamente da definição de subanel e da definição de ideal. □

Se A é um anel comutativo então a condição (ii) do Teorema 2.1.11 é equivalente a mostrar que $xa \in I$ ou $ax \in I$, $\forall x \in I$ e $\forall a \in A$.

Definição 2.1.12. *Um ideal* I *de um anel* A *é dito maximal se* $I \neq A$ *e os únicos ideais de* A *contendo* I *são* I *e* A.

Definição 2.1.13. *Sejam* A *um anel comutativo com unidade e* P *um ideal de* A. *Dizemos que* P *é um ideal primo de* A *se* $P \neq A$ *e, para todo* $x, y \in A$, *se* $xy \in P$, *então* $x \in P$ *ou* $y \in P$.

Teorema 2.1.14. *Seja* K *um anel comutativo com unidade. Então as seguintes condições são equivalentes:*

(i) K *é um corpo.*

(ii) $\{0\}$ *é um ideal maximal em* K*.*

(iii) Os únicos ideais de K *são* $\{0\}$ *e* K*.*

Demonstração. Ver em [5], Capítulo III, Teorema 1. □

Sejam A um anel e J um ideal de A. Para cada $x \in A$ considere o conjunto

$$\overline{x} = x + J = \{x + z; z \in J\}.$$

Denote por A/J o conjunto formado por todos os elementos $\bar{x}$, onde $x \in A$. Considere as seguintes operações em A/J:

$$+ : \begin{cases} A/J \times A/J & \longrightarrow & A/J \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a+b} \end{cases} \quad e \quad \cdot : \begin{cases} A/J \times A/J & \longrightarrow & A/J \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a \cdot b} \end{cases}$$

Uma conta simples mostra que $(A/J, +, \cdot)$ é um anel.

Definição 2.1.15. *O anel* $(A/J, +, \cdot)$ *é dito anel quociente de* A *por* J*.*

Dados um anel comutativo A e um ideal J de A, uma conta simples mostra que A/J é um anel comutativo.

Proposição 2.1.16. *Seja* A *um anel comutativo com unidade. Então, um ideal* P *de* A *é um ideal primo se, e somente se,* A/P *é um domínio de integridade.*

Demonstração. Primeiramente observemos que como A é um anel comutativo com unidade, então A/P é um anel comutativo com unidade para todo ideal P de A. Desta forma, basta mostrarmos que se P é um ideal primo, então A/P não tem divisores de zero. Assim, suponha que P é um ideal primo de A e que $\overline{a} \cdot \overline{b} = (a + P)(b + P) = 0 + P = P$. Então, por definição $ab \in P$ e como P é um ideal primo $a \in P$ ou $b \in P$. Portanto, $a + P = P$ ou $b + P = P$, ou seja, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Reciprocamente, suponha que A/P é um domínio de integridade e que $ab \in P$. Então, $(a + P)(b + P) = (ab + P) = 0 + P = P$. Assim, $a + P = P$ ou $b + P = P$, uma vez que A/P é um domínio de integridade. Portanto, segue que $a \in P$ ou $b \in P$, implicando que P é um ideal primo. □

Proposição 2.1.17. *Sejam A um anel comutativo com unidade e J um ideal de A. Então J é um ideal maximal de A se, e somente se, A/J é um corpo.*

Demonstração. Ver em [5], Capítulo III, Teorema 3. □

Definição 2.1.18. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ anéis. Uma função $f : A \longrightarrow B$ é dita um homomorfismo de A em B se satisfaz as seguintes condições:*

(i) $f(x + y) = f(x) \oplus f(y), \qquad \forall x, y \in A.$

(ii) $f(x \cdot y) = f(x) \otimes f(y), \qquad \forall x, y \in A.$

Se $f : A \longrightarrow B$ é um homomorfismo bijetivo dizemos que f é um isomorfismo de A sobre B.

Definição 2.1.19. *Seja A um anel. Um homomorfismo $f : A \longrightarrow A$ é chamado de endomorfismo. Um isomorfismo $f : A \longrightarrow A$ é chamado de automorfismo.*

Proposição 2.1.20. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ anéis e $f : A \to B$ um homomorfismo. Então:*

(i) $f(0_A) = 0_B$.

(ii) $f(-a) = -f(a)$, $\forall a \in A$.

(iii) Se A e B são domínios de integridade então ou f é a função constante igual a zero ou $f(1_A) = 1_B$.

(iv) Se A e B são corpos então ou f é a função nula ou f é injetiva.

Demonstração. Ver em [5], Capítulo III, Proposição 5. □

Exemplo 2.1.21. Se J é um ideal de um anel A e $\overline{A} = A/J$, a projeção canônica $\pi : A \longrightarrow \overline{A}$ definida por $\pi(x) = \overline{x}$, $\forall x \in A$, é tal que:

(i) $\pi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \pi(x) + \pi(y)$, $\forall x, y \in A$.

(ii) $\pi(xy) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \pi(x)\,\pi(y)$, $\forall x, y \in A$.

Portanto, π é um homomorfismo de A sobre $\overline{A}$.

Teorema 2.1.22. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ anéis e $f : A \to B$ um homomorfismo. Então:*

(a) $Im(f) = \{f(a); a \in A\}$ é um subanel de B.

(b) $N(f) = \{a \in A; f(a) = 0_B\}$ é um ideal de A.

(c) f é injetiva se e somente se $N(f) = \{0\}$.

(d) Os anéis $A/N(f)$ e $Im(f)$ são isomorfos.

Demonstração. Ver em [5], Capítulo III, Teorema 4. □

2.2 POLINÔMIOS EM UMA VARIÁVEL

Definição 2.2.1. *Seja K um corpo. Chamamos de polinômio sobre K em uma indeterminada x a uma expressão formal*

$$p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$$

onde $a_i \in K, \forall i \in \mathbb{N}$, e existe $n \in \mathbb{N}$ tal que $a_j = 0 \, \forall j \geq n$.

Dizemos que dois polinômios $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots$ sobre K são iguais se $a_i = b_i, \forall i \in \mathbb{N}$.

Se $p(x) = 0 + 0x + \cdots + 0x^k + \cdots$, indicaremos $p(x)$ por 0 e o chamaremos de polinômio identicamente nulo.

Se $a \in K$ indicaremos por a o polinômio $p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ onde $a_0 = a$ e $a_i = 0, \forall i \geq 1$. Chamamos o polinômio $p(x) = a$ de polinômio constante a.

Se $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ é tal que $a_n \neq 0$ e $a_i = 0$, $\forall i > n$, dizemos que n é o grau do polinômio $p(x)$ e o indicaremos por $gr(p(x))$. Além disso, escrevemos $p(x) = a_0 + a_1x + \cdots + a_nx^n$.

Vamos denotar por $K[x]$ o conjunto de todos os polinômios sobre K em uma indeterminada x. Dados polinômios $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots$ definimos:

(i) $p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots$, onde $c_i = (a_i + b_i)$.

(ii) $p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots$, onde $c_i = \sum_{k=0}^{i} a_k b_{i-k}, \forall i \in \mathbb{N}$.

É de fácil verificação que $(K[x], +, \cdot)$ é um domínio de integridade.

Segue diretamente da definição duas propriedades muito importantes à respeito do grau de polinômios:

P1) $gr(p(x) + q(x)) \leq \max\{gr(p(x)), gr(q(x))\}$.

P2) $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

De modo análogo as definições e construções que fizemos para $K[x]$ se estendem a $K[x_1, x_2]$, $K[x_1, x_2, x_3]$, ..., $K[x_1, x_2, \ldots, x_n]$. Esses anéis são chamados de Anéis de Polinômios em 2, 3, $\cdots$, n indeterminadas, respectivamente, sobre o corpo K.

Proposição 2.2.2. *Seja K um corpo. O conjunto*

$$K(x) \coloneqq \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

com as operações seguintes é um corpo.

$$+ : \begin{cases} K(x) \times K(x) & \longrightarrow & K(x) \\ \left(\dfrac{f(x)}{f_1(x)}, \dfrac{g(x)}{g_1(x)}\right) & \longmapsto & \dfrac{g_1(x)f(x) + f_1(x)g(x)}{f_1(x)g_1(x)} \end{cases}$$

$$\cdot : \begin{cases} K(x) \times K(x) & \longrightarrow & K(x) \\ \left(\dfrac{f(x)}{f_1(x)}, \dfrac{g(x)}{g_1(x)}\right) & \longmapsto & \dfrac{f(x)g(x)}{f_1(x)g_1(x)}. \end{cases}$$

Demonstração. Ver em [5], Capítulo III, Seção 5. □

Teorema 2.2.3. *Sejam K um corpo e $K[x]$ o anel de polinômios sobre K na indeterminada x. Sejam $f(x)$, $g(x) \in K[x]$ e $g(x) \neq 0$. Então existe um único par de polinômios $q(x)$ e $r(x) \in K[x]$ tais que*

$$f(x) = q(x) \cdot g(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } gr(r(x)) < gr(g(x)).$$

Demonstração. Ver em [5], Capítulo IV, Teorema 1. □

Definição 2.2.4. *Dado $p(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $K[x]$, dizemos que $\alpha \in K$ é raiz de $p(x)$ se $p(\alpha) = 0$.*

Proposição 2.2.5. *Seja K um corpo e seja $p(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio de grau n em $K[x]$. Então, o número de raízes de $p(x)$ em K é no máximo igual a n.*

Demonstração. Ver em [5], Capítulo IV, Proposição 1. □

Definição 2.2.6. *Sejam L e K corpos. Se $L \supset K$ dizemos que L é uma extensão de K.*

Corolário 2.2.7. *Seja $p(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo de grau n em $K[x]$. Então, $p(x)$ possui no máximo n raízes em qualquer extensão L de K.*

Demonstração. Observemos que se $p(x) \in K[x]$ e $K \subset L$, então $p(x) \in L[x]$ e usando Proposição 2.2.5 para o corpo L obtemos o resultado. □

Corolário 2.2.8. *Sejam $f(x)$, $g(x) \in K[x]$ e K um corpo com um número infinito de elementos. Então,*

$$f(x) = g(x) \Leftrightarrow f(b) = g(b), \forall\, b \in K.$$

Demonstração. Primeiramente, supondo $f(x) = g(x)$, segue imediatamente pela definição de igualdade de polinômios que $f(b) = g(b)$, $\forall b \in K$.

Reciprocamente, seja $h(x) = f(x) - g(x) \in K[x]$. Assim, por hipótese temos que $h(b) = 0$, $\forall\, b \in K$, e pela Proposição 2.2.5 segue que $h(x) \equiv 0$. Portanto, $f(x) = g(x)$.

□

Definição 2.2.9. *Seja K um corpo. Dizemos que K é um corpo algebricamente fechado se $\forall f(x) \in K[x]$ existe $\alpha \in K$ tal que $f(\alpha) = 0$.*

É de fácil verificação, que se K é um corpo algebricamente fechado, então todo polinômio $f(x) \in K[x]$ de grau $n \geq 1$ pode ser fatorado em K do seguinte modo: $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, onde $c \in K$ e $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ são raízes de $f(x) \in K[x]$.

Definição 2.2.10. *Seja $f(x) \in K[x]$ tal que $gr(f(x)) \geq 1$. Dizemos que $f(x)$ é um polinômio irredutível sobre K se toda vez que $f(x) = g(x)h(x)$, $g(x)$, $h(x) \in K[x]$ tivermos que $g(x)$ ou $h(x)$ é um polinômio constante.*

Se $f(x)$ for não irredutível sobre K dizemos que f é redutível sobre K

Teorema 2.2.11. *Sejam K um corpo e $p(x) \in K[x]$. Então as seguintes condições são equivalentes:*

(a) $p(x)$ é irredutível sobre K.

(b) $J = K[x] \cdot p(x)$ é um ideal maximal em $K[x]$.

(c) $K[x]/J$ é um corpo (onde $J = K[x] \cdot p(x)$).

Demonstração. Ver em [5], Capítulo IV, Teorema 4. □

Teorema 2.2.12 (Fatoração única)**.** *Seja K um corpo. Então todo polinômio não nulo $f(x) \in K[x]$ pode ser escrito na forma*

$$f(x) = u \cdot p_1(x) \cdot p_2(x) \cdots p_m(x),$$

onde $u \in K \setminus \{0\}$ e $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre K (não necessariamente distintos). Essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), \ldots, p_m(x)$.

Demonstração. Ver em [5], Capítulo IV, Teorema 5. □

Verificar a irredutibilidade de um polinômio não é uma tarefa fácil, portanto apresentaremos um teste de irredutibilidade conhecido como Critério de Eisenstein.

Definição 2.2.13. *Sejam um domínio de integridade D e um elemento $p \in D$, com $p \neq 0$ e não invertível em D. Dizemos que p é um elemento primo se dados a, $b \in D$ com $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Lema 2.2.14. *(Lema de Gauss) Se D um domínio de fatoração única com corpo de frações K e $f(x) \in D[x]$ um polinômio irredutível, então $f(x)$ é irredutível sobre K.*

Demonstração. Ver em [7], Capítulo 6, Lema 6.13. □

Teorema 2.2.15 (Critério de Eisenstein)**.** *Sejam D um domínio de fatoração única com corpo de frações K e $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio em $D[x]$. Suponha que exista um elemento primo $p \in D$ tal que:*

(i) $p \nmid a_n$,

(ii) $p \mid a_0, \ldots, a_{n-1}$,

(iii) $p^2 \nmid a_0$,

Então $f(x)$ é irredutível sobre K.

Demonstração. Ver em [7], Capítulo 6, Teorema 6.15. □

2.3 EXTENSÕES ALGÉBRICAS

Definição 2.3.1. *Sejam K um corpo e $L \supset K$ uma extensão de K. Dizemos que $\alpha \in L$ é algébrico sobre K se existe $f(x) \in K[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. Caso contrário, dizemos que α é transcendente sobre K.*

Se todo elemento $\alpha \in L$ é algébrico sobre K, dizemos que $L \supset K$ é uma extensão algébrica de K.

Definição 2.3.2. *Sejam K um corpo, $L \supset K$ uma extensão de K, $\alpha \in L$ algébrico sobre K. O polinômio $p(x) \in K[x]$, mônico e de menor grau, tal que $p(\alpha) = 0$ é dito polinômio minimal de α. Ele será denotado por $irr(\alpha, K)$.*

Se $\alpha \in L \supset K$, definimos

$$K[\alpha] \coloneqq \{f(\alpha); f(x) \in K[x]\}.$$

Temos que $K[\alpha]$ é um subdomínio de L que contém K. Se α é um elemento algébrico sobre K, então $K[\alpha]$ é um subcorpo de L.

Teorema 2.3.3. *Sejam $\alpha \in L \supset K$ e $\Psi : K[x] \to L$ definida por $\Psi(f(x)) = f(\alpha)$. Então Ψ é um homomorfismo de anéis tal que:*

(i) $Im(\Psi) = K[\alpha]$ *e* $K \subset K[\alpha] \subset L$.

(ii) α *é transcendente sobre* K *se, e somente se,* $N(\Psi) = \{0\}$.

(iii) se α *é algébrico sobre* K *e* $p(x) = irr(\alpha, K)$, *então* $N(\Psi) = K[x] \cdot p(x)$ *é um ideal maximal de* $K[x]$.

(iv) $K[x]/N(\Psi) \simeq K[\alpha]$.

Demonstração. Ver em [5], Capítulo V, Teorema 1. □

Corolário 2.3.4. *Se α, $\beta \in K \supset K$ são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha] \simeq K[\beta]$.*

Demonstração. Por hipótese, temos que $irr(\alpha, K) = irr(\beta, K)$. Agora, pelos itens (iii) e (iv) do Teorema 2.3.3, temos que $J = K[x] \cdot (irr(\alpha, K))$ e

$$K[\alpha] \simeq K[x]/J \simeq K[\beta].$$

□

Definição 2.3.5. *(Espaço Vetorial) Seja K um corpo qualquer e seja V um conjunto não vazio onde está definida uma operação soma. Suponhamos também que esteja definida uma operação ente elementos de K e elementos de V que chamaremos produto por escalar. Ou seja, temos:*

$$+ : \begin{cases} V \times V & \longrightarrow & V \\ (u, v) & \longmapsto & u + v \end{cases} \qquad e \qquad \cdot : \begin{cases} K \times V & \longrightarrow & V \\ (\lambda, v) & \longmapsto & \lambda \cdot v = \lambda v \end{cases} .$$

Dizemos que V munido destas operações é um espaço vetorial sobre o corpo K se as seguintes propriedades são verificadas para quaisquer $u, v, w \in V$ e $\alpha, \beta \in K$:

(1) $u + (v + w) = (u + v) + w$.

(2) Existe $0 \in V$ *tal que* $0 + u = u + 0 = u$.

(3) Para cada $u \in V$, existe um único $v \in V$ tal que $u + v = v + u = 0$.

(4) $u + v = v + u$.

(5) $1 \cdot v = v$, *onde* 1 *é a unidade do corpo* K.

(6) $\alpha(u + v) = \alpha u + \alpha v$.

(7) $(\alpha + \beta)u = \alpha u + \beta u$.

(8) $\alpha(\beta v) = \beta(\alpha v) = (\alpha\beta)v$.

Exemplo 2.3.6. Seja $L \supset K$ uma extensão do corpo K. L pode ser visto como um espaço vetorial sobre o corpo K. De fato, as operações

$$+ : \begin{cases} L \times L & \longrightarrow & L \\ (u, v) & \longmapsto & u + v \end{cases} \qquad e \qquad \cdot : \begin{cases} K \times L & \longrightarrow & L \\ (\lambda, v) & \longmapsto & \lambda \cdot v = \lambda v \end{cases}$$

já existem de modo natural no corpo L. As propriedades que definem o espaço vetorial decorrem de forma direta uma vez que L é corpo e K também.

Definição 2.3.7. *Seja V um espaço vetorial sobre um corpo K. Um subconjunto W não vazio de V diz-se um subespaço vetorial de V se as seguintes condições são satisfeitas, quaisquer que sejam $w_1, w_2, w \in W$ e $\alpha \in K$:*

- $w_1,\ w_2 \in W \Rightarrow w_1 + w_2 \in W$.
- $\alpha \in K,\ w \in W \Rightarrow \alpha w \in W$.

