Universidade Federal de Juiz de Fora

Departamento de Matemática - ICE

Programa de Mestrado Acadêmico em Matemática

Mariana de Almeida Nery Coutinho

Corpos de Funções com um Número Prescrito de Lugares de Grau Superior

Juiz de Fora

2015

Mariana de Almeida Nery Coutinho

Corpos de Funções com um Número Prescrito de Lugares de Grau Superior

Dissertação apresentada ao Programa de Mestrado Acadêmico em Matemática do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2015

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

Coutinho, Mariana de Almeida Nery.
Corpos de Funções com um Número Prescrito de Lugares de Grau Superior / Mariana de Almeida Nery Coutinho. – 2015.
147 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Departamento de Matemática - ICE. Programa de Mestrado Acadêmico em Matemática, 2015.

1. Corpos Finitos. 2. Corpos de Funções. 3. Corpos de Funções sobre Corpos Finitos. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

MARIANA DE ALMEIDA NERY COUTINHO

CORPOS DE FUNÇÕES COM UM NÚMERO PRESCRITO DE LUGARES DE GRAU SUPERIOR

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

Beatriz C. M. R.

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

Flaviana Andrea Ribeiro

Profª. Drª. Flaviana Andrea Ribeiro
Mestrado Acadêmico em Matemática
UFJF

Prof. Dr. Herivelto Martins Borges Filho
ICMC - USP

Juiz de Fora, 10 de março de 2015.

Às minhas avós, Idelacy e Ondina, à minha tia Flávia, e à memória dos meus avôs Newton e Jean.

AGRADECIMENTOS

A Deus em primeiro lugar.

Aos meus pais e irmão, pelo incentivo incessante e por terem sido os meus primeiros professores. Aos meus avós, tios e primos, por todo o apoio. Aos meus tios de coração, Solange, Carlúcio, Glória, Nelson e Cida, e primos de coração, Mari e Juninho, por todo o carinho.

À professora e orientadora Beatriz Casulari da Motta Ribeiro, por ter me proporcionado as primeiras oportunidades de estudar e conhecer a Álgebra, desde a Introdução à Teoria dos Números até os Corpos de Funções sobre Corpos Finitos; pela alegria com que explicava cada tópico em suas aulas e horários de atendimento; pelo exemplo de pessoa, professora e orientadora; e, especialmente, pela amizade, apoio e incentivo durante todo esse período, que contribuíram de forma fundamental para as escolhas acadêmicas que fiz.

À professora Flaviana Andrea Ribeiro, por ter me ensinado boa parte do que hoje sei sobre Álgebra, motivando, a cada aula e horário de atendimento, o meu interesse por essa área; por ter me apresentado as primeiras noções de Geometria Algébrica; e, nesta última fase, por toda a ajuda com a avaliação e correção deste trabalho.

Ao professor Herivelto Martins Borges Filho, por ter aceitado o convite para fazer parte da banca que avaliou este trabalho, contribuindo com sugestões e questões de grande importância.

Ao professor Frederico Sercio Feitosa, pelas contribuições para este trabalho.

A cada um dos meus professores da graduação, por tudo que ensinaram e contribuíram para o meu crescimento acadêmico e pessoal. Em especial, agradeço ao professor Regis Castijos Alves Soares Junior, por toda a ajuda nas decisões que tive que tomar ao longo dos últimos anos.

Ao professor Carlos Alberto Santana Soares, por ter contribuído para que eu gostasse um pouquinho mais de Análise; à professora Valeria Mattos da Rosa, por ter me feito entender um pouco mais sobre as Equações Diferenciais Ordinárias; aos professores Laercio José dos Santos e Luis Fernando Crocco Afonso, por terem

despertado o meu interesse pela Geometria e, sobretudo, por todo o apoio.

Ao professor Maikel Yusat Ballester Furones, pela enorme contribuição para a minha formação acadêmica e pessoal enquanto sua aluna de Iniciação Científica.

Às minhas amigas de infância, por todos os momentos especiais.

Ao amigo Bruno Marques, pelo apoio incondicional.

Ao amigo Eli Vilela, pelas conversas sobre Matemática e diversos outros assuntos.

Às amigas Delizett, Isabela e Rosana, por todo o carinho e ajuda.

A todos os meus amigos da graduação. Em especial, agradeço à Adriele, à Janaína e ao Leandro, amigos que estiveram sempre ao meu lado compartilhando momentos de alegria e estudo, bem como me ajudando nos momentos mais difíceis; à Patrícia e à Priscila, por todo o carinho; ao Gladston, pela enorme companhia durante as aulas de Álgebra Linear, por todas as risadas e por toda a ajuda no momento em que decidi cursar Matemática.

A todos os meus amigos do mestrado, em especial à Sandra, pelo exemplo que foi para mim durante todos esses anos; ao Weslley, pela ajuda, juntamente com a Sandra, para que diversos problemas pudessem ser resolvidos; à Eliza, pela companhia e amizade ao longo dos últimos dois anos; à Yulia, ao Vladimir, ao Julio, à Lívia, à Taís e ao Erasmo, pelos momentos de estudo e descontração; ao Eduardo e ao Pavel, por toda a ajuda com os problemas de Geometria Diferencial e Medida e Integração; ao Carlos, pela amizade e pelas dicas sobre o latex; ao Juan, pela amizade, pelas conversas sobre o Peru, além da ajuda e explicações nas aulas de Álgebra; ao Oscar, por todo o apoio; ao Santiago, por toda a companhia, bem como por todas as conversas e explicações de espanhol; e à Gisele, pelo grande exemplo.

À Universidade Federal de Juiz de Fora e ao Departamento de Matemática.

À FAPEMIG pela bolsa de Mestrado.

"In learning you will teach
And in teaching you will learn"
Son of Man (Phil Collins)

RESUMO

O estudo das curvas algébricas sobre corpos finitos, o qual está intrinsecamente relacionado à teoria dos corpos de funções sobre corpos finitos, é de grande interesse na álgebra abstrata, com destaque para aplicações na teoria dos números e na teoria dos códigos. Com essa motivação, estamos aqui interessados em estudar a existência de corpos de funções $F/\mathbb{F}_q$ com um número prescrito de lugares de determinados graus, estando baseados em algumas seções do artigo de ANBAR e STICHTENOTH (2013). Para isso, faremos também uma abordagem acerca da teoria geral dos corpos de funções, apresentando os principais elementos que nos auxiliarão na compreensão dos resultados anteriormente mencionados.

Palavras-chave: Corpos Finitos. Corpos de Funções. Corpos de Funções sobre Corpos Finitos.

ABSTRACT

The study of algebraic curves over finite fields, which is intrinsically related to the theory of function fields over finite fields, is of great interest in abstract algebra, especially for applications in number theory and coding theory. With this motivation, we are here interested in studying the existence of function fields with a prescribed number of places of certain degrees, based on some sections of the paper of ANBAR and STICHTENOTH (2013). For this, we will also make a study of the general theory of function fields, showing the main elements that will assist us in understanding the results mentioned above.

Key-words: Finite Fields. Function Fields. Function Fields over Finite Fields.

SUMÁRIO

1 INTRODUÇÃO

O estudo das curvas algébricas sobre corpos finitos é de grande importância na álgebra abstrata, com destaque para aplicações na teoria dos números e na teoria dos códigos. Tal assunto pode também ser abordado do ponto de vista dos corpos de funções sobre corpos finitos, linguagem esta que será empregada ao longo deste trabalho. Nesse sentido, surgem algumas questões no estudo da teoria das curvas algébricas sobre corpos finitos, traduzidas aqui na linguagem de corpos de funções.

Por exemplo, podemos construir códigos corretores de erros, como o código de Goppa clássico, considerando n lugares racionais distintos $P_1, \ldots, P_n$ de um corpo de funções $F/\mathbb{F}_q$ e um divisor G de F com suporte disjunto de $\{P_1, \ldots, P_n\}$. Nesse caso, o código de Goppa $C_{\mathcal{L}}(D, G) \subseteq \mathbb{F}_q^n$ é definido por

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n));\ f \in \mathcal{L}(G)\},$$

onde $D = P_1 + \ldots + P_n$ e $\mathcal{L}(G)$ é o espaço de Riemann-Roch associado a G. Os parâmetros $[n, k, d]$ (comprimento, dimensão e distância mínima) de um código de Goppa dependem do número $N = N(F)$ de lugares racionais considerados e do gênero $g = g(F)$ do corpo de funções $F/\mathbb{F}_q$, dentre outras constantes. É interessante ainda que g seja pequeno em relação a N.

Dessa forma, a seguinte questão torna-se interessante: em que condições é possível garantir a existência de um corpo de funções sobre $\mathbb{F}_q$ com gênero g e exatamente N lugares racionais? Em outras palavras, deseja-se estudar o seguinte conjunto

$$\mathcal{M}_q(g) = \{N \in \mathbb{N};\ \text{existe um corpo de funções } F/\mathbb{F}_q \text{ tal que } g(F) = g \text{ e } N(F) = N\}.$$

Um primeiro resultado nesse sentido pode ser encontrado no Teorema 1.1 em ELKIES et al. (2004):

Teorema 1.1.1. *Existe uma constante $c > 0$ tal que, para toda potência q de um número primo e para qualquer inteiro $g \geqslant 0$,*

$$N_q(g) := max\, \mathcal{M}_q(g) \geqslant c\, log\, (q)\, .\, g.$$

Em outras palavras, para todo $g \geqslant 0$ *existe um corpo de funções* F *sobre* $\mathbb{F}_q$ *com* $g(F) = g$ *e* $N(F) \geqslant \gamma_q \, . \, g$, *onde* $\gamma_q = c \log(q) > 0$.

Modificando um pouco o foco de interesse, podemos ainda estudar o conjunto

$$\mathcal{M}_q = \{(N, g);\ \text{existe um corpo de funções } F/\mathbb{F}_q \text{ tal que } g(F) = g \text{ e } N(F) = N\}.$$

Nesse sentido, temos o teorema a seguir (ANBAR e STICHTENOTH, 2013):

Teorema 1.1.2. *Para toda potência* q *de um número primo, existem constantes* a_q, $b_q > 0$ *tais que*

$$\{(N, g);\ g \geqslant a_q \, . \, N + b_q\} \subseteq \mathcal{M}_q.$$

Notemos que, escrevendo $\alpha_q = a_q^{-1}$ e $\beta_q = a_q^{-1} \, b_q$, o Teorema 1.1.2 nos dá que para todo inteiro $g \geqslant 0$ e todo inteiro N tal que $0 \leqslant N \leqslant \alpha_q g - \beta_q$, existe um corpo de funções $F/\mathbb{F}_q$ com gênero g e N lugares racionais.

Ainda, o teorema anterior aprimora o seguinte resultado (STICHTENOTH, 2011):

Teorema 1.1.3. *Dados um corpo finito* $\mathbb{F}_q$ *e um inteiro* $N \geqslant 0$, *existe um inteiro* g_0 *tal que para todo* $g \geqslant g_0$ *existe um corpo de funções sobre* $\mathbb{F}_q$ *com gênero* g *e exatamente* N *lugares racionais.*

Voltando aos códigos corretores de erros, notemos que a construção clássica utiliza como lugares base apenas lugares racionais do corpo de funções $F/\mathbb{F}_q$. Porém, há também construções que utilizam lugares de graus maiores e que contornam o problema de encontrar um número grande de lugares racionais em relação ao gênero do corpo de funções. Em NIEDERREITER et. al. (1999), os autores apresentam uma construção que generaliza a clássica, cujos objetos utilizados são um corpo de funções $F/\mathbb{F}_q$ de gênero g, $P_1, \ldots, P_s$ lugares de $F/\mathbb{F}_q$ tais que $deg(P_i) = k_i \in \mathbb{N}$, para $i = 1, \ldots, s$, B um divisor não-especial e $A \geqslant 0$ um divisor com suporte disjunto de $\{P_1, \ldots, P_s\}$. O código é então definido como a imagem do espaço de Riemann-Roch $\mathcal{L}(B + P_1 + \cdots + P_s - A)$ por certa aplicação que não definiremos aqui mas que possui imagem contida em $\mathbb{F}_q^n$, onde $n = k_1 + \cdots + k_s$.

Torna-se importante, dessa forma, garantir a existência de um corpo de funções de gênero g e com número de lugares de graus superiores fixados. Nesse sentido, e como uma generalização do Teorema 1.1.3, temos o próximo resultado (ANBAR e STICHTENOTH, 2013):

Teorema 1.1.4. *Sejam $\mathbb{F}_q$ um corpo finito e $b_1, \ldots, b_m$ inteiros não negativos. Então existe um inteiro $g_0 \geqslant 0$ com a seguinte propriedade: para todo $g \geqslant g_0$ existe um corpo de funções $F/\mathbb{F}_q$ com gênero g tal que $F/\mathbb{F}_q$ possui exatamente b_r lugares de grau r, para $r = 1, \ldots, m$.*

Com esse teorema como objetivo, apresentaremos a seguir a divisão de capítulos que nos conduzirá a ele.

No Capítulo 2, coletamos alguns resultados clássicos da álgebra abstrata que nos auxiliarão na compreensão dos demais capítulos.

No Capítulo 3, iniciamos o estudo sobre a teoria geral dos corpos de funções, abordando desde as primeiras definições até resultados importantes como o Teorema de Riemann-Roch.

No Capítulo 4, estudamos um pouco sobre extensões de corpos de funções, apresentando, dentre outros, o Teorema de Kummer e a Fórmula do Gênero de Hurwitz. Além disso, fazemos uma introdução às extensões de Artin-Schreier.

Por último, no Capítulo 5, fazemos um estudo dos Teoremas 1.1.2 e 1.1.4 anteriormente apresentados, com base nas seções 1, 2, 3, 5 e 6 do artigo de ANBAR e STICHTENOTH (2013).

2 FUNDAMENTOS ALGÉBRICOS

O objetivo deste capítulo é apresentar algumas definições e resultados clássicos que serão necessários para o desenvolvimento dos demais assuntos a serem apresentados neste trabalho.

2.1 EXTENSÕES DE CORPOS

Definição 2.1.1. Sejam F e K corpos. Dizemos que F é uma extensão de K, e escrevemos F/K, se K for um subcorpo de F, isto é, se $K \subseteq F$, $(K, +)$ for subgrupo de $(F, +)$ e $(K \setminus \{0\}, \cdot)$ for subgrupo de $(F \setminus \{0\}, \cdot)$.

Observação 2.1.2. Se F é uma extensão do corpo K, então as operações

$$\begin{array}{rccc} + : & F \times F & \to & F \\ & (u, v) & \mapsto & u + v \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot : & K \times F & \to & F \\ & (\lambda, u) & \mapsto & \lambda \cdot u \end{array}$$

fazem de F um espaço vetorial sobre K.

Desse modo, chegamos à seguinte definição para uma extensão F de K.

Definição 2.1.3. Chamamos de grau da extensão a dimensão de F como espaço vetorial sobre K. Tal dimensão será denotada por $[F : K]$. Ainda, dizemos que F é uma extensão finita de K se $[F : K] < \infty$. Caso contrário, dizemos que F é uma extensão infinita de K.

Teorema 2.1.4. *Sejam F/K e L/F extensões finitas de corpos. Então L/K é uma extensão finita, com*

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

Demonstração. Pode ser encontrada em [15] (Teorema 4.2). ■

Definição 2.1.5. Seja F uma extensão do corpo K. Dizemos que $u \in F$ é algébrico sobre K se existe $p(T) \in K[T] \setminus \{0\}$ tal que $p(u) = 0$. Caso contrário, dizemos que u é transcendente sobre K. Ainda, dizemos que o corpo F é uma extensão algébrica do corpo K se $u \in F$ é algébrico sobre K, para todo $u \in F$. Se pelo

menos um elemento de F for transcendente sobre K, dizemos que F é uma extensão transcendente de K.

Definição 2.1.6. Seja $\alpha \in F$ um elemento algébrico sobre K. O polinômio $m(T) \in K[T]$ mônico de menor grau tal que $m(\alpha) = 0$ é chamado polinômio minimal de α e denotado por $irr(\alpha, K)$.

Segue da Definição 2.1.6 que o polinômio minimal $irr(\alpha, K)$ é o único polinômio mônico irredutível que anula α. Além disso, se $q(T) \in K[T]$ é um outro polinômio tal que $q(\alpha) = 0$, então $irr(\alpha, K)|q(T)$.

Definição 2.1.7. Sejam F um corpo e $X \subseteq F$ um subconjunto qualquer. O subcorpo gerado por X é a interseção de todos os subcorpos de F que contêm X. Se K é um subcorpo de F e $X \subseteq F$, então o subcorpo gerado por $K \cup X$ é dito corpo obtido de K adjuntando X e é denotado por $K(X)$.

Se o subconjunto X de F é finito, digamos $X = \{\alpha_1, \ldots, \alpha_n\}$, então escrevemos $K(X) = K(\alpha_1, \ldots, \alpha_n)$.

Definição 2.1.8. Dizemos que um corpo F é uma extensão simples do corpo K se existe $\alpha \in F$ tal que $F = K(\alpha)$. Neste caso, α é chamado elemento definidor de F sobre K.

Teorema 2.1.9. *Seja F/K uma extensão de corpos. Então F/K é uma extensão finita se, e somente se, F/K é uma extensão algébrica e existe um número finito de elementos $\alpha_1, \ldots, \alpha_s \in F$ tais que $F = K(\alpha_1, \ldots, \alpha_s)$.*

Demonstração. Pode ser encontrada em [15] (Lema 4.4). ■

Teorema 2.1.10. *Sejam F uma extensão do corpo K e $\alpha \in F$. Então α é algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K.*

Demonstração. ($\Rightarrow$) Pode ser encontrada em [15] (Proposição 4.3).
($\Leftarrow$) Segue do Teorema 2.1.9. ■

Teorema 2.1.11. *Sejam L/F e F/K extensões de corpos. Então L/K é uma extensão algébrica se, e somente se, L/F e F/K são extensões algébricas.*

Demonstração. Supondo que L/K é uma extensão algébrica, temos que o resultado segue da definição de extensão algébrica e do fato de $K \subseteq F \subseteq L$. A recíproca pode ser encontrada em [11] (Teorema 1.13, Cap. V). ■

2.2 CORPO DE DECOMPOSIÇÃO

Definição 2.2.1. Sejam K é um corpo e $f(T) \in K[T]$. Dizemos que $f(T)$ fatora-se em $K[T]$ se $f(T)$ pode ser escrito como o produto de fatores lineares

$$f(T) = c(T - \alpha_1) \dots (T - \alpha_n),$$

com c, $\alpha_1, \dots, \alpha_n \in K$.

Nas condições da Definição 2.2.1, temos que os zeros de $f(T)$ em K são exatamente os elementos $\alpha_1, \dots, \alpha_n$. Além disso, se F é uma extensão de K, então $f(T)$ também pertence a $F[T]$. Dessa forma, podemos falar na fatoração de $f(T)$ em $F[T]$, significando que $f(T)$ é o produto de fatores lineares com coeficientes em F.

Definição 2.2.2. Sejam K um corpo e Σ uma extensão de K. Então Σ é um corpo de decomposição para o polinômio $f(T) \in K[T]$ se:

a) $f(T)$ fatora-se em $\Sigma[T]$.

b) Se $K \subseteq \Sigma' \subseteq \Sigma$ e $f(T)$ fatora-se em $\Sigma'[T]$, então $\Sigma = \Sigma'$, ou seja, Σ é o menor corpo que contém K e todas as raízes de $f(T)$.

A seguir, apresentaremos dois resultados que podem ser encontrados em [15] (Teoremas 8.1 e 8.2).

Teorema 2.2.3. *Se K é um corpo qualquer e $f(T) \in K[T]$, então existe um corpo de decomposição de $f(T)$ sobre K.*

Seja $i : K \to F$ um homomorfismo injetor entre corpos. Definimos a aplicação $\hat{i} : K[T] \to F[T]$ como

$$\hat{i}(a_0 + a_1T + \ldots + a_nT^n) = i(a_0) + i(a_1)T + \ldots + i(a_n)T^n\,.$$

Desse modo, $\hat{i}$ é um homomorfismo injetor. Além disso, se i for um isomorfismo, $\hat{i}$ também será. Temos ainda a unicidade do corpo de decomposição de um polinômio $f(T)$ sobre um corpo K no sentido do teorema a seguir.

Teorema 2.2.4. *Seja $i : K \to K'$ um isomorfismo entre corpos. Sejam Σ um corpo de decomposição de $f(T) \in K[T]$ e Σ' um corpo de decomposição de $\hat{i}(f(T))$ sobre K'. Então existe um isomorfismo $j : \Sigma \to \Sigma'$ tal que $j|_K = i$. Em outras palavras, as extensões Σ e Σ' são isomorfas.*

Como consequência do Teorema 2.2.4, temos que polinômios possuem corpos de decomposição isomorfos.

2.3 MERGULHOS E $K-$ISOMORFISMOS

Definição 2.3.1. Sejam F_1/K e F_2/K extensões de corpos. Um homomorfismo de corpos $\sigma : F_1 \to F_2$ é chamado um mergulho de F_1 em F_2 sobre K se $\sigma(a) = a$, para todo $a \in K$. Se ainda σ for sobrejetor, diremos que σ é um $K-$isomorfismo.

Observação 2.3.2. Seja σ um mergulho de F_1 em F_2 sobre K. Notemos que, como σ é injetor, temos que F_1 é isomorfo a um subcorpo de F_2, a saber $\sigma(F_1)$.

2.4 FECHO ALGÉBRICO

Definição 2.4.1. Um corpo Φ é dito algebricamente fechado se todo polinômio $f(T) \in \Phi[T]$, tal que $deg(f(T)) \geqslant 1$, possui pelo menos uma raiz em Φ.

Teorema 2.4.2. *Para todo corpo K existe uma extensão algébrica Φ/K, onde Φ é um corpo algebricamente fechado. Ainda, a extensão anterior é única a menos de $K-$isomorfismos.*

Demonstração. Pode ser encontrada em [11] (Teorema 3.6, Cap. V). ■

Definição 2.4.3. À extensão algébrica apresentada no Teorema 2.4.2 damos o nome de fecho algébrico do corpo K.

2.5 POLINÔMIOS E EXTENSÕES SEPARÁVEIS

Definição 2.5.1. Sejam K um corpo e $f(T) \in K[T]$ um polinômio irredutível. Dizemos que $f(T)$ é separável sobre K se $f(T)$ não possui raízes múltiplas em um corpo de decomposição.

Definição 2.5.2. Seja K um corpo. Um polinômio arbitrário em $K[T]$ é separável sobre K se todos os seus fatores irredutíveis são separáveis sobre K.

Proposição 2.5.3. *Seja K um corpo. Um polinômio irredutível $f(T) \in K[T]$ é separável se, e somente se, $f'(T) \neq 0$.*

Proposição 2.5.4. *Seja K um corpo. Se a característica de K é zero, então todo polinômio irredutível em $K[T]$ é separável sobre K. Se, contudo, a característica de K é um número primo p, então um polinômio irredutível $f(T) = \sum_{i=0}^{n} a_i T^i \in K[T]$ é separável sobre K se, e somente se, $a_i \neq 0$ para algum $i \not\equiv 0 \pmod{p}$.*

As Proposições 2.5.3 e 2.5.4 podem ser encontradas em [12] (Proposição 1.11, Cap. IV) e em [15] (Proposição 8.6), respectivamente.

Definição 2.5.5. Seja F/K uma extensão algébrica. Um elemento $\alpha \in F$ é dito separável sobre K se o seu polinômio minimal $irr(\alpha, K)$ é separável sobre K. A extensão F/K é dita separável se todos os elementos de F são separáveis sobre K.

Definição 2.5.6. Um corpo K é dito perfeito se todas as extensões algébricas F de K são separáveis.

Proposição 2.5.7. *Um corpo K de característica $p > 0$ é perfeito se, e somente se, para todo elemento $\alpha \in K$ tivermos $\alpha = \beta^p$, para algum $\beta \in K$.*

Demonstração. Pode ser encontrada em [2] (Teorema 8.2.6). ■

Teorema 2.5.8. *Seja Φ um corpo algebricamente fechado contendo o corpo K e suponhamos que F/K é uma extensão finita de grau $[F : K] = n$. Se F/K é separável, então existem precisamente n mergulhos distintos $\sigma_1, \ldots, \sigma_n : F \to \Phi$ sobre K.*

Demonstração. Pode ser encontrada em [15] (Teorema 10.6). ■

Proposição 2.5.9. *Consideremos as extensões algébricas de corpos L/F e F/K. Então L/K é uma extensão separável se, e somente se, L/F e F/K são extensões separáveis.*

Demonstração. ($\Rightarrow$) Esta implicação pode ser encontrada em [15] (Lema 8.7). ($\Leftarrow$) Esta implicação pode ser encontrada em [11] (Corolário 6.8, Cap. V). ■

Proposição 2.5.10. *Seja K um corpo perfeito. Então toda extensão algébrica F de K também é perfeita.*

Demonstração. A demonstração deste resultado segue da Proposição 2.5.9. ■

Teorema 2.5.11 (Teorema do Elemento Primitivo)**.** *Seja F uma extensão finita do corpo K. Se F/K é uma extensão separável, então F/K é uma extensão simples.*

Demonstração. Pode ser encontrada em [11] (Proposição 6.15, Cap. V). ■

Definição 2.5.12. Consideremos uma extensão algébrica F/K, onde a característica de K é um número primo p. Um elemento $\gamma \in F$ é dito puramente inseparável sobre K se $\gamma^{p^r} \in K$ para algum $r \geqslant 0$. A extensão F/K é dita puramente inseparável se todos os elementos de F são puramente inseparáveis sobre K.

Observação 2.5.13. Nas condições da Definição 2.5.12, temos que o polinômio minimal de γ sobre K possui a forma $f(T) = T^{p^r} - e$ para algum $e \in K$. Este fato pode ser encontrado em [11] (Teorema 6.4, Cap. V).