Exemplo 2.3.8. Se V é um espaço vetorial sobre um corpo K e $u_1, u_2, \ldots, u_n \in V$, então é de fácil verificação que

$$W = \{\sum_{i=1}^{n} \alpha_i\, v_i\,;\ \alpha_i \in K, i = 1, 2, \ldots, n\},$$

é um subespaço vetorial de V. O subespaço W é chamado de subespaço gerado por $u_1, u_2, \ldots, u_n$ e será denotado $W = \langle u_1, \ldots, u_n \rangle$.

Definição 2.3.9. *Seja V um espaço vetorial sobre um corpo K. Se $v_1, \ldots, v_n \in V$, dizemos que $v_1, \ldots, v_n$ são linearmente independentes, se a equação vetorial*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0,$$

com $\alpha_i \in K$, é satisfeita apenas para os escalares $\alpha_i = 0$, $\forall i \in \{1, \cdots, n\}$. Caso contrário, dizemos que $v_1, \ldots, v_n$ são linearmente dependentes.

Definição 2.3.10. *Dizemos que um espeço vetorial V é finitamente gerado se existe $S = \{v_1, v_2, \ldots, v_n\} \subset V$, tal que $\langle v_1, v_2, \ldots, v_n \rangle = V$.*

Definição 2.3.11. *Seja V um espaço vetorial finitamente gerado. Uma base de V é um subconjunto $\{v_1, v_2, \ldots, v_n\} \subset V$ tal que:*

(i) $\langle v_1, v_2, \ldots, v_n \rangle = V$,

(ii) $v_1, v_2, \ldots, v_n$ *são linearmente independentes sobre* V.

Proposição 2.3.12. *Todo espaço vetorial finitamente gerado admite uma base.*

Demonstração. Ver em [1], Capítulo 3, Proposição 1. □

Teorema 2.3.13 (Teorema da Invariância)**.** *Seja V um espaço vetorial finitamente gerado. Então duas bases de V têm o mesmo número de vetores.*

Demonstração. Ver em [1] (Apêndice III). □

Teorema 2.3.14. *Seja W um espaço vetorial sobre um corpo K de dimensão finita. Se U e V são subespaços vetoriais de W, então:*

$$\dim(U \cup V) + \dim(U + V) = \dim U + \dim V.$$

Demonstração. Ver em [1], Capítulo 3, Proposição 5. □

Definição 2.3.15. *Seja V um espaço vetorial sobre K. Se V possui uma base de n elementos, dizemos que V tem dimensão n sobre K e escrevemos $[V : K] = n$.*

Definição 2.3.16. *Seja K um corpo qualquer. Uma extensão $L \supset K$ diz-se finita se $[L : K] = n < \infty$. Caso contrário, $L \supset K$ diz-se uma extensão infinita.*

Proposição 2.3.17. *Seja K um corpo e $L \supset K$ uma extensão de K. Então,*

(a) se $L \supset K$ é finita, então $L \supset K$ é algébrica.

(b) *se $\alpha \in L \supset K$ é um elemento algébrico sobre K e o grau $irr(\alpha, K)$ é igual a n, então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre K. Ou seja, $[K[\alpha] : K] = n < \infty$.*

(c) *se $\alpha \in L \supset K$ é um elemento transcendente sobre K, então $K[\alpha] \supset K$ é um domínio que não é corpo.*

Demonstração. Ver em [5], Capítulo V, Proposição 3. □

Corolário 2.3.18. *Seja $\alpha \in L \supset K$. Então as seguintes afirmações são equivalentes:*

(i) *α é algébrico sobre K.*

(ii) *$[K[\alpha] : K] < \infty$.*

(iii) *$K[\alpha]$ é uma extensão algébrica de K.*

Demonstração. $(i) \Rightarrow (ii)$ Se α é algébrico sobre K então pelo item (b) da Proposição 2.3.17 temos que $[K[\alpha] : K] < \infty$.
$(ii) \Rightarrow (iii)$ Se $[K[\alpha] : K] < \infty$ então item (a) da Proposição 2.3.17 temos que $K[\alpha]$ é uma extensão algébrica sobre K.
$(iii) \Rightarrow (i)$ Se $K[\alpha]$ é uma extensão algébrica sobre K então por definição temos que α é algébrico sobre K. □

2.4 EXTENSÕES TRANSCENDENTES

Definição 2.4.1. *Sejam F uma extensão do corpo K e S um subconjunto de F. Dizemos que S é algebricamente dependente sobre K se existe $f \in K[x_1, \ldots, x_n]$, com $f \neq 0$, tal que $f(s_1, \ldots, s_n) = 0$ com $s_1, \ldots, s_n \in S$. Caso contrário S é dito algebricamente independente sobre K.*

Definição 2.4.2. *Seja F uma extensão do corpo K. Uma base de transcendência de F sobre K é subconjunto $\beta \subset F$ tal que:*

(i) *β é um conjunto algebricamente independente de F sobre K,*

(ii) se $\beta \subseteq \beta'$ e β' é um conjunto algebricamente independente de F sobre K, então $\beta = \beta'$.

Teorema 2.4.3. *Seja F uma extensão do corpo K. Se S é uma base de transcendência de F sobre K, então toda base de transcendência de F sobre K tem a mesma cardinalidade.*

Demonstração. Ver em [7], Capítulo VI, Teoremas 1.8 e 1.9. □

Definição 2.4.4. *Seja F uma extensão do corpo K. O grau de transcendência de F sobre K é a cardinalidade de uma base de transcendência β de F sobre K. Denotamos o grau de transcendência de F sobre K por* $\mathrm{trdeg}(F|K)$.

Teorema 2.4.5. *Se F é uma extensão do corpo E e E é uma extensão do corpo K, então:*

$$\mathrm{trdeg}(F|K) = (\mathrm{trdeg}(F|E)) + (\mathrm{trdeg}(E|K)).$$

Demonstração. Ver em [7], Capítulo VI, Teorema 1.11. □

Proposição 2.4.6. *F é uma extensão algébrica do corpo K se, e somente se,* $\mathrm{trdeg}(F|K) = 0$.

Demonstração. Por definição temos que $\mathrm{trdeg}(F|K) \neq 0$ se, e somente se, existe pelo menos um elemento $x \in F$ que é transcendente sobre K. □

3 FUNDAMENTOS DA TEORIA DE CORPOS DE FUNÇÕES ALGÉBRICAS

Neste capítulo serão apresentadas as definições de lugar, corpo de funções algébricas e valorizações que são os principais objetos de investigação do trabalho. Por meio destas definições e resultados conseguiremos tecer as primeiras ferramentas necessárias para a demonstração do Teorema de Riemann-Roch.

No decorrer deste capítulo, vamos denotar por K um corpo arbitrário.

3.1 LUGARES

Definição 3.1.1. *Um corpo de funções algébricas F/K, em uma variável, sobre o corpo K é uma extensão de corpos $F \supseteq K$, tal que F é uma extensão algébrica finita de $K(x)$, para algum elemento $x \in F$ transcendente sobre K.*

Para simplificar vamos nos referir à F/K como corpo de funções.

O conjunto $\overline{K} := \{z \in F; z \text{ é algébrico sobre } K\}$ é um subcorpo de F, pois a soma, o produto e o inverso de elementos algébricos ainda são algébricos.

Definição 3.1.2. *O corpo $\overline{K}$ é dito corpo de constantes de F/K.*

Observemos que $K \subseteq \overline{K} \subsetneq F$ e que $F/\overline{K}$ é um corpo de funções sobre $\overline{K}$.

Dizemos que K é algebricamente fechado em F se $\overline{K} = K$.

Proposição 3.1.3. *Seja F/K uma extensão de corpos. Um elemento $z \in F$ é transcendente sobre K se, e somente se, a extensão $F/K(z)$ tem grau finito.*

Demonstração. ($\Leftarrow$) Seja $z \in F$ um elemento algébrico sobre K. Então $K(z)/K$ é uma extensão finita. Como F/K é um corpo de funções, temos que a extensão F/K é infinita. Da relação

$$[F : K] = [F : K(z)][K(z) : K],$$

segue que $F/K(z)$ é uma extensão infinita.

($\Rightarrow$) Segue da definição que F é uma extensão infinita de $K(x)$, para algum $x \in F$ transcendente sobre K. Agora, seja $z \in F$ transcendente sobre K. Então

o grau de transcendência de $K(z)$ sobre K é 1. Temos ainda, que o grau de transcendência de $K(x)/K$ é 1. Como $[F : K(x)] < \infty$ e vale a igualdade

$$[F : K(x)] = [F : K(x, z)][K(x, z) : K(x)],$$

concluímos que $[K(x, z) : K(x)] < \infty$. Assim, $K(x, z)/K(x)$ é uma extensão algébrica, de forma que o grau de transcendência de $K(x, z)/K(x)$ é 0. Como

$$\text{trdeg}(K(x, z)|K) = \text{trdeg}(K(x, z)|K(x)) + \text{trdeg}(K(x)|K),$$

segue que $\text{trdeg}(K(x, z)|K) = 1$. Agora,

$$\text{trdeg}(K(x, z)|K) = \text{trdeg}(K(x, z)|K(z)) + \text{trdeg}(K(z)|K)$$

implica que $\text{trdeg}(K(x, z)|K(z)) = 0$. Portanto, x é um elemento algébrico sobre $K(z)$ e $[F : K(z)] < \infty$. □

Exemplo 3.1.4. O exemplo mais simples de um corpo de funções é o corpo das funções racionais: uma extensão F/K é dita racional se $F = K(x)$, para algum $x \in F$ que é transcendente sobre K. Desta forma, sabemos que $0 \neq z \in K(x)$ tem uma única representação:

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

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

Definição 3.1.5. *Um anel de valorização de um corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:*

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

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

Exemplo 3.1.6. Seja $p(x)$ um polinômio mônico e irredutível em $K[x]$. O conjunto

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

é um anel de valorização de $K(x)/K$.

Primeiramente, é fácil vermos que $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$. Agora, tome $h(x) = a(x)/b(x) \in K(x)$ onde $a(x), b(x)$ não tem fatores em comum. Sabemos que $p(x) \mid b(x)$, ou $p(x) \nmid b(x)$. Assim, se $p(x) \nmid b(x)$ então $h(x) \in \mathcal{O}_{p(x)}$. Agora, se $p(x) \mid b(x)$ então por hipótese $p(x) \nmid a(x)$, então $1/h(x) = b(x)/a(x) \in \mathcal{O}_{p(x)}$.

Proposição 3.1.7. *Seja $\mathcal{O}$ um anel de valorização sobre o corpo de funções F/K. Então:*

(i) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ tem $P = \mathcal{O} \setminus \mathcal{O}^\times$ como o único ideal maximal, onde

$$\mathcal{O}^\times = \{z \in \mathcal{O};\ \text{existe } w \in \mathcal{O} \text{ com } zw = 1\}$$

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

(ii) Seja $0 \neq x \in F$. Então $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.

(iii) Para o corpo $\overline{K}$ de constantes sobre F/K temos que $\overline{K} \subseteq \mathcal{O}$ e $\overline{K} \cap P = \{0\}$.

Demonstração. (i) Primeiro vamos provar que P é um ideal de $\mathcal{O}$.

Se $a \in \mathcal{O}$ e $b \in P$, então $ab \notin \mathcal{O}^\times$, pois caso contrário teríamos que $b \in \mathcal{O}^\times$, o que é uma contradição. Portanto, $ab \in P$.

Agora, tomemos x, $y \in P \setminus \{0\}$. Pela definição de $\mathcal{O}$, temos que $xy^{-1} \in \mathcal{O}$ ou $yx^{-1} = (xy^{-1})^{-1} \in \mathcal{O}$. Sem perda de generalidade, suponhamos que $xy^{-1} \in \mathcal{O}$. Então, $xy^{-1} + 1 \in \mathcal{O}$ e $x + y = (xy^{-1} + 1)y \in P$. Como $\mathcal{O}$ é um anel comutativo com unidade, segue que P é ideal de $\mathcal{O}$.

Resta provarmos que P é um ideal maximal de $\mathcal{O}$. Se $P \subsetneq J \subseteq \mathcal{O}$, então existe $x \in J$ e $x \notin P$. Pela definição de P, temos que $x \in \mathcal{O}^\times$, ou seja, $xx^{-1} = 1 \in J$. Donde segue que $J = \mathcal{O}$. Portanto, P é um ideal maximal.

Por fim, a unicidade de P: suponhamos que J é um outro ideal maximal de $\mathcal{O}$. Se J possui elementos invertíveis, temos que $J = \mathcal{O}$. Caso contrário, temos que $J \subseteq P$. Como J é maximal segue que $J = P$.

(ii) Decorre diretamente da definição de P e do fato de $\mathcal{O}$ ser um anel de valorização.

(*iii*) Primeiro vamos mostrar que $\overline{K} \subseteq \mathcal{O}$: suponhamos que exista $t \in \overline{K}$ e $t \notin \mathcal{O}$. Então, pela definição de $\mathcal{O}$, temos que $t^{-1} \in \mathcal{O}$. Além disso, como $\overline{K}$ é um corpo e t é algébrico sobre K, então t^{-1} também é algébrico sobre K. Assim, existem $a_i \in K$, $i \in \{1, 2, \cdots, m\}$, tais que

$$a_m(t^{-1})^m + \cdots + a_1(t^{-1}) + 1 = 0.$$

Daí,

$$t^{-1}[a_m(t^{-1})^{m-1} + \cdots + a_1] = -1$$

$$t = -[a_m(t^{-1})^{m-1} + \cdots + a_1] \in K[t^{-1}] \subseteq \mathcal{O}$$

O que é uma contradição, pois $t \notin \mathcal{O}$. Logo $\overline{K} \subseteq \mathcal{O}$.

Agora, mostremos que $\overline{K} \cap P = \{0\}$: suponhamos que exista $x \in \overline{K} \cap P$ e $x \neq 0$. Portanto, $x \in \mathcal{O} \setminus \mathcal{O}^\times$ e existem $a_i \in K, i \in \{1, 2, \cdots, m\}$ tais que

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + 1 = 0.$$

Da igualdade anterior obtemos que

$$x^{-1} = -(a_m x^{m-1} + \cdots + a_1) \in K[x] \subseteq \mathcal{O}.$$

O que é uma contradição.

□

Lema 3.1.8. *Sejam $\mathcal{O}$ um anel de valorização de um corpo de funções algébricas F/K, P seu ideal maximal e $0 \neq x \in P$. Sejam $x_1, x_2, \ldots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, para $i = 1, 2, \ldots, n-1$. Então*

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

Demonstração. Como $x \in P$ e $x \neq 0$, temos pela Proposição 3.1.7, item (*iii*), que $x \notin \overline{K}$. Temos assim que x é transcendente sobre K e pela Observação 3.1.3, $[F : K(x)] < \infty$. Então basta mostrarmos que $x_1, x_2, \ldots, x_n$ são linearmente independentes sobre $K(x)$. Suponhamos que $\{x_1, x_2, \ldots, x_n\}$ é um conjunto linearmente depende sobre $K(x)$, ou seja, existem elementos $\phi_i(x) \in K(x)$, com $1 \leq i \leq n$, não todos nulos, tais que $\sum_{i=1}^{n} \phi_i(x)x_i = 0$. Sem perda de generalidade, podemos supor

que $\phi_i(x) \in K[x]$ e $x \nmid \phi_i(x)$ para algum i. Denotemos por $a_i = \phi_i(0)$ o termo independente de $\phi_i(x)$ e fixemos $j \in \{1, 2, \cdots, n\}$ tal que $a_j \neq 0$, mas $a_i = 0$ para cada $i > j$. Assim, obtemos:

$$\sum_{i \neq j} \phi_i(x)x_i + \phi_j(x)x_j = 0 \Rightarrow -\phi_j(x)x_j = \sum_{i \neq j} \phi_i(x)x_i. \tag{3.1}$$

Temos ainda que $\phi_i(x) \in \mathcal{O}$, para cada $i \in \{1, 2, \cdots, n\}$, pois $x = x_1 \in P$, $x_i \in x_j P$, para $i < j$ e $\phi_i(x) = xg_i(x)$, para $i > j$, onde $g_i(x) \in K[x] \subseteq \mathcal{O}$.

Dividindo-se a igualdade (3.1) por x_j obtemos

$$\phi_j(x) = \sum_{i<j} \phi_i(x)\frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x)x_i.$$

Da última relação, concluímos que $a_j \in P$. Portanto, $a_j = \phi_j(x) - xg_j(x) \in P$ e $a_j \in K$, implicam que:

$$a_j \in P \cap K \subseteq P \cap \overline{K} = \{0\}.$$

Contradizendo o fato de $a_j \neq 0$. Logo, $\{x_1, \ldots, x_n\}$ é linearmente independente. □

Teorema 3.1.9. *Sejam $\mathcal{O}$ o anel de valorização do corpo de funções algébricas F/K e P seu único ideal maximal. Então:*

(i) P é um ideal principal.

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

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

Demonstração. (i) Suponhamos que P não seja um ideal principal, ou seja, ele não é gerado por nenhum elemento de $\mathcal{O}$. Tomemos um elemento $0 \neq x_1 \in P$. Como $P \neq x_1\mathcal{O}$, existe $x_2 \in P \setminus x_1\mathcal{O}$. Note que $x_2x_1^{-1} \notin \mathcal{O}$, então, pela Proposição 3.1.7, item (ii), $x_2^{-1}x_1 \in P$. Logo, $x_1 \in x_2P$. Repetindo o argumento, obtemos uma sequência infinita $a_1, a_2, \ldots, a_n, \ldots$ de elementos de P tais que $a_{n-1} \in a_nP$, para $n \geq 2$, contradizendo o Lema 3.1.8.

(*ii*) Sabemos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Podemos supor, sem perda de generalidade, que $z \in \mathcal{O}$. Se $z \in \mathcal{O}^\times$, então $z = t^0 z$.

Se $z \notin \mathcal{O}^\times$, então $z \in P$. Como $P = t\mathcal{O}$, então $z = tz_1$, para algum $z_1 \in \mathcal{O}$. Assim, se $z_1 \in \mathcal{O}^\times$, então terminamos a demonstração. Caso contrário, temos que

$$z_1 \in P \Rightarrow z_1 = tz_2 \Rightarrow z = t^2 z_2, \text{ para algum } z_2 \in \mathcal{O}.$$

Agora, se $z_2 \in \mathcal{O}^\times$, então terminamos a demonstração. Caso contrário, temos que

$$z_2 \in P \Rightarrow z_2 = tz_3 \Rightarrow z = t^3 z_3 \text{ para algum } z_3 \in \mathcal{O}.$$

Repetindo este processo construímos a sequência

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

que satisfaz a condição $x_i \in x_{i+1}P$, para todo $i \in \{1, \ldots, m\}$. Pelo Lema 3.1.8 esta sequência tem comprimento limitado. Logo, existe um número máximo, digamos m, de elementos nesta sequência. Donde concluímos que existe um número máximo $m \in \mathbb{N}$ tal que $z = t^m z_m$, com $z_m \in \mathcal{O}^\times$

(Unicidade) Suponhamos que $z = ut^m = vt^n$, onde $u, v \in \mathcal{O}^\times$ e $n \geq m$. Logo, $uv^{-1} = t^{n-m}$. Portanto, como t é não invertível, $n = m$ e $uv^{-1} = 1$.

(*iii*) Seja I um ideal tal que $\{0\} \subsetneq I \subsetneq \mathcal{O}$. Note que se $x \in I \setminus \{0\}$, então $x = t^r u$, onde $u \in \mathcal{O}^\times$, $r \in \mathbb{Z}$ e $r \geq 0$. Isso implica que $t^r = u^{-1}x \in I$. Portanto, o conjunto $A \coloneqq \{r \in \mathbb{N};\ t^r \in I\}$ é não vazio. Segue do Princípio da Boa Ordenação que o conjunto A possui um menor elemento, o qual denotaremos por $n = \min\{A\}$.

Provaremos que $I = t^n\mathcal{O}$. De fato, temos que $t^n\mathcal{O} \subseteq I$, pois $t^n \in I$. Seja $0 \neq y \in I$, então $y = t^s u$, com $u \in \mathcal{O}^\times$ e $s > 0$. Mas sendo $t^s = u^{-1}y$ e $n = \min\{A\}$, então $n \leq s$. Logo, $t^n \mid t^s$. Portanto, $t^n \mid y$, ou seja, $y \in t^n\mathcal{O}$. Logo, $I = t^n\mathcal{O}$

□

Definição 3.1.10. *Um lugar P de um corpo de funções F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Cada elemento $t \in P$ tal que $P = t\mathcal{O}$ é dito elemento primo de P.*

Denotaremos por $\mathbb{P}_F$ o conjunto formado por todos os lugares P de F/K

Observação 3.1.11. *Se $\mathcal{O}$ é um anel de valorização do corpo de funções F/K e P é seu ideal maximal, então $\mathcal{O}$ fica unicamente determinado por P, isto é,*

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

Por esta razão denotamos $\mathcal{O}_P \coloneqq \mathcal{O}$ o anel de valorização associado ao lugar P.

Definição 3.1.12. *Uma valorização discreta de um corpo de funções F/K é uma função*

$$v : F \to \mathbb{Z} \cup \{\infty\}$$

com as seguintes propriedades:

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

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

(c) $v(x + y) \geq \min\{v(x), v(y)\}$*, para todo* $x, y \in F$ *(Desigualdade Triangular);*

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

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

No contexto da definição acima vale ressaltar algumas propriedades do elemento $\infty \notin \mathbb{Z}$:

- $\infty + \infty = \infty$;
- $\infty + n = \infty$; $\forall n \in \mathbb{Z}$;
- $n + \infty = \infty$; $\forall n \in \mathbb{Z}$;
- $\infty > n$; $\forall n \in \mathbb{Z}$.

Segue da Definição 3.1.12 (itens 2 e 4) que a toda valorização $v : F \to \mathbb{Z} \cup \{\infty\}$ é uma função sobrejetiva.

Lema 3.1.13. *(Desigualdade Triangular Estrita) Sejam v uma valorização discreta do corpo de funções F/K e x, $y \in F$, com $v(x) \neq v(y)$. Então,*

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

Demonstração. Se $a \in K$ e $a \neq 0$, temos que

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

Portanto,

$$v(-y) = v(-1) + v(y) = 0 + v(y) = v(y).$$

Agora, sem perda de generalidade, podemos supor que $v(x) < v(y)$. Suponhamos por absurdo que

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

ou seja, $v(x+y) > v(x)$. Assim,

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

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

O que é uma contradição. □

Definição 3.1.14. *Para cada lugar $P \in \mathbb{P}_F$ associamos uma função*

$$v_P : F \to \mathbb{Z} \cup \{\infty\},$$

definida da seguinte maneira: escolha um elemento primo $t \in P$. Então para todo $0 \neq z \in F$ existe uma única representação $z = t^n u$, com $u \in \mathcal{O}_P^\times$ e $n \in \mathbb{Z}$. Sendo assim definimos:

$$v_P(z) \coloneqq n, \text{ se } z \neq 0 \quad e \quad v_P(0) \coloneqq \infty.$$

Observemos que a definição acima depende apenas do lugar P, isto é, não depende da escolha de t. De fato, seja t' um outro elemento primo de P. Como $P = t\mathcal{O} = t'\mathcal{O}$, então $t = t'w$ para algum $w \in \mathcal{O}_P^\times$. Assim,

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

onde $k = w^n u \in \mathcal{O}_P^\times$.

Teorema 3.1.15. *Seja F/K um corpo de funções.*

(1) Para um lugar $P \in \mathbb{P}_F$, a função v_P definida acima é uma valorização discreta de F/K. Além disso, temos que:

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

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

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

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

(3) Se v é uma valorização discreta de F/K, então $P := \{z \in F; v(z) > 0\}$ é um lugar sobre F/K e $\mathcal{O}_P = \{z \in F; v(z) \geq 0\}$ é o anel valorização correspondente.

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

Demonstração. (1) Vamos mostrar inicialmente que a função v_P é uma valorização discreta:

(a) Por definição $v_P(x) = \infty \Leftrightarrow x = 0$

Agora, sejam x, $y \in F \setminus \{0\}$. Se $v_P(x) = n$ e $v_P(y) = m$, então existem $u_1, u_2 \in \mathcal{O}_P^{\times}$ tais que $x = t^n u_1$ e $y = t^m u_2$.

(b) Então,

$$v_P(xy) = v_P(t^n u_1 t^m u_2) = v_P(t^{n+m} u_1 u_2) = n + m = v_P(x) + v_P(y).$$

(c) Suponha que $n \leq m$, então

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

Seja $z = u_1 + t^{m-n} u_2 \in \mathcal{O}_P$. Se $z = 0$, então

$$v_P(z) = \infty > \min\{n, m\}.$$

Se $z \neq 0$, então $z = t^k u$, onde $u \in \mathcal{O}_P^{\times}$ e $k \in \mathbb{Z}_+^*$. Assim,

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

(d) Por definição, $v_P(t) = 1$.

(e) Se $a \in K$, então a é invertível. Portanto, $a = t^0$, ou seja, $v_P(a) = 0$.

Assim, v_P é uma valorização discreta.

Mostremos que $\mathcal{O}_P = \{z \in F;\, v_P(z) \geq 0\}$: seja $z \in F$ tal que $v_P(z) \geq 0$. Se $v_P(z) = \infty$, então $z = 0 \in \mathcal{O}_P$. Se $v_P(z) = n \neq \infty$, então existem um elemento primo $t \in P$ e $u \in \mathcal{O}_P^\times$ tais que $z = t^n u$. Se $n = 0$, temos que $z = u \in \mathcal{O}_P^\times \subseteq \mathcal{O}$. Se $n > 0$, então $z \in t\mathcal{O} = P \subseteq \mathcal{O}$. Portanto,

$$\{z \in F;\, v_P(z) \geq 0\} \subset \mathcal{O}_P.$$

Reciprocamente, se $z \in \mathcal{O} \setminus \{0\}$, pelo Teorema 3.1.9, item (iii), temos que $z = t^n u$ para algum número inteiro positivo n e $u \in \mathcal{O}_P^\times$. Assim $v_P(z) = n \geq 0$. No caso em que $z = 0$, temos que $v_P(z) = \infty > 0$.

Mostremos que $\mathcal{O}_P^\times = \{z \in F; v_P(z) = 0\}$: seja $z \in F$ tal que $v_P(z) = 0$. Então, $z = t^0 u$, onde $u \in \mathcal{O}_P^\times$. Reciprocamente, se $z \in \mathcal{O}_P^\times$, então, $z = t^0 u$. Logo, $v_P(x) = 0$.

Por fim, $P = \{z \in F; v_P(z) > 0\}$: segue do fato que $P \coloneqq \mathcal{O}_P \setminus \mathcal{O}_P^\times$.

(2) Se z um elemento primo de P, então $z = z \cdot 1$ e $1 \in \mathcal{O}_P^\times$. Logo, $v_P(z) = 1$. Reciprocamente, tome $z \in F$ tal que $v_P(z) = 1$, fixando um elemento primo t de P, temos que $z = tu$, onde $u \in \mathcal{O}_P^\times$. Assim, $P = t\mathcal{O}_P = z\mathcal{O}_P$. Portanto, z é um elemento primo de P.

(3) Primeiro mostraremos que $\mathcal{O}_P$ é um subanel de F. Se x, $y \in \mathcal{O}_\mathcal{P}$ temos:

a) $0 \in \mathcal{O}_P$, pois $v(0) = \infty > 0$.

b) Como $v(x) \geq 0$ e $v(y) \geq 0$ temos

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

Portanto, $x - y \in \mathcal{O}_P$.

c) Como $v(xy) = v(x) + v(y) \geq 0$, segue que $xy \in \mathcal{O}_P$.

Assim, $\mathcal{O}_P$ é subanel de F. Observemos que $O_P \subsetneq F$ e mais, como $v(a) = 0$, $\forall a \in K \setminus \{0\}$, também temos que $K \subsetneq \mathcal{O}_P$. Agora, dado $z \in F \setminus \{0\}$, temos

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

Logo, $v(z) \leq 0$ ou $v(z^{-1}) \leq 0$, ou seja, $z \in \mathcal{O}_P$ ou $z^{-1} \in \mathcal{O}_P$. Desta forma, obtemos que $\mathcal{O}_P$ é um anel de valorização.

Falta mostrarmos que $P = \{z \in F; v(z) > 0\}$ é um lugar de F/K, com $\mathcal{O}_P = \{z \in F; v(z) \geq 0\}$ sendo o anel da valorização correspondente. Vamos mostrar que P é um ideal maximal de $\mathcal{O}_P$.

(*a*) $P \neq \emptyset$, pois $0 \in F$ e $v(0) = \infty > 0$;

(*b*) Dados x, $y \in P$, temos que $v(x) > 0$ e $v(y) > 0$. Assim, como

$$v(x + y) \geq \{v(x), v(y)\} > 0,$$

segue que $x + y \in P$.

(*c*) Dados $a \in \mathcal{O}_P$ e $x \in P$, temos que $v(a) \geq 0$ e $v(x) > 0$. Logo,

$$v(ax) = v(a) + v(x) > 0,$$

ou seja, $ax \in P$.

(*d*) Suponha que exista um ideal Q de $\mathcal{O}_P$, tal que $P \subsetneq Q \subsetneq \mathcal{O}_P$. Então existe $x \in Q$ mas $x \notin P$, ou seja, $v(x) = 0$. Logo, x é invertível em $\mathcal{O}_P$. Portanto, $Q = \mathcal{O}_P$, o que é uma contradição.

Concluímos que P é um lugar de F/K e $\mathcal{O}_P$ é o seu anel de valorização correspondente.

(4) Sejam $\mathcal{O}$ um anel de valorização de F/K, P seu ideal maximal, v_P a valorização discreta associada a P e $z \in F \setminus \mathcal{O}$. Vamos mostrar que $F = \mathcal{O}[z]$. Se $y \in F$, como $v_P(z^{-1}) > 0$,então $v_P(yz^{-k}) \geq 0$ para algum $k \geq 0$ suficientemente grande. Consequentemente, $w \coloneqq yz^{-k} \in \mathcal{O}$ e $y = wz^k \in \mathcal{O}[z]$. Desta forma mostramos que se $\mathcal{O} \subsetneq R \subseteq F$, onde R é uma anel então $R = F$. Portanto todo anel de valorização $\mathcal{O}$ de F/K é um subanel próprio maximal de F.

□

De acordo com o Teorema 3.1.15 lugares, anéis de valorização e valorizações discreta de um corpo de funções são essencialmente a mesma coisa.

Seja P um lugar de F/K e seja $\mathcal{O}_P$ o anel de valorização correspondente. Como P é um ideal maximal, a 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, para $x \in F \setminus \mathcal{O}_P$ definimos $x(P) := \infty$.

Observação 3.1.16. *Pela Proposição 3.1.7, temos que $K \subseteq \mathcal{O}_P$ e $K \cap P = \{0\}$, então a função*

$$\begin{array}{ccc} \mathcal{O}_P & \longrightarrow & \mathcal{O}_P/P \\ x & \longmapsto & x(P) \end{array}$$

induz um mergulho canônico de K em $\mathcal{O}_P/P$. Sendo assim, podemos considerar K como um subcorpo de $\mathcal{O}_P/P$. Do mesmo modo, temos que $\overline{K}$ pode ser considerado um subcorpo de $\mathcal{O}_P/P$.

Definição 3.1.17. *Seja $P \in \mathbb{P}_F$.*

(i) $F_P := \mathcal{O}_P/P$ é dito o corpo de classe residual módulo P. A função $x \longmapsto x(P)$ de F em $F_P \cup \{\infty\}$ é chamada a função da classe residual com respeito a P. Usaremos a notação: $x + P := x(P)$, para $x \in \mathcal{O}_P$.

(ii) $gr(P) := [F_P : K]$ é chamado o grau de P. Um lugar de grau um é também chamado de lugar racional de F/K.

Proposição 3.1.18. *Se P é um lugar de F/K e $0 \neq x \in P$, então*

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

Demonstração. Pela Observação 3.1.3 temos que $[F : K(x)] < \infty$. Assim, é suficiente mostrarmos que se $z_1, z_2, \ldots, z_n$ são elementos em $\mathcal{O}_P$, cujas classes de equivalência $z_1(P), z_2(P), \ldots, z_n(P) \in \mathbb{F}_P$ são linearmente independentes sobre K, então $z_1, z_2, \ldots, z_n$ também são linearmente independentes sobre $K(x)$.

Suponhamos, por absurdo, que $z_1, z_2, \ldots, z_n$ são L.D. sobre $K(x)$, isto é, que existem elementos $\phi_i \in K(x)$, não todos nulos, tais que

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

Sem perda de generalidade assumimos que $\phi_i(x)$ são polinômios em x e nem todos são divisíveis por x, isto é, $\phi_i(x) = a_i + xg_i(x)$, com $a_i \in K$, $g_i(x) \in K[x]$ e $a_i \neq 0$ para algum i. Se $x \in P$, como $g_i(x) \in \mathcal{O}_P$, segue que

$$\phi_i(x)(P) = a_i(P) = a_i.$$

Aplicando a classe residual, obtemos

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

contradizendo a independência linear de $z_1(P), \ldots, z_n(P)$ sobre K. □

Corolário 3.1.19. *O corpo $\overline{K}$ de constantes de F/K é uma extensão finita de K.*

Demonstração. Vamos usar o fato de que $\mathbb{P}_F \neq \emptyset$, que será provado no Corolário 3.1.23. Seja $P \in \mathbb{P}_F$. Como $\overline{K}$ pode ser visto como um subcorpo de F_P, via a função de classe residual $\mathcal{O}_P \longmapsto F_P$, temos que

$$[F_P : \overline{K}][\overline{K} : K] = [F_P : K] < \infty.$$

Portanto, $[\overline{K} : K] \leq [F_P : K] < \infty$. □

Observação 3.1.20. *Seja P um lugar racional de F/K, isto é, $gr(P) = 1$. Então temos que $F_P = K$ e a função de classe residual aplica F em $K \cup \{\infty\}$.*

Se K é um corpo algebricamente fechado, então todos os lugares de F/K são racionais. Logo, podemos definir para cada $z \in F$, uma função

$$z : \mathbb{P}_F \longrightarrow K \cup \{\infty\}$$

$$P \longmapsto z(P).$$

Por isso, F/K é chamado corpo de funções e K é dito corpo de constantes de F.

Definição 3.1.21. *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 $v_P(z) = m > 0$, P é dito zero de z de ordem m e se $v_P(z) = m < 0$, P é dito polo de z de ordem m.

Teorema 3.1.22. *Sejam F/K um corpo de funções e R um subanel de F tal que $K \subseteq R \subseteq F$. Suponha que I é um ideal próprio de R. Então, existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Demonstração. Consideremos o conjunto

$$\mathcal{F} = \{S;\ S \text{ é um subanel de } F,\ R \subseteq S \text{ e } IS \neq S\}.$$

Observemos que $\mathcal{F} \neq \emptyset$, pois $R \in \mathcal{F}$, e $\mathcal{F}$ é indutivamente ordenado por inclusão. De fato, se $\mathcal{H} \subseteq \mathcal{F}$ é um subconjunto totalmente ordenado de $\mathcal{F}$, então $T = \bigcup_{S \in \mathcal{H}} S$ é um subanel de F e $R \subset T$. Temos que provar que $IT \neq T$. Assim, suponha que $IT = T$, então

$$1 = \sum_{v=1}^{n} a_v s_v, \text{ com } a_v \in I, s_v \in T.$$

Como $\mathcal{H}$ é totalmente ordenado, existe um $S_0 \in \mathcal{H}$ tal que $s_1, s_2, \cdots, s_n \in S_0$. Logo,

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

o que é uma contradição. Assim, pelo lema de Zorn, $\mathcal{F}$ contém um elemento maximal, isto é, existe $\mathcal{O} \subseteq F$ tal que $R \subseteq \mathcal{O} \subseteq F$ e $\mathcal{O}$ é maximal com respeito a estas propriedades.