2.6 EXTENSÕES DE GALOIS

Definição 2.6.1. Para um extensão F/K, definimos o grupo de $K-$automorfismos de F sobre K como

$$Aut(F/K) = \{\sigma : F \to F;\ \sigma \text{ é um automorfismo e } \sigma(k) = k,\ \text{para todo } k \in K\}.$$

Proposição 2.6.2. *Nas condições anteriores, se F/K é uma extensão finita, então $|Aut(F/K)| \leqslant [F : K]$.*

Demonstração. Pode ser encontrada em [11] (Lema 2.8, Cap. V). ■

Definição 2.6.3. Ainda nas condições da Proposição 2.6.2, temos que a extensão F/K é dita uma extensão de Galois se $|Aut(F/K)| = [F : K]$. Neste caso escrevemos $Gal(F/K) = Aut(F/K)$.

Teorema 2.6.4. *Seja F/K uma extensão finita. Então, são equivalentes:*

a) *F/K é uma extensão de Galois.*

b) *F é o corpo de decomposição sobre K de r polinômios separáveis em $K[T]$.*

c) *F/K é uma extensão separável e todo polinômio irredutível $p(T) \in K[T]$ que possui uma raiz em F fatora-se em $F[T]$.*

Demonstração. Pode ser encontrada em [11] (Teorema 3.11, Cap. V). ■

Definição 2.6.5. Uma extensão de Galois F/K é dita cíclica se $Gal(F/K)$ é um grupo cíclico.

Como exemplos de extensões de Galois cíclicas, temos as extensões de Artin-Schreier, que serão estudas na Seção 4.7.

2.7 NORMA E TRAÇO DE EXTENSÕES DE CORPOS

Definição 2.7.1. Seja F/K uma extensão de corpos de grau $[F : K] = n < \infty$. Cada elemento $\alpha \in F$ determina uma transformação linear $\mu_\alpha : F \to F$ definida por $\mu_\alpha(z) = \alpha \,.\, z$, para todo $z \in F$. Definimos a norma e o traço de α com respeito à extensão F/K como

$$N_{F/K}(\alpha) = det\,(\mu_\alpha)$$

e

$$Tr_{F/K}(\alpha) = \text{Traço}\,(\mu_\alpha),$$

respectivamente.

Observação 2.7.2. Consideremos as condições da Definição 2.7.1. Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de F/K e

$$\alpha \,.\, \alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \text{ com } a_{ij} \in K,$$

então

$$N_{F/K}(\alpha) = det\,(a_{ij})_{1 \leqslant i,\, j \leqslant n}$$

e

$$Tr_{F/K}(\alpha) = \sum_{i=1}^{n} a_{ii}.$$

Proposição 2.7.3. *Nas condições da Definição 2.7.1, temos que as funções norma e traço possuem as seguintes propriedades:*

a) *Para todos* $\alpha, \beta \in F$, $N_{F/K}(\alpha \,.\, \beta) = N_{F/K}(\alpha) \,.\, N_{F/K}(\beta)$.

b) $N_{F/K}(\alpha) = 0$ *se, e somente se,* $\alpha = 0$.

c) *Para todo* $a \in K$, $N_{F/K}(a) = a^n$.

d) *Para todos* $\alpha, \beta \in F$ *e para todo* $a \in K$, *temos que*

$$Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta),$$

$$Tr_{F/K}(a \,.\, \alpha) = a \,.\, Tr_{F/K}(\alpha)$$

e

$$Tr_{F/K}(a) = n \,.\, a.$$

Em particular, $Tr_{F/K}$ *é uma transformação* $K-$*linear.*

e) *Se* L/F *é uma extensão finita, então*

$$N_{L/K}(\alpha) = N_{F/K}(N_{L/F}(\alpha))$$

e

$$Tr_{L/K}(\alpha) = Tr_{F/K}(Tr_{L/F}(\alpha)),$$

para todo $\alpha \in L$.

f) *A extensão F/K é separável se, e somente se, existe um elemento $\gamma \in F$ tal que $Tr_{F/K}(\gamma) \neq 0$. Notemos neste caso que, sendo os únicos subespaços de K o conjunto $\{0\}$ e próprio conjunto K, e $Tr_{F/K}$ uma aplicação linear, temos que existir um elemento $\gamma \in F$ tal que $Tr_{F/K}(\gamma) \neq 0$ implica que $Tr_{F/K}$ é uma aplicação sobrejetora.*

g) *Seja $\varphi(T) = T^r + a_{r-1}T^{r-1} + \ldots + a_0 \in K[T]$ o polinômio minimal de $\alpha \in F$ sobre K e escrevamos $[F : K] = n = r \,.\, s$, onde $s = [F : K(\alpha)]$. Então*

$$N_{F/K}(\alpha) = (-1)^n a_0^s$$

e

$$Tr_{F/K}(\alpha) = -sa_{r-1}.$$

h) *Suponhamos que F/K seja uma extensão separável. Consideremos os mergulhos $\sigma_1, \ldots, \sigma_n : F \to \Phi$ de F sobre K em um corpo algebricamente fechado $\Phi \supseteq K$. Então*

$$N_{F/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

e

$$Tr_{F/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

para todo $\alpha \in F$. Em particular, se F/K é uma extensão de Galois com grupo de Galois $G = Gal(F/K)$, então

$$N_{F/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

e

$$Tr_{F/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha),$$

para todo $\alpha \in F$.

Demonstração. Pode ser encontrada em [12] (Seção 5, Cap. VI). ■

2.8 EXTENSÕES TRANSCENDENTES

Definição 2.8.1. Seja F/K uma extensão de corpos. Um subconjunto finito $\{x_1, \ldots, x_n\} \subseteq F$ é algebricamente independente sobre K se não existe $f(T_1, \ldots, T_n)$ em $K[T_1, \ldots, T_n]$ satisfazendo $f(x_1, \ldots, x_n) = 0$. Um subconjunto arbitrário $S \subseteq F$ é algebricamente independente sobre K se todos os subconjuntos finitos de S são algebricamente independentes sobre K.

Definição 2.8.2. Uma base de transcendência da extensão F/K é um subconjunto $\mathcal{B}$ de F que satisfaz:

a) $\mathcal{B}$ é algebricamente independente.

b) $\mathcal{B} \subseteq \mathcal{B}'$ e $\mathcal{B}'$ é um subconjunto algebricamente independente de F, então $\mathcal{B} = \mathcal{B}'$.

Teorema 2.8.3. *Quaisquer duas bases de transcendência da extensão F/K possuem a mesma cardinalidade.*

Demonstração. Pode ser encontrada em [11] (Teorema 1.8, Cap. VI). ■

Definição 2.8.4. Sejam F/K uma extensão de corpos e $\mathcal{B}$ uma base de transcendência de F/K. À cardinalidade de $\mathcal{B}$ damos o nome de grau de transcendência de F/K, sendo esta denotada por $trdeg(F|K)$.

Proposição 2.8.5. *Para extensões de corpos L/F e F/K temos que:*

a) Se F é algébrico sobre $K(X)$, para algum subconjunto X de F, então X contém uma base de transcendência de F/K.

b) F/K é uma extensão algébrica se, e somente se, $trdeg(F|K) = 0$.

c) $trdeg(L|K) = trdeg(L|F) + trdeg(F|K)$.

Demonstração. Pode ser encontrada em [11] (Corolário 1.7 e Teorema 1.11, Cap. VI). ■

3 FUNDAMENTOS DA TEORIA DE CORPOS DE FUNÇÕES ALGÉBRICAS

3.1 LUGARES

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

Definição 3.1.2. Seja F/K um corpo de funções. O conjunto

$$\tilde{K} = \{z \in F;\ z \text{ é algébrico sobre } K\}$$

é um subcorpo de F denominado corpo de constantes de F/K.

Observação 3.1.3. Notemos que $K \subseteq \tilde{K} \subsetneq F$ e $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$.

Definição 3.1.4. Seja F/K um corpo de funções. Dizemos que K é algebricamente fechado em F se $\tilde{K} = K$.

Observação 3.1.5. Os elementos de F que são transcendentes sobre K podem ser caracterizados da seguinte forma

$z \in F$ é transcendente sobre K se, e somente se, a extensão $F/K(z)$ possui grau finito.

Com efeito

($\Leftarrow$) Seja $z \in F$ um elemento algébrico sobre K. Então $K(z)/K$ é uma extensão finita, de modo que sendo F/K um corpo de funções e, portanto, uma extensão infinita, temos que $F/K(z)$ é uma extensão infinita, uma vez que

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

($\Rightarrow$) Seja F/K um corpo de funções. Então F é uma extensão finita 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.

Também temos que o grau de transcendência de $K(x)/K$ é 1 e que

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

Então $[K(x, z) : K(x)] < \infty$, pois $[F : K(x)] = [F : K(x, z)] \, . \, [K(x, z) : K(x)]$. 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

$$trdeg(K(x, z)|K) = trdeg(K(x, z)|K(x)) + trdeg(K(x)|K),$$

temos que $trdeg(K(x, z)|K) = 1$. Agora,

$$trdeg(K(x, z)|K) = trdeg(K(x, z)|K(z)) + trdeg(K(z)|K)$$

nos dá que $trdeg(K(x, z)|K(z)) = 0$. Logo x é algébrico sobre $K(z)$. Portanto, analisando as extensões aqui trabalhadas, temos que $[F : K(z)] < \infty$.

Definição 3.1.6. Um anel de valorização de um corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:

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

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

Observação 3.1.7. As duas condições da Definição 3.1.6 nos dão que $\mathcal{O}$ é um domínio de integridade que não é um corpo, pois se $\mathcal{O}$ fosse um corpo, então a condição b) nos daria que $\mathcal{O} = F$, o que contraria a letra a).

Proposição 3.1.8. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K. Então:*

a) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ possui um único ideal maximal $P = \mathcal{O} \backslash \mathcal{O}^{\times}$, onde $\mathcal{O}^{\times} = \{z \in \mathcal{O}; \, z \text{ é } invertível\}$.

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

c) Se $\tilde{K}$ é o corpo de constantes de F/K, então $\tilde{K} \subseteq \mathcal{O}$ e $\tilde{K} \cap P = \{0\}$.

Demonstração. a) Primeiramente, afirmamos que P é um ideal em $\mathcal{O}$. Com efeito:

- Se $x \in P$ e $z \in \mathcal{O}$, então $xz \notin \mathcal{O}^\times$ (pois, caso contrário, teríamos que ter x invertível, o que seria uma contradição, pois $x \notin \mathcal{O}^\times$). Logo, $xz \in \mathcal{O}\backslash\mathcal{O}^\times = P$.
- Sejam x, $y \in P\backslash\{0\}$. Então, xy^{-1} e $yx^{-1} \in F$, de modo que $xy^{-1} \in \mathcal{O}$ ou $yx^{-1} \in \mathcal{O}$. Sem perda de generalidade, suponhamos que $xy^{-1} \in \mathcal{O}$. Então, $1 + xy^{-1} \in \mathcal{O}$, de modo que, $x + y = y(1 + xy^{-1}) \in P$ pelo item anterior.

Ainda, P é um ideal maximal, pois se $P \subsetneq J \subseteq \mathcal{O}$, então existe $a \in J$ tal que $a \notin P = \mathcal{O}\backslash\mathcal{O}^\times$, e assim a é invertível em $\mathcal{O}$, de modo que $J = \mathcal{O}$.

Agora, se M é um ideal maximal, então M não possui elementos invertíveis, de modo que $M \subseteq P \subsetneq \mathcal{O}$. Daí $M = P$, o que mostra que P é o único ideal maximal.

b) ($\Rightarrow$) Se $0 \neq x \in P$, então x^{-1} não pode pertencer a $\mathcal{O}$, pois se isso ocorresse, teríamos que x seria invertível em $\mathcal{O}$, o que seria uma contradição.

($\Leftarrow$) Agora, se $x^{-1} \notin \mathcal{O}$, então x não é invertível em $\mathcal{O}$, de forma que $x \in P = \mathcal{O}\backslash\mathcal{O}^\times$.

c) Seja $z \in \tilde{K}$ e suponhamos que $z \notin \mathcal{O}$. Então $z^{-1} \in \mathcal{O}$, pois $\mathcal{O}$ é um anel de valorização. Como z^{-1} é algébrico sobre K, existem elementos $a_1, \ldots, a_r \in K$, com

$$a_r(z^{-1})^r + \ldots + a_1(z^{-1}) + 1 = 0.$$

Logo

$$(z^{-1})(a_r(z^{-1})^{r-1} + \ldots + a_1) = -1,$$

de forma que $z = -(a_r(z^{-1})^{r-1} + \ldots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, o que é uma contradição com o fato de que $z \notin \mathcal{O}$. Portanto, $\tilde{K} \subseteq \mathcal{O}$. Agora, repetindo os passos anteriores, é possível mostrar que se $0 \neq z \in \tilde{K}$, então $z^{-1} \in \mathcal{O}$, de forma que z é invertível e assim $z \notin P$. Isso mostra que $P \cap \tilde{K} = \{0\}$. ■

Lema 3.1.9. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K, P o ideal maximal de $\mathcal{O}$ e $0 \neq x \in P$. Sejam $x_1, \ldots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, para $i = 1, \ldots, n-1$. Então $n \leqslant [F : K(x)] < \infty$.*

Demonstração. Pela Observação 3.1.5 e pela Proposição 3.1.8, temos que

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

Logo, é suficiente mostrarmos que $x_1, \ldots, x_n \in P \subseteq F$ são linearmente independentes sobre $K(x)$.

Suponhamos que exista uma combinação linear não trivial $\sum_{i=1}^{n} \varphi_i(x)x_i = 0$, onde $\varphi_i(x) \in K(x)$. Podemos assumir, sem perda de generalidade, que $\varphi_i(x) \in K[x]$ e que x não divide $\varphi_i(x)$ para todo i.

Neste caso, seja $a_i = \varphi_i(0)$ o termo constante de $\varphi_i(x)$ e definamos $j \in \{1, \ldots, n\}$ pela condição $a_j \neq 0$, mas $a_i = 0$, para todo $i > j$. Então obtemos

$$-\varphi_j(x)x_j = \sum_{i \neq j} \varphi_i(x)x_i,$$

com $\varphi_i(x) \in \mathcal{O}$, para todo $i = 1, \ldots, n$ (já que $x = x_1 \in P$), $x_i \in x_j P$, para $i < j$ e $\varphi_i(x) = xg_i(x)$, para $i > j$, onde $g_i(x) \in K[x]$. Assim

$$\begin{aligned} -\varphi_j(x) &= \sum_{i<j} \varphi_i(x)\frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i(x)x_i \\ &= \sum_{i<j} \varphi_i(x)\frac{x_j p_i}{x_j} + \sum_{i>j} \frac{x_j p}{x_j} g_i(x)x_i, \end{aligned}$$

com p, $p_i \in P$, de modo que o lado direito da igualdade anterior pertence à P.

Por outro lado, $\varphi_j(x) = a_j + xg_j(x)$, com $g_j(x) \in K[x] \subseteq \mathcal{O}$. Assim,

$$a_j = \varphi_j(x) - xg_j(x) \in P \cap K \subseteq P \cap \tilde{K} = \{0\}.$$

Mas isso é uma contradição, pois $a_j \neq 0$. ■

Teorema 3.1.10. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções F/K e P o único ideal maximal de $\mathcal{O}$. Então:*

a) P é um ideal principal.

b) Se $P = t\mathcal{O}$, então cada $z \in F\backslash\{0\}$ possui uma única representação na forma $z = t^n u$, para algum $n \in \mathbb{Z}$ e $u \in \mathcal{O}^\times$.

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

Demonstração. *a*) Suponhamos que P não seja um ideal principal. Então, escolhamos um elemento $0 \neq x_1 \in P$. Como $P \neq x_1\mathcal{O}$, existe $x_2 \in P \backslash x_1\mathcal{O}$. Então $x_2x_1^{-1} \notin \mathcal{O}$ (se $x_2x_1^{-1} \in \mathcal{O}$, então $x_2 = x_1(x_2 \,.\, x_1^{-1}) \in x_1\mathcal{O}$, o que seria uma contradição), donde $x_2^{-1} \,.\, x_1 \in P$, pela Proposição 3.1.8. Logo, $x_1 = x_2(x_2^{-1}x_1) \in x_2P$.

Utilizando o argumento anterior, podemos obter uma sequência

$$x_1,\, x_2, \ldots,\, x_n, \ldots$$

em P tal que $x_n \in P \backslash x_{n-1}\mathcal{O}$ e $x_{n-1} \in x_nP$, para todo $n \geqslant 2$, o que é uma contradição pelo Lema 3.1.9.

b) (*Existência*) Como z ou $z^{-1} \in \mathcal{O}$, podemos assumir, sem perda de generalidade, que $z \in \mathcal{O}$. Se $z \in \mathcal{O}^\times$, então $z = t^0z$. Seja agora $z \in P = t\mathcal{O}$. Então existe um elemento $m \geqslant 1$ máximo tal que $z \in t^m\mathcal{O}$, pois o comprimento da sequência

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

é limitado pelo Lema 3.1.9. Escrevamos $z = t^mu$, onde $u \in \mathcal{O}$. Então u deve pertencer a $\mathcal{O}^\times$, isto é, u deve ser invertível, pois, caso contrário,

$$u \in \mathcal{O} \backslash \mathcal{O}^\times = P = t\mathcal{O}$$

e assim $z \in t^{m+1}\mathcal{O}$, o que é um contradição, pois o valor m considerado é o máximo tal que $z \in t^m\mathcal{O}$.

(*Unicidade*) Suponhamos $z = ut^n = vt^m$, onde $u,\, v \in \mathcal{O}^\times$ e $m \geqslant n$. Então $uv^{-1} = t^{m-n}$, donde $m = n$ e $uv^{-1} = 1$, isto é, $m = n$ e $u = v$.

c) Seja $\{0\} \neq I \subseteq \mathcal{O}$ um ideal. O conjunto $A = \{r \in \mathbb{N};\, t^r \in I\}$ é não vazio (de fato, se $0 \neq x \in I$, então $x = t^ru$, onde $u \in \mathcal{O}^\times$, de modo que $t^r = u^{-1}x \in I$). Pelo Princípio da Boa Ordenação, A possui um menor elemento, de modo que podemos definir $n = min(A)$. Afirmamos agora que $I = t^n\mathcal{O}$. Com efeito, como $t^n \in I$, temos que $t^n\mathcal{O} \subseteq I$. Por outro lado, seja $0 \neq y \in I$. Então, $y = t^ru$, onde $u \in \mathcal{O}^\times$ e $r \geqslant 0$. Como $t^r = u^{-1}y \in I$ e $n = min(A)$, temos que ter $r \geqslant n$, de modo que $t^n | t^r$ e desse modo $t^n | y$, o que mostra que $y \in t^n\mathcal{O}$. Portanto, $t^n\mathcal{O} = I$. ■

Definição 3.1.11. Um anel que possui as propriedades do Teorema 3.1.10 é chamado anel de valorização discreta.

Definição 3.1.12. Um lugar P do corpo de funções F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de F/K. Todo elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado um elemento primo para P. Definimos ainda

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

Observação 3.1.13. Se $\mathcal{O}$ é um anel de valorização discreta de F/K e P é o seu ideal maximal, então $\mathcal{O}$ é unicamente determinado por P, a saber

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

pela Proposição 3.1.8. Dessa forma, denotaremos por $\mathcal{O}_P = \mathcal{O}$ o anel de valorização associado ao lugar P.

Definição 3.1.14. Uma valorização discreta do corpo de funções F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

a) $v(x) = \infty$ se, e somente se, $x = 0$.

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

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

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

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

Observação 3.1.15. Pelas propriedades b) e d) da Definição 3.1.14, temos as valorizações discretas são funções sobrejetoras.

Lema 3.1.16 (Desigualdade Triangular Estrita)**.** *Seja v uma valorização discreta do corpo de funções F/K e sejam $x,\ y \in F$ tais que $v(x) \neq v(y)$. Então*

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

Demonstração. Observemos que $v(az) = v(a) + v(z) = v(z)$, para todo $a \in K\backslash\{0\}$ e para todo $z \in F$. Em particular, $v(z) = v(-z)$, para todo $z \in F$. Como $v(x) \neq v(y)$, podemos assumir, sem perda de generalidade, que $v(x) < v(y)$.

Suponhamos que $v(x+y) \neq min\{v(x),\, v(y)\} = v(x)$, isto é, $v(x+y) > v(x)$. Então $v(x) = v((x+y)-y) \geqslant min\{v(x+y),\, v(-y)\} = min\{v(x+y),\, v(y)\} > v(x)$, o que é uma contradição. Portanto, $v(x+y) = min\{v(x),\, v(y)\}$, como queríamos mostrar. ■

Definição 3.1.17. A um lugar $P \in \mathbb{P}_F$ associamos uma função $v_P : F \to \mathbb{Z} \cup \{\infty\}$ definida como a seguir.

Escolhamos um elemento primo t de P. Então, cada elemento $0 \neq z \in F$ possui uma única representação na forma $z = t^n u$, onde $u \in \mathcal{O}_P^\times$ e $n \in \mathbb{Z}$. Definamos $v_P(z) = n$ e $v_P(0) = \infty$.

Observação 3.1.18. Observemos que a definição anterior depende unicamente do lugar P e não da escolha do elemento primo t. Com efeito, se t' é um outro elemento primo para P, então $t = t'w$, onde $w \in \mathcal{O}_P^\times$. Daí, $z = t^n u = t'^n w^n u$, com $w^n u \in \mathcal{O}_P^\times$.

Teorema 3.1.19. *Seja F/K um corpo de funções.*

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

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

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

e

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

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

c) *Reciprocamente, suponhamos que v seja uma valorização discreta de F/K. Então o conjunto $P = \{z \in F;\, v(z) > 0\}$ é um lugar de F/K e*

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

é o anel de valorização correspondente.

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

Demonstração. a) Etapa 1. v_P é uma valorização discreta.

Seja t um elemento primo para P. Então, dados x, $y \in F\backslash\{0\}$, temos que $x = t^n u$ e $y = t^m w$, com n, $m \in \mathbb{Z}$, u, $w \in \mathcal{O}_P^\times$.

(*i*) $v_P(z) = \infty$ se, e somente se, $z = 0$.

Este fato segue da definição de v_P.

(*ii*) $v_P(0\,.\,0) = v_P(0) = \infty = \infty + \infty = v_P(0) + v_P(0)$,
$v_P(0\,.\,x) = v_P(0) = \infty = \infty + n = v_P(0) + v_P(x)$
e
$v_P(x\,.\,y) = v_P(t^{m+n}u\,.\,w) = n + m = v_P(x) + v_P(y)$.

(*iii*) $v_P(0 + 0) = v_P(0) = \infty = min\{\infty, \infty\} = min\{v_P(0), v_P(0)\}$
e
$v_P(x + 0) = v_P(x) = n = min\{n, \infty\} = min\{v_P(x), v_P(0)\}$.

Agora, sem perda de generalidade, suponhamos $n \leqslant m$. Então

$$x + y = t^n u + t^m w = t^n(u + t^{m-n}w)$$

de modo que podemos ter $v_P(x+y) = n$, se $u+t^{m-n}w \in \mathcal{O}_P^\times$, ou $v_P(x+y) > n$, se $u + t^{m-n}w \notin \mathcal{O}_P^\times$ (notemos que este último caso abrange a situação na qual $x + y = 0$). Isso mostra que temos sempre

$$v_P(x + y) \geqslant n = min\{m, n\} = min\{v_P(x), v_P(y)\}.$$

(*iv*) $v_P(t) = 1$.

(*v*) Como $K\backslash\{0\} \subseteq \tilde{K}\backslash\{0\} \subseteq \mathcal{O}_P^\times$, temos que $v_P(a) = 0$, para todo $a \in K\backslash\{0\}$.

Etapa 2. $\mathcal{O}_P = \{z \in F;\, v_P(z) \geqslant 0\}$.

Com efeito, seja t um elemento primo para P. Então, dado $x \in \{z \in F;\, v_P(z) \geqslant 0\}$, temos que $v_P(x) \geqslant 0$. Se $v_P(x) = \infty$, então $x = 0$ e assim $x \in \mathcal{O}_P$. Caso contrário, $x = t^n u$, onde $n = v_P(x) \geqslant 0$ e $u \in \mathcal{O}_P^\times$. Isso nos dá que $x \in \mathcal{O}_P$, pois $x \in \mathcal{O}_P^\times \subseteq \mathcal{O}_P$, se $n = 0$, ou $x \in t\mathcal{O}_P = P \subseteq \mathcal{O}_P$, se $n > 0$. Por outro lado, a demonstração do Teorema 3.1.10 b) nos dá que se $z \in \mathcal{O}_P\backslash\{0\}$, então existem $n \in \mathbb{Z}_+$ e $u \in \mathcal{O}_P^\times$

tais que $z = t^n u$, donde $v_P(z) \geqslant 0$. Ainda, se $z = 0$, então $v_P(z) = \infty > 0$, o que mostra a igualdade dos conjuntos acima.

Etapa 3. $\mathcal{O}_P^\times = \{z \in F;\, v_P(z) = 0\}$.

Pode ser mostrado de modo análogo ao que foi feito na *Etapa 2*.

Etapa 4. Das duas etapas anteriores, temos que $P = \mathcal{O}_P \backslash \mathcal{O}_P^\times = \{z \in F;\, v_P(z) > 0\}$.

b) ($\Rightarrow$) Seja z um elemento primo para P. Então, pela definição de v_P, temos que $v_P(z) = 1$.

($\Leftarrow$) Fixemos t um elemento primo para P. Dado $z \in F$ tal que $v_P(z) = 1$, temos que $z = tu$, onde $u \in \mathcal{O}_P^\times$. Assim, $P = t\mathcal{O}_P = z\mathcal{O}_P$, de modo que z é um elemento primo para P.

c) Seja v uma valorização discreta. Então

$$\mathcal{O} = \{z \in F;\, v(z) \geqslant 0\}$$

é um anel de valorização de F/K.

Com efeito, $\mathcal{O}$ é um subanel de F, pois $0 \in \mathcal{O}$, já que $v(0) = \infty > 0$, e, dados $x,\, y \in \mathcal{O}$, temos que $v(x) \geqslant 0$ e $v(y) \geqslant 0$, donde $v(xy) = v(x) + v(y) \geqslant 0$ e $v(x-y) \geqslant min\{v(x),\, v(-y)\} = min\{v(x),\, v(y)\} \geqslant 0$, de modo que xy e $x - y \in \mathcal{O}$. Além disso, como existe $z \in F$ tal que $v(z) = -1$, temos que $z \notin \mathcal{O}$, o que mostra que a inclusão $\mathcal{O} \subseteq F$ é estrita. Ainda, $v(a) = 0$, para todo $a \in K\backslash\{0\}$, implica que $K \subseteq \mathcal{O}$, e, como existe $z \in \mathcal{O}$ tal que $v(z) = 1$, temos que $z \notin K$. Isso mostra que $K \subsetneq \mathcal{O}$.