Então, basta mostrar que $\mathcal{O}$ é um anel de valorização de F/K. Como $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$ temos que $\mathcal{O} \subsetneq F$ e $I \subseteq \mathcal{O} \setminus \mathcal{O}^{\times}$. Suponhamos que exista um elemento $z \in F$ tal que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Então $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. De fato, como $\mathcal{O}$ é elemento maximal de $\mathcal{F}$, $\mathcal{O} \subsetneq \mathcal{O}[z^{-1}]$ e $\mathcal{O} \subsetneq \mathcal{O}[z]$, segue que $\mathcal{O}[z]$ e $\mathcal{O}[z^{-1}]$ não pertencem a $\mathcal{F}$. Como $R \subseteq \mathcal{O}[z] \subseteq F$, $R \subseteq \mathcal{O}[z^{-1}] \subseteq F$, temos $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Podemos obter $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in I\mathcal{O}$ tais que

$$1 = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n, \tag{3.2}$$

$$1 = b_0 + b_1 z^{-1} + b_2 z^{-2} + \cdots + b_m z^{-m}, \tag{3.3}$$

com $m \geq 1$ e $n \geq 1$. Sem perda de generalidade, podemos supor $m \leq n$ e assumirmos m e n como elementos minimais. Assim, multiplicando (3.2) por $1 - b_0$

e (3.3) por $a_n z^n$, obtemos

$$1 - b_0 = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n,$$

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots b_n a_n z^{n-m}.$$

Somando as equações acima chegamos a igualdade

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

com $c_i \in I\mathcal{O}, \forall i \in \{0, 1, \ldots, n-1\}$. O que é uma contradição, pois n foi escolhido de forma minimal. Assim, provamos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$, para todo $z \in F$. Portanto, $\mathcal{O}$ é um anel de valorização de F/K. □

Corolário 3.1.23. *Sejam F/K um corpo de funções e $z \in F$ um elemento transcendente sobre K. Então z tem pelo menos um zero e um polo. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Consideremos o anel $R = K[z]$ e o ideal $I = z\,K[z]$. Pelo teorema anterior, podemos garantir que existe um lugar $P \in \mathbb{P}_F$ com $z \in P$. Logo, P é um zero de z. Um argumento análogo mostra que existe um lugar $Q \in \mathbb{P}_F$ contendo z^{-1}, ou seja, tal que Q é um polo de z. □

Observação 3.1.24. *Seja $z \in F$, com $z \notin \overline{K}$, então, pelo Corolário 3.1.23, z produz uma função não constante, no sentido da Observação 3.1.20.*

3.2 CORPO DE FUNÇÕES ALGÉBRICAS

Nesta seção, vamos apresentar os elementos que definimos na seção anterior sobre o corpo de funções racionais. Ou seja, vamos considerar o corpo $F = K(x)$, onde x é transcendente sobre K.

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

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

da extensão $K(x)/K$, cujo o ideal maximal é

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

Em particular, quando $p(x)$ é linear, isto é, $p(x) = x - \alpha$, com $\alpha \in K$, vamos denotar $P_{x-\alpha}$ por P_α.

Existe um outro anel de valorização de $K(x)/K$, a saber:

$$\mathcal{O}_\infty \coloneqq \left\{ \frac{f(x)}{g(x)};\ g(x) \in K[x], gr(f(x)) \leq gr(g(x)) \right\},$$

com ideal maximal sendo

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

Este lugar é chamado de lugar infinito de $K(x)$.

Proposição 3.2.1. *Seja $F = K(x)$ um corpo de funções racionais sobre um corpo K.*

(a) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$, onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo de P e a valorização correspondente v_P pode ser dada em cada $z \in K(x) \setminus \{0\}$ por:

$$v_P(z) = n \text{ se, e somente se, } z = p(x)^n \ \frac{f(x)}{g(x)},$$

onde $f(x)$, $g(x) \in K[x]$, $p(x) \mid f(x)$ e $p(x) \nmid g(x)$.

O corpo de classes residuais $K(x)_P = \mathcal{O}_P/P$ é isomorfo à $K[x]/\langle p(x) \rangle$ e $gr(P) = gr(p(x))$.

(b) Se $p(x) = x - \alpha$, com $\alpha \in K$, então $gr(P_{x-\alpha}) = 1$. Além disso, se para cada $z = f(x)/g(x) \in K(x)$, definimos

$$z(\alpha) = \begin{cases} f(x)/g(x), & \text{se} \quad g(\alpha) \neq 0 \\ \infty \quad , & \text{se} \quad g(\alpha) = 0, \end{cases}$$

então o mapa da classe residual é dado por

$$z(P) = z(\alpha);\ \forall z \in K(x).$$

(c) *Um elemento primo de* P_∞ *é* $t = 1/x$ *e* $gr(P_\infty) = 1$. *A valorização discreta* v_∞ *correspondente a* P_∞ *é dada por*

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

onde $f(x)$, $g(x) \in K[x]$. *Além disso, se escrevemos um elemento* $z \in K(x)$ *na forma*

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

com a_n, $b_m \neq 0$, *e definimos*

$$z(\infty) = \begin{cases} a_n/b_m, & se \quad n = m \\ 0, & se \quad n < m \\ \infty, & se \quad n > m, \end{cases}$$

então o mapa residual correspondente a P_∞ *é dado por*

$$z(P_\infty) = z(\infty).$$

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

Demonstração. (a) Seja $P = P_{p(x)} \in \mathbb{P}_F$, $p(x) \in K[x]$ irredutível.

O ideal $P_{p(x)} \subset \mathcal{O}_{p(x)}$ é gerado por $p(x)$. De fato, se $f(x)/g(x) \in P_{p(x)}$ temos que $p(x) \mid f(x)$ e $p(x) \nmid g(x)$, então $\frac{f(x)}{g(x)} = \frac{u(x)}{g(x)} \cdot p(x) \in \mathcal{O}_{p(x)} \cdot p(x)$. Portanto, $P_{p(x)} \subset \mathcal{O}_{p(x)} \cdot p(x)$. Como $p(x) \in P_{p(x)}$, segue que $P_{p(x)} = p(x) \cdot \mathcal{O}_{p(x)}$.

Agora definamos a função

$$\begin{array}{rccc} \psi: & K[x] & \longrightarrow & K(x)_P \\ & f(x) & \longmapsto & f(x)(P). \end{array}$$

Temos que ψ está bem definida, pois como $f(x) = f(x)/1$, segue que $f(x) \in \mathcal{O}_{p(x)}$. Além disso, ψ é um homomorfismo de anéis pois:

$$\psi(f(x)+g(x)) = [f(x)+g(x)](P) = f(x)(P)+g(x)(P) = \psi(f(x))+\psi(g(x)),$$

$$\psi(f(x)) \cdot \psi(g(x)) = f(x)(P) \cdot g(x)(P) = (f(x) \cdot g(x))(P) = \psi(f(x) \cdot g(x)).$$

Agora, observemos que $N(\psi) = \langle p(x)\rangle$. De fato,

$$f(x) \in N(\psi) \Leftrightarrow f(x)(P) = P \Leftrightarrow p(x) \mid f(x) \Leftrightarrow f(x) \in \langle p(x)\rangle.$$

Por fim, temos que ψ é sobrejetiva. De fato, seja $z = u(x)/v(x) \in \mathcal{O}_{p(x)}$, onde $p(x) \nmid v(x)$. Como $p(x)$ é irredutível temos $\mathrm{mdc}(p(x), v(x)) = 1$, assim existem $a(x), b(x) \in K[x]$, onde $a(x)p(x) + b(x)v(x) = 1$. Então,

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

Logo, $z(P) = (b(x)u(x))(P)$, ou ainda, $\psi(b(x)u(x))(P) = z(P)$. Portanto,

$$\frac{K[x]}{\langle p(x)\rangle} \simeq K(x)_P \text{ e } [K(x)_P : K] = \left[\frac{K[x]}{\langle p(x)\rangle} : K\right].$$

Donde segue que $gr(P) = gr(p(x))$.

(b) Seja $P = P_\alpha$, com $\alpha \in K$. Se $f(x) \in K[x]$, então $(x - \alpha) \mid (f(x) - f(\alpha))$. Daí,

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

Se $z = f(x)/g(x) \in \mathcal{O}_P$, então,

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

Além disso, $g(\alpha) \neq 0 \Leftrightarrow g(x)(P) \neq P$. Se $z \notin \mathcal{O}_P$, então $z = f(x)/g(x)$, onde $p(x) \mid g(x)$. Portanto, $g(\alpha) = 0$ e $z(P) = \infty = z(\alpha)$.

(c) Seja $f(x)/g(x) \in P_\infty$. Então

$$f(x)/g(x) = 1/x \cdot (xf(x)/g(x)) \in 1/x\,\mathcal{O}_\infty,$$

pois, sendo $\mathrm{gr}(xf(x)) \leq gr(g(x))$, temos que $(xf(x)/g(x)) \in \mathcal{O}_\infty$. Logo, $P_\infty \subset (1/x)\,\mathcal{O}_\infty$. Por outro lado, como $1/x \in P_\infty$, segue que $(1/x)\mathcal{O}_\infty \subset P_\infty$. Logo, $(1/x)\mathcal{O}_\infty = P_\infty$.

Como $1/x \in P_\infty$ e $K(x) = K(1/x)$, segue que $[K(x) : K(1/x)] = 1$. Então, pela Proposição 3.1.18

$$gr(P_\infty) \leq [K(x) : K(1/x)] = 1.$$

Portanto, $gr(P_\infty) = 1$.

Agora, se $f(x)/g(x) \in P_\infty$, então existe um número inteiro positivo n tal que

$$\frac{f(x)}{g(x)} = \left(\frac{1}{x}\right)^n \frac{f_1(x)}{g_1(x)},$$

onde $f_1(x)/g_1(x)$ é invertível em $\mathcal{O}_\infty$. Como $f_1(x)$ e $g_1(x)$ tem o mesmo grau, segue que

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = n = gr(f(x)) - gr(g(x)).$$

Por fim, considere $z \in K(x)$ na forma

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}.$$

Se $z \notin \mathcal{O}_\infty$, então $z(P_\infty) = \infty$ e $z(\infty) = \infty$, pois $n > m$. Se $z \in \mathcal{O}_\infty$ e $n < m$, então $z(P_\infty) = 0$, pois $z \in P_\infty$, e $z(\infty) = 0$, pois $n < m$. Por último, se $z \in \mathcal{O}_\infty$ e $n = m$, então, dividindo o numerador de z pelo seu denominador,

$$z = \frac{\frac{a_n}{b_m}(b_m x^m + \cdots + b_0) + s(x)}{b_m x^m + \cdots + b_0} = \frac{a_n}{b_m} + \frac{s(x)}{b_m x^m + \cdots + b_0},$$

onde $gr(s(x)) < m$. Logo, $z(\infty) = a_n/b_m$ e $z(P_\infty) = a_n/b_m$, pois

$$(s(x)/(b_m x^m + \cdots + b_0))(P_\infty) = 0.$$

(d) Escolha um lugar P de $K(x)/K$ de grau 1, isto é, $P = P_\alpha$, com $\alpha \in K$. Pela Observação 3.1.16 existe um mergulho do corpo de constantes $\overline{K}$ de $K(x)$ em $K(x)_P$, donde

$$K \subseteq \overline{K} \subseteq K(x)_P = K.$$

□

Teorema 3.2.2. $\mathbb{P}_{K(x)} = \{P_{p(x)}; p(x)$ *é polinômio mônico e irredutível*$\} \cup P_\infty$.

Demonstração. Sejam $P \in \mathbb{P}_{K(x)}$ e $\mathcal{O}_P$ o anel de valorização correspondente a P. Vamos dividir a demonstração em dois casos.

Caso 1: $x \in \mathcal{O}_P$

Se $x \in \mathcal{O}_P$, então $K[x] \subset \mathcal{O}_P$. Assim, temos que $I = K[x] \cap P$ é um ideal de $K[x]$. Como P é ideal maximal de $\mathcal{O}_P$, então I é ideal primo de $K[x]$. Considere a função:

$$K[x]/I \longrightarrow K(x)_P$$

$$z + I \mapsto z(P).$$

Esta função é um mergulho. De fato,

$$z_1(P) = z_2(P) \Rightarrow (z_1 - z_2)(P) = 0 \Rightarrow (z_1 - z_2) \in I \Rightarrow z_1 + I = z_2 + I.$$

Temos ainda que $I \neq \{0\}$. De fato, se $I = \{0\}$, então

$$[\mathcal{O}_P/P : K] \geq [K(x) : K] = \infty,$$

o que é um absurdo.

Como K é corpo, segue que $K[x]$ é domínio de ideais principais. Logo, existe um polinômio $p(x) \in K[x]$ mônico e irredutível, tal que $I = p(x) \cdot K[x]$.

Assim, se $g(x) \in K[x]$ e $p(x) \nmid g(x)$, temos que, como $g(x) \notin I$, $g(x) \notin P$. Portanto, $1/g(x) \in \mathcal{O}_P$. Desta forma, dado $f(x)/g(x) \in \mathcal{O}_{p(x)}$, como $p(x) \nmid g(x)$, temos que

$$f(x)/g(x) = f(x) \cdot (1/g(x)) \in \mathcal{O}_P,$$

pois $[g(x)]^{-1} \in \mathcal{O}_P$. Logo, $\mathcal{O}_{p(x)} \subset \mathcal{O}_P$. Como $\mathcal{O}_{p(x)}$ é anel de valorização, segue que $\mathcal{O}_{p(x)} = \mathcal{O}_P$ e $P_{p(x)} = P$.

Caso 2: $x \notin \mathcal{O}_P$

Como $x \notin \mathcal{O}_P$, então $x^{-1} \in \mathcal{O}_P$. Assim, $K[x^{-1}] \subset \mathcal{O}_P$ e $x^{-1} \in P \cap K[x^{-1}]$. Como x^{-1} é irredutível em $K[x^{-1}]$, segue que $x^{-1}K[x^{-1}]$ é ideal maximal de $K[x^{-1}]$. Sabendo que

$$x^{-1}K[x^{-1}] \subset P \cap K[x^{-1}],$$

concluímos que $x^{-1}K[x^{-1}] = P \cap K[x^{-1}]$. Assim,

$$\mathcal{O}_P \supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})}; f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \nmid g(x^{-1}) \right\} =$$

$$= \left\{ \frac{a_0 + a_1x^{-1} + \cdots + a_nx^{-n}}{b_0 + b_1x^{-1} + \cdots + b_mx^{-m}}; b_0 \neq 0 \right\} =$$

$$= \left\{ \frac{x^{-n}(a_0x^n + a_1x^{n-1} + \cdots + a_n)}{x^{-m}(b_0x^m + b_1x^{m-1} + \cdots + b_m)}; b_0 \neq 0 \right\} =$$

$$= \left\{ \frac{x^m(a_0x^n + a_1x^{n-1} + \cdots + a_n)}{x^n(b_0x^m + b_1x^{m-1} + \cdots + b_m)}; b_0 \neq 0 \right\} =$$

$$= \left\{ \frac{a_0x^{m+n} + a_1x^{m+n-1} + \cdots + a_nx^m}{b_0x^{m+n} + b_1x^{n+m-1} + \cdots + b_mx^n}; b_0 \neq 0 \right\}.$$

Ou seja,

$$\mathcal{O}_P \supseteq \left\{ \frac{u(x)}{v(x)}; u(x), v(x) \in K[x] \text{ e } gr(u) \leq gr(v) \right\} = \mathcal{O}_\infty.$$

Como $\mathcal{O}_\infty$ é maximal, segue que $\mathcal{O}_\infty = \mathcal{O}_P$ e $P = P_\infty$. □

Corolário 3.2.3. *Os lugares de $K(x)/K$ de grau 1 estão em bijeção com os elementos de $K \cup \{\infty\}$.*

Demonstração. Seja $\Lambda = \{$ lugares de $K(x)/K$ com grau $1\}$. Pelo Teorema 3.2.2, $\Lambda = \{P_\alpha; \alpha \in K\} \cup \{\infty\}$.

□

3.3 INDEPENDÊNCIA DE VALORIZAÇÕES

O principal resultado desta seção é o Teorema da Aproximação Fraca, também conhecido por Teorema da Independência das Valorizações. Essencialmente ele diz que: se $v_1, \ldots, v_n$ são valorizações duas a duas distintas de F/K e $z \in F$, mesmo se conhecermos os valores $v_1(z), \ldots, v_{n-1}(z)$, então ainda assim nada poderemos afirmar sobre o valor de $v_n(z)$.

Teorema 3.3.1 (Teorema da Aproximação Fraca)**.** *Sejam F/K um corpo de funções algébricas, $P_1, P_2, \ldots, P_n \in \mathbb{P}_F$ 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 $v_{P_i}(x - x_i) = r_i$, para $i = 1, 2, \cdots, n$.*

Demonstração. A prova do Teorema se dará em de três passos. Usaremos a seguinte notação $v_i = v_{P_i}$.

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

De fato: Vamos mostrar por indução sobre n.

Para $n = 2$, temos que $\mathcal{O}_{P_1}$ não está contido em $\mathcal{O}_{P_2}$ e $\mathcal{O}_{P_2}$ não está contido em $\mathcal{O}_{P_1}$, por conta da maximalidade dos anéis de valorização. Assim, podemos tomar $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Então, $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geq 0$. Tomemos $u = y_1/y_2$. Então,

$$v_1(u) = v_1\left(\frac{y_1}{y_2}\right) = v_1(y_1) + v_1({y_2}^{-1}) > 0,$$

pois $v_1({y_2}^{-1}) = -v_1(y_2) > 0$ e

$$v_2(u) = v_2\left(\frac{y_1}{y_2}\right) = v_2(y_1) + v_2({y_2}^{-1}) < 0,$$

pois $v_2(y_2^{-1}) = -v_2(y_2)$.

Para $n > 2$, suponha que $v_1(y) > 0, v_2(y) < 0, \ldots, v_{n-1}(y) < 0$, para algum $y \in F$. Vamos mostrar que existe $u \in F$ tal que $v_1(u) > 0, v_2(u) < 0, \ldots, v_n(u) < 0$.

Se $v_n(y) < 0$, não temos nada a provar. Se $v_n(y) \geq 0$. Tome $z \in F$ tal que $v_1(z) > 0$ e $v_n(z) < 0$, como fizemos para $n = 2$. Então considere $u = y + z^r$, onde $r \geq 1$, $r \in \mathbb{Z}$ e $rv_i(z) \neq v_i(y)$ para $i = 1, \ldots, n-1$. Assim,

$$v_1(u) \geq \min\{v_1(y), rv_1(z)\} >, 0$$

$$v_i(u) = \min\{v_i(y), rv_i(z)\} < 0, \text{ para } i = 1, 2, \ldots, n.$$

Passo 2: Existe $w \in F$ tal que $v_1(w-1) > r_1$ e $v_i(w) > r_i$, para $i = 2, \ldots, n$.