Agora, dado $z \in F\backslash\{0\}$, temos que $0 = v(1) = v(z \,.\, z^{-1}) = v(z) + v(z^{-1})$, de modo que z ou $z^{-1} \in \mathcal{O}$.

Isso completa a prova de que $\mathcal{O}$ é um anel de valorização.

Agora, mostremos que $x \in \mathcal{O}$ é invertível se, e somente se, $v(x) = 0$. De fato, se $x \in \mathcal{O}$ é invertível, então existe $y \in \mathcal{O}$ tal que $xy = 1$. Assim,

$$0 = v(1) = v(x \,.\, y) = v(x) + v(y)$$

e, como $v(x) \geqslant 0$ e $v(y) \geqslant 0$, temos que $v(x) = v(y) = 0$. Reciprocamente, se $x \in \mathcal{O}$, é tal que $v(x) = 0$, mostremos que $x^{-1} \in F$ também pertence à $\mathcal{O}$. Com efeito,

$x \,.\, x^{-1} = 1$ implica que $v(x) + v(x^{-1}) = v(x \,.\, x^{-1}) = v(1) = 0$, donde $v(x^{-1}) = 0$ e $x^{-1} \in \mathcal{O}$. Portanto $P = \mathcal{O} \backslash \mathcal{O}^{\times} = \{z \in F;\, v(z) > 0\}$.

d) Sejam $\mathcal{O}$ um anel de valorização de F/K, $P = \mathcal{O} \backslash \mathcal{O}^{\times}$ o seu ideal maximal, v_P a valorização discreta associada à P e $z \in F \backslash \mathcal{O}$. Temos que mostrar que $F = \mathcal{O}[z]$ (pois assim mostramos que se $\mathcal{O} \subsetneq A \subseteq F$, onde A é um anel, então $A = F$). Para isso, consideremos um elemento $y \in F$. Como $z \notin \mathcal{O}$, temos que $z^{-1} \in \mathcal{O} \backslash \mathcal{O}^{\times}$, donde $v_P(z^{-1}) > 0$. Assim, para algum $k \geqslant 0$ suficientemente grande,

$$v_P(yz^{-k}) = v_P(y) + k \,.\, v_P(z^{-1}) \geqslant 0.$$

Consequentemente, $w = yz^{-k} \in \mathcal{O}$ e $y = wz^k \in \mathcal{O}[z]$. ■

Observação 3.1.20. Notemos que, sendo P um ideal maximal de $\mathcal{O}_P$, temos que $\mathcal{O}_P/P$ é um corpo. Consideremos o homomorfismo

$$\begin{array}{rccc} \pi_P : & \mathcal{O}_P & \to & \mathcal{O}_P/P \\ & x & \mapsto & x + P \end{array}.$$

Como $K \subseteq \mathcal{O}_P$ e $\tilde{K} \subseteq \mathcal{O}_P$, temos que π_P induz homomorfismos injetores naturais de K e $\tilde{K}$ em $\mathcal{O}_P/P$, de modo que podemos considerar $\mathcal{O}_P/P$ como sendo uma extensão de K e $\tilde{K}$.

Definição 3.1.21. Sejam $P \in \mathbb{P}_F$.

a) Definimos $F_P = \mathcal{O}_P/P$. A função $x \mapsto x + P$ de $\mathcal{O}_P$ em F_P é chamada mapa das classes residuais com respeito à P. Em alguns momentos, utilizaremos também a notação $x + P = x(P)$.

b) $deg(P) = [F_P : K]$ é dito o grau do lugar P. Um lugar de grau 1 é também chamado lugar racional de F/K.

Proposição 3.1.22. *Se P é um lugar de F/K e $0 \neq x \in P$, então*

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

Demonstração. Em primeiro lugar, pela Observação 3.1.5, temos que

$$[F : K(x)] < \infty,$$

pois $0 \neq x \in P$ nos diz que x é um elemento transcendente sobre K.

Gostaríamos agora de mostrar que se $z_1(P), \ldots, z_n(P)$ são linearmente independentes sobre K, então $z_1, \ldots, z_n \in \mathcal{O}_P$ são linearmente independentes sobre $K(x)$, o que nos dá que $n \leqslant [F : K(x)]$ e assim $deg(P) \leqslant [F : K(x)]$.

Suponhamos agora que existam $\varphi_1(x), \ldots, \varphi_n(x) \in K(x)$, não todos nulos, tais $\sum_{i=1}^{n} \varphi_i(x) z_i = 0$.
Sem perda de generalidade, podemos assumir que $\varphi_i(x) \in K[x]$ e que x não divide todos $\varphi_i(x)$, ou seja, podemos escrever $\varphi_i(x) = a_i + x \,.\, g_i(x)$, com $a_i \in K$, $g_i(x) \in K[x]$ e nem todos $a_i = 0$. Como $x \in P$ e $g_i(x) \in \mathcal{O}_P$, temos que $\varphi_i(x)(P) = a_i(P) = a_i$.

Assim,

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

o que contradiz o fato de $z_1(P), \ldots, z_n(P)$ serem linearmente independentes sobre K. ■

Corolário 3.1.23. *O corpo de constantes $\tilde{K}$ de F/K é uma extensão de corpos finita sobre K.*

Demonstração. Utilizaremos aqui o fato de que $\mathbb{P}_F \neq \emptyset$, o que será demonstrado no Corolário 3.1.27.

Escolhamos $P \in \mathbb{P}_F$. Como $\tilde{K}$ é um subcorpo de F_P, temos que

$$[\tilde{K} : K] \leqslant [F_P : K] < \infty,$$

como queríamos mostrar. ■

Observação 3.1.24. Seja P um lugar racional de F/K. Então $F_P = K$. Em particular, se K é um corpo algebricamente fechado, então todos os lugares são racionais, uma vez que K não possui extensão algébrica própria, isto é, se K'/K é uma extensão algébrica, então $K' = K$.

Definição 3.1.25. Sejam $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se $v_P(z) > 0$. Ainda, P é dito um polo de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, então P

é dito um zero de ordem m. Agora, se $v_P(z) = -m < 0$, então P é um polo de z de ordem m.

Teorema 3.1.26. *Sejam F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponhamos que $\{0\} \neq I \subsetneq R$ 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

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

Temos dessa forma que $\mathcal{F} \neq \emptyset$, pois $R \in \mathcal{F}$. Ainda, $\mathcal{F}$ é parcialmente ordenado pela relação de inclusão e toda cadeia $\mathcal{C} \subseteq \mathcal{F}$ possui um limite superior em $\mathcal{F}$. Com efeito, se $\mathcal{C} \subseteq \mathcal{F}$ é uma cadeia em $\mathcal{F}$, então $T = \bigcup_{S \in \mathcal{C}} S$ é um subanel de F, com $R \subseteq T$. Resta-nos mostrar que $IT \neq T$. Para isso, suponhamos que $IT = T$. Então, $1 = \sum_{i=1}^{n} a_i s_i$, onde $a_i \in I$ e $s_i \in T$, de modo que, sendo $\mathcal{C}$ totalmente ordenado, temos que existe $S_0 \in \mathcal{C}$ tal que $s_1, \ldots, s_n \in S_0$, o que nos dá que $1 \in S_0$ e assim $IS_0 = S_0$. Mas isso é uma contradição, pois $S_0 \in \mathcal{C}$ implica que $IS_0 \neq S_0$.

Pelo Lema de Zorn, temos, dessa forma, que $\mathcal{F}$ possui elemento maximal, ou seja, existe $\mathcal{O} \subseteq F$ tal que $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$ e $\mathcal{O}$ é maximal com respeito a essas propriedades.

Queremos agora 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 $I \subseteq \mathcal{O} \backslash \mathcal{O}^{\times}$. De fato, se $\mathcal{O} = F$, então, como $I \neq \{0\}$, temos que $IF = F$, o que é uma contradição. Isso mostra que $\mathcal{O} \subsetneq F$. Ainda, se algum elemento $z \in I$ fosse invertível em $\mathcal{O}$, teríamos que $z \,.\, z^{-1} = 1 \in I\mathcal{O}$, donde $I\mathcal{O} = \mathcal{O}$, o que é novamente uma contradição. Portanto, $I \subseteq \mathcal{O} \backslash \mathcal{O}^{\times}$.

Além disso, se $\mathcal{O} = K$, de $K \subseteq R \subseteq K = \mathcal{O}$, teríamos que $R = K$, donde não é possível existir um ideal I tal que $\{0\} \neq I \subsetneq R$, o que contradiz a nossa hipótese inicial.

Portanto $K \subsetneq \mathcal{O} \subsetneq F$.

Por outro lado, 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 $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$, pois $\mathcal{O}$ é um elemento maximal de $\mathcal{F}$, $\mathcal{O}[z] \supsetneq \mathcal{O}$ e $\mathcal{O}[z^{-1}] \supsetneq \mathcal{O}$, donde $\mathcal{O}[z]$ e $\mathcal{O}[z^{-1}]$ não pertencem a $\mathcal{F}$ e, como $R \subseteq \mathcal{O}[z] \subseteq F$ e $R \subseteq \mathcal{O}[z^{-1}] \subseteq F$, temos que ter $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$.

Dessa forma, existem $a_0, \ldots, a_n$, $b_0, \ldots, b_m \in I\mathcal{O}$ com $1 = a_0 + a_1 z + \ldots + a_n z^n$ e $1 = b_0 + b_1 z^{-1} + \ldots + b_m z^{-m}$. Como $I\mathcal{O} \neq \mathcal{O}$, temos que $n \geqslant 1$ e $m \geqslant 1$.

Consideremos m, n os menores valores para os quais z e z^{-1} satisfazem uma equação como acima e, sem perda de generalidade, suponhamos $m \leqslant n$.

Assim,

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

implica que

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

donde somando as duas últimas equações obtemos

$$\begin{aligned} 1 - b_0 + a_n z^n = {} & a_0(1 - b_0) + a_1(1 - b_0)z + \ldots + a_{n-m-1}(1 - b_0)z^{n-m-1} \\ & + [a_{n-m}(1 - b_0) + a_n b_m]z^{n-m} + \ldots + [a_{n-1}(1 - b_0) + a_n b_1]z^{n-1} \\ & + [a_n(1 - b_0) + a_n b_0]z^n, \end{aligned}$$

o que nos dá que

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

Mas a igualdade anterior é uma contradição pela minimalidade de n.

Portanto, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$, para todo $z \in F$.

Isso conclui a prova de que $\mathcal{O}$ é um anel de valorização de F/K. ■

Corolário 3.1.27. *Sejam F/K um corpo de funções e $z \in F$ um elemento transcendente sobre K. Então z possui pelo menos um zero e um polo. Em particular, $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Consideremos o anel $R = K[z]$ e o ideal $I = z\,.\,K[z]$. Como $\{0\} \neq I \subsetneq R$, temos que existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Daí $z \in I \subseteq P$, donde $v_P(z) > 0$, ou seja, P é um zero de z. Aplicando o mesmo argumento à z^{-1}, temos que z^{-1} possui um zero $Q \in \mathbb{P}_F$ e assim Q é um polo de z. ■

3.2 INDEPENDÊNCIA DAS VALORIZAÇÕES

Teorema 3.2.1 (Teorema da Aproximação Fraca ou Teorema da Independência)**.** *Sejam F/K um corpo de funções, $P_1, \ldots, P_n \in \mathbb{P}_F$ lugares de F/K dois a dois distintos, $x_1, \ldots, x_n \in F$ 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 $i = 1, \ldots, n$.*

Demonstração. A demonstração desse resultado será feita em algumas etapas. Ainda, com o intuito de simplificar a notação, escrevamos $v_i = v_{P_i}$.

Etapa 1. Existe $u \in F$ tal que $v_1(u) > 0$ e $v_i(u) < 0$, para $i = 2, \ldots, n$.

Prova da Etapa 1.

Façamos a demonstração por indução. Para $n = 2$, observemos que $\mathcal{O}_{P_1} \nsubseteq \mathcal{O}_{P_2}$ e $\mathcal{O}_{P_2} \nsubseteq \mathcal{O}_{P_1}$, já que anéis de valorização são subanéis próprios maximais de F, pelo Teorema 3.1.19. Deste modo, podemos encontrar $y_1 \in \mathcal{O}_{P_1} \backslash \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \backslash \mathcal{O}_{P_1}$, de modo que $v_1(y_1) \geqslant 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geqslant 0$, também pelo Teorema 3.1.19.

O elemento $u = y_1/y_2$ possui a propriedade que desejamos, pois

$$v_1(u) = v_1(y_1) + v_2(y_2^{-1}) = v_1(y_1) - v_1(y_2) > 0$$

e

$$v_2(u) = v_2(y_1) + v_2(y_2^{-1}) = v_2(y_1) - v_2(y_2) < 0.$$

Para $n > 2$, temos, pela hipótese de indução, que existe um elemento y com $v_1(y) > 0$, $v_2(y) < 0$, $\ldots$, $v_{n-1}(y) < 0$.

Se $v_n(y) < 0$, então a demonstração termina considerando $u = y$. Caso contrário, isto é, se $v_n(y) \geqslant 0$, escolhemos z tal que $v_1(z) > 0$ e $v_n(z) < 0$ e escrevemos

$u = y + z^r$, onde $r \geqslant 1$ é escolhido de modo que $rv_i(z) \neq v_i(y)$, para $i = 1, \ldots, n-1$. Daí, $v_1(u) \geqslant min\{v_1(y), r \,.\, v_1(z)\} > 0$ e $v_i(u) = min\{v_i(y), rv_i(z)\} < 0$, para $i = 2, \ldots, n$.

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

Prova da Etapa 2.

Escolhamos u como na *Etapa 1* e escrevamos $w = (1+u^s)^{-1}$. Temos, para $s \in \mathbb{N}$ suficientemente grande, que

$$\begin{aligned} v_1(w-1) &= v_1((1+u^s)^{-1} - 1) \\ &= v_1\left(\frac{1-1-u^s}{1+u^s}\right) \\ &= v_1(-u^s(1+u^s)^{-1}) \\ &= s \,.\, v_1(u) - v_1(1+u^s) \\ &= s \,.\, v_1(u) - min\{v_1(1),\, s \,.\, v_1(u)\} \quad (*) \\ &= s \,.\, v_1(u) - 0 \\ &= s \,.\, v_1(u) > r_1 \end{aligned}$$

e

$$\begin{aligned} v_i(w) &= -v_i(w^{-1}) \\ &= -v_i(1+u^s) \\ &= -s \,.\, v_i(u) > r_i \quad (*) \end{aligned}$$

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

$(*)$ Temos que $v_1(1) = 0 < v_1(u^s)$, para qualquer $s \in \mathbb{N}$, donde, pelo Lema 3.1.16, temos que $v_1(1+u^s) = min\{v_1(1), v_1(u^s)\}$. Um resultado análogo vale para v_i, $i = 2, \ldots, n$.

Etapa 3. Dados $y_1, \ldots, y_n \in F$, existe um elemento $z \in F$ com $v_i(z - y_i) > r_i$, para $i = 1, \ldots, n$.

Prova da Etapa 3.

Escolhamos $s \in \mathbb{Z}$ tal que $v_i(y_j) \geqslant s$, para todos $i, j \in \{1, \ldots, n\}$. Pela *Etapa 2*,

temos que existem $w_1, \ldots, w_n$ tais que

$$\begin{array}{lcl} v_1(w_1-1) & > & r_1-s \\ v_2(w_1) & > & r_2-s \\ & \vdots & \\ v_n(w_1) & > & r_n-s \end{array} \quad \begin{array}{lcl} v_1(w_2) & > & r_1-s \\ v_2(w_2-1) & > & r_2-s \\ v_3(w_2) & > & r_3-s \\ & \vdots & \\ v_n(w_2) & > & r_n-s \end{array} \quad \cdots \quad \begin{array}{lcl} v_1(w_n) & > & r_1-s \\ v_2(w_n) & > & r_2-s \\ & \vdots & \\ v_{n-1}(w_n) & > & r_{n-1}-s \\ v_n(w_n-1) & > & r_n-s \end{array}$$

Considerando $z = \sum_{j=1}^{n} y_j w_j$, temos que

$$\begin{aligned} v_i(z-y_i) &= v_i(y_i(w_i-1) + \sum_{j\neq i} y_j w_j) \\ &\geqslant min\{v_i(y_i(w_i-1)),\, v_i(y_1w_1), \ldots,\, v_i(y_{i-1}w_{i-1}),\, v_i(y_{i+1}w_{i+1}), \ldots,\, v_i(y_nw_n)\} \\ &> r_i. \end{aligned}$$

Conclusão da Demonstração.

Pela *Etapa 3*, podemos encontrar $z \in F$ tal que $v_i(z-x_i) > r_i$, para $i = 1, \ldots, n$. A seguir, escolhemos z_i tal que $v_i(z_i) = r_i$ (isso pode ser sempre feito, pois v_i é sobrejetora para todo i). Novamente, pela *Etapa 3*, existe z' tal que $v_i(z'-z_i) > r_i$, para $i = 1, \ldots, n$. Daí temos que

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

Escrevendo $x = z + z'$, temos que

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

■

Corolário 3.2.2. *Todo corpo de funções possui um número infinito de lugares.*

Demonstração. Suponhamos que exista um número finito de lugares, a saber $P_1, \ldots, P_n$. Pelo Teorema 3.2.1, existe um elemento $x \neq 0$ pertencente à F com $v_{P_i}(x) > 0$, para todo $i = 1, \ldots, n$. Então x é um elemento transcendente sobre K (pois $0 \neq x \in P_i$ para todo i, e, com exceção de 0, todos os demais elementos de P_i são transcendentes sobre K) e x não possui polos (pois todos os lugares de F/K são $P_1, \ldots, P_n$ e todos estes são zeros de x). Mas isso é uma contradição, pelo Corolário 3.1.27. ■

Proposição 3.2.3. *Sejam F/K um corpo de funções e $P_1, \ldots, P_r$ zeros do elemento $x \in F$. Então*

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

Demonstração. Para simplificar a notação, escrevamos $v_i = v_{P_i}$, $f_i = deg(P_i)$ e $e_i = v_i(x)$.

Pelo Teorema 3.2.1, para cada i existe um elemento t_i tal que $v_i(t_i) = 1$ e $v_k(t_i) = 0$, para $k \neq i$.

Escolhamos $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ formam uma base para $F_{P_i} = \mathcal{O}_{P_i}/P_i$ sobre K.

Por uma aplicação mais fraca do Teorema 3.2.1, podemos encontrar $z_{ij} \in F$ tais que para todos i, j

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

Afirmamos que os elementos $t_i^a z_{ij}$, com $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant f_i$ e $0 \leqslant a \leqslant e_i - 1$, são linearmente independentes sobre $K(x)$. Como o número de elementos dessa forma é igual à

$$\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \,.\, deg(P_i),$$

temos que a prova dessa proposição seguirá dessa afirmação.

Suponhamos que exista um combinação linear não trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija}(x) t_i^a z_{ij} = 0 \quad (*)$$

sobre $K(x)$. Sem perda de generalidade, podemos assumir $\varphi_{ija}(x) \in K[x]$ e que nem todos $\varphi_{ija}(x)$ são divisíveis por x.

Então existem índices $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$ tais que $x | \varphi_{kja}(x)$, para todo $a < c$ e para todo $j \in \{1, \ldots, f_k\}$, e $x \nmid \varphi_{kjc}(x)$, para algum $j \in \{1, \ldots, f_k\}$.

Multiplicando $(*)$ por tk^{-c}, obtemos

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

Para $i \neq k$, todas as parcelas da soma anterior estão em P_k, já que

$$v_k(\varphi_{ija}(x)t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}(x)) + v_k(t_i^a) + v_k(t_k^{-c}) + v_k(z_{ij}) \geqslant -c + e_k > 0.$$

Para $i = k$ e $a < c$, temos que

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

Para $i = k$ e $a > c$, temos que

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

Combinando os casos anteriores, temos que

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

Notemos que $\varphi_{kjc}(x)(P_k) \in K$, uma vez que tudo que for múltiplo de x pertence à P_k, de modo que no quociente F_{P_k} só resta o termo constante, e que nem todos $\varphi_{kjc}(x)(P_k) = 0$, pois x não divide todos os $\varphi_{kjc}(x)$, donde temos uma combinação linear não trivial

$$\sum_{j=1}^{f_k} \varphi_{kjc}(x)(P_k) \,.\, z_{k_j}(P_k) = 0$$

sobre K. Mas isso é uma contradição, pois $\{z_{k_1}(P_k), \ldots, z_{kf_k}(P_k)\}$ é uma base de F_{P_k}/K (pois $v_i(s_{ij} - z_{ij}) > 0$ implica que $s_{ij} - z_{ij} \in P_i$ e assim $s_{ij}(P_i) = z_{ij}(P_i)$, com $\{s_{i1}(P_i), \ldots, s_{if_i}(P_i)\}$ sendo uma base de F_{P_i}/K). ■

Corolário 3.2.4. *Em um corpo de funções F/K, todo elemento $0 \neq x \in F$ possui um número finito de zeros e de polos.*

Demonstração. Se $x \in \tilde{K}$, como $\tilde{K} \subseteq \mathcal{O}_P$, para todo lugar P, temos que $x \notin P$ e $x^{-1} \notin P$, para todo lugar P. Daí, x não possui zeros nem polos. Por outro lado, se x é transcendente sobre K, então o número de zeros de x é menor ou igual a $[F : K(x)]$, pela Proposição 3.2.3. Um argumento análogo a esse aplicado à x^{-1} nos mostra que x^{-1} possui um número finito de zeros, donde x possui um número finito de polos. ■

3.3 DIVISORES

Consideremos ao longo dessa seção F/K um corpo de funções em uma variável tal que K é algebricamente fechado em F.

Definição 3.3.1. O grupo dos divisores de F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K e é denotado por $Div(F)$. Os elementos de $Div(F)$ são chamados divisores de F/K. Em outras palavras, um divisor D é uma soma formal

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

com $n_P \in \mathbb{Z}$ e quase todo n_P igual a zero. O suporte de D é definido como sendo o conjunto

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

Definimos a adição de dois divisores $D = \sum_{P \in \mathbb{P}_F} n_P \, . \, P$ e $D' = \sum_{P \in \mathbb{P}_F} n'_P \, . \, P$ como

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

Ainda, o elemento neutro do grupo de divisores $Div(F)$ é o divisor

$$0 = \sum_{P \in \mathbb{P}_F} r_P \, . \, P,$$

onde $r_P = 0$, para todo $P \in \mathbb{P}_F$.

Definição 3.3.2. Um divisor $D = P$, com $P \in \mathbb{P}_F$, é chamado divisor primo.

Definição 3.3.3. Para $Q \in \mathbb{P}_F$ e $D = \sum n_P \, . \, P \in Div(F)$, definimos $v_Q(D) = n_Q$.

Observação 3.3.4. Com base na definição anterior, temos que

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

Definição 3.3.5. Uma relação de ordem parcial em $Div(F)$ pode ser definida por

$$D_1 \leqslant D_2 \text{ se, e somente se, } v_P(D_1) \leqslant v_P(D_2), \text{ para todo } P \in \mathbb{P}_F.$$

Se $D_1 \leqslant D_2$ e $D_1 \neq D_2$, escrevemos $D_1 < D_2$. Ainda, se $D \geqslant 0$, então D é chamado um divisor positivo.

Definição 3.3.6. O grau de um divisor é definido como

$$deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) \, . \, deg(P).$$

Observação 3.3.7. A aplicação

$$\begin{array}{rccc} deg: & Div(F) & \to & \mathbb{Z} \\ & D & \mapsto & deg(D) \end{array}$$

é um homomorfismo de grupos.

Definição 3.3.8. Seja $0 \neq x \in F$ e denotemos por $\mathcal{Z}$ e por $\mathcal{N}$ o conjunto de zeros e de polos de x, respectivamente. Então definimos:

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

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

c) $(x) = (x)_0 - (x)_\infty$ o divisor principal de x.

Observação 3.3.9. Com base na definição anterior, temos que $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) \, . \, P$.

Definição 3.3.10. O conjunto de divisores

$$Princ(F) = \{(x);\, 0 \neq x \in F\}$$

é chamado o grupo dos divisores principais de F/K. O grupo quociente

$$C\ell(F) = Div(F)/Princ(F)$$

é chamado grupo das classes de divisores de F/K. Para um divisor $D \in Div(F)$, o correspondente elemento em $C\ell(F)$ é denotado por $[D]$.

Definição 3.3.11. Dois divisores D e D' são ditos equivalentes, e escrevemos $D \sim D'$, se $[D] = [D']$, ou seja, se $D = D' + (x)$, para algum $x \in F \backslash \{0\}$.

Observação 3.3.12. A relação estabelecida na Definição 3.3.11 é uma relação de equivalência em $Div(F)$.

Definição 3.3.13. Para um divisor $A \in Div(F)$, definimos o espaço de Riemann-Roch associado a A por

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

Observação 3.3.14. Seja $A \in Div(F)$. Então:

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

b) $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe $A' \in Div(F)$ tal que $A' \sim A$ e $A' \geqslant 0$.

A demonstração do item a) segue das definições. Agora,

$$\begin{aligned} \mathcal{L}(A) \neq \{0\} &\Leftrightarrow \exists\ x \in F\backslash\{0\} \text{ tal que } (x) \geqslant -A \\ &\Leftrightarrow A' = A + (x) \text{ é tal que } A' \sim A \text{ e } A' \geqslant 0 \\ &\Leftrightarrow \exists\ A' \in Div(F) \text{ tal que } A' \sim A \text{ e } A' \geqslant 0, \end{aligned}$$

o que mostra o item b).