De fato: Tome u do passo anterior e defina $w = (1 + u^s)^{-1}$, onde s é o menor número inteiro maior ou igual ao máximo de

$$\left\{ \frac{r_1}{v_1(u)}, \frac{r_i}{-v_i(u)}; \, i = 2, \cdots, n \right\}.$$

Temos que

$$v_1(w-1) = v_1\left(\frac{1}{1+u^s} - 1\right) = v_1(-u^s(1+u^s)^{-1}) = v_1(-u^s) + v_1((1+u^s)^{-1}) =$$

$$= v_1(-u^s) - v_1(1+u^s) = v_1(-u^s) - \min\{v_1(1), v_1(u^s)\} = v_1(u^s) = sv_1(u) > r_1,$$

e

$$v_i(w) = v_i((1+u^s)^{-1}) = -v_i(1+u^s) = -sv_i(u) > r_i, \text{ para } i = 2, \ldots, n.$$

Passo 3: Dados $y_1, \ldots, y_n \in F$, existe $z \in F$ onde $v_i(z - y_i) > r_i$, $\forall i = 1, \ldots, n$.

Demonstração do Passo 3: Escolha $s \in \mathbb{Z}$ de forma que $v_i(y_j) \geq s$, $\forall i \in \{1, 2, \ldots, n\}$ e $\forall j \in \{1, 2, \ldots, n\}$. Pelo passo 2, existem $w_1, w_2, \ldots, w_n \in F$ tais que $v_i(w_i - 1) > r_i - s$ e $v_i(w_j) > r_i - s$ quando $j \neq i$. Tomando $z = \sum_{j=1}^{n} y_j w_j$, temos

$$v_i(z - y_i) = v_i((\sum_{j=1, j\neq i}^{n} y_j w_j) + (w_i - 1)y_i) > r_i,$$

$\forall i = 1, \ldots, n$.

Agora, estamos numa posição para finalizar a prova do teorema. Pelo passo 3, existe $z \in F$, onde $v_i(z - x_i) > r_i, \forall i = 1, \ldots, n$. Escolha $z_i \in F$ tais que $v_i(z_i) = r_i$, para cada $i \in \{1, 2, , \ldots, n\}$. Aplicando o passo 3 mais uma vez, existe um elemento $z' \in F$ tal que $v_i(z' - z_i) > r_i, \forall i = 1, \ldots, n$. Assim,

$$v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i, \forall i = 1, \ldots, n.$$

Tome $x \coloneqq z + z'$. Daí,

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

□

Corolário 3.3.2. *Todo corpo de funções tem uma quantidade infinita de lugares.*

Demonstração. Suponha que exista uma quantidade finita de lugares, digamos $P_1, \ldots, P_n$. Pelo Teorema 3.3.1, existe $0 \neq x \in F$ tal que $v_{P_i}(x) > 0$, $\forall i = 1, \ldots, n$. Donde x é transcendente sobre K, mas não tem polo, contradizendo o Corolário 3.1.23. □

Proposição 3.3.3. *Sejam F/K um corpo de funções e $P_1, \ldots P_r$ os zeros de um elemento $x \in F$. Então,*

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

Demonstração. Para facilitar vamos usar as seguintes notações: $v_i = v_{p_i}$, $f_i = gr(P_i)$ e $e_i = v_i(x)$. Pelo Teorema da Aproximação Fraca (Teorema 3.3.1), para cada $i \in \{1, 2, \ldots, r\}$ existe $t_i \in F$ tal que $v_i(t_i) = 1$ e $v_k(t_i) = 0$ para $k \neq i$. Sejam $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ formam uma base do corpo de classe residual F_{P_i} sobre K. Daí, pelo Teorema da Aproximação Fraca(Teorema 3.3.1), existem $z_{ij} \in F$ tais que para todos i e j temos

$$v_i(s_{ij} - z_{ij}) > 0 \quad \text{e} \quad v_k(z_{ij}) \geq e_k,\ k \neq i.$$

Vamos mostrar que $v_k(z_{kj}) = 0$ para todo k. Temos que $v_k(s_{kj} - z_{kj}) > 0$ e, como $s_{kj} \notin P_k$, $v_k(s_{kj}) = 0$. Logo, se $v_k(z_{kj}) > 0$, então $v_k(s_{kj} - z_{kj}) = 0$. Por outro lado, se $v(z_{kj}) < 0$, então $v_k(s_{kj} - z_{kj}) = v_k(z_{kj}) < 0$. Ambos geram uma contradição, pois $v_k(s_{kj} - z_{kj}) > 0$. Portanto, $v_k(z_{kj}) = 0$ para todo k fixado.

Os elementos ${t_i}^a z_{ij}$, $1 \leq i \leq r$, $1 \leq j \leq f_i$ e $0 \leq a < e_i$ são linearmente independentes sobre $K(x)$. De fato, suponha que existe uma combinação não trivial:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \phi_{ija}(x) {t_i}^a z_{ij} = 0. \tag{3.4}$$

Sem perda de generalidade podemos assumir que $\phi_{ija}(x) \in K[x]$ e que nem todos os $\phi_{ija}(x)$ são divisíveis por x. Então, existem índices $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$, tais que:

- $x \mid \phi_{ija}(x)$, $\forall a < c$ e $\forall j \in \{1, \ldots, f_k\}$;
- $x \nmid \phi_{kjc}$, para algum $j \in \{1, \ldots, f_k\}$.

Multiplicando (3.4) por ${t_k}^{-c}$ obtemos:

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \phi_{ija}(x) {t_i}^a {t_k}^{-c} z_{ij} = 0. \tag{3.5}$$

Para $i \neq k$ todas as parcelas de (3.5) estão em P_k, pois

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

Quando $i = k$ e $a < c$, temos:

$$v_k(\phi_{kja}(x){t_k}^{a-c}z_{kj}) = v_k(\phi_{kja}(x)) + (a-c)v_k(t_k) + v_k(z_{kj}) \geq -c + e_k > 0.$$

Se $i = k$ e $a > c$, temos:

$$v_k(\phi_{kja}(x){t_k}^{a-c}z_{kj}) = v_k(\phi_{kja}(x))+(a-c)v_k(t_k)+v_k(z_{kj}) \geq e_k+(a-c)+0 \geq a-c \geq 0.$$

Portanto, se $k = i$ e $a \neq c$, temos $v_k(\phi_{kja})(x){t_k}^a t_k^{-c} z_{kj} > 0$, ou ainda, $\phi_{kja}(x){t_k}^a {t_k}^{-c} z_{kj} \in P_k$.

Para $k \neq i$ temos que $v_k(\phi_{ija}(x){t_i}^a {t_k}^{-c} z_{ij}) > 0$, ou seja, $\phi_{ija}(x){t_i}^a {t_k}^{-c} z_{ij} \in P_k$.

Pelo que foi demonstrado, pela igualdade:

$$\sum_{i=1}^{r}\sum_{j=1}^{f_i}\sum_{a=0}^{e_i-1} \phi_{ija}(x){t_i}^a {t_k}^{-c} z_{ij} = 0,$$

obtemos

$$\sum_{j=1}^{k} \phi_{kjc}(x) z_{kj} \in P_k.$$

Além disso, temos que, $\phi_{kjc}(x)(P_k) \in K$ e nem todos $\phi_{kjc}(x)$ se anulam em P_k.

Daí, temos uma combinação linear não-trivial

$$\sum_{j=1}^{f_k} \phi_{kjc}(x)(P_k) \cdot z_{kj}(P_k) = 0,$$

sobre K, o que é uma contradição pois, $s_{kj}(P_k) = z_{kj}(P_k)$ e $\{s_{k1}(P_k), \ldots, s_{kf_k}(P_k)\}$ é uma base de F_{P_k} sobre K.

Portanto, os elementos $t_i^a z_{ij}$ são linearmente independentes sobre $K(x)$ e consequentemente:

$$\sum_{i=1}^{r} f_i\, e_i = \sum_{i=1}^{r} v_{pi}(x)\, gr(P_i) \leq [F : K(x)].$$

□

Corolário 3.3.4. *Em um corpo de funções F/K, todo elemento $0 \neq x \in F$ tem um número finito de zeros e polos.*

Demonstração. Se $x \in \overline{K}$, então x não tem polos e nem zeros.

Se $x \notin \overline{K}$, então x é transcendente sobre K, então pela Proposição 3.3.3 o número de zeros de x é no máximo $[F : K(x)]$.

Usando o mesmo argumento para x^{-1}, obtemos que x^{-1} tem finitos zeros, ou seja, x tem finitos polos. □

4 DIVISORES

Neste capítulo e nos seguintes F/K denotará um corpo de funções em uma variável sobre K tal que K é o corpo de constantes de F/K.

4.1 GRUPO DE DIVISORES

Definição 4.1.1. *O grupo de divisores de F/K, denotado por* $\mathrm{Div}(F)$, *é definido como sendo o grupo abeliano (aditivo) livre gerado pelos lugares de F/K. Os elementos de* $\mathrm{Div}(F)$ *são ditos divisores de F/K. Em outras palavras, um divisor é uma soma da forma:*

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

O suporte de D é definido por:

$$supp\, D \coloneqq \{P \in \mathbb{P}_F;\, n_P \neq 0\}.$$

Observação 4.1.2. *Dado um divisor $D \in \mathrm{Div}(F)$, será conveniente escrevermos:*

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

onde $S \subset \mathbb{P}_F$ é um subconjunto finito com $S \supset supp\, D$.

Definição 4.1.3. *Um divisor $D \in \mathrm{Div}(F)$ da forma $D = P$, com $P \in \mathbb{P}_F$, é dito um divisor primo.*

Observação 4.1.4. *Dados dois divisores $D = \sum n_P \, P$ e $D' = \sum n'_P \, P \in \mathrm{Div}(F)$ temos que:*

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

O elemento nulo de $\mathrm{Div}(F)$ *é o divisor*

$$0 \coloneqq \sum_{P \in \mathbb{P}_F} n_P \, P,\ n_P = 0 \text{ para todo } P \in \mathbb{P}_F.$$

Definição 4.1.5. *Dado um divisor $D = \sum n_P \, P \in \mathrm{Div}(F)$ e um elemento $Q \in \mathbb{P}_F$, definimos $v_Q(D) \coloneqq n_Q$.*

Com a definição acima temos que:

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

Definição 4.1.6. *Dados dois divisores D_1 e D_2 da extensão $F|K$, dizemos que*

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

Observação 4.1.7. *A relação acima define uma ordem parcial em* $\mathrm{Div}(F)$.

Se $D_1 \leq D_2$ e $D_1 \neq D_2$ escrevemos $D_1 < D_2$.

Definição 4.1.8. *Um divisor $D \in \mathrm{Div}(F)$ que satisfaz $D \geq 0$ é dito positivo.*

Definição 4.1.9. *O grau de um divisor D é definido como sendo*

$$gr(D) \coloneqq \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \mathrm{gr}(P).$$

Pelo Corolário 3.3.4 um elemento $0 \neq x \in F$ tem um número finito de zeros e polos sobre $\mathbb{P}_F$. Assim, faz sentido a definição seguinte.

Definição 4.1.10. *Sejam $0 \neq x \in F$, Z o conjunto de zeros de x em $\mathbb{P}_F$ e N o conjunto de polos de x em $\mathbb{P}_F$. Então definimos:*

$$\begin{aligned}(x)_0 &\coloneqq \sum_{P \in Z} v_P(x)P, \text{ o divisor de zeros de } x,\\ (x)_\infty &\coloneqq \sum_{P \in N} (-v_P(x))P, \text{ o divisor de polos de } x,\\ (x) &\coloneqq (x)_0 - (x)_\infty, \text{ o divisor principal de } x.\end{aligned}$$

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

Observação 4.1.11. *Dado $0 \neq x \in F$ temos que: $x \in K \iff (x) = 0$.*

Definição 4.1.12. *O conjunto* $\mathrm{Princ}(F) \coloneqq \{(x);\, 0 \neq x \in F\}$ *é dito o grupo dos divisores principais de F/K.*

Segue, diretamente da definição, que $\mathrm{Princ}(F)$ é um subgrupo de $Div(F)$, pois $(x\, y) = (x) + (y)$.

Definição 4.1.13. *O grupo quociente* $Cl(F) \coloneqq \mathrm{Div}(F)/\mathrm{Princ}(F)$ *é chamado grupo das classes de divisores de* F/K.

Para cada divisor $D \in \mathrm{Div}(F)$, *o elemento correspondente no grupo quociente* $Cl(F)$ *é denotado por* $[D]$, *a classe do divisor* D.

Definição 4.1.14. *Dois divisores* D, $D' \in \mathrm{Div}(F)$ *são ditos equivalentes e escrevemos* $D \sim D'$ *se* $[D] = [D']$, *isto é,* $D = D' + (x)$ *para algum* $x \in F \setminus \{0\}$.

A relação definida acima é uma relação de equivalência.

4.2 O ESPAÇO DE RIEMANN-ROCH

Definição 4.2.1. *Seja um divisor* $A \in \mathrm{Div}(F)$. *Definimos o espaço de Riemann-Roch associado à* A *por:*

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

Se $A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, com $n_i > 0$, $m_j > 0$, então $\mathcal{L}(A)$ consiste de todos os elementos $x \in F$ tais que:

- x tem zeros de ordem maior ou igual à m_j em Q_j, para $j = 1, \ldots, s$.
- x pode ter polos sobre os lugares $P_1, \ldots, P_r$ com a ordem do polo sobre P_i limitados por n_i com $i \in \{1, \ldots, r\}$.

Proposição 4.2.2. *Seja* $A \in \mathrm{Div}(F)$. *Então:*

a) $x \in \mathcal{L}(A)$ *se, e somente se,* $v_P(x) \geq -v_P(A)$ *para todo* $P \in \mathbb{P}_F$.

b) $\mathcal{L}(A) \neq \{0\}$ *se, e somente se, há um divisor* $A' \sim A$ *tal que* $A' \geq 0$.

Demonstração. *a)* Decorre diretamente da definição:

$$x \in \mathcal{L}(A) \Leftrightarrow (x) \geq -A \Leftrightarrow v_P(x) \geq v_P(-A) \Leftrightarrow v_P(x) \geq -v_P(A).$$

b) Temos que

$$\mathcal{L}(A) \neq \{0\} \Leftrightarrow \exists\, x \in F \setminus \{0\} \text{ tal que } (x) \geq -A \Leftrightarrow$$
$$\Leftrightarrow A' = A + (x) \text{ é tal que } A' \sim A \text{ e } A' \geq 0 \Leftrightarrow$$
$$\Leftrightarrow \exists A' \in \mathrm{Div}(F) \text{ tal que } A' \sim A \text{ e } A' \geq 0$$

□

Lema 4.2.3. *Seja $A \in \mathrm{Div}(F)$. Então:*

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

(b) Se $A' \sim A$, então $\mathcal{L}(A) \sim \mathcal{L}(A')$.

Demonstração. (*a*) Primeiramente observemos que $\mathcal{L}(A) \neq \emptyset$, pois $0 \in \mathcal{L}(A)$. Vamos mostrar que $\mathcal{L}(A)$ é fechado para as operações de soma de vetores e multiplicação por escalar. Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$, para cada $P \in \mathbb{P}_F$ temos que:

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

e

$$v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A).$$

Portanto, pela Proposição 4.2.2 temos que $x+y \in \mathcal{L}(A)$ e $a\,x \in \mathcal{L}(A)$. Como $F \supset K$, segue diretamente que $\mathcal{L}(A)$ é um K-espaço vetorial.

(*b*) Como $A \sim A'$, então existe $z \in F \setminus \{0\}$ tal que $A = A' + (z)$. Considere as funções

$$\phi : \begin{cases} \mathcal{L}(A) & \longrightarrow & F \\ x & \longmapsto & xz, \end{cases}$$

$$\psi : \begin{cases} \mathcal{L}(A') & \longrightarrow & F \\ x & \longmapsto & xz^{-1}. \end{cases}$$

As funções ϕ e ψ são lineares. De fato, dados $x, y \in \mathcal{L}(A)$, $x', y' \in \mathcal{L}(A')$ e $a \in K$. Temos que

$$\phi(ax+y) = (ax+y)z = a(xz) + yz = a\phi(x) + \phi(y)$$

e

$$\psi(ax' + y') = (ax' + y')z^{-1} = a(x'z^{-1}) + y'z^{-1} = a\psi(x') + \psi(y').$$

A imagem de ϕ está contida em $\mathcal{L}(A')$. De fato, seja $x \in \mathcal{L}(A)$. Se $x = 0$, então $\phi(x) = \phi(0) = 0 \in \mathcal{L}(A')$. Se $x \neq 0$, então $\phi(x) = xz \neq 0$ e

$$(xz) = (x) + (z) = (x) + A - A' \geq -A + A - A' = -A'.$$

Logo, $\phi(x) \in \mathcal{L}(A')$.

A imagem de ψ está contida em $\mathcal{L}(A)$. De fato, seja $x \in \mathcal{L}(A')$. Se $x = 0$, então $\psi(x) = \psi(0) = 0 \in \mathcal{L}(A)$. Se $x \neq 0$, então $\psi(x) = xz^{-1} \neq 0$ e

$$(xz^{-1}) = (x) + (z^{-1}) = (x) + A' - A \geq -A' + A' - A = -A.$$

Logo, $\psi(x) \in \mathcal{L}(A)$.

Além disso,

$$\phi(\psi(x)) = \phi(xz^{-1}) = xz^{-1} \cdot z = x$$

e

$$\psi(\phi(x)) = \phi(xz) = xz \cdot z^{-1} = x.$$

Portanto, ϕ e ψ são inversas uma da outra, e, segue que, $\mathcal{L}(A) \sim \mathcal{L}(A')$.

□

Lema 4.2.4. *Seja A um divisor de F/K. Então,*

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

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

Demonstração. (a) Primeiramente, se $x \in K \setminus \{0\}$, então $(x) = 0$. Portanto, $K \subset \mathcal{L}(0)$. Reciprocamente, se $x \in \mathcal{L}(0) \setminus \{0\}$, então $(x) \geq 0$. Assim, segue que x não possui polos. Logo, pelo Corolário 3.1.23, temos que $x \in \overline{K} = K$.

(b) Suponha que exista $x \in \mathcal{L}(A) \setminus \{0\}$. Então, $(x) \geq -A$. Isto implica que x não possui nenhum polo, o que é uma contradição, pelo Corolário 3.1.23.