Lema 3.3.15. *Seja $A \in Div(F)$. Então, temos que:*

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

b) *Se A' é um divisor equivalente a A, então $\mathcal{L}(A)$ é isomorfo à $\mathcal{L}(A')$.*

Demonstração. *a)* Mostremos que $\mathcal{L}(A)$ é um subespaço vetorial de F sobre K. Em primeiro lugar, notemos que $\mathcal{L}(A) \neq \emptyset$, pois $0 \in \mathcal{L}(A)$. Sejam agora x, $y \in \mathcal{L}(A)$ e $a \in K$. Então, para todo $P \in \mathbb{P}_F$, $v_P(x+y) \geqslant min\{v_P(x), v_P(y)\} \geqslant -v_P(A)$ e $v_P(ax) = v_P(a) + v_P(x) \geqslant -v_P(A)$. Logo, $x+y$ e $ax \in \mathcal{L}(A)$, pela Observação 3.3.14.

b) Por hipótese, temos que $A = A' + (z)$, com $0 \neq z \in F$. Consideremos a aplicação

$$\begin{array}{rccc} \varphi: & \mathcal{L}(A) & \to & F \\ & x & \mapsto & xz \end{array}.$$

Então, φ é uma transformação linear cuja imagem está contida em $\mathcal{L}(A')$. Com efeito, se $x \in \mathcal{L}(A)\backslash\{0\}$, então $(x) \geqslant -A$. Daí, $\varphi(x) = xz \neq 0$ é tal que

$(xz) = (x)+(z) = (x)+A-A' \geqslant -A+A-A' = -A'$. Logo, $\varphi(x) = xz \in \mathcal{L}(A')\backslash\{0\}$. Se $x = 0$, então $\varphi(x) = \varphi(0) = 0 \in \mathcal{L}(A')$. Logo, $\varphi(\mathcal{L}(A)) \subseteq \mathcal{L}(A')$. A linearidade segue diretamente da definição.

Do mesmo modo, temos que

$$\begin{array}{rccc} \varphi' : & \mathcal{L}(A') & \to & F \\ & x & \mapsto & xz^{-1} \end{array}$$

é uma transformação linear cuja imagem está contida em $\mathcal{L}(A)$.

Como φ' é a inversa de φ, mostramos que φ é um isomorfismo de $\mathcal{L}(A)$ em $\mathcal{L}(A')$. ■

Lema 3.3.16. *a)* $\mathcal{L}(0) = K$.

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

Demonstração. a) Temos que $(x) = 0$, para $0 \neq x \in K$, de modo que $K \subseteq \mathcal{L}(0)$. Reciprocamente, se $0 \neq x \in \mathcal{L}(0)$, então $(x) \geqslant 0$. Isso significa que x não possui polos, donde $x \in K$, pelo Corolário 3.1.27.

b) Assumamos que existe um elemento $0 \neq x \in \mathcal{L}(A)$. Então $(x) \geqslant -A > 0$. Isso nos dá que x possui pelo menos um zero e nenhum polo, o que é uma contradição pelo Corolário 3.1.27. ■

Lema 3.3.17. *Sejam* A, B *divisores de* F/K, *com* $A \leqslant B$. *Então* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e* $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leqslant deg(B) - deg(A)$.

Demonstração. Em primeiro lugar, mostremos que $\mathcal{L}(A) \subseteq \mathcal{L}(B)$. Com efeito, seja $0 \neq x \in \mathcal{L}(A)$. Então $v_P(x) \geqslant -v_P(A)$, para todo $P \in \mathbb{P}_F$. Como $A \leqslant B$, temos que $v_P(B) \geqslant v_P(A)$, para todo $P \in \mathbb{P}_F$. Daí, $-v_P(A) \geqslant -v_P(B)$, para todo $P \in \mathbb{P}_F$, donde $v_P(x) \geqslant -v_P(B)$, para todo $P \in \mathbb{P}_F$. Isso nos dá que $x \in \mathcal{L}(B)$.

Com o intuito de mostrar a outra parte do lema, podemos assumir que $B = A + P$, para algum $P \in \mathbb{P}_F$. O caso geral segue deste por indução.

Escolhamos um elemento $t \in F$ com $v_P(t) = v_P(B) = v_P(A) + 1$. Para $x \in \mathcal{L}(B)$, temos que $v_P(x) \geqslant -v_P(B) = -v_P(t)$, donde $v_P(xt) = v_P(x)+v_P(t) \geqslant 0$ e $xt \in \mathcal{O}_P$.

Assim, obtemos uma aplicação $K-$linear

$$\begin{array}{rccc} \psi: & \mathcal{L}(B) & \to & F_P \\ & x & \mapsto & (xt)(P) \end{array}.$$

Um elemento $x \in Ker(\psi)$ se, e somente se, $xt \in P$, o que ocorre se, e somente se, $v_P(xt) > 0$, ou seja, $v_P(x) + v_P(t) > 0$. Assim,

$$\begin{aligned} x \in Ker(\psi) &\Leftrightarrow v_P(x) > -v_P(t) \\ &\Leftrightarrow v_P(x) > -v_P(A) - 1 \\ &\Leftrightarrow v_P(x) \geqslant -v_P(A). \end{aligned}$$

Consequentemente, $Ker(\psi) = \mathcal{L}(A)$ (pois $v_Q(x) \geqslant -v_Q(B) = -v_Q(A)$, para $Q \neq P$ e $x \in \mathcal{L}(B)$).

Daí, ψ induz uma transformação linear injetiva de $\mathcal{L}(B)/\mathcal{L}(A)$ em F_P.

Portanto, $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leqslant dim(F_P) = deg(B) - deg(A)$. ■

Proposição 3.3.18. *Para cada divisor $A \in Div(F)$, o espaço $\mathcal{L}(A)$ é um espaço vetorial de dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, onde A_+ e A_- são divisores positivos, então $dim(\mathcal{L}(A)) \leqslant deg(A_+) + 1$.*

Demonstração. Como $A \leqslant A_+$, temos, pelo Lema 3.3.17, que $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Logo, é suficiente mostrarmos que $dim(\mathcal{L}(A_+)) \leqslant deg(A_+) + 1$.

Temos que $0 \leqslant A_+$, donde, pelo Lema 3.3.17, segue que

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

Como $\mathcal{L}(0) = K$, concluímos que

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

■

Definição 3.3.19. Para $A \in Div(F)$, o inteiro $\ell(A) = dim(\mathcal{L}(A))$ é chamado a dimensão do divisor A.

Teorema 3.3.20. *Todos os divisores principais possuem grau zero. Mais precisamente, seja $x \in F\backslash K$. Então $deg((x)_0) = deg((x)_\infty) = [F : K(x)]$.*

Demonstração. Escrevamos $n = [F : K(x)]$ e $B = (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$, onde $P_1, \ldots, P_r$ são todos os polos de x. Então

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

pela Proposição 3.2.3. Resta-nos mostrar que $n \leqslant deg(B)$.

Escolhamos uma base $u_1, \ldots, u_n$ de $F/K(x)$ e um divisor $C \geqslant 0$ tal que $(u_i) \geqslant -C$, para $i = 1, \ldots, n$. Então temos que $\ell(kB + C) \geqslant n(k + 1)$, para todo $k \geqslant 0$ $(*)$.

Escrevendo $c = deg(C)$, obtemos que

$$\begin{aligned} n(k+1) &\leqslant \ell(kB + C) \\ &\leqslant deg((kB + C)_+) + 1 \\ &= deg(kB + C) + 1 \\ &= k \,.\, deg(B) + deg(C) + 1 \\ &= k \,.\, deg(B) + c + 1, \end{aligned}$$

pela Proposição 3.3.18.

Logo $n(k + 1) \leqslant k \,.\, deg(B) + c + 1$ implica que $k(deg(B) - n) \geqslant n - c - 1$, para todo $k \in \mathbb{N}$.

Como o lado direito da última desigualdade não depende de k, temos que ter $deg(B) \geqslant n$.

Desse modo, provamos que $deg((x)_\infty) = [F : K(x)]$. Como $(x)_0 = (x^{-1})_\infty$, podemos concluir que $deg((x)_0) = deg((x^{-1})_\infty) = [F : K(x^{-1})] = [F : K(x)]$.

$(*)$ Para provarmos essa desigualdade, basta mostrarmos que os elementos $x^i u_j$, $0 \leqslant i \leqslant k$ e $1 \leqslant j \leqslant n$, pertencem à $\mathcal{L}(kB + C)$ e são linearmente independentes sobre K, pois isso nos dá que $\ell(kB + C) = dim(\mathcal{L}(kB + C)) \geqslant n(k + 1)$.

Com efeito, $(x^i) = i(x) = i(x)_0 - i(x)_\infty \geqslant -i(x)_\infty \geqslant -k(x)_\infty = -kB$, pois $i \leqslant k$, e $(u_j) \geqslant -C$, para todo $j = 1, \ldots, n$. Daí, $(x^i u_j) = (x^i) + (u_j) \geqslant -kB - C$, ou seja, $x^i u_j \in \mathcal{L}(kB + C)$.

Ainda, se $\sum_{j=1}^{n}\sum_{i=1}^{k} a_{ij}x^i u_j = 0$, com $a_{ij} \in K$, temos que $\sum_{j=1}^{n}\left(\sum_{i=1}^{k} a_{ij}x^i\right) u_j = 0$, donde $\sum_{i=1}^{k} a_{ij}x^i = 0$, para todo $j = 1, \ldots, n$. Como x é um elemento transcendente sobre K, temos que $a_{ij} = 0$, para todos $i = 1, \ldots, k$, $j = 1, \ldots, n$. Isso mostra que os elementos $x^i u_j$ são linearmente independentes sobre K. ■

Corolário 3.3.21. *Seja $A \in Div(F)$.*

a) Se $A' \in Div(F)$ é tal que $A' \sim A$, então $\ell(A) = \ell(A')$ e $deg(A) = deg(A')$.

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

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

$(*)$ A é um divisor principal.

$(**)$ $\ell(A) \geqslant 1$.

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

Demonstração. a) Etapa 1. Pelo Lema 3.3.15, como $A \sim A'$, temos que $\mathcal{L}(A)$ é isomorfo à $\mathcal{L}(A')$, donde $\ell(A) = \ell(A')$.

Etapa 2. Como $A \sim A'$, temos que $A = A' + (x)$. Pela Observação 3.3.7, temos que $deg(A) = deg(A' + (x)) = deg(A') + deg((x)) = deg(A')$, onde a última igualdade segue do Teorema 3.3.20.

b) Suponhamos que $\ell(A) > 0$. Pela Observação 3.3.14, temos que existe $A' \in Div(F)$ tal que $A' \sim A$ e $A' \geqslant 0$. Mas daí, temos, pela letra a), que $deg(A) = deg(A')$ e $deg(A') \geqslant 0$ (pela definição de grau de um divisor), o que é uma contradição, pois $deg(A) < 0$.

c) $(*) \Rightarrow (**)$

Se $A = (x)$ é um divisor principal, então $x^{-1} \in \mathcal{L}(A)$, pois $(x^{-1}) = -(x)$. Logo, $\ell(A) \geqslant 1$.

$(**) \Rightarrow (***)$ Suponhamos que $\ell(A) \geqslant 1$. Por hipótese, temos que $deg(A) = 0$. Então, $A \sim A'$, para algum $A' \geqslant 0$ (pela Observação 3.3.14). As condições $A' \geqslant 0$

e $deg(A') = deg(A) = 0$ nos dão que $A' = 0$. Logo $\ell(A) = \ell(A') = \ell(0) = 1$ pelo Lema 3.3.16.

$(***) \Rightarrow (*)$ Suponhamos que $\ell(A) = 1$. Por hipótese também temos que $deg(A) = 0$. Seja $0 \neq z \in \mathcal{L}(A)$. Então $(z) + A \geqslant 0$. Como $deg((z) + A) = 0$, temos que $(z) + A = 0$. Daí, $A = -(z) = (z^{-1})$ é um divisor principal. ■

Proposição 3.3.22. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todos os divisores $A \in Div(F)$ temos que $deg(A) - \ell(A) \leqslant \gamma$.*

Notemos que o valor γ independe do divisor A, estando relacionado somente com o corpo de funções F/K.

Demonstração. Para iniciarmos a demonstração, observemos que $A_1 \leqslant A_2$ nos dá que $deg(A_1) - \ell(A_1) \leqslant deg(A_2) - \ell(A_2)$. Com efeito, pelo Lema 3.3.17, temos que

$$\ell(A_2) - \ell(A_1) = dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leqslant deg(A_2) - deg(A_1).$$

Fixemos um elemento $x \in F \backslash K$ e consideremos o divisor $B = (x)_\infty$.

Como na demonstração do Teorema 3.3.20, existe um divisor $C \geqslant 0$ (dependendo de x) tal que $\ell(kB + C) \geqslant (k + 1) \,.\, deg(B)$, para todo $k \geqslant 0$.

Por outro lado, pelo Lema 3.3.17, temos que $\ell(kB + C) \leqslant \ell(kB) + deg(C)$. De fato,

$$\begin{aligned} \ell(kB + C) - \ell(kB) &= dim(\mathcal{L}(kB + C)/\mathcal{L}(kB)) \\ &\leqslant deg(kB + C) - deg(kB) \\ &= deg(kB) + deg(C) - deg(kB) = deg(C), \end{aligned}$$

donde $\ell(kB + C) \leqslant \ell(kB) + deg(C)$.

Combinando as duas últimas desigualdades, temos que

$$\begin{aligned} \ell(kB) &\geqslant (k + 1) \,.\, deg(B) - deg(C) \\ &= deg(kB) + (deg(B) - deg(C)) \\ &= deg(kB) + ([F : K(x)] - deg(C)). \end{aligned}$$

Portanto, $deg(kB) - \ell(kB) \leqslant \gamma$, para todo $k \geqslant 0$, para algum $\gamma \in \mathbb{Z}$.

Queremos mostrar que a desigualdade anterior vale mesmo substituindo kB por $A \in Div(F)$.

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

Temos que essa afirmação conclui o resultado pois

$$\begin{aligned} deg(A) - \ell(A) &\leqslant deg(A_1) - \ell(A_1) \\ &= deg(D) - \ell(D) \text{ (pelo Corolário 3.3.21)} \\ &\leqslant deg(kB) - \ell(kB) \\ &\leqslant \gamma. \end{aligned}$$

Prova da Afirmação.

Escolhamos $A_1 \geqslant A$ tal que $A_1 \geqslant 0$. Então

$$\begin{aligned} \ell(kB - A_1) &\geqslant \ell(kB) - deg(A_1) \text{ (pelo Lema 3.3.17)} \\ &\geqslant deg(kB) - \gamma - deg(A_1) \\ &> 0 \end{aligned}$$

para k suficientemente grande. Logo, existe um elemento $0 \neq z \in \mathcal{L}(kB - A_1)$. Definindo $D = A_1 - (z)$, obtemos $A_1 \sim D$ e $D \leqslant A_1 - (A_1 - kB) = kB$, como desejado. ■

Definição 3.3.23. O gênero g de F/K é definido por

$$g = max\,\{deg(A) - \ell(A) + 1;\ A \in Div(F)\}.$$

Observação 3.3.24. O gênero de F/K é um inteiro não negativo. Com efeito, $g \geqslant deg(0) - \ell(0) + 1 = 0$.

Teorema 3.3.25 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então:*

a) Para todos os divisores $A \in Div(F)$, $\ell(A) \geqslant deg(A) + 1 - g$.

b) Existe um inteiro c, dependendo somente do corpo de funções F/K, tal que $\ell(A) = deg(A) + 1 - g$, sempre que $deg(A) \geqslant c$.

Demonstração. *a*) Esse item segue da definição do gênero g.

b) Escolhamos um divisor A_0 com $g = deg(A_0) - \ell(A_0) + 1$ e definamos

$$c = deg(A_0) + g.$$

Se $deg(A) \geqslant c$, então

$$\ell(A - A_0) \geqslant deg(A - A_0) + 1 - g = deg(A) - deg(A_0) + 1 - g \geqslant c - deg(A_0) + 1 - g = 1.$$

Logo existe um elemento $0 \neq z \in \mathcal{L}(A - A_0)$. Consideremos o divisor

$$A' = A + (z) \geqslant A_0.$$

Então, temos que

$$\begin{aligned} deg(A) - \ell(A) &= deg(A') - \ell(A') \text{ (pelo Corolário 3.3.21)} \\ &\geqslant deg(A_0) - \ell(A_0) \text{ (pelo Lema 3.3.17)} \\ &= g - 1. \end{aligned}$$

Isso nos dá que $\ell(A) \leqslant deg(A) - g + 1$, o que, pelo item a), nos dá a igualdade. ■

3.4 O TEOREMA DE RIEMANN-ROCH

Definição 3.4.1. Para $A \in Div(F)$, o inteiro

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

é chamado o índice de especialidade de A.

Observação 3.4.2. Pelo Teorema de Riemann (Teorema 3.3.25), $i(A) \geqslant 0$, para todo $A \in Div(F)$, e $i(A) = 0$, se $deg(A)$ for suficientemente grande.

Definição 3.4.3. Um adele de F/K é uma função

$$\begin{array}{rccc} \alpha: & \mathbb{P}_F & \to & F \\ & P & \mapsto & \alpha_P \end{array}$$

tal que $\alpha_P \in \mathcal{O}_P$, para quase todo $P \in \mathbb{P}_F$. Considerando um adele como um elemento do produto direto $\prod_{P\in\mathbb{P}_F} F$, utilizaremos a notação $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$ ou simplesmesmente $\alpha = (\alpha_P)$.

O conjunto

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

é chamado o espaço de adeles de F/K. Notemos que $\mathcal{A}_F$ pode ser considerado um espaço vetorial sobre K definindo as operações de adição e multiplicação por escalar da forma usual.

Para $x \in F$, definimos o adele principal de x como

$$\begin{array}{rccc} \alpha_x: & \mathbb{P}_F & \to & F \\ & P & \mapsto & x \end{array}.$$

Notemos que α_x é efetivamente um adele, uma vez que x possui um número finito de polos pelo Corolário 3.2.4.

Através do adele principal, obtemos um mergulho de F em $\mathcal{A}_F$ dado por

$$\begin{array}{rccc} \varphi: & F & \to & \mathcal{A}_F \\ & x & \mapsto & \alpha_x \end{array}$$

Ainda, as valorizações discretas v_P de F/K se estendem naturalmente para $\mathcal{A}_F$ definindo $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a componente P do adele α. Por definição, temos que $v_P(\alpha) \geqslant 0$, para quase todo $P \in \mathbb{P}_F$.

Definindo ainda

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F;\ v_P(\alpha) \geqslant -v_P(A),\ \text{para todo } P \in \mathbb{P}_F\},$$

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

Teorema 3.4.4. *Para cada divisor $A \in Div(F)$, temos que*

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

Demonstração. Faremos a demonstração desse teorema em algumas etapas.

Etapa 1. Sejam A_1, $A_2 \in Div(F)$ tais que $A_1 \leqslant A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e

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

Prova da Etapa 1.

Dado $\alpha \in \mathcal{A}_F(A_1)$, temos que $v_P(\alpha) \geqslant -v_P(A_1) \geqslant -v_P(A_2)$, para todo $P \in \mathbb{P}_F$, pois $A_1 \leqslant A_2$. Logo $\alpha \in \mathcal{A}_F(A_2)$. Isso mostra que $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.

Façamos a prova para o caso em que $A_2 = A_1 + P$, com $P \in \mathbb{P}_F$ (o caso geral resultará deste por indução).

Escolhamos $t \in F$ com $v_P(t) = v_P(A_1) + 1$ e consideremos a transformação linear

$$\begin{array}{rccc} \varphi: & \mathcal{A}_F(A_2) & \to & F_P \\ & \alpha & \mapsto & (t\alpha_P)(P) \end{array}.$$

Notemos que φ está bem definida pois

$$v_P(t\alpha_P) = v_P(t) + v_P(\alpha_P) \geqslant v_P(A_1) + 1 - v_P(A_2) = v_P(A_1) + 1 - (v_P(A_1) + 1) = 0,$$

donde $t\alpha_P \in \mathcal{O}_P$.

Ainda, φ é uma transformação linear sobrejetiva, pois dado $z(P) \in F_P$, $z \in \mathcal{O}_P$, definamos $\alpha = (\alpha_Q) \in \mathcal{A}_F$ por

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

Assim,

$$v_Q(\alpha) = v_Q(t_Q^{-v_Q(A_2)}) = -v_Q(A_2),$$

se $Q \neq P$, e

$$\begin{aligned} v_P(\alpha) = v_P(\alpha_P) &= v_P(t^{-1}z) = -v_P(t) + v_P(z) \\ &= -v_P(A_1) - 1 + v_P(z) = -v_P(A_2) + v_P(z) \\ &\geqslant -v_P(A_2), \end{aligned}$$

o que nos dá que $\alpha \in \mathcal{A}_F(A_2)$. Assim, $z(P) = \varphi(\alpha)$.

Ainda,

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

Daí, $deg(A_2) - deg(A_1) = deg(P) = [F_P : K] = dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1))$.

Etapa 2. Sejam A_1, $A_2 \in Div(F)$ tais que $A_1 \leqslant A_2$. Então

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

Prova da Etapa 2.

Temos a seguinte sequência exata de transformações lineares

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

onde

$$\begin{array}{rccc} \sigma_1: & \mathcal{L}(A_2)/\mathcal{L}(A_1) & \to & \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \\ & \alpha + \mathcal{L}(A_1) & \mapsto & \alpha + \mathcal{A}_F(A_1) \end{array}$$

e

$$\begin{array}{rccc} \sigma_2: & \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) & \to & (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \\ & \alpha + \mathcal{A}_F(A_1) & \mapsto & \alpha + (\mathcal{A}_F(A_1) + F) \end{array}.$$

Com efeito:

- σ_1 está bem definida e é uma transformação linear injetora.

  De fato,

  $$\begin{aligned} \alpha + \mathcal{L}(A_1) = \beta + \mathcal{L}(A_1) &\Leftrightarrow \alpha - \beta \in \mathcal{L}(A_1) \\ &\Leftrightarrow v_P(\alpha - \beta) \geqslant -v_P(A_1), \text{ para todo } P \in \mathbb{P}_F \\ &\Leftrightarrow \alpha - \beta \in \mathcal{A}_F(A_1) \\ &\Leftrightarrow \alpha + \mathcal{A}_F(A_1) = \beta + \mathcal{A}_F(A_1), \text{ para } \alpha,\, \beta \in \mathcal{L}(A_2). \end{aligned}$$

  Ainda, σ_1 é uma transformação linear por definição.

- σ_2 está bem definida e é uma transformação linear sobrejetora.

  De fato, dados $\alpha, \beta \in \mathcal{A}_F(A_2)$ tais que $\alpha + \mathcal{A}_F(A_1) = \beta + \mathcal{A}_F(A_1)$, temos que $\alpha - \beta \in \mathcal{A}_F(A_1)$ implica que $\alpha - \beta \in \mathcal{A}_F(A_1) + F$, donde

  $$\alpha + (\mathcal{A}_F(A_1) + F) = \beta + (\mathcal{A}_F(A_2) + F),$$

  o que mostra que σ_2 está bem definida. Ainda, dado

  $$\alpha + (\mathcal{A}_F(A_1) + F) \in (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F),$$

  com $\alpha \in \mathcal{A}_F(A_2) + F$, temos que $\alpha = \alpha_2 + f$, $\alpha_2 \in \mathcal{A}_F(A_2)$, $f \in F$. Daí,

  $$\begin{aligned}\sigma_2(\alpha_2 + \mathcal{A}_F(A_1)) &= \alpha_2 + (\mathcal{A}_F(A_1) + F)\\ &= \alpha - f + (\mathcal{A}_F(A_1) + F)\\ &= \alpha + (\mathcal{A}_F(A_1) + F),\end{aligned}$$

  o que mostra σ_2 é sobrejetora.

- $Im(\sigma_1) = Ker(\sigma_2)$

  ($\subseteq$) Seja $\alpha + \mathcal{A}_F(A_1) \in \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)$ tal que $\alpha \in \mathcal{L}(A_2) \subseteq F$. Então $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = \alpha + (\mathcal{A}_F(A_1) + F) = \mathcal{A}_F(A_1) + F$, donde

  $$\alpha + \mathcal{A}_F(A_1) \in Ker(\sigma_2).$$

  Isso mostra que $Im(\sigma_1) \subseteq Ker(\sigma_2)$.

  ($\supseteq$) Seja $\alpha \in \mathcal{A}_F(A_2)$, com $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$. Então, $\alpha \in \mathcal{A}_F(A_1) + F$, donde 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 $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$. Daí, $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathcal{L}(A_1))$. Isso mostra que $Ker(\sigma_2) \subseteq Im(\sigma_1)$.

Como a sequência inicial é uma sequência exata, obtemos que

$$\begin{aligned}dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) &= dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - dim(Ker(\sigma_2))\\ &= dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - dim(Im(\sigma_1))\\ &= dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - dim(\mathcal{L}(A_2)/\mathcal{L}(A_1))\\ &= (deg(A_2) - deg(A_1)) - (\ell(A_2) - \ell(A_1)),\end{aligned}$$

onde a última igualdade segue da *Etapa 1* e do Lema 3.3.17.

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

Prova da Etapa 3.

Inicialmente, observemos que, para $B_1 \geqslant B$, temos, pelo Lema 3.3.17, que

$$\ell(B_1) - \ell(B) = dim(\mathcal{L}(B_1)/\mathcal{L}(B)) \leqslant deg(B_1) - deg(B),$$

donde

$$\ell(B_1) \leqslant deg(B_1) + \ell(B) - deg(B) = deg(B_1) + 1 - g.$$

Por outro lado, $\ell(B_1) \geqslant deg(B_1) + 1 - g$, pelo Teorema de Riemann. Portanto, $\ell(B_1) = deg(B_1) + 1 - g$, para cada $B_1 \geqslant B$.

Seja $\alpha \in \mathcal{A}_F$. Se $\alpha \in \mathcal{A}_F(B)$, então $\alpha \in \mathcal{A}_F(B) + F$. Caso contrário, seja

$$B_1 = \sum_{v_P(\alpha_P) \geqslant -v_P(B)} v_P(B) \, . \, P + \sum_{v_P(\alpha_P) < -v_P(B)} -v_P(\alpha_P) \, . \, P.$$

Notemos que B_1 é um divisor bem definido, pois $v_P(B) = 0$, para quase todo P, e $v_P(\alpha_P) \geqslant 0$, para quase todo P, donde, na primeira parcela da soma anterior, $v_P(B) \neq 0$, para um número finito de lugares P, e, na segunda parcela, temos que $-v_P(\alpha_P) \neq 0$ para um número finito de lugares P. De fato, se $v_P(B) = 0$, temos que $v_P(\alpha_P) < 0$, o que ocorre para um número finito de lugares P pela definição α. Se $v_P(B) \neq 0$, temos que $v_P(\alpha_P) < -v_P(B) \neq 0$, o que ocorre para um número finito de lugares P. Logo, na segunda parcela, também temos um número finito de lugares tais que $v_P(\alpha_P) \neq 0$.

Ainda $B_1 \geqslant B$, pois $v_P(B_1) = v_P(B)$, se $v_P(\alpha_P) \geqslant -v_P(B)$, e $v_P(B_1) = -v_P(\alpha_P) > v_P(B)$, se $v_P(\alpha_P) < -v_P(B)$. Além disso, $\alpha \in \mathcal{A}_F(B_1)$, pois $v_P(\alpha_P) \geqslant -v_P(B_1)$, se $v_P(\alpha_P) \geqslant -v_P(B)$, e $v_P(\alpha_P) = -v_P(B_1)$, se $v_P(\alpha_P) < -v_P(B)$.

Pela *Etapa 2*, temos que

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

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

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

Etapa 4. Conclusão da demonstração do teorema.

Consideremos um divisor arbitrário A. Pelo Teorema de Riemann (Teorema 3.3.25), existe um divisor $A_1 \geqslant A$ tal que $\ell(A_1) = deg(A_1) + 1 - g$. Pela *Etapa 3*, $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$, e, pela *Etapa 2*, temos que

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

■

Corolário 3.4.5. $g = dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Demonstração. Com efeito,

$$i(0) = \ell(0) - deg(0) + g - 1 = g \quad \text{e} \quad i(0) = dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)),$$

pelo Teorema 3.4.4. ■

Definição 3.4.6. Um diferencial de Weil de F/K é uma tranformação linear $w : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A) + F$, para algum divisor $A \in Div(F)$. Chamaremos

$$\Omega_F = \{w;\ w \text{ é um diferencial de Weil de } F/K\}$$

o conjunto dos diferenciais de Weil de F/K. Para $A \in Div(F)$, definimos

$$\Omega_F(A) = \{w \in \Omega_F;\ w \text{ se anula em } \mathcal{A}_F(A) + F\}.$$

Observação 3.4.7. Consideraremos Ω_F como um espaço vetorial sobre K e $\Omega_F(A)$ um subespaço vetorial de Ω_F.

Lema 3.4.8. *Para $A \in Div(F)$, temos que $dim(\Omega_F(A)) = i(A)$.*

Demonstração. Seja $(\mathcal{A}_F/(\mathcal{A}_F(A) + F))^* = V^*$ o espaço dual de

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

Então, $dim(V) = dim(V^*)$.

Consideremos a aplicação

$$\varphi: \begin{array}{ccc} \Omega_F(A) & \to & V^* \\ w & \mapsto & \varphi(w) \end{array}, \quad \text{onde} \quad \varphi(w): \begin{array}{ccc} V & \to & K \\ \overline{\alpha} & \mapsto & w(\alpha) \end{array}.$$

Então:

$\varphi(w)$ é um funcional linear.

Com efeito, $\varphi(w)$ está bem definido, pois se $\overline{\alpha} = \overline{\beta}$, então $\alpha - \beta \in \mathcal{A}_F(A) + F$, donde $w(\alpha - \beta) = 0$ e assim $\varphi(w)(\overline{\alpha}) = w(\alpha) = w(\beta) = \varphi(w)(\overline{\beta})$. A linearidade de $\varphi(w)$ segue da linearidade de w.

φ é injetora.

Com efeito, se w, $w' \in \Omega_F(A)$ são tais que $\varphi(w) = \varphi(w')$, então, para todo $\overline{\alpha} \in V$ temos que $\varphi(w)(\overline{\alpha}) = w(\overline{\alpha}) = w'(\overline{\alpha}) = \varphi(w')(\overline{\alpha})$. Assim, para todo $\alpha \in \mathcal{A}_F$, $\overline{\alpha} \in V$ e $w(\alpha) = \varphi(w)(\overline{\alpha}) = \varphi(w')(\overline{\alpha}) = w'(\alpha)$, o que mostra que φ é injetora.

φ é sobrejetora.

Com efeito, dado $g \in V^*$, seja

$$w: \begin{array}{ccc} \mathcal{A}_F & \to & K \\ \alpha & \mapsto & g(\overline{\alpha}) \end{array}.$$

Então:

- w é linear, pois g é linear.
- $w \in \Omega_F(A)$, pois se $\alpha = \alpha_A + f \in \mathcal{A}_F(A) + F$, com $\alpha_A \in \mathcal{A}_F(A)$ e $f \in F$, temos que $w(\alpha) = g(\overline{\alpha}) = g(\overline{0}) = 0$.

Ainda, $\varphi(w)(\overline{\alpha}) = w(\alpha) = g(\overline{\alpha})$, para todo $\overline{\alpha} \in V$, donde $\varphi(w) = g$.

φ é linear.

Segue do fato de w ser linear.

As passagens anteriores nos mostram que $V^* \simeq \Omega_F(A)$, donde

$$i(A) = dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = dim(V^*) = dim(\Omega_F(A)),$$

pelo Teorema 3.4.4. ■

Corolário 3.4.9. $\Omega_F \neq \{0\}$.

Demonstração. Escolhamos um divisor A tal que $deg(A) \leqslant -2$. Então

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

donde $\Omega_F(A) \neq \{0\}$. Como $\Omega_F(A) \subseteq \Omega_F$, temos que o resultado segue. ■

Definição 3.4.10. Para $x \in F$ e $w \in \Omega_F$, definimos

$$\begin{array}{rccc} xw: & \mathcal{A}_F & \to & K \\ & \alpha & \mapsto & w(x\alpha) \end{array}.$$

Observação 3.4.11. *a)* $xw \in \Omega_F$.

Se w se anula em $\mathcal{A}_F(A)+F$, então xw se anula em $\mathcal{A}_F(A+(x))+F$. De fato, se $\alpha = \alpha_{Ax}+f$, onde $\alpha_{Ax} \in \mathcal{A}_F(A+(x))$ e $f \in F$, temos que $x\alpha \in \mathcal{A}_F(A)+F$, pois

$$\begin{aligned} v_P(x\alpha_{Ax}) &= v_P(x) + v_P(\alpha_{Ax}) \\ &\geqslant v_P(x) - v_P(A+(x)) \\ &= v_P(x) - (v_P(A) + v_P(x)) \\ &= -v_P(A) \end{aligned}$$

e $xf \in F$. Daí, $xw(\alpha) = w(x\alpha) = 0$, pois $w \in \mathcal{A}_F(A) + F$.

A linearidade de xw segue da linearidade de w e da distributividade do produto por escalar.

b) Definindo o produto por escalar como na Definição 3.4.10, temos que Ω_F pode ser considerado um espaço vetorial sobre F.

Proposição 3.4.12. *Ω_F é um espaço vetorial de dimensão* 1 *sobre F.*

Demonstração. Escolhamos $0 \neq w_1 \in \Omega_F$ (notemos que esse elemento existe pelo Corolário 3.4.9). Temos que mostrar que para todo $w_2 \in \Omega_F$ existe $z \in F$ tal que $w_2 = zw_1$.

Se $w_2 = 0$, basta tomarmos $z = 0$. Suponhamos agora que $w_2 \neq 0$. Escolhamos A_1, $A_2 \in Div(F)$ tais que $w_1 \in \Omega_F(A_1)$ e $w_2 \in \Omega_F(A_2)$, onde a existência desses divisores segue da definição de diferencial de Weil. Para cada $B \in Div(F)$ consideremos as transforações lineares injetivas

$$\begin{array}{rccc} \varphi_i : & \mathcal{L}(A_i + B) & \to & \Omega_F(-B) \\ & x & \mapsto & xw_i \end{array}, \text{ para } i = 1, 2.$$

Afirmação. Para uma escolha apropriada do divisor B, temos que

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

Utilizando essa afirmação, podemos concluir a demonstração do seguinte modo: escolhamos $x_i \in \mathcal{L}(A_i + B)$, $i = 1, 2$, tal que $x_1 w_1 = x_2 w_2 \neq 0$. Então

$$w_2 = (x_2^{-1} x_1) w_1,$$

como queríamos mostrar.

Prova da Afirmação. Para iniciarmos a demonstração, recordemos que se U_1, U_2 são subespaços de um espaço vetorial V de dimensão finita, então

$$dim(U_1 \cap U_2) \geqslant dim(U_1) + dim(U_2) - dim(V),$$

pois

$$dim(U_1 \cap U_2) = dim(U_1) + dim(U_2) - dim(U_1 + U_2) \;\text{ e }\; dim(U_1 + U_2) \leqslant dim(V).$$

Seja $B > 0$ um divisor de grau suficientemente grande tal que

$$\ell(A_i + B) = deg(A_i + B) + 1 - g,$$

para $i = 1, 2$ (vejamos que isso é possível pelo Teorema de Riemann).

Definamos $U_i = \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Como

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

onde a segunda igualdade segue do Lema 3.3.16, obtemos

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

Como o termo $deg(A_1) + deg(A_2) + 3(1 - g)$ independe de B, temos que

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

se $deg(B)$ for suficientemente grande.

Pela propriedade apresentada no início da demonstração dessa afirmação, temos que $dim(U_1 \cap U_2) > 0$, o que nos dá que $U_1 \cap U_2 \neq \{0\}$, como queríamos mostrar. ■

Definição 3.4.13. Definimos o conjunto

$$M(w) = \{A \in Div(F);\ w \text{ se anula em } \mathcal{A}_F(A) + F\},$$

onde $w \in \Omega_F \backslash \{0\}$.

Lema 3.4.14. *Seja $0 \neq w \in \Omega_F$. Então existe um único divisor $W \in M(w)$ tal que $A \leqslant W$, para todo $A \in M(w)$.*

Demonstração. Pelo Teorema de Riemann, existe uma constante c, que depende unicamente do corpo de funções F/K, tal que $i(A) = 0$, para todo $A \in Div(F)$, com $deg(A) \geqslant c$.

Como $dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$ pelo Teorema 3.4.4, temos que $deg(A) < c$, para todo $A \in M(w)$. Daí, podemos escolher um divisor $W \in M(w)$ de grau máximo.

Suponhamos que W não satisfaça a propriedade do enunciado do lema. Então existe um divisor $A_0 \in M(w)$ com $A_0 \nleqslant W$, isto é, $v_Q(A_0) > v_Q(W)$, para algum $Q \in \mathbb{P}_F$.

Afirmamos que $W + Q \in M(w)$, o que é uma contradição com a maximalidade de W.

De fato, consideremos um adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Podemos escrever $\alpha = \alpha' + \alpha''$, com

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

e

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

Então $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in \mathcal{A}_F(A_0)$. Com efeito, $v_P(\alpha_P) \geqslant -v_P(W)$, se $P \neq Q$, e $v_Q(0) = \infty > -v_Q(W)$, donde $\alpha' \in \mathcal{A}_F(W)$, e $v_P(0) = \infty > -v_P(A_0)$, se $P \neq Q$, e $v_Q(\alpha_Q) \geqslant -v_Q(W) - 1 \geqslant v_Q(A_0)$, pois $v_Q(A_0) > v_Q(W)$ implica que $v_Q(A_0) \geqslant v_Q(W) + 1$, donde $\alpha'' \in \mathcal{A}_F(A_0)$.

Daí, $w(\alpha) = w(\alpha') + w(\alpha'') = 0$, de modo que w se anula em $\mathcal{A}_F(W + Q) + F$, como queríamos mostar.

A unicidade de W segue então do fato de $A \leqslant W$, para todo $A \in M(w)$. ■

Definição 3.4.15. *a)* O divisor (w) do diferencial de Weil $w \neq 0$ é o único divisor de F/K satisfazendo:

($*$) w se anula em $\mathcal{A}_F((w)) + F$;

($**$) Se w se anula em $\mathcal{A}_F(A) + F$, então $A \leqslant (w)$.

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

c) Um divisor W é chamado divisor canônico de F/K se $W = (w)$, para algum $w \in \Omega_F$.

Observação 3.4.16. Segue das definições que

$$\Omega_F(A) = \{w \in \Omega_F;\ w = 0 \text{ ou } (w) \geqslant A\}.$$

Proposição 3.4.17. *Para $0 \neq x \in F$ e $0 \neq w \in \Omega_F$, temos que $(xw) = (x) + (w)$.*

Demonstração. Se w se anula em $\mathcal{A}_F(A)+F$, então xw se anula em $\mathcal{A}_F(A+(x))+F$, pela Observação 3.4.11. Em particular, como w se anula em $\mathcal{A}_F((w))+F$, temos que xw se anula em $\mathcal{A}_F((w)+(x))+F$, donde, pela Definição 3.4.15, temos que $(w)+(x) \leqslant (xw)$.

Do mesmo modo, podemos mostrar que $(xw)+(x^{-1}) \leqslant (x^{-1}xw) = (w)$.

Combinando as duas desigualdades anteriores, temos que

$$(w)+(x) \leqslant (xw) \leqslant -(x^{-1})+(w) = (x)+(w),$$

o que conclui a demonstração. ■

Teorema 3.4.18 (Teorema da Dualidade)**.** *Sejam A um divisor arbitrário e $W = (w)$ um divisor canônico de F/K. Então a aplicação*

$$\begin{array}{rccc} \mu: & \mathcal{L}(W-A) & \to & \Omega_F(A) \\ & x & \mapsto & xw \end{array}$$

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

Demonstração. Para $x \in \mathcal{L}(W-A)$, temos que

$$(xw) = (x)+(w) \geqslant A - W + W = A.$$

Logo $xw \in \Omega_F(A)$, pela Observação 3.4.16 e μ é efetivamente uma aplicação de $\mathcal{L}(W-A)$ em $\Omega_F(A)$.

Temos também que μ é uma transformação linear, em virtude da linearidade do produto por escalar.

Ainda, μ é injetora, pois se $x \,.\, w = 0$, com $x \in \mathcal{L}(W-A)$, como $w \neq 0$, temos que ter $x = 0$, o que mostra que $Ker(\mu) = \{0\}$.

Com o intuito de mostrarmos que μ é sobrejetora, consideremos um diferencial de Weil $w_1 \in \Omega_F(A)$. Pela Proposição 3.4.12, podemos escrever $w_1 = xw$, para algum $x \in F$. Como

$$(x)+W = (x)+(w) = (xw) = (w_1) \geqslant A,$$

obtemos que $(x) \geqslant A - W$, de modo que $x \in \mathcal{L}(W-A)$. Logo $w_1 = \mu(x)$.

Portanto, $\ell(W-A) = dim(\Omega_F(A)) = i(A)$. ■

Teorema 3.4.19 (Teorema de Riemann-Roch)**.** *Seja W um divisor canônico de F/K. Então, para cada divisor $A \in Div(F)$,*

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

Demonstração. Pela Definição 3.4.1, temos que $i(A) = \ell(A) - deg(A) + g - 1$. Ainda, pelo Teorema 3.4.18, temos que $i(A) = \ell(W - A)$. Portanto,

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

como queríamos mostrar. ■

Corolário 3.4.20. *Para um divisor canônico W, temos que $deg(W) = 2g - 2$ e $\ell(W) = g$.*

Demonstração. Para $A = 0$, o Teorema de Riemann-Roch e o Lema 3.3.16 nos dão que $1 = \ell(0) = deg(0) + 1 - g + \ell(W - 0)$, donde $\ell(W) = g$.

Fazendo $A = W$, temos, pelo Teorema de Riemann-Roch, que

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

isto é, $deg(W) = 2g - 2$, o que conclui a demonstração. ■

Teorema 3.4.21. *Se A é um divisor de F/K de grau $deg(A) \geqslant 2g - 1$, então $\ell(A) = deg(A) + 1 - g$.*

Demonstração. Temos que $\ell(A) = deg(A) + 1 - g + \ell(W - A)$, onde W é um divisor canônico.

Como $deg(A) \geqslant 2g - 1$ e $deg(W) = 2g - 2$, concluímos que $deg(W - A) = deg(W) - deg(A) \leqslant 2g - 2 - (2g - 1) = -1 < 0$. Pelo Corolário 3.3.21, temos que $\ell(W - A) = 0$.

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

Teorema 3.4.22 (Teorema da Aproximação Forte)**.** *Sejam $S \subsetneq \mathbb{P}_F$ e $P_1, \ldots, P_r \in S$. Suponhamos que sejam dados elementos $x_1, \ldots, x_r \in F$ e inteiros $n_1, \ldots, n_r \in \mathbb{Z}$. Então existe um elemento $x \in F$ tal que $v_{P_i}(x - x_i) = n_i$, para $i = 1, \ldots, r$, e $v_P(x) \geqslant 0$, para todo $P \in S \backslash \{P_1, \ldots, P_r\}$.*

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

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

Escolhamos um lugar $Q \in \mathbb{P}_F \backslash S$. Para $m \in \mathbb{N}$ suficientemente grande, temos que

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

Com efeito, para m suficientemente grande,

$$\begin{aligned} deg\left(mQ - \sum_{i=1}^{r}(n_i+1)P_i\right) &= \sum_{P\in\mathbb{P}_F} v_P(A)\,.\,deg(P) \\ &= m\,.\,deg(Q) - \sum_{i=1}^{r}(n_i+1)\,.\,deg(P_i) \\ &\geqslant 2g-1, \end{aligned}$$

onde $A = mQ - \sum_{i=1}^{r}(n_i+1)P_i$. Daí, $0 = i(A) = dim\,(\mathcal{A}_F/(\mathcal{A}_F(A)+F))$, onde a primeira igualdade segue do Teorema 3.4.21 e a segunda igualdade segue do Teorema 3.4.4. Em outras palavras, $\mathcal{A}_F = \mathcal{A}_F(A) + F$.

Pela igualdade anterior, existe $z \in F$ tal que $z - \alpha \in \mathcal{A}_F(A)$. Isso significa que $v_{P_i}(z - x_i) \geqslant n_i + 1 > n_i$, para $i = 1, \ldots, r$, e $v_P(z) \geqslant 0$, para todo P pertencente à $S\backslash\{P_1, \ldots, P_r\}$.

Escolhamos $y_1, \ldots, y_r \in F$, com $v_{P_i}(y_i) = n_i$. Pelo mesmo processo realizado acima, podemos obter $y \in F$ tal que $v_{P_i}(y - y_i) > n_i$, para $i = 1, \ldots, r$, e $v_P(y) \geqslant 0$, para todo $P \in S\backslash\{P_1, \ldots, Pr\}$.

Daí, pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que

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

Definindo $x = y + z$, temos que

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = min\{v_{P_i}(y),\, v_{P_i}(z - x_i)\} = v_{P_i}(y) = n_i,\ \forall\, i = 1, \ldots, r.$$

Para $P \in S\backslash\{P_1, \ldots, P_r\}$, $v_P(x) = v_P(y + z) \geqslant min\{v_P(y),\, v_P(z)\} \geqslant 0$. ■

Proposição 3.4.23. *Seja $P \in \mathbb{P}_F$. Então, para cada $n \geqslant 2g$, existe um elemento $x \in F$ com divisor de polos $(x)_\infty = nP$.*

Demonstração. Pelo Teorema 3.4.21, temos que $\ell((n-1)P) = (n-1)\,deg(P)+1-g$ e $\ell(nP) = n\,.\,deg(P)+1-g$. Logo $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$, pelo Lema 3.3.17. Todo elemento $x \in \mathcal{L}(nP)\backslash\mathcal{L}((n-1)P)$ possui divisor de polos nP. De fato, $v_Q(x) \geqslant 0$ $(*)$, para todo $Q \in \mathbb{P}_F\backslash\{P\}$, e $v_P(x) \geqslant -n$, pois $x \in \mathcal{L}(nP)$. Por outro lado, como $x \notin \mathcal{L}((n-1)P)$, pela desigualdade $(*)$ temos que ter $v_P(x) < -(n-1)$. Daí, temos que $v_P(x) = -n < 0$. Como $v_P(x) = -n < 0$ e $v_Q(x) \geqslant 0$, para todo $Q \in \mathbb{P}_F\backslash\{P\}$, temos que $(x)_\infty = nP$. ■

3.5 COMPONENTES LOCAIS DE DIFERENCIAIS DE WEIL

Definição 3.5.1. Seja $P \in \mathbb{P}_F$.

a) Para $x \in F$, definimos $\iota_P(x) \in \mathcal{A}_F$ como o adele cuja componente P é x e todas as outras componentes são nulas.

b) Para um diferencial de Weil $w \in \Omega_F$, definimos sua componente local

$$\begin{array}{rccc} w_P: & F & \to & K \\ & x & \mapsto & w(\iota_P(x)) \end{array}.$$

Observação 3.5.2. Notemos que w_P é uma transformação linear sobre K.

Proposição 3.5.3. *a) Seja $w \neq 0$ um diferencial de Weil de F/K e $P \in \mathbb{P}_F$. Então $v_P(w) = max\{r \in \mathbb{Z};\ w_P(x) = 0$ para todo $x \in F$ com $v_P(x) \geqslant -r\}$. Em particular, w_P não é a função identicamente nula.*

b) Se w e $w' \in \Omega_F$ e $w_P = w'_P$, para algum $P \in \mathbb{P}_F$, então $w = w'$.

Demonstração. a) Recordemos que, por definição $v_P(w) = v_P(W)$, onde $W = (w)$ denota o divisor do diferencial de Weil w. Seja $s = v_P(w)$. Para $x \in F$ com $v_P(x) \geqslant -s$, temos que $\iota_P(x) \in \mathcal{A}_F(W)$. Logo $w_P(x) = w(\iota_P(x)) = 0$.

Suponhamos agora que $w_P(x) = 0$ para todo $x \in F$, com $v_P(x) \geqslant -(s+1)$. Seja $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W+P)$. Então $\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$, com $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$, pois

$$\alpha - \iota_P(\alpha_P) = \begin{cases} \alpha_Q, & \text{se } Q \neq P \\ 0, & \text{se } Q = P, \end{cases}$$

e $v_P(\alpha_P) \geqslant -(s+1)$, pois $v_P(W+P) = v_P(W) + 1 = s+1$.

Logo,

$$w(\alpha) = w(\alpha - \iota_P(\alpha_P)) + w(\iota_P(\alpha_P)) = w(\alpha - \iota_P(\alpha_P)) + w_P(\alpha_P) = 0.$$

Assim, w se anula em $\mathcal{A}_F(W+P)$, o que é uma contradição com a definição de W, pois $W \leqslant W+P$.

b)

$$\begin{aligned} w_P = w'_P &\Rightarrow w_P(x) = w'_P(x), \text{ para todo } x \in F \\ &\Rightarrow w(\iota_P(x)) = w'(\iota_P(x)), \text{ para todo } x \in F \\ &\Rightarrow (w - w')(\iota_P(x)) = 0, \text{ para todo } x \in F \\ &\Rightarrow (w - w')_P(x) = 0, \text{ para todo } x \in F \\ &\Rightarrow (w - w')_P = 0 \\ &\Rightarrow w - w' = 0, \end{aligned}$$

onde a última igualdade segue da letra a). ■

4 EXTENSÕES DE CORPOS DE FUNÇÕES ALGÉBRICAS

Ao longo deste capítulo, F/K irá denotar um corpo de funções, onde K é um corpo perfeito e algebricamente fechado em F. Também consideraremos um corpo de funções F'/K', onde K' é algebricamente fechado em F', F'/F é uma extensão algébrica e $K' \supseteq K$. Fixaremos ainda um corpo algebricamente fechado $\Phi \supseteq F$ e consideraremos apenas extensões F'/F com $F' \subseteq \Phi$.

4.1 EXTENSÕES ALGÉBRICAS DE CORPOS DE FUNÇÕES

Definição 4.1.1. *a)* Um corpo de funções F'/K' é dito uma extensão algébrica de F/K se F'/F é uma extensão algébrica e $K \subseteq K'$.

b) A extensão algébrica F'/K' de F/K é chamada uma extensão por constantes se $F' = FK'$, onde FK' é o compósito de F e K', isto é, $F' = FK'$ é o menor subcorpo de Φ que contém F e K'.

c) A extensão algébrica F'/K' de F/K é chamada uma extensão finita se $[F' : F] < \infty$.

Lema 4.1.2. *Seja F'/K' uma extensão algébrica de F/K. Então:*

a) K'/K é uma extensão algébrica e $F \cap K' = K$.

b) F'/K' é uma extensão finita de F/K se, e somente se, $[K' : K] < \infty$.

c) Seja $F_1 = FK'$. Então F_1/K' é uma extensão por constantes de F/K e F'/K' é uma extensão finita de F_1/K'.

Demonstração. a) Sejam $z \in F$ e $z' \in F'$ tais que

$$[F : K(z)] < \infty \quad \text{e} \quad [F' : K'(z')] < \infty.$$

Recordando as propriedades apresentadas na Seção 2.8, temos que:

- F'/F ser uma extensão algébrica implica que $trdeg(F'|F) = 0$.

- Como $F/K(z)$ é uma extensão finita (algébrica), segue que $trdeg(F|K(z)) = 0$.
- Temos que $\{z\}$ é uma base de transcendência de $K(z)/K$, de modo que $trdeg(K(z)|K) = 1$.
- Como $F'/K'(z)$ é uma extensão finita (algébrica), $trdeg(F'|K'(z')) = 0$.
- $\{z'\}$ é uma base de transcedência de $K'(z')/K'$, donde $trdeg(K'(z')|K') = 1$.

Pelos itens anteriores, temos que $trdeg(K'|K) = 0$. Assim, K'/K é uma extensão algébrica. Ainda, temos que $K \subseteq F$ e $K \subseteq K'$, donde $K \subseteq F \cap K'$. Por outro lado, se $x \in F \cap K'$, temos que $x \in F$ e x é algébrico sobre K, pois $x \in K'$. Como K é algebricamente fechado em F, temos que $x \in K$, o que mostra que $F \cap K' \subseteq K$.