□

Lema 4.2.5. *Sejam A, $B \in \mathrm{Div}(F)$ tais que $A \leq B$. Então $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ e*

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq gr(B) - gr(A).$$

Demonstração. Seja $x \in \mathcal{L}(A) \setminus \{0\}$, então $v_P(x) \geq -v_P(A)$ para cada $P \in \mathbb{P}_F$. Por hipótese, como $B \geq A$, temos que $-v_P(A) \geq -v_P(B)$ para cada $P \in \mathbb{P}_F$. Assim, $v_P(x) \geq v_P(B)$ e, portanto, $x \in \mathcal{L}(B)$.

Sendo $A \leq B$, temos que

$$B = A + P_1 + \cdots + P_r,$$

com $P_1, \ldots, P_n \in \mathbb{P}_F$ Vamos assumir inicialmente que $B = A + P$.

Consideremos $t \in F$ tal que

$$v_P(t) = v_P(B) = v_P(A) + v_P(P) = v_P(A) + 1.$$

Para $x \in \mathcal{L}(B)$, temos que $v_P(x) \geq -v_P(B) = -v_P(t)$ e, consequentemente,

$$v_P(x\,t) = v_P(x) + v_P(t) \geq 0.$$

Assim $x\,t \in \mathcal{O}_P$. Logo, podemos definir a função K-linear:

$$\begin{array}{rccc} \phi: & \mathcal{L}(B) & \longrightarrow & F_P \\ & x & \longmapsto & (x\,t)(P). \end{array}$$

Note que:

$$x \in N(\phi) \Longleftrightarrow xt \in P \Longleftrightarrow v_P(x) + v_P(t) > 0 \Longleftrightarrow$$
$$v_P(x) > -v_P(A) - 1 \Longleftrightarrow v_P(x) \geq -v_P(A).$$

Além disso, se $x \in N(\phi)$ e $Q \in \mathbb{P}_F \setminus \{P\}$, temos que

$$v_Q(x) \geq -v_Q(A),$$

e, portanto, $x \in \mathcal{L}(A)$. Reciprocamente, se $x \in \mathcal{L}(A)$, então $v_P(x) \geq -v_P(A)$. Logo, $x \in N(\phi)$. Portanto, $N(\phi) = \mathcal{L}(A)$. Consequentemente, ϕ induz a transformação linear injetiva

$$\begin{array}{rccc} \overline{\phi}: & \dfrac{\mathcal{L}(B)}{\mathcal{L}(A)} & \longrightarrow & F_P \\ & \overline{x} & \longmapsto & \phi(x). \end{array}$$

Pelo Teorema do núcleo e imagem de transformações lineares, segue que

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) = \dim(Im(\overline{\phi})) \leq \dim(F_P) = gr(P) = gr(B) - gr(A).$$

Agora mostraremos o caso geral por indução. Como mostramos inicialmente o lema vale para $B = A + P_1$. Agora suponhamos que o lema é valido para $B = A + P_1 + \cdots + P_{n-1}$. Vamos mostrar para $B = A + P_1 + \cdots + P_{n-1} + P_n$.

De fato,

$$B = A + P_1 + \cdots + P_{n-1} + P_n = (A + P_1 + \cdots + P_{n-1}) + P_n.$$

Denote $B' = A + P_1 + \cdots + P_{n-1}$. Assim, $B = B' + P_n$, e como $B' \leq B$ segue que

$$\dim(\mathcal{L}(B)/\mathcal{L}(B')) \leq gr(B) - gr(B').$$

Além disso, pela hipótese de indução temos

$$\dim(\mathcal{L}(B')/\mathcal{L}(A)) \leq gr(B') - gr(A).$$

Portanto,

$$\begin{aligned} \dim(\mathcal{L}(B)/\mathcal{L}(A)) = \dim(\mathcal{L}(B)/\mathcal{L}(B')) + \dim(\mathcal{L}(B')/\mathcal{L}(A)) \leq \\ \leq gr(B) - gr(B') + g(B') + gr(A) = gr(B) - gr(A). \end{aligned}$$

□

Proposição 4.2.6. *Para cada divisor A de uma extensão F/K, o conjunto $\mathcal{L}(A)$ é um espaço de dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos, então:*

$$\dim\, \mathcal{L}(A) \leq gr(A_+) + 1.$$

Demonstração. Primeiro observe que como $A \leq A_+$, temos que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Logo, $\dim \mathcal{L}(A) \leq \dim \mathcal{L}(A_+)$. Pelo Lema 4.2.4, temos que $\mathcal{L}(0) = K$. Então, segue que:

$$\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) = \dim \mathcal{L}(A_+) - 1.$$

Assim,

$$\dim \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1.$$

Por outro lado, como $0 \leq A_+$, aplicando o Lema 4.2.5 obtemos:

$$\dim\ \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1 \leq gr(A_+) - gr(0) + 1 = gr(A_+) + 1.$$

□

Definição 4.2.7. *Dado $A \in \mathrm{Div}(F)$ o inteiro $l(a) \coloneqq \dim \mathcal{L}(A)$ é dito a dimensão do divisor A.*

Teorema 4.2.8. *Todos os divisores principais possuem grau zero. Mais precisamente, se $x \in F \setminus K$, então*

$$gr((x)_0) = gr((x)_\infty) = [F : K(x)].$$

Demonstração. Vamos adotar a seguinte notação no decorrer da demonstração: P_i, com $i \in \{1, \cdots, r\}$, denotarão todos os polos de x,

$$n \coloneqq [F : K(x)] \text{ e } B \coloneqq (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i.$$

Pela Proposição 3.3.3 , temos que:

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

Basta provarmos então a desigualdade recíproca. Considere $\{u_1, \ldots, u_n\}$ uma base de F sobre $K(x)$ e $C \geq 0$ um divisor tal que $(u_j) \geq -C$, para cada $j \in \{1, \ldots, n\}$. Observemos que os elementos $x^i u_j$, com $0 \leq i \leq k$ e $1 \leq j \leq n$, pertencem a $\mathcal{L}(kB + C)$ e são linearmente independentes sobre K, para todo $k \geq 0$.

De fato, como $-i \geq -k$ temos que:

$$(x^i) = i(x) = i(x)_0 - i(x)_\infty \geq -kB.$$

Por outro lado, como $(u_j) \geq -C$ para cada $j = 1, \ldots, n$, segue que

$$(x^i u_j) = (x^i) + (u_j) \geq -kB - C \Rightarrow x^i u_j \in \mathcal{L}(kB + C).$$

Se $a_{ij} \in K$ são tais que:

$$\sum_{j=1}^{n} \sum_{i=1}^{k} a_{ij} x^i u_j = 0, \text{ ou ainda, } \sum_{j=1}^{n} (\sum_{i=1}^{k} a_{ij} x^i) u_j = 0,$$

Temos que $\sum_{i=1}^{n} a_{ij} x^i = 0$, para todo $j \in \{1, \ldots, n\}$. Mas, como x é um elemento transcendente sobre K, segue que $a_{ij} = 0$, para cada $i = 1, \ldots, k$ e $j = 1, \ldots, n$. Assim, temos que $x^i u_j$ são linearmente independentes sobre K.

Além disso, notemos que o número de elementos $x^i u_j$ é $n(k+1)$, e assim pela Proposição 4.2.6 segue que:

$$n\,(k+1) \leq l(kB + C) \leq k[gr(B)] + gr(C) + 1.$$

Logo, $k\,(gr(B) - n) \geq n - gr(C) - 1$, para todo $k \geq 0$. Como o lado direito da desigualdade depende apenas de k, concluímos que $gr(B) \geq n$. Assim, obtemos que

$$gr((x)_\infty) = [F : K(x)].$$

Por fim, como $(x)_0 = (x^{-1})_\infty$, segue que

$$gr((x)_0) = [F : K(x^{-1})] = [F : K(x)].$$

□

Corolário 4.2.9. *Seja A um divisor de F/K.*

(a) Se $A' \in \mathrm{Div}(F)$ é tal que $A' \sim A$, então $l(A) = l(A')$ e $gr(A') = gr(A)$.

(b) Se $gr(A) < 0$, então $l(A) = 0$.

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

(i) A é principal.

(ii) $l(A) \geq 1$.

(iii) $l(A) = 1$.

Demonstração. (a) Como, por hipótese, $A \sim A'$ o Lema 4.2.3, item (b) nos garante diretamente que $l(A) = l(A')$. Além disso, $A = A' + (x)$, onde $x \in F \setminus \{0\}$. Portanto, pelo Teorema 4.2.8 segue que

$$gr(A) = gr(A') + gr(x) = gr(A').$$

(b) Suponhamos que $l(A) > 0$. Assim, existe $A' \in \mathrm{Div}(F)$ tal que $A' \sim A$ e $A' \geq 0$. Logo, pelo que acabamos de mostrar no item (a), temos que

$$gr(A) = gr(A') \geq 0,$$

o que é uma contradição, pois $gr(A) < 0$.

(c) *(i)* $\Rightarrow$ *(ii)* Se A é principal, então $A = (x)$ para algum $x \in F \setminus \{0\}$. Sabemos que $(x^{-1}) = -(x)$. Assim, $x^{-1} \in \mathcal{L}(A)$ e $l(A) \geq 1$.

(ii) $\Rightarrow$ *(iii)* Suponha que $l(A) \geq 1$. Logo, $A' \sim A$ para algum $A' \geq 0$. Assim, como $A' \geq 0$ e $gr(A) = gr(A') = 0$ temos que $A' = 0$. Portanto, $l(A) = l(A') = l(0) = 1$.

(iii) $\Rightarrow$ *(i)* Suponha que $l(A) = 1$. Daí, podemos escolher $z \in \mathcal{L}(A) \setminus \{0\}$. Então $(z) + A \geqq 0$ e

$$gr((z) + A) = gr(z) + gr(A) = 0.$$

Logo, $(z) + A = 0$. Portanto, $A = -(z) = (z^{-1})$.

□

Exemplo 4.2.10. Considere $F = K(x)$ e $0 \neq z \in K(x)$.

Temos que $z = af(x)/g(x)$, com $a \in K \setminus \{0\}$, $f(x)$, $g(x) \in K[x]$, mônicos e primos entre si. Suponhamos que:

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i} \text{ e } g(x) = \prod_{j=1}^{s} g_j(x)^{m_j},$$

com $p_i(x)$ e $g_j(x)$ mônicos, dois a dois distintos e irredutíveis em $K[x]$. Então o divisor principal de z em $\mathrm{Div}(K(x))$ é dado por:

$$(z) = (z)_0 + (z)_\infty = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (gr(g(x)) - gr(f(x)))P_\infty,$$

onde P_i e Q_j são os lugares correspondente a $p_i(x)$ e $g_j(x)$ respectivamente.

Proposição 4.2.11. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que*

$$gr(A) - l(A) \leq \gamma, \text{ para todo } A \in \mathrm{Div}(F).$$

Demonstração. Dados A_1, $A_2 \in \mathrm{Div}(F)$ tais que $A_1 \leq A_2$, pelo Lema 4.2.5 temos:

$$l(A_2) - l(A_1) = \dim(\mathcal{L}(A_1)/\mathcal{L}(A_2)) \leq gr(A_2) - gr(A_1).$$

Fixemos $x \in F \setminus K$ e seja $B = (x)_\infty$. Assim, podemos obter $C \geq 0$, que depende de x, tal que

$$l(kB + C) \geq (k+1)gr(B), \ \forall\, k > 0 \tag{4.1}$$

como fizemos na demonstração do Teorema 4.2.8. Além disso, temos que:

$$l(kB + C) - l(kB) = \dim(\mathcal{L}(kB + C)/\mathcal{L}(kB)) \leq gr(kB + C) - gr(kB) = gr(C).$$

Portanto,

$$l(kB + C) \leq l(kB) + gr(C). \tag{4.2}$$

De (4.1), (4.2) e $gr(B) = n = [F : K(x)]$, segue que:

$$l(kB) \geq (k+1)gr(B) - gr(C) = gr(kB) + ([F : K(x)] - gr(C)).$$

Assim,

$$gr(kB) - l(kB) \leq \gamma,$$

$\forall k > 0$, onde $\gamma = gr(C) - [F : K(x)]$.

Afirmação: Dado um divisor A, existem divisores A_1 e D e um inteiro $k \geq 0$, tais que $A \leq A_1$, $A_1 \sim D$ e $D \leq kB$.

De fato: Seja $A_1 \geq A$ tal que $A_1 \geq 0$. Logo, para k suficientemente grande, temos que:

$$l(kB) - l(kB - A_1) = \dim(\mathcal{L}(kB)/\mathcal{L}(kB - A_1)) \leq gr(kB) - gr(kB - A_1).$$

Então,

$$\begin{aligned} l(kB - A_1) &\geq l(kB) - gr(A_1) \\ &\geq gr(kB) - \gamma - gr(A_1)\ , \\ &> 0 \end{aligned}$$

se k é suficientemente grande. Assim, existe $z \in \mathcal{L}(kB - A_1) \setminus \{0\}$.

Definindo $D \coloneqq A_1 - (z)$, obtemos $A_1 \sim D$ e

$$D \leq A_1 - (A_1 - kB) = kB,$$

como desejamos. Por fim,

$$\begin{aligned} gr(A) - l(A) &\leq gr(A_1) - l(A_1) \\ &= gr(D) - l(D) \\ &\leq gr(kB) - l(kB) \\ &\leq \gamma. \end{aligned}$$

□

Definição 4.2.12. *O gênero g de F/K é definido por:*

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

Corolário 4.2.13. *O gênero de F/K é um inteiro não negativo.*

Demonstração. De fato, $g \geq gr(0) - l(0) + 1 = 0$. □

Teorema 4.2.14 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então:*

(a) Para todos os divisores $A \in \mathrm{Div}(F)$, temos que

$$l(A) \geq gr(A) + 1 - g.$$

(b) Existe um inteiro c, dependendo do corpo de funções F/K, tal que

$$l(A) = gr(A) + 1 - g, \text{ sempre que } gr(A) \geq c.$$

Demonstração. (a) Pela definição de gênero temos que

$$g \geq gr(A) - l(A) + 1.$$

(b) Tome A_0 um divisor tal que $g = gr(A_0) - l(A_0) + 1$ e defina $c = gr(A_0) + g$. Se $gr(A) \geq c$, então

$$l(A-A_0) \geq gr(A-A_0)+1-g = gr(A)-g(A_0)+1-g \geq c-gr(A_0)+1-g = 1.$$

Assim, existe $0 \neq z \in \mathcal{L}(A-A_0)\setminus\{0\}$. Denote $A' := A+(z)$. Então, $A' \geq A_0$, $l(A') = l(A)$ e $gr(A') = gr(A)$. Logo,

$$gr(A) - l(A) = gr(A') - l(A') \geq gr(A_0) - l(A_0) = g - 1,$$

então $l(A) \leq gr(A) + 1 - g$.

□

Exemplo 4.2.15. O corpo de funções racionais $K(x)/K$ tem gênero $g = 0$.

Sejam P_∞ o lugar infinito de $K(x)/K$ e $r \geq 0$ um número inteiro. Considere ainda o espaço vetorial $\mathcal{L}(rP_\infty)$.

Temos que $1, x, \ldots, x^r$ são linearmente independentes sobre K, pois x é transcendente sobre K.

Além disso, $1, x, \ldots, x^r \in \mathcal{L}(rP_\infty)$. De fato, sabemos que

$$y \in \mathcal{L}(rP_\infty) \Leftrightarrow v_P(y) \geq -v_P(rP_\infty),\ \forall P \in \mathbb{P}_F.$$

Se $y \in \{1, x, \ldots, x^r\}$, temos que $v_{P_\infty}(y) = iv_{P_\infty}(x)$, com, $i \in \{0, 1, \ldots, r\}$. Portanto,

$$v_{P_\infty}(y) \geq rv_{P_\infty}(x) = -v_P(rP_\infty),\ \forall\, i \in \{0, 1, \ldots, r\}.$$

Além disso, já que $v_P(x) \geq 0$, $\forall P \in \mathbb{P}_F \setminus \{P_\infty\}$, obtemos que $v_P(y) \geq v_P(rP_\infty)$, para todo $P \in \mathbb{P}_F \setminus \{P_\infty\}$.

Portanto, $r + 1 \leq l(rP_\infty)$. Como $gr(rP_\infty) = r$, usando o Teorema de Riemann, para r suficientemente grande,temos:

$$r + 1 \leq l(rP_\infty) = gr(rP_\infty) + 1 - g = r + 1 - g.$$

Portanto, $g = 0$.

5 TEOREMA DE RIEMANN-ROCH

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

5.1 ÍNDICE DE ESPECIALIDADE E ADELE

Definição 5.1.1. *Dado $A \in \mathrm{Div}(F)$, o inteiro*

$$i(A) \coloneqq l(A) - gr(A) + g - 1$$

é chamado índice de especialidade de A.

Pelo item *(a)* do Teorema de Riemann 4.2.14, temos que $i(A) \geq 0$. Além disso, segue do item *(b)*, que $i(A) = 0$, se o $gr(A)$ for suficientemente grande.

Definição 5.1.2. *Um adele de F/K é uma função:*

$$\begin{array}{rccc} \alpha: & \mathbb{P}_F & \longrightarrow & F \\ & P & \longmapsto & \alpha_P, \end{array}$$

tal que $\alpha_P \in \mathcal{O}_P$, para quase todo $P \in \mathbb{P}_F$.

Vamos considerar um adele como sendo um elemento de $\prod_{P \in \mathbb{P}_F} F$. Usaremos a seguinte notação:

$$\alpha = (\alpha_P)_{P \in \mathbb{P}_F} = (\alpha_P)$$

Definição 5.1.3. *O conjunto*

$$\mathcal{A}_F \coloneqq \{\alpha; \alpha \text{ é um adele de } F/K\}$$

é chamado o espaço adele de F/K.

O espaço adele de F/K é um espaço vetorial sobre K.

O adele principal de um elemento $x \in F$ é o adele que tem todas as componentes iguais a x. Desta forma, essa definição induz um mergulho:

$$F \hookrightarrow \mathcal{A}_F.$$

As valorizações de v_P de F/K são estendidas da seguinte forma para $\mathcal{A}_F$:

$$v_P(\alpha) \coloneqq v_P(\alpha_P), \text{ onde } \alpha_P \text{ é dita a } P\text{-componente do adele } \alpha.$$

Temos que $v_P(\alpha) \geq 0$, para quase todo $P \in \mathbb{P}_F$, uma vez que $\alpha_P \in \mathcal{O}_P$, para quase todo $P \in \mathbb{P}_F$.

Definição 5.1.4. *Para $A \in \mathrm{Div}(F)$ definimos:*

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

Observe que $\mathcal{A}_F(A)$ é um K-subespaço vetorial de $\mathcal{A}_F$.

Lema 5.1.5. *Sejam A_1, $A_2 \in \mathrm{Div}(F)$ e $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e*

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

Demonstração. Como $A_1 \leq A_2$, temos que $v_P(A_1) \leq v_P(A_2)$, $\forall P \in \mathbb{P}_F$. Agora, seja $\alpha \in \mathcal{A}_F(A_1)$, então

$$v_P(\alpha) \geq -v_P(A_1) \geq -v_P(A_2).$$

Portanto, $\alpha \in \mathcal{A}_F(A_2)$.

Considere inicialmente que $A_2 = A_1 + P$ com $P \in \mathbb{P}_F$. O caso geral, segue por indução. Dado $t \in F$ com $v_P(t) = v_P(A_1) + 1$, tal t existe pois v_P é sobrejetiva, considere a função

$$\varphi : \begin{cases} \mathcal{A}_F(A_2) & \longrightarrow & F_P \\ \alpha & \longmapsto & (t\alpha_P)(P). \end{cases}$$

Observamos que φ está bem definida. De fato, como

$$v_P(t\alpha_P) = v_P(t) + v_p(\alpha_p) \geq v_P(A_1) + 1 - v_P(A_2) = \\ v_P(A_1) + 1 - (v_P(A_1) + 1) = 0,$$

segue que $t\alpha_P \in \mathcal{O}_P$.

Além disso, φ é uma transformação linear sobrejetiva. Se $a \in K$ e α, $\beta \in \mathcal{A}_F(A_2)$, então

$$\varphi(a\alpha + \beta) = (t(a\alpha + \beta)_P)(P) = (at\alpha_P + t\beta_P)(P) = \\ a(t\alpha_P)(P) + (t\beta_P)(P) = a\varphi(\alpha) + \varphi(\beta).$$

Dado $z(P) \in \mathbb{F}_P$, com $z \in \mathcal{O}_P$, definimos $\alpha = (\alpha_Q) \in \mathcal{A}_F$ por:

$$\alpha_Q = \begin{cases} t^{-1}z, & \text{se } Q = P, \\ t_Q^{-v_Q(A_2)}, & \text{se } Q \neq P \text{ (onde } t_Q \text{ é um elemento primo de } Q). \end{cases}$$

Assim,

$$v_Q(\alpha) = v_Q(t_Q^{-v_Q(A_2)}) = -v_Q(A_2) \text{ se } Q \neq P \text{ e}$$

$$\begin{aligned} v_P(\alpha) = v_P(\alpha_P) = v_p(t^{-1}z) = -v_P(t) + v_P(z) = \\ - v_P(A_1) - 1 + v_P(z) = -v_P(A_2) + v_P(z) \geq -v_P(A_2). \end{aligned}$$

E portanto, $\alpha \in \mathcal{A}_F(A_2)$.

Agora mostraremos que $N(\varphi) = \mathcal{A}_F(A_1)$.

$$\begin{aligned} N(\varphi) = \{\alpha \in \mathcal{A}_F(A_2);\, t\alpha_P \in P\} = \{\alpha \in \mathcal{A}_F(A_2);\, v_P(t\alpha_P) > 0\} = \\ = \{\alpha \in \mathcal{A}_F(A_2);\, v_P(\alpha_P) > -v_P(t)\} = \{\alpha \in \mathcal{A}_F(A_2);\, v_P(\alpha_P) + 1 > -v_P(A_1)\} = \\ = \{\alpha \in \mathcal{A}_F(A_2); v_P(\alpha_p) \geq -v_P(A_1)\} = \mathcal{A}_F(A_1). \end{aligned}$$

Portanto,

$$gr(A_2) - gr(A_1) = gr(P) = [\mathbb{F}_P : K] = \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)).$$

□

Lema 5.1.6. *Sejam A_1, $A_2 \in Div(F)$ com $A_1 \leq A_2$. Então*

$$\dim(\mathcal{A}_F(A_2) + F/\mathcal{A}_F(A_1) + F) = (grA_2 - l(A_2)) - (grA_1 - l(A_1)).$$

Demonstração. Consideremos a sequência exata de funções lineares:

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

onde

$$\sigma_1 : \begin{cases} \mathcal{L}(A_2)/\mathcal{L}(A_1) & \longrightarrow & \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \\ \alpha + \mathcal{L}(A_1) & \longmapsto & \alpha + \mathcal{A}_F(A_1) \end{cases}$$

e

$$\sigma_2 : \begin{cases} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) & \longrightarrow & (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \\ \alpha + \mathcal{A}_F(A_1) & \longmapsto & \alpha + (\mathcal{A}_F(A_1) + F). \end{cases}$$

Mostraremos inicialmente que σ_1 está bem definida e é uma transformação linear injetora. De fato, para todo α, $\beta \in \mathcal{L}(A_2)$, temos

$$\alpha + \mathcal{L}(A_1) = \beta + \mathcal{L}(A_1) \Leftrightarrow \alpha - \beta \in \mathcal{L}(A_1) \Leftrightarrow$$
$$v_P(\alpha - \beta) \geq -v_P(A_1),\ \forall P \in \mathbb{P}_F \Leftrightarrow \alpha - \beta \in \mathcal{A}_F(A_1) \Leftrightarrow$$
$$\alpha + \mathcal{A}_F(A_1) = \beta + \mathcal{A}_F(A_1).$$

Além disso, σ_1 é uma transformação linear pela definição.

Agora mostraremos que σ_2 está bem definida e é uma transformação linear sobrejetiva.

Sejam $\alpha, \beta \in \mathcal{A}_F(A_2)$ tais que $\alpha + \mathcal{A}_F(A_1) = \beta + \mathcal{A}_F(A_1)$. Então,

$$\alpha - \beta \in \mathcal{A}_F(A_1) \Rightarrow \alpha - \beta \in \mathcal{A}_F(A_1) + F \Rightarrow \alpha + (\mathcal{A}(A_1) + F) = \beta + (\mathcal{A}_F(A_2) + F),$$

o que mostra que σ_2 está bem definida.

Por fim, seja

$$\alpha + (\mathcal{A}_F(A_1) + F) \in (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F),$$

com $\alpha \in \mathcal{A}_F(A_2) + F$. Temos que $\alpha = \alpha_2 + f$, com $\alpha_2 \in \mathcal{A}_F(A_2), f \in F$. Assim,

$$\sigma_2(\alpha + \mathcal{A}_F(A_1)) = \alpha_2 + (\mathcal{A}_F(A_1) + F) =$$
$$= \alpha - f + (\mathcal{A}_f(A_1) + F) = \alpha + (\mathcal{A}_F(A_1) + F),$$

o que prova que σ_2 é sobrejetiva.

Resta verificar que $Im(\sigma_1) = N(\sigma_2)$:

($\subseteq$) Seja $\alpha + \mathcal{A}_F(A_1) \in \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)$, com $\alpha \in \mathcal{L}(A_2) \subseteq F$. Então

$$\sigma_2(\alpha + \mathcal{A}_F(A_1)) = \alpha + (\mathcal{A}_F(A_1) + F) = \mathcal{A}_F(A_1) + F,$$

donde $\alpha + \mathcal{A}_F(A_1) \in N(\sigma_2)$.

($\supseteq$) Seja $\alpha \in \mathcal{A}_F(A_2)$, com $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$. Então, já que $\alpha \in \mathcal{A}_F(A_1) + F$, existe $x \in F$ com $\alpha - x \in \mathcal{A}_F(A_1)$. Como $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$, temos que $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$. Assim,

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

Portanto, como a sequência de transformações lineares é uma sequência exata, segue que:

$$\dim((\mathcal{A}_F(A_2)+F)/(\mathcal{A}_F(A_1)+F)) = \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \dim(N(\sigma_2)) =$$
$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) = (gr(A_2) - gr(A_1)) - (l(A_2) - l(A_1).$$

□

Lema 5.1.7. *Se B é um divisor com $l(B) = gr(B)+1-g$, então $\mathcal{A}_F = \mathcal{A}_F(B)+F$.*

Demonstração. Suponha que exista $B_1 \geq B$. Pelo Lema 4.2.5, temos que

$$l(B_1) \leq gr(B_1) + l(B) - gr(B) = gr(B_1) + 1 - g.$$

Pelo Teorema de Riemann (Teorema 4.2.14), temos que $l(B_1) \geq gr(B_1) + 1 - g$. Portanto, $l(B_1) = gr(B_1) + 1 - g$ para todo $B_1 \geq B$.

Seja $\alpha \in \mathcal{A}$. Suponha que $P_1, \ldots, P_n \in \mathbb{P}_F$ são tais que $v_Q(\alpha) = 0$ e $v_Q(B) = 0$, se $Q \in S$, onde $S = \mathbb{P}_F \setminus \{P_1, \ldots, P_n\}$. Defina $B_1 = \sum v_P(B_1)P$ por $v_P(B_1) = 0$, se $P \in S$, e $v_{P_i}(B_1) \geq \max\{-v_{P_i}(\alpha), -v_{P_i}(B)\}$. Então, $B_1 \geq B$ e $\alpha \in \mathcal{A}_F(B_1)$. Assim, pelo Lema 5.1.6,

$$\dim(\mathcal{A}_F(B_1)+F/\mathcal{A}_F(B)+F) = (gr(B_1)-l(B_1))-(gr(B)-l(B)) = (g-1)-(g-1) = 0.$$

Daí, $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$. Como $\alpha \in \mathcal{A}_F(B_1) \subset \mathcal{A}_F(B_1) + F$, segue que $\alpha \in \mathcal{A}_F(B) + F$. A continência contrária é trivial.

□

Teorema 5.1.8. *Para todo divisor A o índice de especialidade é dado por:*

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

Demonstração. Pelo Teorema de Riemann (Teorema 4.2.14,) existe um divisor $A_1 \geq A$ tal que

$$l(A_1) = gr(A_1) + 1 - g.$$

Assim, pelo Lema 5.1.7 $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$. Agora, pelo Lema 5.1.6, segue que

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

□

Corolário 5.1.9. *O gênero de um corpo de funções algébricas F/K pode ser caracterizado por:*

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

Demonstração. $i(0) = l(0) + gr(0) + g - 1 = 1 - 0 + g - 1 = g.$ □

5.2 DIFERENCIAIS DE WEIL

Definição 5.2.1. *Uma diferencial de Weil do corpo de funções F/K é uma transformação K-linear*

$$\omega : \mathcal{A}_F \longrightarrow K,$$

que se anula em $\mathcal{A}_F(A) + F$, para algum divisor $A \in \mathrm{Div}(F)$.

Definição 5.2.2. *Definimos o conjunto das diferenciais de Weil da extensão F/K por*

$$\Omega_F \coloneqq \{\omega;\ \omega \text{ é diferencial de Weil de } F/K\}.$$

Além disso, para cada $A \in \mathrm{Div}(F)$ definimos:

$$\Omega_F(A) \coloneqq \{\omega \in \Omega_F;\ \omega \text{ se anula em } \mathcal{A}_F(A) + F\}.$$

Definição 5.2.3. *Seja V um espaço vetorial sobre o corpo K. Um funcional linear de V é uma transformação linear $g : V \longrightarrow K$.*

Definição 5.2.4. *Seja V um espaço vetorial sobre o corpo K. O espaço vetorial de todos os funcionais lineares $f : V \longrightarrow K$ é chamado de espaço vetorial dual de V e será denotado por V^*.*

Teorema 5.2.5. *Se V é um espaço vetorial de dimensão finita, então*

$$\dim(V^*) = \dim(V).$$

Demonstração. Ver em [1], Capítulo 5, Teorema 1. □

Lema 5.2.6. *Dado* $A \in \mathrm{Div}(F)$ *temos que* $\dim(\Omega_F(A)) = i(A)$.

Demonstração. Seja $(\mathcal{A}_F/(\mathcal{A}_F(A)+F))^*$ o espaço dual de $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$. Pelo Teorema 5.2.5,

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

Consideremos desta forma a função:

$$\begin{array}{rccc} \varphi: & \Omega_F(A) & \longrightarrow & (\mathcal{A}_F/(\mathcal{A}_F(A)+F))^* \\ & \omega & \longmapsto & \varphi(\omega), \end{array}$$

onde

$$\begin{array}{rccc} \varphi(\omega): & (\mathcal{A}_F/(\mathcal{A}_F(A)+F)) & \longrightarrow & K \\ & \bar{\alpha} & \longmapsto & \omega(\alpha). \end{array}$$

Primeiramente temos que mostrar que $\varphi(\omega)$ está bem definida. De fato, se $\bar{\alpha} = \bar{\beta}$, então $\alpha - \beta \in \mathcal{A}_F(A) + F$, com $\omega(\alpha - \beta) = 0$. Portanto,

$$\varphi(\omega)(\bar{\alpha}) = \omega(\alpha) = \omega(\beta) = \varphi(\omega)(\bar{\beta}).$$

Além disso, temos que $\varphi(\omega)$ é um funcional linear devido a linearidade de ω.

Agora, mostraremos que $\varphi(\omega)$ é bijetora. Se $\omega, \omega' \in \Omega_F(A)$ são tais que $\varphi(\omega) = \varphi(\omega')$ então

$$\omega(\alpha) = \varphi(\omega)(\bar{\alpha}) = \varphi(\omega')(\bar{\alpha}) = \omega'(\alpha).$$

Logo, $\omega = \omega'$.

Agora, sejam $g \in (\mathcal{A}_F/(\mathcal{A}_F(A)+F))^*$ e

$$\omega: \begin{cases} \mathcal{A}_F & \longrightarrow & K \\ \alpha & \longmapsto & g(\bar{\alpha}). \end{cases}$$

Como g é linear temos que ω é linear. Além disso, $\omega \in \Omega_F(A)$, pois se

$$\alpha = \alpha_A + f \in \mathcal{A}_F(A) + F,$$

temos que $\omega(\alpha) = g(\bar{\alpha}) = g(\bar{0}) = 0$. Assim,

$$\varphi(\omega)(\bar{\alpha}) = \omega(\alpha) = g(\bar{\alpha}),\ \forall \bar{\alpha} \in \mathcal{A}_F/(\mathcal{A}_F(A) + F),$$

donde $\varphi(\omega) = g$.

Temos ainda que φ é uma transformação linear devido a linearidade de ω. Assim, obtemos o seguinte isomorfismo:

$$\Omega_F(A) \simeq (\mathcal{A}_F/(\mathcal{A}_F(A) + F))^*.$$

Logo,

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

□

Observação 5.2.7. *Uma consequência do Lema 5.2.6 é que* $\Omega_F \neq 0$.

De fato, seja $A \in \mathrm{Div}(F)$ *tal que* $gr(A) \leq -2$. *Então,*

$$\dim \Omega_F(A) = i(A) = l(A) - gr(A) + g - 1 \geq 1.$$

Então $\Omega_F \neq 0$.

Definição 5.2.8. *Para* $x \in F$ *e* $\omega \in \Omega_F$ *definimos*

$$x\omega : \mathcal{A}_F \longrightarrow K,$$

por $(x\omega)(\alpha) \coloneqq \omega(x\alpha)$.

Observemos que ω se anula em $\mathcal{A}_F(A) + F$, para algum $A \in \mathrm{Div}(F)$, pois se $\omega \in \Omega_F$. Então, $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$, uma vez que $x \in F$. Portanto, $x\omega$ é uma diferencial de Weil de F/K.

Proposição 5.2.9. Ω_F *é um espaço vetorial de dimensão* 1 *sobre* F

Demonstração. Seja $\omega_1 \neq 0 \in \Omega_F$. Dado $0 \neq \omega_2 \in \Omega_F$, com $\omega_2 \neq \omega_1$, temos que mostrar que existe $z \in F$ tal que $\omega_2 = z\omega_1$. Assim, sejam 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 B e para cada $i \in \{1, 2\}$, vamos considerar a função:

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

Primeiramente, mostremos que φ_i está bem definida. Seja $x \in \mathcal{L}(A_i + B)$, ou seja, $(x) \geq -(A_i + B)$. Assim, $\varphi(x) = x\omega_i$ e, portanto,

$$(x\omega_i) = (x) + (\omega_i) \geq -(A_i) - B + (A_i) = -B \Rightarrow (x\omega_i) \in \Omega_F(-B).$$

A função φ_i é uma transformação linear injetiva. De fato, sejam x, $y \in \mathcal{L}(A_i + B)$ e $\alpha \in F$, então:

$$\varphi_i(x + y) = (x + y)\omega_i = x\omega_i + y\omega_i = \varphi_i(x) + \varphi_i(y),$$

pois $\Omega_F(-B)$ é um espaço vetorial sobre k, e

$$\varphi_i(\alpha x) = (\alpha x)\omega_i = \alpha(x\omega_i) = \alpha\varphi_i(x).$$

Sejam $x\omega_i$, $y\omega_i \in \Omega_F(-B)$, tais que $x\omega_i = y\omega_i$. Assim,

$$x\omega_i - y\omega_i = 0 \Rightarrow (x - y)\omega_i = 0.$$

Como $\omega_i \neq 0$, temos que $x = y$.

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

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

Demonstração da Afirmação: Pelo Teorema 2.3.14, sabemos que se U_1, U_2 são subespaços vetoriais de um espaço vetorial V de dimensão finita, então

$$\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim U_1 + \dim U_2.$$

Como $U_1 + U_2$ é subespaço vetorial de V segue que $\dim(U_1 + U_2) \leq \dim V$. Assim,

$$\dim(U_1 \cap U_2) = \dim U_1 + \dim U_2 - \dim(U_1 + U_2)$$

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

Pelo Teorema de Riemann (Teorema 4.2.14), podemos escolher um divisor $B > 0$ tal que

$$l(A_i + B) = gr(A_i + B) + 1 - g$$

para $i = 1, 2$. Definamos $U_i \coloneqq \varphi_i(\mathcal{L}(A_i + B))$, donde $U_i \subseteq \Omega_F(-B)$.

Sabemos que:

$$\dim \Omega_F(-B) = i(-B) = l(-B) - gr(-B) + g - 1 = 0 + gr(B) + g - 1.$$

Assim,

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

O termo entre parênteses é independente de B, portanto

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

se $gr(B) > -(gr(A_1) + gr(A_2) + 3(1 - g))$. Então $U_1 \cap U_2 \neq \{0\}$.