As passagens anteriores concluem a demonstração dessa parte.

b) ($\Rightarrow$) Suponhamos que F'/K' é uma extensão finita de F/K. Então F' pode ser considerado um corpo de funções sobre K cujo corpo de constantes é K'. Com efeito, por hipótese F'/F é uma extensão finita (algébrica) e como F/K é um corpo de funções, temos que existe $z \in F$, z transcendente sobre K, tal que $[F : K(z)] < \infty$. Isso nos dá que $F'/K(z)$ é uma extensão finita. Ainda, como K' é algebricamente fechado em F', temos que o corpo de constantes de F'/K é K'.

Portanto, pelo Corolário 3.1.23, é possível concluirmos que $[K' : K] < \infty$.

($\Leftarrow$) Suponhamos que $[K' : K] < \infty$. Dado $x \in F \backslash K$, temos que $F'/K'(x)$ é uma extensão finita, pois x é transcendente sobre K'. Com efeito, se o contrário ocorresse, teríamos que x seria algébrico sobre K, pelo Teorema 2.1.11, o que seria uma contradição. Como $[K'(x) : K(x)] = [K' : K] < \infty$ pelo Lema 4.1.11, obtemos que $[F' : F] < \infty$.

c) Temos que K' é o corpo de constantes de F_1/K' (tal fato será demonstrado na Proposição 4.6.2). Como F' é uma extensão algébrica de F, segue que F_1 também o é. Isso nos dá que F_1/K' é uma extensão algébrica de F/K, o que mostra que F'/K' é uma extensão por constantes de F/K.

Ainda, sendo $[K' : K'] = 1$, temos, pela letra *b*), que F'/K' é uma extensão finita de F_1/K'. ■

Definição 4.1.3. Consideremos uma extensão algébrica F'/K' de F/K. Um lugar $P' \in \mathbb{P}_{F'}$ é dito estar acima de $P \in \mathbb{P}_F$, e escrevemos $P'|P$, se $P \subseteq P'$. Neste caso, também falamos que P' é uma extensão de P ou que P está abaixo de P'.

Proposição 4.1.4. *Seja F'/K' uma extensão algébrica de F/K. Sejam ainda P um lugar de F/K, P' um lugar de F'/K', $\mathcal{O}_P \subseteq F$ e $\mathcal{O}_{P'} \subseteq F'$ os respectivos anéis de valorização e v_P e $v_{P'}$ as respectivas valorizações discretas. Então as seguintes afirmações são equivalentes:*

a) $P'|P$.

b) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

c) Existe um inteiro $e \geqslant 1$ tal que $v_{P'}(x) = e \,.\, v_P(x)$, para todo $x \in F$.

Mais ainda: se $P'|P$, então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Por isso, P é também chamada a restrição de P' a F.

Demonstração. Etapa 1. a) $\Rightarrow$ b)

Suponhamos que $P'|P$, mas $\mathcal{O}_P \nsubseteq \mathcal{O}_{P'}$. Então existe $u \in F$ tal que $v_P(u) \geqslant 0$ e $v_{P'}(u) < 0$. Como $P \subseteq P'$, temos que $v_P(u) = 0$.

Escolhamos $t \in F$ tal que $v_P(t) = 1$. Então $t \in P \subseteq P'$ e $r = v_{P'}(t) > 0$. Consequentemente,

$$v_P(u^r t) = r \,.\, v_P(u) + v_P(t) = 1$$

e

$$v_{P'}(u^r t) = r \,.\, v_{P'}(u) + v_{P'}(t) \leqslant -r + r = 0.$$

Logo $u^r t \in P \backslash P'$, o que é uma contradição, pois $P \subseteq P'$.

Etapa 2. $\mathcal{O}_P \subseteq \mathcal{O}_{P'} \Rightarrow \mathcal{O}_P = F \cap \mathcal{O}_{P'}$.

Temos que $F \cap \mathcal{O}_{P'}$ é um subanel de F e $\mathcal{O}_P \subseteq F \cap \mathcal{O}_{P'}$. Portanto, pelo Teorema 3.1.19 d), temos que $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$ ou $F \cap \mathcal{O}_{P'} = F$.

Suponhamos que $F \cap \mathcal{O}_{P'} = F$, isto é, $F \subseteq \mathcal{O}_{P'}$. Escolhendo um elemento $z \in F' \backslash \mathcal{O}_{P'}$, como F'/F é uma extensão algébrica, existe uma equação da forma

$z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + c_0 = 0$, com $c_\nu \in F$. Temos então que

$$v_{P'}(z^n) = n \,.\, v_{P'}(z) < 0,$$

pois $z \notin \mathcal{O}_{P'}$. Portanto, $v_{P'}(c_\nu z^\nu) = v_{P'}(c_\nu) + \nu \,.\, v_{P'}(z) > n \,.\, v_{P'}(z) = v_{P'}(z^n)$, para $\nu = 1, \ldots, n-1$, e $v_{P'}(c_0) \geqslant 0 > v_{P'}(z^n)$.

Pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que

$$v_{P'}(z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + c_0) = n \,.\, v_{P'}(z) < \infty = v_{P'}(0),$$

o que é uma contradição.

Portanto, $F \nsubseteq \mathcal{O}_{P'}$, donde $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$.

Etapa 3. $b) \Rightarrow a)$

Suponhamos que $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Dado $y \in P$, temos que $y^{-1} \notin \mathcal{O}_P$, pela Proposição 3.1.8. Pela *Etapa 2*, isso nos dá que $y^{-1} \notin \mathcal{O}_{P'}$. Aplicando novamente a Proposição 3.1.8, obtemos que $y = (y^{-1})^{-1} \in P'$. Logo $P \subseteq P'$.

Etapa 4. $b) \Rightarrow c)$

Seja $u \in F$ um elemento com $v_P(u) = 0$. Então, temos que u, $u^{-1} \in \mathcal{O}_{P'}$, uma vez que u, $u^{-1} \in \mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Logo $v_{P'}(u) = 0$.

Escolhamos $t \in F$ com $v_P(t) = 1$ e coloquemos $e = v_{P'}(t)$. Como $P \subseteq P'$ (pela *Etapa 3*), temos que $e \geqslant 1$.

Sejam $0 \neq x \in F$ e $v_P(x) = r \in \mathbb{Z}$. Então $v_P(xt^{-r}) = v_P(x) - r \,.\, v_P(t) = 0$ e obtemos

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + r \,.\, v_{P'}(t) = r \,.\, e = e \,.\, v_P(x).$$

Etapa 5. $c) \Rightarrow b)$

Se $x \in \mathcal{O}_P$, então $v_P(x) \geqslant 0$ e assim $v_{P'}(x) = e \,.\, v_P(x) \geqslant 0$. Logo $x \in \mathcal{O}_{P'}$.

Etapa 6. $P'|P \Rightarrow P = P' \cap F$.

A inclusão $P \subseteq P' \cap F$ segue do fato de $P \subseteq P'$ e $P \subseteq F$. Agora, se $x \in F$ e $v_{P'}(x) > 0$, então $e \,.\, v_P(x) = v_{P'}(x) > 0$, donde $v_P(x) > 0$, pois $e \geqslant 1$. Isso mostra que $P' \cap F \subseteq P$. ■

Observação 4.1.5. Uma consequência da Proposição 4.1.4 é que, para $P'|P$, existe um homomorfismo injetor canônico de $F_P = \mathcal{O}_P/P$ em $F'_{P'} = \mathcal{O}_{P'}/P'$ dado por

$$x(P) \mapsto x(P') \text{ para } x \in \mathcal{O}_P.$$

Dessa forma, podemos considerar F_P um subcorpo de $F'_{P'}$.

Definição 4.1.6. Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$.

a) O inteiro $e(P'|P)$ tal que $v_{P'}(x) = e(P'|P)\,.\,v_P(x)$, para todo $x \in F$, é chamado índice de ramificação de P' sobre P. Dizemos que $P'|P$ é ramificado se $e(P'|P) > 1$ e que $P'|P$ é não ramificado se $e(P'|P) = 1$.

b) $f(P'|P) = [F'_{P'} : F_P]$ é chamado o grau relativo de $P'|P$.

Proposição 4.1.7. *Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$. Então:*

a) $f(P'|P) < \infty$ *se, e somente se,* $[F' : F] < \infty$.

b) Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ é uma extensão de P', então $e(P''|P) = e(P''|P')\,.\,e(P'|P)$ e $f(P''|P) = f(P''|P')\,.\,f(P'|P)$.

Demonstração. a) Consideremos as inclusões $K \subseteq F_P \subseteq F'_{P'}$ e $K \subseteq K' \subseteq F'_{P'}$, onde $[F_P : K] < \infty$ e $[F'_{P'} : K'] < \infty$. Então, segue que $[F'_{P'} : F_P] < \infty$ se, e somente se, $[K' : K] < \infty$. Dessa forma, o Lema 4.1.2 b) nos dá que $[F'_{P'} : F_P] < \infty$ se, e somente se, $[F' : F] < \infty$.

b) Como $v_{P'}(x) = e(P'|P)\,.\,v_P(x)$, para todo $x \in F$, e $v_{P''}(y) = e(P''|P')\,.\,v_{P'}(y)$, para todo $y \in F'$, temos que $v_{P''}(x) = e(P''|P')\,.\,e(P'|P)\,.\,v_P(x)$, para todo $x \in F$, donde $e(P''|P) = e(P''|P')\,.\,e(P'|P)$. A outra parte segue do fato de termos

$$F''_{P''} \supseteq F'_{P'} \supseteq F_P.$$

■

Proposição 4.1.8. *Seja F'/K' uma extensão algébrica de F/K.*

a) Para cada lugar $P' \in \mathbb{P}_{F'}$, existe exatamente um lugar $P \in \mathbb{P}_F$ tal que $P'|P$, a saber $P = P' \cap F$.

b) Reciprocamente, todo lugar $P \in \mathbb{P}_F$ possui pelo menos uma e no máximo um número finito de extensões $P' \in \mathbb{P}_{F'}$.

Demonstração. a) Afirmação. Existe $0 \neq z \in F$, com $v_{P'}(z) \neq 0$.

Prova da Afirmação. Assumamos que essa afirmação seja falsa.

Escolhamos $t \in F'$ com $v_{P'}(t) > 0$. Como F'/F é uma extensão algébrica, existe uma equação $c_n t^n + c_{n-1}t^{n-1} + \ldots + c_1 t + c_0 = 0$, com $c_i \in F$, $c_0 \neq 0$ e $c_n \neq 0$.

Por hipótese, temos que $v_{P'}(c_0) = 0$ e $v_{P'}(c_i t^i) = v_{P'}(c_i) + i v_{P'}(t) = i v_{P'}(t) > 0$, para $i = 1, \ldots, n$, donde $v_{P'}(c_n t^n + \ldots + c_1 t + c_0) = 0$, pela Desigualdade Triangular Estrita (Lema 3.1.16), o que é uma contradição.

Prova da Letra a). Definamos $\mathcal{O} = \mathcal{O}_{P'} \cap F$ e $P = P' \cap F$. Então

- $\mathcal{O}$ é um anel de valorização de F/K.

  Notemos em primeiro lugar que $K \subsetneq \mathcal{O}$. Com efeito, como $K \subseteq K' \subseteq \mathcal{O}_{P'}$ e $K \subseteq F$, temos que $K \subseteq \mathcal{O}_{P'} \cap F = \mathcal{O}$. Seja agora $0 \neq z \in F$ tal que $v_{P'}(z) \neq 0$. Então $z^{-1} \in F$ e temos que $v_{P'}(z) > 0$ ou $v_{P'}(z^{-1}) > 0$. Isso nos dá que $z \in \mathcal{O}_{P'}$ ou $z^{-1} \in \mathcal{O}_{P'}$, isto é, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$, mas z, $z^{-1} \notin K$, pela Definição 3.1.14 e).

  Ainda, considerando o mesmo elemento z acima, temos que ou $z \in F \backslash \mathcal{O}$ ou $z^{-1} \in F \backslash \mathcal{O}$.

  Agora, seja $x \in F$ tal que $x \notin \mathcal{O}$. Então $x \notin \mathcal{O}_{P'}$, donde $v_{P'}(x) < 0$. Mas isso nos dá que $x \neq 0$ e $v_{P'}(x^{-1}) > 0$, isto é, $x^{-1} \in \mathcal{O}_{P'} \cap F = \mathcal{O}$.

  As passagens anteriores nos mostram que $\mathcal{O}$ é um anel de valorização de F/K.

- $\mathcal{O} \backslash \mathcal{O}^\times = P' \cap F$ é o lugar associado ao anel de valorização $\mathcal{O}$.

  Com efeito, temos a seguinte equivalência: $x \in \mathcal{O}^\times$ se, e somente se, $x \in F$ e $x \in \mathcal{O}_{P'}^\times$.

A unicidade do lugar P segue da Proposição 4.1.4.

b) Seja P um lugar de F/K. Escolhamos $x \in F \backslash K$ de forma que o seu único zero seja P, notando que a existência desse elemento segue da Proposição 3.4.23.

Afirmamos que, para $P' \in \mathbb{P}_{F'}$, a seguinte equivalência é verdadeira:

$$P'|P \text{ se, e somente se, } v_{P'}(x) > 0.$$

O resultado segue dessa afirmação, visto que x possui no mínimo um e no máximo um número finito de zeros.

Provemo-la então.

Se $P'|P$, então $v_{P'}(x) = e(P'|P)v_P(x) > 0$. Reciprocamente, se $v_{P'}(x) > 0$, seja Q o lugar de F/K tal que $P'|Q$. Então $v_Q(x) = e(P'|Q)^{-1}v_{P'}(x) > 0$. Logo, $P = Q$, já que P é o único zero de x. ■

Definição 4.1.9. Seja F'/K' uma extensão algébrica de F/K. Para um lugar $P \in \mathbb{P}_F$ definimos sua conorma, com respeito a F'/F, como

$$Con_{F'/F}(P) = \sum_{\substack{P'|P \\ P' \in \mathbb{P}_{F'}}} e(P'|P) \, . \, P'.$$

Tal função se estende a um homomorfismo de $Div(F)$ em $Div(F')$ definindo

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

Proposição 4.1.10. *Seja F'/K' uma extensão algébrica do corpo de funções F/K. Para $0 \neq x \in F$, sejam $(x)_0^F$, $(x)_\infty^F$, $(x)^F$, $(x)_0^{F'}$, $(x)_\infty^{F'}$, $(x)^{F'}$ os divisores de zeros, de polos e principal de x em $Div(F)$ e em $Div(F')$, respectivamente. Então*

$$Con_{F'/F}((x)_0^F) = (x)_0^{F'}, \;\; Con_{F'/F}((x)_\infty^F) = (x)_\infty^{F'} \;\; e \;\; Con_{F'/F}((x)^F) = (x)^{F'}.$$

Demonstração. Da definição do divisor principal de x, temos que

$$\begin{aligned}(x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x) \, . \, P' \\ &= \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P) v_P(x) \, . \, P' \text{ (pelas Proposições 4.1.4 e 4.1.8)}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{P \in \mathbb{P}_F} v_P(x) Con_{F'/F}(P) \\
&= Con_{F'/F}\left(\sum_{P \in \mathbb{P}_F} v_P(x) \,.\, P \right) \\
&= Con_{F'/F}((x)^F).
\end{aligned}
$$

Considerando as partes positiva e negativa do divisor principal, obtemos um resultado análogo para o divisor de polos e o divisor de zeros. ■

Lema 4.1.11. *Sejam K'/K uma extensão finita e x um elemento transcendente sobre K. Então*

$$[K'(x) : K(x)] = [K' : K].$$

Demonstração. Pelo Teorema 2.1.9, como K'/K é uma extensão finita, temos que K'/K é uma extensão algébrica e existem elementos $\alpha_1, \ldots, \alpha_s \in K'$ tais que $K' = K(\alpha_1, \ldots, \alpha_s)$.

Assumamos que $K' = K(\alpha)$, $\alpha \in K'$. Então $[K'(x) : K(x)] \leqslant [K' : K]$, pois $K'(x) = K(\alpha)(x) = K(x)(\alpha)$ nos dá que

$$[K'(x) : K(x)] = deg(irr(\alpha, K(x))) \leqslant deg(irr(\alpha, K)) = [K' : K],$$

uma vez que $irr(\alpha, K) \in K[T] \subseteq K(x)[T]$.

Para mostrarmos a outra desigualdade, temos que mostrar que $irr(\alpha, K)$ é um polinômio irredutível sobre $K(x)$.

Suponhamos que $irr(\alpha, K)$ seja redutível, isto é, que $irr(\alpha, K) = g(T) \,.\, h(T)$, onde $g(T)$, $h(T)$ são polinômios mônicos pertencentes à $K(x)[T]$, com

$$1 \leqslant deg(g(T)),\, deg(h(T)) < deg(irr(\alpha, K)).$$

Como $irr(\alpha, K)(\alpha) = 0$, temos, sem perda de generalidade, que $g(\alpha) = 0$. Escrevendo $g(T) = T^r + \dfrac{c_{r-1}(x)}{d_{r-1}(x)} T^{r-1} + \ldots + \dfrac{c_0(x)}{d_0(x)}$, com $c_i(x)$, $d_i(x) \in K[x]$ e $r < deg(irr(\alpha, K))$, temos que $\alpha^r + \dfrac{c_{r-1}(x)}{d_{r-1}(x)} \alpha^{r-1} + \ldots + \dfrac{c_0(x)}{d_0(x)} = 0$. Multiplicando a última igualdade pelo mínimo múltiplo comum de $d_i(x)$, $i = 0, \ldots, r-1$, obtemos uma igualdade $g_r(x)\alpha^r + \ldots + g_1(x)\alpha + g_0(x) = 0$, para certos $g_i(x) \in K[x]$, para

todo $i = 1, \ldots, r$. Podemos supor ainda que nem todos $g_i(x)$ são divisíveis por x. Fazendo $x = 0$, obtemos uma equação não trivial para α sobre K com grau menor que $deg(irr(\alpha, K))$, o que é uma contradição. ■

Teorema 4.1.12 (Igualdade Fundamental)**.** *Sejam F'/K' uma extensão finita de F/K, P um lugar de F/K e $P_1, \ldots, P_m$ todos os lugares de F'/K' que são extensão de P. Sejam $e_i = e(P_i|P)$ e $f_i = f(P_i|P)$. Então*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Demonstração. Escolhamos $x \in F$ tal que P seja o único zero de x em F/K (ver Proposição 3.4.23). Seja $r = v_P(x) > 0$. Então os lugares $P_1, \ldots, P_m \in \mathbb{P}_F$ são exatamente os zeros de x em F'/K' de acordo com a afirmação feita na demonstração da Proposição 4.1.8 b).

Temos que

$$\begin{aligned}
[F' : K(x)] &= [F' : K'(x)] \,.\, [K'(x) : K(x)] \\
&= \left(\sum_{i=1}^{m} v_{P_i}(x) \,.\, deg(P_i) \right) [K' : K] \text{ (pelo Teorema 3.3.20 e pelo Lema 4.1.11)} \\
&= \left(\sum_{i=1}^{m} e_i \,.\, v_P(x) \,.\, [F'_{P_i} : K'] \right) [K' : K] \\
&= \left(\sum_{i=1}^{m} e_i \,.\, v_P(x) \,.\, [F'_{P_i} : K'] \,.\, [K' : K] \right) \\
&= \left(\sum_{i=1}^{m} e_i \,.\, v_P(x) \,.\, [F'_{P_i} : K] \right) \\
&= v_P(x) \,.\, \left(\sum_{i=1}^{m} e_i \,.\, [F'_{P_i} : F_P] \,.\, [F_P : K] \right) \\
&= r \,.\, deg(P) \,.\, \sum_{i=1}^{m} e_i \,.\, f_i.
\end{aligned}$$

Por outro lado,

$$[F' : K(x)] = [F' : F] \,.\, [F : K(x)] = [F' : F] \,.\, r \,.\, deg(P),$$

já que $(x)_0^F = rP$. Comparando as duas últimas igualdades, temos que

$$[F' : F] = \sum_{i=1}^{m} e_i f_i,$$

como queríamos demonstrar. ■

Corolário 4.1.13. *Sejam F'/K' uma extensão finita de F/K e $P \in \mathbb{P}_F$. Então temos que:*

a) $|\{P' \in \mathbb{P}_{F'};\ P' \text{ é extensão de } P\}| \leqslant [F' : F]$.

b) Se $P' \in \mathbb{P}_{F'}$ é uma extensão de P, então

$$e(P'|P) \leqslant [F' : F] \ \ e \ \ f(P'|P) \leqslant [F' : F].$$

Definição 4.1.14. Sejam F'/K' uma extensão de F/K, com $[F' : F] = n$, e $P \in \mathbb{P}_F$.

a) P se decompõe completamente em F'/F se existem exatamente n lugares distintos $P' \in \mathbb{P}_{F'}$ com $P'|P$.

b) P é totalmente ramificado em F'/F se existe um lugar $P' \in \mathbb{P}_{F'}$ com $P'|P$ e $e(P'|P) = n$.

Observação 4.1.15. Pela Igualdade Fundamental, temos que $P \in \mathbb{P}_F$ se decompõe completamente em F'/F se, e somente se, $e(P'|P) = f(P'|P) = 1$, para todos os lugares $P'|P$ em F'.

Se P é totalmente ramificado em F'/F, então existe um único lugar $P' \in \mathbb{P}_{F'}$, com $P'|P$.

Corolário 4.1.16. *Seja F'/K' uma extensão finita de F/K. Então, para cada divisor $A \in Div(F)$, temos que*

$$deg(Con_{F'/F}(A)) = \frac{[F' : F]}{[K' : K]} \, . \, deg(A).$$

Demonstração. É suficiente mostrarmos o resultado para um divisor primo

$$A = P \in \mathbb{P}_F,$$

uma vez que as aplicações deg e $Con_{F'/F}$ são homomorfismos.

Neste caso, temos que

$$\begin{aligned} deg(Con_{F'/F}(P)) &= deg\left(\sum_{P'|P} e(P'|P)\,.\,P'\right) \\ &= \sum_{P'|P} e(P'|P)\,.\,deg(P') \\ &= \sum_{P'|P} e(P'|P)\,.\,[F'_{P'} : K'] \\ &= \sum_{P'|P} e(P'|P)\,.\,\frac{[F'_{P'} : K]}{[K' : K]} \\ &= \frac{1}{[K' : K]} \cdot \sum_{P'|P} e(P'|P)\,.\,[F'_{P'} : F_P]\,.\,[F_P : K] \\ &= \frac{1}{[K' : K]} \cdot \left(\sum_{P'|P} e(P'|P)\,.\,f(P'|P)\right)\,.deg(P) \\ &= \frac{[F' : F]}{[K' : K]}\,.deg(P), \end{aligned}$$

onde a última igualdade segue da Igualdade Fundamental (Teorema 4.1.12). ■

4.2 SUBANÉIS DE CORPOS DE FUNÇÕES

Ao longo dessa seção, F/K irá denotar um corpo de funções com corpo de constantes K.

Definição 4.2.1. Um subanel de F/K é um anel R tal que $K \subseteq R \subseteq F$ e R não é um corpo.

Observação 4.2.2. Nas condições da Definição 4.2.1, temos que se R é um subanel de F/K, então $K \subsetneq R \subsetneq F$.

Exemplo 4.2.3. Pela Definição 3.1.6 e pela Observação 3.1.7, temos que, dado $P \in \mathbb{P}_F$, $\mathcal{O}_P$ é um subanel de F/K.

Definição 4.2.4. Para $\emptyset \neq S \subsetneq \mathbb{P}_F$, seja

$$\mathcal{O}_S = \{z \in F;\, v_P(z) \geqslant 0,\ \text{para todo } P \in S\}$$

a interseção de todos os anéis de valorização $\mathcal{O}_P$, com $P \in S$. Um anel $R \subseteq F$ que é da forma $R = \mathcal{O}_S$, para algum $\emptyset \neq S \subsetneq \mathbb{P}_F$, é chamado um anel holomorfo de F/K.

Lema 4.2.5. *a) Todo anel de valorização $\mathcal{O}_P$ é um anel holomorfo, a saber $\mathcal{O}_P = \mathcal{O}_S$, onde $S = \{P\}$.*

b) Todo anel holomorfo $\mathcal{O}_S$ é um subanel de F/K.

c) Para $P \in \mathbb{P}_F$ e $\emptyset \neq S \subsetneq \mathbb{P}_F$ temos que $\mathcal{O}_S \subseteq \mathcal{O}_P$ se, e somente se, $P \in S$. Consequentemente, $\mathcal{O}_S = \mathcal{O}_T$ se, e somente se, $S = T$.

Demonstração. a) Segue da Definição 4.2.4.

b) Já temos que $\mathcal{O}_S$ é um anel e que $K \subsetneq \mathcal{O}_S \subsetneq F$, pois $K \subsetneq \mathcal{O}_P \subsetneq F$, para todo $P \in S$. Resta-nos mostrar, portanto, que $\mathcal{O}_S$ não é um corpo.

Escolhamos um lugar $P_1 \in S$. Como $S \subsetneq \mathbb{P}_F$, o Teorema da Aproximação Forte (Teorema 3.4.22) nos fornece a existência de um elemento $0 \neq x \in F$ tal que $v_{P_1}(x) > 0$ e $v_P(x) \geqslant 0$, para todo $P \in S \backslash \{P_1\}$. Deste modo, temos que $x \in \mathcal{O}_S$, mas $x^{-1} \notin \mathcal{O}_S$, já que $v_{P_1}(x^{-1}) < 0$.

Isso nos mostra que x não é invertível, donde $\mathcal{O}_S$ não é um corpo.

c) *Etapa 1:* $\mathcal{O}_S \subseteq \mathcal{O}_P$ se, e somente se, $P \in S$.

($\Rightarrow$) Suponhamos que $P \notin S$. Pelo Teorema da Aproximação Forte, temos que existe $z \in F$ com $v_P(z) < 0$ e $v_Q(z) \geqslant 0$, para todo $Q \in S$. Com efeito, se $S \cup \{P\} \neq \mathbb{P}_F$, temos que o resultado segue diretamente do Teorema da Aproximação Forte. Por outro lado, se $S \cup \{P\} = \mathbb{P}_F$, escolhamos $z \in \mathcal{O}_S \backslash K$. Então $v_Q(z) \geqslant 0$, para todo $Q \in S$. Como z deve ter pelo menos um polo, temos que ter, pela condição anterior, que o polo de z deve ser P.

Cada elemento $z \in F$ tal que $v_P(z) < 0$ e $v_Q(z) \geqslant 0$, para todo $Q \in S$, pertence à $\mathcal{O}_S$ mas não pertence à $\mathcal{O}_P$. Logo, $\mathcal{O}_S \nsubseteq \mathcal{O}_P$, como queríamos mostrar.

($\Leftarrow$) Segue da Definição 4.2.4.

Etapa 2: $\mathcal{O}_S = \mathcal{O}_T$ se, e somente se, $S = T$.

Suponhamos que $S \neq T$. Então, sem perda de generalidade, existe $P \in S$ tal que $P \notin T$, donde, pela *Etapa 1*, $\mathcal{O}_S \subseteq \mathcal{O}_P$ e $\mathcal{O}_T \nsubseteq \mathcal{O}_P$. Isso nos dá que $\mathcal{O}_S \neq \mathcal{O}_T$. A recíproca é imediata. ■

Definição 4.2.6. Seja R um subanel de F/K.

a) Um elemento $z \in F$ é dito integral sobre R se $f(z) = 0$ para algum polinômio mônico $f(T) \in R[T]$, isto é, se existem $a_0, \ldots, a_{n-1} \in R$ tais que

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0.$$

Uma tal equação é chamada equação integral para z sobre R.

b) O conjunto $ic_F(R) = \{z \in F;\ z \text{ é integral sobre } R\}$ é chamado fecho integral de R em F.

c) Seja $F_0 \subseteq F$ o corpo de frações de R. O anel R é chamado integralmente fechado se $ic_{F_0}(R) = R$, isto é, todo elemento $z \in F_0$ que é integral sobre R pertence a R.

Proposição 4.2.7. *Seja $\mathcal{O}_S$ um anel holomorfo de F/K. Então:*

a) *F é o corpo de frações de $\mathcal{O}_S$.*

b) *$\mathcal{O}_S$ é integralmente fechado.*

Demonstração. a) Seja $0 \neq x \in F$. Escolhamos um lugar $P_0 \in S$. Pelo Teorema da Aproximação Forte (Teorema 3.4.22), existe um elemento $z \in F$ tal que $v_{P_0}(z) = max\{0,\, v_{P_0}(x^{-1})\}$ e $v_P(z) \geqslant max\{0,\, v_P(x^{-1})\}$, para todo $P \in S$.

De fato, suponhamos que $x \in \mathcal{O}_S$. Então $v_P(x) \geqslant 0$, para todo $P \in S$, donde $v_P(x^{-1}) \leqslant 0$, para todo $P \in S$, e assim $max\{0,\, v_P(x^{-1})\} = 0$, para todo $P \in S$. Logo, pelo Teorema da Aproximação Forte, temos que existe z tal que $v_{P_0}(z) = 0 = max\{0,\, v_{P_0}(x^{-1})\}$ e $v_P(z) \geqslant 0 = max\{0,\, v_P(x^{-1})\}$, para todo $P \in S \backslash \{P_0\}$. Se $x \notin \mathcal{O}_S$, então existe $P \in S$ tal que $v_P(x) < 0$. Sejam $P_1, \ldots, P_S$ todos os polos de x que pertencem à S (essa quantidade é finita pelo Corolário 3.2.4). Então, $v_{P_i}(x) < 0$, para todo $i = 1, \ldots, s$, donde $v_{P_i}(x^{-1}) > 0$, para todo $i = 1, \ldots, s$.

Novamente, pelo Teorema da Aproximação Forte, temos que existe $z \in F$ tal que $v_{P_0}(z) = max\{0, v_{P_0}(x^{-1})\}$, $v_{P_i}(z) = v_{P_i}(x^{-1}) = max\{0, v_{P_i}(x^{-1})\}$, para $i = 1, \ldots, s$, e $v_P(z) \geqslant 0 = max\{0, v_P(x^{-1})\}$, para todo $P \in S\backslash\{P_0, P_1, \ldots, P_s\}$.

Daí temos que $z \in \mathcal{O}_S$, $z \neq 0$ (pois $v_{P_0}(z) = max\{0, v_{P_0}(x^{-1})\} < \infty$) e

$$y = zx \in \mathcal{O}_S,$$

pois $v_P(y) = v_P(z) + v_P(x) \geqslant v_P(x^{-1}) + v_P(x) = -v_P(x) + v_P(x) = 0$.

Isso nos dá que $x = yz^{-1} \in Fr(\mathcal{O}_S)$, onde $Fr(\mathcal{O}_S)$ denota o corpo de frações de $\mathcal{O}_S$.

b) Seja $u \in F$ um elemento integral sobre $\mathcal{O}_S$. Então existem $a_{n-1}, \ldots, a_0 \in \mathcal{O}_S$ tais que $u^n + a_{n-1}u^{n-1} + \ldots + a_1u + a_0 = 0$. Precisamos mostrar que $v_P(u) \geqslant 0$, para todo $P \in S$.

Suponhamos que exista $P \in S$ tal que $v_P(u) < 0$. Como $v_P(a_i) \geqslant 0$, temos que $v_P(u^n) = n \,.\, v_P(u) < i \,.\, v_P(u) \leqslant i \,.\, v_P(u) + v_P(a_i) = v_P(a_i \,.\, u^i)$, para $i = 0, \ldots, n-1$. Pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que

$$v_P(0) = v_P(u^n + a_{n-1}u^{n-1} + \ldots + a_1u + a_0) = n \,.\, v_P(u),$$

o que é uma contradição, pois $v_P(0) = \infty > n \,.\, v_P(u)$. ■

Teorema 4.2.8. *Sejam R um subanel de F/K e $S(R) = \{P \in \mathbb{P}_F;\ R \subseteq \mathcal{O}_P\}$. Então:*

a) $\emptyset \neq S(R) \subsetneq \mathbb{P}_F$.

b) O fecho integral de R em F é $ic_F(R) = \mathcal{O}_{S(R)}$. Em particular, $ic_F(R)$ é um subanel integralmente fechado de F/K com corpo de frações F.

Demonstração. a) Como R não é um corpo, podemos encontrar um ideal $\{0\} \neq I \subsetneq R$, e, pelo Teorema 3.1.26, existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$. Isso nos dá que $S(R) \neq \emptyset$. Por outro lado, considerando um elemento $x \in R$ que é transcendente sobre K $(*)$, temos que qualquer lugar $Q \in \mathbb{P}_F$ que seja um polo de x não pertence à $S(R)$. Como x possui pelo menos um polo pelo Corolário 3.1.27, temos que $S(R) \subsetneq \mathbb{P}_F$.

($*$) Notemos que a existência desse elemento pode ser garantida pelos seguintes fatos:

- $\{0\} \subsetneq I \subsetneq R$.
- $I \subseteq P$.
- O único elemento de P algébrico sobre K é o elemento 0 (pela Proposição 3.1.8).

b) Como $R \subseteq \mathcal{O}_{S(R)}$ e $\mathcal{O}_{S(R)}$ é integralmente fechado pela Proposição 4.2.7, temos que $ic_F(R) \subseteq ic_F(\mathcal{O}_{S(R)}) = \mathcal{O}_{S(R)}$.

Consideremos agora um elemento $z \in \mathcal{O}_{S(R)}$. Afirmamos que $z^{-1} \,.\, R[z^{-1}] = R[z^{-1}]$.

Suponhamos que a última igualdade seja falsa, isto é, que $z^{-1} \,.\, R[z^{-1}]$ seja um ideal próprio de $R[z^{-1}]$. Então, pelo Teorema 3.1.26, existe um lugar $Q \in \mathbb{P}_F$ tal que $z^{-1} \,.\, R[z^{-1}] \subseteq Q$ e $R[z^{-1}] \subseteq \mathcal{O}_Q$.

Disso segue que $Q \in S(R)$ e $z \notin \mathcal{O}_Q$, pois $z^{-1} \in Q$, o que é uma contradição, já que $z \in \mathcal{O}_{S(R)}$. Portanto, a afirmação anterior é válida.

Da afirmação, temos que $1 = z^{-1} \,.\, \sum_{i=0}^{s} a_i (z^{-1})^i$, com $a_i \in R$, para todo $i = 0, \ldots, s$.

Multiplicando a última igualdade por z^{s+1}, temos que $z^{s+1} - \sum_{i=0}^{s} a_i z^{s-i} = 0$, onde esta última é uma equação integral para z sobre R. ■

Observação 4.2.9. Na demonstração do Teorema 4.2.8 nós não utilizamos o fato de que $K = \tilde{K}$. Assim, o Teorema 4.2.8 continua válido mesmo supondo que F/K é um corpo de funções qualquer, onde K não é necessariamente fechado em F.

Proposição 4.2.10. *Seja $\mathcal{O}_S$ um anel holomorfo de F/K. Então existe uma correspondência biunívoca entre S e o conjunto dos ideais maximais de $\mathcal{O}_S$ dada por*

$$\begin{array}{rccc} h: & S & \to & \{M \subseteq \mathcal{O}_S;\ M \text{ é um ideal maximal de } \mathcal{O}_S\} \\ & P & \mapsto & M_P = P \cap \mathcal{O}_S. \end{array}$$

Ainda, a aplicação

$$\begin{array}{rccc} \varphi: & \mathcal{O}_S/M_P & \to & F_P = \mathcal{O}_P/P \\ & x + M_P & \mapsto & x + P \end{array}$$

é um isomorfismo.

Demonstração. Consideremos para $P \in S$ o homomorfismo de anéis

$$\begin{array}{rccc} \phi: & \mathcal{O}_S & \to & F_P \\ & x & \mapsto & x + P. \end{array}$$

Afirmamos que ϕ é um homomorfismo sobrejetor. De fato, seja $z + P \in F_P$, onde $z \in \mathcal{O}_P$. Pelo Teorema da Aproximação Forte (Teorema 3.4.22), existe $x \in F$ satisfazendo $v_P(x - z) > 0$ e $v_Q(x) \geqslant 0$, para todo $Q \in S\backslash\{P\}$. Isso nos dá que $x \in \mathcal{O}_S$ (notemos que $v_P(x) = v_P((x - z) + z) \geqslant min\{v_P(x - z),\, v_P(z)\} \geqslant 0$, isto é, $x \in \mathcal{O}_P$) e $\phi(x) = x + P = z + P$, pois $v_P(x - z) > 0$ nos dá que $x - z \in P$.

Ainda, $Ker(\phi) = P \cap \mathcal{O}_S$, de modo que ϕ induz um isomorfismo $\varphi : \mathcal{O}_S/M_P \to F_P$. Como F_P é um corpo, temos que M_P é um ideal maximal de $\mathcal{O}_S$.

Se $P \neq Q$, o Teorema da Aproximação Forte nos dá que $M_P \neq M_Q$. Com efeito, existe $x \in F$ tal que $v_P(x) > 0$, $v_Q(x) = 0$ e $v_R(x) \geqslant 0$, para todo $R \in S\backslash\{P, Q\}$. Daí, temos que $x \in \mathcal{O}_S$, $x \in P$, mas $x \notin Q$, donde $x \in M_P$, mas $x \notin M_Q$. Isso mostra que $M_P \neq M_Q$. Logo, h é uma aplicação injetiva.

Resta-nos mostrar que h é sobrejetora, isto é, que cada ideal maximal de $\mathcal{O}_S$ é da forma $P \cap \mathcal{O}_S$, onde $P \in S$.

Seja $M \subseteq \mathcal{O}_S$ um ideal maximal. Pelo Teorema 3.1.26, existe um lugar $P \in \mathbb{P}_F$ com $M \subseteq P$ e $\mathcal{O}_S \subseteq \mathcal{O}_P$. Ainda, pelo Lema 4.2.5, temos que $P \in S$. Como $M \subseteq P \cap \mathcal{O}_S = M_P$ e M é um ideal maximal de $\mathcal{O}_S$, temos que $M = P \cap \mathcal{O}_S = M_P$, como queríamos mostrar. ■

Em geral, anéis holomorfos não são domínios de ideais principais, ao contrário do que ocorre com os anéis $\mathcal{O}_P$, $P \in \mathbb{P}_F$. Contudo, temos o resultado a seguir.

Proposição 4.2.11. *Se $S \subseteq \mathbb{P}_F$ é um conjunto não vazio e finito de lugares de F/K, então $\mathcal{O}_S$ é um domínio de ideais principais.*

Demonstração. Sejam $S = \{P_1, \ldots, P_s\}$ e $\{0\} \neq I \subseteq \mathcal{O}_S$. Para $i = 1, \ldots, s$, escolhamos $x_i \in I$ tal que $v_{P_i}(x_i) = n_i \leqslant v_{P_i}(u)$, para todo $u \in I$. Notemos que a escolha anterior é possível pelo Princípio da Boa Ordenação, já que $v_{P_i}(u) \geqslant 0$, para todo $u \in I$, e $I \neq \{0\}$.

Pelo Teorema da Aproximação Fraca (Teorema 3.2.1), existe $z_i \in F$ tal que $v_{P_i}(z_i) = 0$ e $v_{P_j}(z_i) > n_j$, para $j \neq i$.

Ainda, $z_i \in \mathcal{O}_S$, para todo i, donde o elemento $x = \sum_{i=1}^{s} x_i z_i \in I$. Pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que $v_{P_i}(x) = n_i$, para $i = 1, \ldots, s$.

Se mostrarmos que $I \subseteq x\mathcal{O}_s$, então teremos que $I = x\mathcal{O}_S$, isto é, I é um ideal principal.

Para isso, consideremos $z \in I$. Definindo $y = x^{-1} \,.\, z$, temos que

$$v_{P_i}(y) = v_{P_i}(z) + v_{P_i}(x^{-1}) = v_{P_i}(z) - v_{P_i}(x) = v_{P_i}(z) - n_i \geqslant 0,$$

para todo $i = 1, \ldots, s$. Desse modo, $y \in \mathcal{O}_S$ e $z = xy \in x\mathcal{O}_S$. ■

4.3 BASES INTEGRAIS LOCAIS

Nesta seção, F/K será um corpo de funções com corpo de constantes K e F'/F será um extensão finita, onde o corpo de constantes K' de F' pode conter estritamente o corpo K.

Proposição 4.3.1. *Seja R um subanel integralmente fechado de F/K tal que F é o corpo de frações de R. Para $z \in F'$, seja $\varphi(T) \in F[T]$ o seu polinômio minimal sobre F. Então*

$$z \text{ é } \textit{integral sobre } R \textit{ se, e somente se, } \varphi(T) \in R[T].$$

Demonstração. Por definição, $\varphi(T)$ é o único polinômio mônico irredutível com coeficientes em F tal que $\varphi(z) = 0$. Se $\varphi(T) \in R[T]$, então z é integral sobre R. Suponhamos agora que $z \in F'$ seja um elemento integral sobre R. Escolhamos um polinômio mônico $f(T) \in R[T]$ tal que $f(z) = 0$. Como $\varphi(T)$ é o polinômio minimal de z, temos que existe $\psi(T) \in F[T]$ tal que $f(T) = \varphi(T) \,.\, \psi(T)$. Sejam

$F'' \supseteq F'$ uma extensão finita de F contendo todas as raízes de $\varphi(T)$ e $R'' = ic_{F''}(R)$ o fecho integral de R em F''. Como todas as raízes de $\varphi(T)$ são raízes de $f(T)$, temos que estas estão em R''. Os coeficientes de $\varphi(T)$ são expressões polinomiais das raízes de $\varphi(T)$, donde $\varphi(T) \in R''[T]$. Mas $\varphi(T) \in F[T]$ e $F \cap R'' = ic_F(R) = R$, pois R é integralmente fechado. Isso mostra que $\varphi(T) \in R[T]$. ■

Corolário 4.3.2. *Seguindo a notação como na Proposição 4.3.1, sejam $Tr_{F'/F} : F' \to F$ a função traço de F' em F e $x \in F'$ um elemento integral sobre R. Então $Tr_{F'/F}(x) \in R$.*

Demonstração. A demonstração deste resultado segue da Proposição 2.7.3 g) e da Proposição 4.3.1. ■

Proposição 4.3.3. *Seja M/L uma extensão finita e separável e consideremos $\{z_1, \ldots, z_n\}$ uma base de M/L. Então existem únicos elementos $z_1^*, \ldots, z_n^* \in M$ tais que*

$$Tr_{M/L}(z_i z_j^*) = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}.$$

O conjunto $\{z_1^*, \ldots, z_n^*\}$ é uma base de M/L denominada base dual de $\{z_1, \ldots, z_n\}$ com respeito à função traço.

Demonstração. Consideremos o espaço dual M^* de M sobre L, isto é, M^* é o espaço de todas as transformações $L-$lineares. É bem conhecido da Álgebra Linear que $[M : L] = dim_L(M^*)$. Agora, para $z \in M$ e $\lambda \in M^*$, definamos $z \,.\, \lambda \in M^*$ por $(z \,.\, \lambda)(w) = \lambda(zw)$. Com a operação anterior, podemos considerar M^* um espaço vetorial sobre M de dimensão 1, já que

$$dim_L(M^*) = [M : L] \,.\, dim_M(M^*).$$

Como M/L é uma extensão separável, temos que $Tr_{M/L}$ não é a transformação linear identicamente nula. Assim, para cada $\lambda \in M^*$, existe um único $z \in M$ tal que $\lambda = z \,.\, Tr_{M/L}$. Em particular, as formas lineares $\lambda_j \in M^*$, dadas por $\lambda_j(z_i) = \delta_{ij}$, $i = 1, \ldots, n$, podem ser escritas como $\lambda_j = z_j^* \,.\, Tr_{M/L}$. Isso significa que

$$Tr_{M/L}(z_i z_j^*) = (z_j^* \,.\, Tr_{M/L})(z_i) = \lambda_j(z_i) = \delta_{ij}.$$

Como $\lambda_1, \ldots, \lambda_n$ são linearmente independentes sobre L, o mesmo deve ocorrer com $z_1^*, \ldots, z_n^*$, de modo que estes elementos constituem uma base de M/L. ■

Teorema 4.3.4. *Sejam R um subanel integralmente fechado de F/K com corpo de frações F, F'/F uma extensão finita e separável de grau n e $R' = ic_{F'}(R)$ o fecho integral de R em F'. Então, temos que:*

a) Para toda base $\{x_1, \ldots, x_n\}$ de F'/F existem elementos $a_i \in R\backslash\{0\}$ tais que $a_1x_1, \ldots, a_nx_n \in R'$. Assim, existem bases de F'/F contidas em R'.

b) Se $\{z_1, \ldots, z_n\} \subseteq R'$ é uma base de F'/F e $\{z_1^*, \ldots, z_n^*\}$ denota a sua base dual com respeito à função traço, então

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

c) Se R é um domínio de ideais principais, então existe uma base $\{u_1, \ldots, u_n\}$ de F'/F com a propriedade

$$R' = \sum_{i=1}^{n} Ru_i.$$

Demonstração. *a*) Devemos mostrar que para cada elemento $x \in F'$ existe $a \in R$, $a \neq 0$, tal que ax é integral sobre R. Como F'/F é uma extensão algébrica, pois é uma extensão finita, e F é o corpo de frações de R, temos que existem elementos a_i, $b_i \in R$, com $a_i \neq 0$ e tais que

$$x^r + \frac{b_{r-1}}{a_{r-1}}x^{r-1} + \ldots + \frac{b_1}{a_1}x + \frac{b_0}{a_0} = 0.$$

Multiplicando essa equação por a^r, onde $a = a_0 \cdot a_1 \cdot \ldots \cdot a_{r-1}$, obtemos

$$(ax)^r + c_{r-1}(ax)^{r-1} + \ldots + c_1(ax) + c_0 = 0,$$

com $c_i \in R$. Portanto, $ax \in R'$.

b) Sejam agora $\{z_1, \ldots, z_n\}$ uma base de F'/F contida em R' e $\{z_1^*, \ldots, z_n^*\}$ a sua base dual. A inclusão $\sum_{i=1}^{n} Rz_i \subseteq R'$ segue do fato de $\{z_1, \ldots, z_n\} \subseteq R'$. Por outro lado, cada $z \in F'$ pode ser escrito na forma

$$z = e_1z_1^* + \ldots + e_nz_n^*,$$

com $e_i \in F$. Se $z \in R'$, então $zz_j \in R'$, para todo $j = 1, \ldots, n$, donde $Tr_{F'/F}(zz_j) \in R$ pelo Corolário 4.3.2. Como

$$Tr_{F'/F}(zz_j) = Tr_{F'/F}\left(\sum_{i=1}^{n} e_i z_j z_i^*\right) = \sum_{i=1}^{n} e_i \, . \, Tr_{F'/F}(z_j z_i^*) = e_j,$$

concluímos que $e_j \in R$, de modo que $R' \subseteq \sum_{i=1}^{n} Rz_i^*$.

c) Escolhamos uma base $\{w_1, \ldots, w_n\}$ de F'/F tal que $R' \subseteq \sum_{i=1}^{n} Rw_i$ (notemos que a existência dessa base é possível pelos itens a) e b)). Para $1 \leqslant k \leqslant n$, definamos

$$R_k = R' \cap \sum_{i=1}^{k} Rw_i.$$

Gostaríamos de construir recursivamente $u_1, \ldots, u_n$ tais que $R_k = \sum_{i=1}^{k} Ru_i$. Para $k = 1$, isto é, $R_1 = R' \cap Rw_1$, consideremos o conjunto

$$I_1 = \{a \in F;\, aw_1 \in R'\}.$$

Esse conjunto está contido em R, já que $R' \subseteq \sum_{i=1}^{n} Rw_i$. Efetivamente, I_1 é um ideal de R, donde $I_1 = a_1 R$ para algum $a_1 \in R$, visto que R é um domínio de ideais principais. Definindo $u_1 = a_1 w_1$, podemos verificar que $R_1 = Ru_1$. Suponhamos agora que para $k \geqslant 2$ tenhamos encontrado $u_1, \ldots, u_{k-1}$ tais que $R_{k-1} = \sum_{i=1}^{k-1} Ru_i$. Seja

$$I_k = \{a \in F;\ \text{existem}\, b_1, \ldots, b_{k-1} \in R \text{ tais que } b_1 w_1 + \ldots + b_{k-1} w_{k-1} + a w_k \in R'\}.$$

Novamente, I_k é um ideal de R, a saber $I_k = a_k R$. Escolhamos $u_k \in R'$ com

$$u_k = c_1 w_1 + \ldots + c_{k-1} w_{k-1} + a_k w_k.$$

Como $R_{k-1} \subseteq R_k$ e $\sum_{i=1}^{k-1} Ru_i \subseteq \sum_{i=1}^{k} Ru_i$, temos que $u_j \in \sum_{i=1}^{k-1} Ru_i = R_{k-1} \subseteq R_k$, para $j = 1, \ldots, k-1$. Como $u_k \in R_k$ por definição, segue que $R_k \supseteq \sum_{i=1}^{k} Ru_i$. Com o intuito de mostrarmos a outra inclusão, seja $w \in R_k$. Escrevamos

$$w = d_1 w_1 + \ldots + d_k w_k,$$

com $d_i \in R$. Então $d_k \in I_k$, donde $d_k = da_k$, com $d \in R$, e assim

$$w - du_k \in R' \cap \sum_{i=1}^{k-1} Rw_i = R_{k-1} = \sum_{i=1}^{k-1} Ru_i.$$

Portanto, $w \in \sum_{i=1}^{k} Ru_i$.

Mostramos que $R' = R_n = \sum_{i=1}^{n} Ru_i$. Como R' contém uma base de F'/F por a), os elementos $u_1, \ldots, u_n$ devem ser linearmente independentes sobre F e assim constituir uma base de F'/F. ■

Corolário 4.3.5. *Sejam F'/F uma extensão finita e separável do corpo de funções F/K e $P \in \mathbb{P}_F$ um lugar de F/K. Então o fecho integral $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F' é*

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

Ainda, existe uma base $\{u_1, \ldots, u_n\}$ de F'/F tal que

$$\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \, . \, u_i.$$

Uma tal base é chamada base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_\mathcal{P}$ (ou uma base integral local de F'/F para um lugar P).

Demonstração. Segue do Teorema 4.2.8 b), da Observação 4.2.9 e do Teorema 4.3.4, observando que $\mathcal{O}_P$ é um domínio de ideais principais. ■

Teorema 4.3.6. *Sejam F/K um corpo de funções, F'/F uma extensão finita e separável. Então, cada base $\{z_1, \ldots, z_n\}$ de F'/F é uma base integral para quase todo lugar $P \in \mathbb{P}_F$.*

Demonstração. Consideremos a base dual $\{z_1^*, \ldots, z_n^*\}$ de $\{z_1, \ldots, z_n\}$. Os polinômios minimais de $z_1, \ldots, z_n, z_1^*, \ldots, z_n^*$ sobre F envolvem somente um número finito de coeficientes. Seja $S \subseteq \mathbb{P}_F$ o conjunto de todos os polos desses coeficientes. Então S é finito, pelo Corolário 3.2.4, e, para $P \notin S$, temos que

$$z_1, \ldots, z_n, z_1^*, \ldots, z_n^* \in \mathcal{O}'_P,$$

pela Proposição 4.1.4 e pelo Corolário 4.3.5, onde $\mathcal{O}'_P = ic_{F'}(\mathcal{O}_P)$. Portanto,

$$\sum \mathcal{O}_P \,.\, z_i \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P \,.\, z_i^* \subseteq \mathcal{O}'_P \subseteq \sum \mathcal{O}_P \,.\, z_i,$$

onde a primeira e a terceira inclusões seguem de $z_1, \ldots, z_n, z_1^*, \ldots, z_n^* \in \mathcal{O}'_P$ e a segunda e a quarta inclusões seguem do Teorema 4.3.4 b), notando-se que $\{z_1, \ldots, z_n\}$ é a base dual de $\{z_1^*, \ldots, z_n^*\}$. Isso nos mostra que $\{z_1, \ldots, z_n\}$ é uma base integral para cada $P \notin S$. ■

Para o próximo resultado, introduziremos algumas notações:

- $\overline{F} = F_P = \mathcal{O}_P/P$.
- $\overline{a} = a(P) \in \overline{F}$ é a classe residual de $a \in \mathcal{O}_P$.
- Se $\psi(T) = \sum c_i T^i$ é um polinômio com coeficientes $c_i \in \mathcal{O}_P$, definimos

$$\overline{\psi}(T) = \sum \overline{c}_i T^i \in \overline{F}[T].$$

Teorema 4.3.7 (Kummer)**.** *Sejam $F' = F(y)$, onde y é um elemento integral sobre $\mathcal{O}_P$, e $\varphi(T) \in \mathcal{O}_P[T]$ o polinômio minimal de y sobre F. Seja*

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i}$$

a decomposição de $\overline{\varphi}(T)$ em componentes irredutíveis sobre $\overline{F}$, ou seja, os polinômios $\gamma_i(T)$, $i = 1, \ldots, r$, são irredutíveis, mônicos, dois a dois distintos em $\overline{F}[T]$ e $\varepsilon_i \geqslant 1$. Escolhamos polinômios mônicos $\varphi_i(T) \in \mathcal{O}_P[T]$ tais que

$$\overline{\varphi_i}(T) = \gamma_i(T) \quad e \quad deg(\varphi_i(T)) = deg(\gamma_i(T)).$$

Então, para $i = 1, \ldots, r$, existem lugares $P_i \in \mathbb{P}_{F'}$ satisfazendo

$$P_i|P, \;\; \varphi_i(y) \in P_i \;\; e \;\; f(P_i|P) \geqslant deg(\gamma_i(T)).$$

Além disso, $P_i \neq P_j$, se $i \neq j$.