Para finalizar a demonstração da proposição, considere um divisor B, $x_1 \in \mathcal{L}(A_1 + B)$ e $x_2 \in \mathcal{L}(A_2 + B)$ que satisfazem a afirmação acima. Então, $x_1\omega_1 = x_2\omega_2 \neq 0$, ou seja, $w_2 = (x_1 x_2^{-1})\,\omega_1$. □

Queremos associar um divisor a cada diferencial de Weil não nula de F/K. Para isso definimos o seguinte conjunto de divisores, para cada $\omega \in \Omega_F$:

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

Lema 5.2.10. *Seja $0 \neq \omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.*

Demonstração. Pelo Teorema 4.2.14, existe uma constante c, dependente somente do corpo de funções F/K, tal que se $A \in \mathrm{Div}(F)$ e $gr(A) \geq c$, então $i(A) = 0$. Sabemos, pelo Teorema 5.1.8, que $\dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) = i(A)$. Assim, $gr(A) < c$, para todo $A \in M(\omega)$, o que nos permite escolher $W \in M(\omega)$ de grau máximo.

Suponha que W não tenha a propriedade requerida, ou seja, existe um divisor $A_0 \in M(\omega)$, tal que $v_Q(A_0) > v_Q(W)$, para algum $Q \in \mathbb{P}_F$. Afirmamos que $W + Q \in M(\omega)$, o que contraria a maximalidade de W.

De fato, considere um adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Podemos escrever $\alpha = \alpha' + \alpha''$, 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 $\alpha'' \in \mathcal{A}_F(A_0)$ e $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Donde segue que ω se anula em $\mathcal{A}_F(W + Q) + F$, ou seja, $W + Q \in M(\omega)$.

A unicidade, segue da maximalidade de W. □

Definição 5.2.11. *(a) O divisor (ω) de uma diferencial de Weil $\omega \neq 0$ é o único divisor de F/K que satisfaz:*

(1) ω se anula em $\mathcal{A}_F((\omega)) + F$;

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

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

(c) Um lugar P é dito um zero de ω, se $v_P(\omega) > 0$.

(d) Um lugar P é dito um polo de ω, se $v_P(\omega) < 0$.

(e) A diferencial de Weil ω é dita regular em um lugar P se $v_P(\omega) \geq 0$. Além disso, ω é dita regular (ou holomórfica) se é regular em todos os lugares $P \in \mathbb{P}_F$.

(f) Um divisor W é dito um divisor canônico sobre F/K, se $W = (\omega)$ para algum $\omega \in \Omega_F$.

Observação 5.2.12. *Segue diretamente da definição anterior que*

$$\Omega_F(A) = \{\omega \in \Omega_F;\ \omega = 0 \text{ ou } (\omega) \geq A\},$$

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

Temos ainda que $\dim \Omega_F(0) = g$, *pois*

$$\dim \Omega_F(0) = i(0) = l(0) - gr(0) + g - 1 = 1 - 0 + g - 1 = g.$$

Proposição 5.2.13. *(a) Se* $0 \neq x \in F$ *e* $0 \neq \omega \in \Omega_F$, *temos que*

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

(b) Quaisquer dois divisores canônicos de F/K *são equivalentes.*

Demonstração. (a) Se ω anula-se em $\mathcal{A}_F(A) + F$, com $A \in$ Div(F), então $x\,\omega$ anula-se em $\mathcal{A}_F(A + (x)) + F$. Consequentemente, $(\omega) + (x) \leq (x\omega)$. Por outro lado, $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Portanto,

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

(b) Como Ω_F é um espaço vetorial de dimensão 1 sobre F e

$$(xy) = (x) + (y),\ \forall x, y \in F \setminus \{0\},$$

segue que $(x) \sim (\,y)$. □

Teorema 5.2.14 (Teorema da Dualidade)**.** *Sejam* A *um divisor arbitrário e* $W = (\omega)$ *um divisor canônico de* F/K. *Então temos o seguinte isomorfismo de* K*-espaços vetoriais:*

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

Em particular, $i(A) = l(W - A)$

Demonstração. Para $x \in \mathcal{L}(W - A)$ temos

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

Logo, pela Observação 5.2.12, $x\omega \in \Omega_F(A)$.

A função μ é uma transformação linear injetiva. Sejam $a \in K$ e $x,\ y \in \mathcal{L}(W - A)$. Temos que

$$\mu(ax + y) = (ax + y)\omega = ax\omega + y\omega = a\mu(x) + \mu(y).$$

Além disso,

$$N(\mu) = \{x \in \mathcal{L}(W - A); \mu(x) = 0\} = \{x \in \mathcal{L}(W - A); x\omega = 0\} =$$
$$= \{x \in \mathcal{L}(W - A); x = 0\} = \{0\},\ \text{pois } \omega \neq 0.$$

Considere uma diferencial de Weil $\omega_1 \in \Omega_F(A)$. Podemos escrever $\omega_1 = x\omega$ para algum $x \in F$. Como

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A,$$

temos $(x) \geq -(W - A)$, então $x \in \mathcal{L}(W - A)$ e $\omega_1 = \mu(x)$. Assim μ é sobrejetiva.

Segue que μ é um isomorfismo e, portanto,:

$$i(A) = \dim \Omega_F(A) = l(W - A).$$

□

5.3 TEOREMA DE RIEMANN-ROCH

Teorema 5.3.1 (Teorema de Riemann-Roch)**.** *Seja W um divisor canônico de F/K. Então para cada divisor $A \in \mathrm{Div}(F)$ temos que*

$$l(A) = gr(A) + 1 - g + l(W - A).$$

Demonstração. Pela definição do índice de especialidade, temos:

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

Pelo Teorema 5.2.14, temos que $i(A) = l(W - A)$. Portanto,

$$l(A) = l(W - A) + gr(A) - g + 1.$$

□

Corolário 5.3.2. *Para um divisor canônico W temos*

$$gr(W) = 2g - 2 \text{ e } l(W) = g.$$

Demonstração. Para $A = 0$, o Teorema de Riemann-Roch (Teorema 5.3.1) e o Lema 4.2.4 dizem que:

$$1 = l(0) = gr(0) + 1 - g + l(W - 0).$$

Então, $l(W) = g$.

Tomando $A = W$ obtemos:

$$g = l(W) = gr(W) + 1 - g + l(W - W) = gr(W) + 2 - g.$$

Então, $gr(W) = 2g - 2$. □

Do Teorema de Riemann (Teorema 4.2.14), já sabemos que existe uma constante c tal que $i(A) = 0$ sempre que $gr(A) \geq c$. Agora, podemos fornecer uma descrição mais precisa de como escolher essa constante.

Teorema 5.3.3. *Se A é um divisor de F/K com $gr(A) \geq 2g - 1$, então*

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

Demonstração. Temos que

$$l(A) = gr(A) + 1 - g + l(W - A),$$

onde W é um divisor canônico. Como $gr(A) \geq 2g - 1$ e $gr(W) = 2g - 2$ segue que $gr(W - A) < 0$. Assim, $l(W - A) = 0$. □

6 CONSEQUÊNCIAS DO TEOREMA DE RIEMANN-ROCH

Neste capítulo apresentamos algumas consequências do Teorema de Riemann-Roch. Consideraremos que F/K é um corpo de funções algébricas de gênero g.

6.1 CARACTERIZAÇÃO DO GÊNERO E DIVISORES CANÔNICOS

Nosso primeiro objetivo é mostrar que o Teorema de Riemann-Roch caracteriza o gênero e os divisores canônicos de F/K.

Proposição 6.1.1. *Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in \mathrm{Div}(F)$ satisfazem:*

$$l(A) = gr(A) + 1 - g_0 + l(W_0 - A),$$

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

Demonstração. Sabemos que se $A = 0$, então $l(W_0) = g$, e para $A = W_0$, temos $gr(W_0) = 2g_0 - 2$. Agora, suponha W um divisor canônico de F/K. Tome A um divisor, tal que $gr(A) > \max\{2g - 2, 2g_0 - 2\}$. Então, pelo Teorema 5.3.3 temos que $l(A) = gr(A) + 1 - g$ e temos q $l(A) = gr(A) + 1 - g_0$. Portanto, $g = g_0$. Além disso, fazendo $A = W$ na hipótese, obtemos:

$$l(W) = gr(W) + 1 - g + l(W_0 - W)$$

$$g = (2g - 2) + 1 - g + l(W_0 - W)$$

Assim, $l(W_0 - W) = 1$ e $gr(W_0 - W) = 0$ ou seja, $W_0 - W$ é divisor principal e portanto $W_0 \sim W$. □

Proposição 6.1.2. *Um divisor $B \in \mathrm{Div}(F)$ é um divisor canônico se, e somente se, $gr(B) = 2g - 2$ e $l(B) \geq g$.*

Demonstração. ($\Rightarrow$) Segue diretamente do Corolário 5.3.2.

($\Leftarrow$) Suponhamos que $gr(B) = 2g - 2$ e $l(B) \geq g$. Tome W um divisor canônico, então:

$$g \leq l(B) = gr(B) + 1 - g + l(W - B) = g - 1 + l(W - B)$$

Assim, $l(W - B) \geq 1$.

Agora, $gr(W) = gr(B) = 2g - 2$, implica que $gr(W - B) = 0$. Logo, segue, do Corolário 4.2.9, que $W \sim B$. □

6.2 CARACTERIZAÇÃO DO CORPO DE FUNÇÕES RACIONAIS

O próximo resultado apresenta uma caracterização do corpo de funções racionais.

Proposição 6.2.1. *Para um corpo de funções F/K as seguintes condições são equivalentes:*

1. *$F = K(x)$, para algum x transcendente sobre o corpo K.*
2. *F/K tem gênero 0 e existe divisor $A \in \mathrm{Div}(F)$ com $gr(A) = 1$.*

Demonstração. (*1* $\Rightarrow$ *2*) Esta implicação foi feita no Exemplo 4.2.15.

(*2* $\Rightarrow$ *1*) Seja $g = 0$ e $gr(A) = 1$. Como $gr(A) > 2g - 1$, segue que

$$l(A) = gr(A) + 1 - g = 2.$$

Então existe $A' \in \mathrm{Div}(F)$ tal que $A \sim A'$ e $A' \geq 0$. Como $l(A') = 2$, existe um elemento $x \in \mathcal{L}(A') \setminus K$ com $(x) \neq 0$ e $(x) + A' \geq 0$. Como $A' \geq 0$ e $gr(A') = 1$, isto é possível apenas se $A' = (x)_\infty$, o divisor polo de x. Assim,

$$[F : K(x)] = gr((x)_\infty) = gr(A') = 1$$

e, portanto, $F = K(x)$. □

6.3 LACUNAS DE WEIESTRASS

Para finalizar, vamos apresentar alguns resultados a respeito dos elementos de F que possuem apenas um polo. O principal resultado aqui será o Teorema das Lacunas de Weiestrass.

Proposição 6.3.1. *Seja $P \in \mathbb{P}_F$. Então para todo $n \geq 2g$ existe um elemento $x \in F$, com divisor polo $(x)_\infty = nP$.*

Demonstração. Pelo Teorema 5.3.3 sabemos que

$$l((n-1)\,P) = (n-1)gr(P) + 1 - g$$

e $l(n\,P) = ngr(P) + 1 - g$. Logo, $l(n\,P) - l((n-1)P) = 1$ e $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$.

Portanto, se $x \in \mathcal{L}(nP)\backslash\mathcal{L}((n-1)P)$, então $(x)+n\,P \geq 0$. Logo, $v_P(x) \geq -n$, mas como $v_P(x) < -(n-1)$, pois $x \notin \mathcal{L}((n-1)P)$, segue que $(x)_\infty = n\,P$. Então, todo elemento $x \in \mathcal{L}(n\,P) \setminus \mathcal{L}((n-1)P)$ tem nP como divisor de polos. □

Definição 6.3.2. *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado de número de polo de P se, e somente se, existe $x \in F$ com $(x)_\infty = nP$. Caso contrário, n é dito um número de lacunas de P.*

Definição 6.3.3. *Seja G um conjunto não vazio e $*$ uma operação em G, ou seja, uma função*

$$\begin{array}{rccc} * : & (G,G) & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b, \end{array}$$

tal que para todo a, b e $c \in G$ verifica-se que:

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

Dizemos que $(G,*)$ (ou simplesmente G) é um semigrupo.

Exemplo 6.3.4. O conjunto dos números naturais $\mathbb{N}$ é um semigrupo considerando a adição.

Observação 6.3.5. *i) Pela proposição anterior segue imediatamente que n é um número de polo de P se, e somente se, $l(nP) > l((n-1)P)$.*

ii) O conjunto dos números de polos de P é um sub-semigrupo do semigrupo aditivo $\mathbb{N}$. Basta notarmos que, se $(x_1)_\infty = n_1P$ e $(x_2)_\infty = n_2P$, então $(x_1x_2)_\infty = (n_1+n_2)P$.

Teorema 6.3.6 (Teorema das Lacunas de Weiestrass)**.** *Suponha que F/K tem gênero $g > 0$ e que P é um lugar de grau um. Então existem exatamente g números de lacunas $i_1 < \cdots < i_g$ de P. Além disso, $i_1 = 1$ e $i_g \leq 2g-1$.*

Demonstração. Pela Proposição 6.3.1 todo número lacunas de P é menor ou igual a $2g-1$. Sabemos que 0 é um número de polo, pois dado $x \in K$ temos que x não tem zeros e nem polos, e assim $(x)_\infty = 0$.

Temos a seguinte caracterização dos números de lacunas:

$$i \text{ é um número de lacunas de } P \iff \mathcal{L}((i-1)P) = \mathcal{L}(iP).$$

($\Rightarrow$) Suponhamos que i é um número lacunas de P. Logo, não existe $x \in F$ tal que $(x)_\infty = iP$. Seja $x \in \mathcal{L}(iP)$. Então $(x) \geq -iP$, ou seja, $(x) + iP \geq 0$. Segue então que x tem polo apenas em P e de ordem no máximo i. Mas, por hipótese, não existe x tal que $(x)_\infty = iP$. Portanto, a ordem do polo P em x é no máximo $i-1$. Logo, $x \in \mathcal{L}((i-1)P)$ e $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$.

($\Leftarrow$) Suponhamos que $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$ e i é um número de polo de P. Logo, existe $x \in F$ tal que $(x)_\infty = iP$, ou seja, $v_P(x) = -i$. Portanto, $x \in \mathcal{L}(iP)$ e $x \notin \mathcal{L}((i-1)P)$. Contradizendo o fato de $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$. Portanto, i é um número de lacunas de P.

Agora, consideremos a sequência de espaços vetoriais:

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

onde $\dim(\mathcal{L}(0)) = 1$ e, pelo Teorema 5.3.3, $\dim(\mathcal{L}((2g-1)P)) = g$.

Sabemos que

$$\dim\left(\frac{\mathcal{L}(iP)}{\mathcal{L}((i-1)P)}\right) \leq gr(iP) - gr((i-1)P).$$

Assim,

$$\dim(\mathcal{L}(iP)) \leq \dim(\mathcal{L}((i-1)P)) + 1$$

para todo i. Portanto, temos uma sequência de espaços vetoriais com exatamente $g-1$ números i, $1 \leq i \leq 2g-1$, satisfazendo a condição $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Pois, se tal número fosse maior que $g-1$, teríamos que $\dim(\mathcal{L}(iP)) > \dim(\mathcal{L}((i-1)P))$, para pelo menos g índices. Donde seguiria que $\dim(\mathcal{L}((2g-1)P)) > g$, o que é uma contradição. Se tal número fosse menor que $g-1$, com $\dim(\mathcal{L}(0)) = 1$ e $\dim(\mathcal{L}((2g-1)P)) = g$, teríamos $\dim(\mathcal{L}(iP)) \geq \dim(\mathcal{L}(i-1)P) + 1$ para algum i, o que também é uma contradição.

Os g números restantes são exatamente os números de lacunas de P.

Resta provar que 1 é de fato um número lacunas de P. Suponha que 1 não seja um número lacunas de P, ou seja, que 1 seja um número de polos de P. Pela Observação 6.3.5, os números polos formam um sub-semigrupo aditivo dos números naturais. Assim, todo $n \in \mathbb{N}$ seria um número de polo de P, o que contradiz o fato de $g > 0$. □

7 CONSIDERAÇÕES FINAIS

A teoria de corpos de funções algébricas se desenvolve sob o pilar de ferramentas simples de Álgebra. Com um pouco da teoria de Álgebra e da Álgebra Linear conseguimos definir e caracterizar elementos importantes como divisores e gênero de corpos de funções algébricas. Os conceitos desenvolvidos nesta teoria nos permite dar uma demonstração simples do Teorema de Riemann-Roch.

A teoria de divisores sobre corpos de funções algébricas se estende para variedades algébricas afins e projetivas. Em particular, com os conceitos de espaço de Riemann-Roch, divisores de Weil e adele sobre curvas projetivas irredutíveis prova-se novamente o Teorema de Riemann-Roch. Através dele pode-se classificar e caracterizar curvas quanto ao seu gênero.

A teoria apresentada neste trabalho também é usada no estudo dos códigos de Goppa.

REFERÊNCIAS

[1] CALLIOLI, Carlos A.; DOMINGUES, Hygino H.; COSTA, Roberto C. F.. **Álgebra Linear e Aplicações**. 6. ed. rev. São Paulo : Atual, 1990.

[2] CHEVALLEY, Claude. **Introduction to theory of algebraic functions of one variable**. AMS Math. Survey Nº 6, 1951.

[3] DEURING, Max. **Lectures on the theory of algebraic functions of one variable**. Lectures Notes in Math. Springer-Verlag, Berlin- Heidelberg -New York, 1973.

[4] GARCIA, Arnaldo L. P.; LEQUAIN, Yves A..**Elementos de Álgebra**. 6. ed. Rio de Janeiro: IMPA, 2012.

[5] GONÇALVES, Adilson. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2015.

[6] HOFFMAN, Kenneth; KUNZE, Ray. **Linear Algebra**. 2. ed. New Jersey: Prentice Hall, INC., 1971.

[7] HUNGERFORD, Thomas W.. **Algebra**. New York: Springer, 1974.

[8] LANG, S. **Algebra**. 3.ed. New York: Springer, 2002.

[9] STICHTENOTH, Henning. **Algebraic Functions Fields and Codes**. 2. ed. New York: Springer, 2009.