Suponhamos ainda que pelo menos uma das hipóteses a seguir seja satisfeita:

(∗) *$\varepsilon_i = 1$, para todo $i = 1, \ldots, r$.*

(**) $\{1, y, \ldots, y^{n-1}\}$ *é uma base integral para* P, *onde* $n = deg(\varphi(T)) = [F' : F]$.

Então existe, para $i = 1, \ldots, r$, *exatamente um lugar* $P_i \in \mathbb{P}_{F'}$ *com* $P_i|P$ *e* $\varphi_i(y) \in P_i$. *Os lugares* $P_1, \ldots, P_r$ *são todos os lugares de* F' *que são extensão de* P *e temos que*

$$Con_{F'/F}(P) = \sum_{i=1}^{r} \varepsilon_i P_i,$$

isto é, $\varepsilon_i = e(P_i|P)$. *Temos também que* $F'_{P_i} = \mathcal{O}_{P_i}/P_i$ *é isomorfo à* $\overline{F}[T]/\langle \gamma_i(T) \rangle$. *Logo* $f(P_i|P) = deg(\gamma_i(T))$.

Demonstração. Definamos $\overline{F}_i = \overline{F}[T]/\langle \gamma_i(T) \rangle$. Como $\gamma_i(T)$ é irredutível, $\overline{F}_i$ é uma extensão de $\overline{F}$ de grau

$$[\overline{F}_i : \overline{F}] = deg(\gamma_i(T)).$$

Consideremos o anel $\mathcal{O}_P[y] = \sum_{j=0}^{n-1} \mathcal{O}_P \,.\, y^j$, onde $n = deg(\varphi(T)) = [F' : F]$. Então existem os seguintes homomorfismos de anéis

$$\rho: \begin{array}{ccc} \mathcal{O}_P[T] & \to & \mathcal{O}_P[y] \\ \sum c_j T^j & \mapsto & \sum c_j y^j \end{array} \quad \text{e} \quad \pi_i: \begin{array}{ccc} \mathcal{O}_P[T] & \to & \overline{F}_i \\ \sum c_j T^j & \mapsto & \sum \overline{c}_j T^j \pmod{\gamma_i(T)}. \end{array}$$

O núcleo de ρ é o ideal gerado por $\varphi(T)$. Como

$$\pi_i(\varphi(T)) = \overline{\varphi}(T) \pmod{\gamma_i(T)} = 0,$$

temos que $Ker(\rho) \subseteq Ker(\pi_i)$. Assim, concluímos que existe um único homomorfismo $\sigma_i : \mathcal{O}_P[y] \to \overline{F}_i$, com $\pi_i = \sigma_i \circ \rho$. A função σ_i é explicitamente dada por

$$\sigma_i: \begin{array}{ccc} \mathcal{O}_P[y] & \to & \overline{F}_i \\ \sum_{j=0}^{n-1} c_j y^j & \mapsto & \sum_{j=0}^{n-1} \overline{c}_j T^j \pmod{\gamma_i(T)}. \end{array}$$

Temos também que σ_i é um epimorfismo. Afirmamos que o núcleo de σ_i é

$$Ker(\sigma_i) = P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y].$$

A inclusão $Ker(\sigma_i) \supseteq P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y]$ segue da definição de σ_i. Com o intuito de mostrarmos a outra inclusão, consideremos um elemento $\sum_{j=0}^{n-1} c_j y^j \in$

$Ker(\sigma_i)$. Então $\sum_{j=0}^{n-1} \overline{c_j} T^j = \overline{\varphi}_i(T) \,.\, \overline{\psi}(T)$, para algum $\psi(T) \in \mathcal{O}_P[T]$. Logo

$$\sum_{j=0}^{n-1} c_j T^j - \varphi_i(T) \,.\, \psi(T) \in P \,.\, \mathcal{O}_P[T].$$

Substituindo $T = y$, obtemos

$$\sum_{j=0}^{n-1} c_j y^j - \varphi_i(y) \,.\, \psi(y) \in P \,.\, \mathcal{O}_P[y],$$

o que mostra que $\sum_{j=0}^{n-1} c_j y^j \in P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y]$.

Pelo Teorema 3.1.26, existe um lugar $P_i \in \mathbb{P}_{F'}$ tal que $Ker(\sigma_i) \subseteq P_i$ e $\mathcal{O}_P[y] \subseteq \mathcal{O}_{P_i}$. Assim, $P_i | P$ e $\varphi_i(y) \in P_i$. O corpo $\mathcal{O}_{P_i}/P_i$ contém $\mathcal{O}_P[y]/Ker(\sigma_i)$, onde $\mathcal{O}_P[y]/Ker(\sigma_i)$ é isomorfo à $\overline{F}_i$, de modo que

$$f(P_i : P) = [\mathcal{O}_{P_i}/P_i : \overline{F}] \geqslant [\overline{F}_i : \overline{F}] = deg(\gamma_i(T)).$$

Para $i \neq j$, os polinômios $\gamma_i(T) = \overline{\varphi}_i(T)$ e $\gamma_j(T) = \overline{\varphi}_j(T)$ são relativamente primos em $\overline{F}[T]$, donde existem $\lambda_i(T)$, $\lambda_j(T) \in \mathcal{O}_P[T]$ tais que

$$1 = \overline{\varphi}_i(T) \,.\, \overline{\lambda}_i(T) + \overline{\varphi}_j(T) \,.\, \overline{\lambda}_j(T).$$

Isso implica que

$$\varphi_i(y) \,.\, \lambda_i(y) + \varphi_j(y) \,.\, \lambda_j(y) - 1 \in P \,.\, \mathcal{O}_P[y].$$

Dessa forma, concluímos que $1 \in Ker(\sigma_i) + Ker(\sigma_j)$, pois $Ker(\sigma_i) = P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y]$, para todo $i = 1, \ldots, r$. Como $P_i \supseteq Ker(\sigma_i)$ e $P_j \supseteq Ker(\sigma_j)$, mostramos com as passagens anteriores que $P_i \neq P_j$, se $i \neq j$. Com efeito, se $P_i = P_j$, então $1 \in P_i$, o que é uma contradição, pois P_i é um ideal maximal de $\mathcal{O}_{P_i}$.

Suponhamos agora que a hipótese $(*)$ seja verdadeira, isto é

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T).$$

Então

$$\begin{aligned}[F' : F] &= deg(\varphi(T)) \\ &= \sum_{i=1}^{r} deg(\varphi_i(T)) \\ &\leqslant \sum_{i=1}^{r} f(P_i|P) \\ &\leqslant \sum_{i=1}^{r} e(P_i|P) \,.\, f(P_i|P) \\ &\leqslant \sum_{P'|P} e(P'|P) \,.\, f(P'|P) \\ &= [F' : F],\end{aligned}$$

pelo Teorema 4.1.12. Isso só é possível, contudo, se $e(P_i|P) = 1$, então

$$f(P_i|P) = deg(\varphi_i(T)) = deg(\gamma_i(T))$$

e não existem outros lugares $P' \in \mathbb{P}_{F'}$ tais que $P'|P$ além dos lugares $P_1, \ldots, P_r$.

Por último, assumamos a hipótese $(**)$. Como antes, escolhamos $P_i \in \mathbb{P}_{F'}$ tal que $P_i|P$ e $\varphi_i(y) \in P_i$.

Afirmação. $P_1, \ldots, P_r$ são as únicas extensões de P em F'.

De fato, seja $P' \in \mathbb{P}_{F'}$, com $P'|P$. Como

$$0 = \varphi(y) \equiv \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \pmod{P \,.\, \mathcal{O}_P[y]},$$

obtemos que

$$\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in P',$$

notando que $y \in \mathcal{O'}_P = \bigcap_{P'|P} \mathcal{O}_{P'} \subseteq \mathcal{O}_{P'}$, pelo Corolário 4.3.5, e que $P \subseteq P'$. Como P' é um ideal primo em $\mathcal{O}_{P'}$, temos que $\varphi_i(y) \in P'$, para algum $i \in \{1, \ldots, r\}$ e

$$P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y] \subseteq P' \cap \mathcal{O}_P[y].$$

Como $Ker(\sigma_i) = P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y]$ e $Ker(\sigma_i)$ é um ideal maximal, pois $\mathcal{O}_P[y]/Ker(\sigma_i)$ é isomorfo à $\overline{F}_i$, temos que a inclusão anterior é uma igualdade. Ainda

$$P \,.\, \mathcal{O}_P[y] + \varphi_i(y) \,.\, \mathcal{O}_P[y] \subseteq P_i \cap \mathcal{O}_P[y]$$

implica que

$$P' \cap \mathcal{O}_P[y] = P_i \cap \mathcal{O}_P[y] = \varphi_i(y) \,.\, \mathcal{O}_P[y] + P \,.\, \mathcal{O}_P[y].$$

Pela hipótese $(**)$, $\mathcal{O}_P[y]$ é o fecho integral de $\mathcal{O}_P$ em F', donde a Proposição 4.2.10 nos dá que $P' = P_i$, o que demonstra a afirmação.

Através da afirmação anterior e do Corolário 4.3.5, vemos que

$$\mathcal{O}_P[y] = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}.$$

Além disso, pelo Teorema da Aproximação, podemos encontrar elementos $t_1, \ldots, t_r \in F'$ satisfazendo

$$v_{P_i}(t_i) = 1 \text{ e } v_{P_j}(t_i) = 0, \text{ para } j \neq i.$$

Escolhamos $t \in F$ um elemento primo para P. Então

$$t_i \in \mathcal{O}_P[y] \cap P_i = \varphi_i(y) \,.\, \mathcal{O}_P[y] + t \,.\, \mathcal{O}_P[y].$$

Assim t_i pode ser escrito como

$$t_i = \varphi_i(y) \,.\, a_i(y) + t \,.\, b_i(y), \text{ com } a_i(y),\, b_i(y) \in \mathcal{O}_P[y],$$

donde obtemos

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = a(y) \,.\, \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + t \,.\, b(y),$$

com $a(y),\, b(y) \in \mathcal{O}_P[y]$. Como

$$\varphi(y) \equiv \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \pmod{t \,.\, \mathcal{O}_P[y]}$$

e $\varphi(y) = 0$, temos que

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = t \,.\, u(y),$$

para algum $u(y) \in \mathcal{O}_P[y]$. Assim,

$$\varepsilon_i = v_{P_i}\left(\prod_{j=1}^{r} t_j^{\varepsilon_j}\right) \geqslant v_{P_i}(t) = e(P_i|P).$$

Por outro lado,

$$f(P_i|P) = deg(\gamma_i(T)).$$

De fato, $\mathcal{O}_P[y] = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}$, $Ker(\sigma_i) = P_i \cap \mathcal{O}_P[y]$ e $\mathcal{O}_P[y]/Ker(\sigma_i)$ é isomorfo à $\overline{F}_i$. Ainda, pela Proposição 4.2.10, $\mathcal{O}_P[y]/(P_i \cap \mathcal{O}_P[y])$ é isomorfo à F'_{P_i}, de modo que $\overline{F}_i$ é isomorfo à F'_{P_i} e assim $f(P_i|P) = [F'_{P_i} : \overline{F}] = [\overline{F}_i : \overline{F}] = deg(\gamma_i(T))$.

Segue então, das passagens anteriores e do Teorema 4.1.12, que

$$\begin{aligned}[F' : F] &= \sum_{i=1}^{r} e(P_i|P) \,.\, f(P_i|P) \\ &\leqslant \sum \varepsilon_i \,.\, deg(\gamma_i(T)) \\ &= deg(\varphi(T)) \\ &= [F' : F].\end{aligned}$$

Portanto, $\varepsilon_i = e(P_i|P)$, para todo $i = 1, \ldots, r$, o que completa a demonstração. ■

4.4 O COTRAÇO DOS DIFERENCIAIS DE WEIL E A FÓRMULA DO GÊNERO DE HURWITZ

Nesta seção, consideraremos F/K um corpo de funções, F'/F uma extensão finita e separável e K' o corpo de constantes de F'. Pelo Lema 4.1.2 e pela consideração inicial de que K é um corpo perfeito, temos que K'/K é uma extensão finita e separável.

Definição 4.4.1. Para $P \in \mathbb{P}_F$, definamos $\mathcal{O}'_P := ic_{F'}(\mathcal{O}_P)$. Então o conjunto

$$\mathcal{C}_P = \{z \in F';\, Tr_{F'/F}(z \,.\, \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

é chamado o módulo complementar sobre $\mathcal{O}_P$.

Proposição 4.4.2. *Com a mesma notação da Definição 4.4.1, temos que:*

a) $\mathcal{C}_P$ *é um* $\mathcal{O}'_P-$*módulo e* $\mathcal{O}'_P \subseteq \mathcal{C}_P$.

b) Se $\{z_1, \ldots, z_n\}$ *é uma base integral de* $\mathcal{O}'_P$ *sobre* $\mathcal{O}_P$, *então*

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \,.\, z_i^*,$$

onde $\{z_1^*, \ldots, z_n^*\}$ *é a base dual de* $\{z_1, \ldots, z_n\}$.

c) Existe um elemento $t \in F'$ dependendo de P tal que $\mathcal{C}_P = t\,.\,\mathcal{O}'_P$. Ainda,

$$v_{P'}(t) \leqslant 0, \text{ para todo } P'|P,$$

e, para todo $t' \in F'$, temos que

$$\mathcal{C}_P = t'\,.\,\mathcal{O}'_P \text{ se, e somente se, } v_{P'}(t') = v_{P'}(t), \text{ para todo } P'|P.$$

d) $\mathcal{C}_P = \mathcal{O}'_P$ para quase todo $P \in \mathbb{P}_F$.

Demonstração. *a*) A afirmação de que $\mathcal{C}_P$ é um $\mathcal{O}'_P-$módulo segue das definições de $\mathcal{C}_P$ e da função traço, bem como das propriedades dessa aplicação. Como o traço de um elemento $y \in \mathcal{O}'_P$ está em $\mathcal{O}_P$, pelo Corolário 4.3.2, temos que $\mathcal{O}'_P \subseteq \mathcal{C}_P$.

b) Em primeiro lugar, consideremos um elemento $z \in \mathcal{C}_P$. Como $\{z_1^*, \ldots, z_n^*\}$ é uma base de F'/F, existem $x_1, \ldots, x_n \in F$ tais que $z = \sum_{i=1}^{n} x_i z_i^*$. Como $z \in \mathcal{C}_P$ e $z_1, \ldots, z_n \in \mathcal{O}'_P$, temos que $Tr_{F'/F}(zz_j) \in \mathcal{O}_P$, para todo $j = 1, \ldots, n$. Agora

$$\begin{aligned} Tr_{F'/F}(zz_j) &= Tr_{F'/F}\left(\sum_{i=1}^{n} x_i z_i^* z_j\right) \\ &= \sum_{i=1}^{n} x_i Tr_{F'/F}(z_i^* z_j) \\ &= x_j \end{aligned}$$

pelas propriedades das bases duais. Portanto, $x_j \in \mathcal{O}_P$ e $z \in \sum_{i=1}^{n} \mathcal{O}_P\,.\,z_i^*$.

Reciprocamente, sejam $z \in \sum_{i=1}^{n} \mathcal{O}_P\,.\,z_i^*$ e $u \in \mathcal{O}'_P$. Escrevamos $z = \sum_{i=1}^{n} x_i\,.\,z_i^*$ e $u = \sum_{j=1}^{n} y_j z_j$, com $x_i,\, y_j \in \mathcal{O}_P$. Então

$$\begin{aligned} Tr_{F'/F}(zu) &= Tr_{F'/F}\left(\sum_{i,\,j=1}^{n} x_i y_j z_i^* z_j\right) \\ &= \sum_{i,\,j=1}^{n} x_i y_j\,.\,Tr_{F'/F}(z_i^* z_j) \\ &= \sum_{i=1}^{n} x_i y_i \in \mathcal{O}_P. \end{aligned}$$

Portanto, $z \in \mathcal{C}_P$.

c) Por *b*) e pelo Corolário 4.3.5, sabemos que $\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \,.\, u_i$ para certos elementos $u_i \in F'$. Escolhamos $x \in F$ tal que

$$v_P(x) \geqslant -v_{P'}(u_i),$$

para todos $P'|P$ e $i = 1, \ldots, n$ (recordemos que v_P é uma aplicação sobrejetora e que o número de lugares $P'|P$ é finito). Então

$$0 \leqslant v_{P'}(xu_i) = e(P'|P) \,.\, v_P(x) + v_{P'}(u_i),$$

para todo $P'|P$ e $i = 1, \ldots, n$, donde $x \,.\, \mathcal{C}_P \subseteq {\mathcal{O}'}_P$, pois temos que

$${\mathcal{O}'}_P = \{u \in F';\, v_{P'}(u) \geqslant 0, \text{ para todo } P'|P\}$$

pelo Corolário 4.3.5. Como ${\mathcal{O}'}_P \subseteq \mathcal{C}_P$ e $x \,.\, \mathcal{C}_P \subseteq {\mathcal{O}'}_P$, temos que $x \,.\, \mathcal{C}_P$ é um ideal de ${\mathcal{O}'}_P$. Daí, $x \,.\, \mathcal{C}_P = y \,.\, {\mathcal{O}'}_P$, para algum $y \in {\mathcal{O}'}_P$, pois ${\mathcal{O}'}_P$ é um domínio de ideais principais pela Proposição 4.2.11. Definindo $t = x^{-1}y$, obtemos que $\mathcal{C}_P = t \,.\, {\mathcal{O}'}_P$. Com efeito, seja $z \in \mathcal{C}_P$. Então $xz = yz'$, onde $z' \in {\mathcal{O}'}_P$. Assim, $z = x^{-1}yz' = t \,.\, z' \in t \,.\, {\mathcal{O}'}_P$. Por outro lado, se $z \in t \,.\, {\mathcal{O}'}_P$, então $z = t \,.\, u$, onde $u \in {\mathcal{O}'}_P$. Logo, $z = x^{-1}yu$, com $yu \in y \,.\, {\mathcal{O}'}_P = x \,.\, \mathcal{C}_P$. Dessa forma, $z = x^{-1}yu = x^{-1}xz' = z'$, com $z' \in \mathcal{C}_P$.

Agora, como ${\mathcal{O}'}_P \subseteq \mathcal{C}_P$, temos que $v_{P'}(t) \leqslant 0$ para todo $P'|P$. De fato, como $1 \in \mathcal{C}_P$, temos, pela igualdade anterior, que existe $z \in {\mathcal{O}'}_P$ tal que $1 = tz$, donde $v_{P'}(t) = -v_{P'}(z) \leqslant 0$, para todo $P'|P$.

Por último, se $t' \in F'$, temos que

$$\begin{aligned} t \,.\, {\mathcal{O}'}_P = t' \,.\, {\mathcal{O}'}_P &\Leftrightarrow tt'^{-1} \in {\mathcal{O}'}_P \text{ e } t't^{-1} \in {\mathcal{O}'}_P \\ &\Leftrightarrow v_{P'}(tt'^{-1}) \geqslant 0 \text{ e } v_{P'}(t't^{-1}) \geqslant 0, \text{ para todo } P'|P \\ &\Leftrightarrow v_{P'}(tt'^{-1}) = 0, \text{ para todo } P'|P \\ &\Leftrightarrow v_{P'}(t) = v_{P'}(t'), \text{ para todo } P'|P. \end{aligned}$$

d) Escolhamos uma base $\{z_1, \ldots, z_n\}$ de F'/F. Pelo Teorema 4.3.6, $\{z_1, \ldots, z_n\}$ e $\{z_1^*, \ldots, z_n^*\}$ são bases integrais para quase todo $P \in \mathbb{P}_F$, de modo que, pela parte *b*), $\mathcal{C}_P = {\mathcal{O}'}_P$, para quase todo $P \in \mathbb{P}_F$. ■

Definição 4.4.3. Consideremos um lugar $P \in \mathbb{P}_F$ e o fecho integral $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F'. Seja $\mathcal{C}_P = t\,.\,\mathcal{O}'_P$ o módulo complementar sobre $\mathcal{O}_P$. Então, definimos, para $P'|P$, o expoente diferente de P' sobre P por

$$d(P'|P) = -v_{P'}(t).$$

Notemos que, pela Proposição 4.4.2, $d(P'|P)$ está bem definido e $d(P'|P) \geqslant 0$. Além disso, $d(P'|P) = 0$, para quase todo P e $P'|P$. Dessa forma, podemos definir o seguinte divisor positivo de F'

$$Diff(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)\,.\,P',$$

chamado a diferente de F'/F.

Observação 4.4.4. Temos que $z \in \mathcal{C}_P$ se, e somente se, $v_{P'}(z) \geqslant -d(P'|P)$ para todo $P'|P$.

Com efeito, escrevamos $\mathcal{C}_P = t\,.\,\mathcal{O}'_P$. Se $z \in \mathcal{C}_P$, então $z = tz'$, com $z' \in \mathcal{O}'_P$, de modo que $v_{P'}(z) = v_{P'}(t) + v_{P'}(z') = -d(P'|P) + v_{P'}(z) \geqslant -d(P'|P)$, para todo $P'|P$. Reciprocamente, se z é tal que $v_{P'}(z) \geqslant -d(P'|P) = v_{P'}(t)$, para todo $P'|P$, então $v_{P'}(zt^{-1}) = v_{P'}(z) - v_{P'}(t) = v_{P'}(z) + d(P'|P) \geqslant 0$, para todo $P'|P$. Logo $zt^{-1} \in \mathcal{O}'_P$, isto é, $z = zt^{-1}t \in t\,.\,\mathcal{O}'_P = \mathcal{C}_P$.

Definição 4.4.5. Definimos

$$\mathcal{A}_{F'/F} = \{\alpha \in \mathcal{A}_{F'};\ \alpha_{P'} = \alpha_{Q'} \text{ sempre que } P' \cap F = Q' \cap F\}.$$

Observação 4.4.6. O conjunto $\mathcal{A}_{F'/F}$ é um espaço vetorial sobre F'. Além disso, a aplicação $Tr_{F'/F} : F' \to F$ que é $F-$linear pode ser estendida a uma aplicação $F-$linear de $\mathcal{A}_{F'/F}$ em $\mathcal{A}_F$, também denotada por $Tr_{F'/F}$, dada por

$$\alpha \mapsto Tr_{F'/F}(\alpha),$$

onde $(Tr_{F'/F}(\alpha))_P := Tr_{F'/F}(\alpha_{P'})$ e P' é qualquer lugar que é extensão de P. Observemos que a função $Tr(F'/F)$ está bem definida, pois se P' e Q' são extensões de P, então $P = P' \cap F$ e $P = Q' \cap F$, de modo que pela definição de $\mathcal{A}_{F'/F}$, temos que $\alpha_{P'} = \alpha_{Q'}$. Além disso, $\alpha_{P'} \in \mathcal{O}_{P'}$ para quase todo $P' \in \mathbb{P}_{F'}$, onde tal

fato segue da definição de um adele, de modo que $Tr_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$, para quase todo $P \in \mathbb{P}_F$, pelo Corolário 4.3.2. Isso garante que $Tr_{F'/F}(\alpha)$ é um adele de F/K. Notemos ainda que o traço de um adele principal é também um adele principal.

Definição 4.4.7. Definimos

$$\mathcal{A}_{F'/F}(A') = \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}.$$

Nas mesmas condições descritas anteriormente, temos os resultados a seguir.

Lema 4.4.8. *Para cada $C' \in Div(F')$, temos que $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$.*

Demonstração. Seja $\alpha = (\alpha_{P'})_{P' \in \mathbb{P}_{F'}}$ um adele de F'. Para todo $P \in \mathbb{P}_F$, existe, pelo Teorema da Aproximação Fraca, um elemento $x_P \in F'$ com

$$v_{P'}(\alpha_{P'} - x_P) \geqslant -v_{P'}(C'),$$

para todo $P'|P$. Definamos $\beta = (\beta_{P'})_{P' \in \mathbb{P}_{F'}}$ escrevendo $\beta_{P'} = x_P$, sempre que $P'|P$. Então $\beta \in \mathcal{A}_{F'/F}$ e $\alpha - \beta \in \mathcal{A}_{F'}(C')$. Como $\alpha = \beta + (\alpha - \beta)$, temos que o lema segue. ■

Lema 4.4.9. *Sejam M/L uma extensão finita e separável, V um espaço vetorial sobre M e $\mu : V \to L$ uma aplicação $L-$linear. Então existe uma única aplicação $M-$linear $\mu' : V \to M$ tal que $Tr_{M/L} \circ \mu' = \mu$.*

Demonstração. Como na demonstração da Proposição 4.3.3, consideremos o espaço das transformações lineares

$$M^* = \{\lambda : M \to L;\ \lambda \text{ é } L - \text{linear}\}$$

como um espaço vetorial sobre M, definindo $(z\,.\,\lambda)(w) = \lambda(z\,.\,w)$, para $\lambda \in M^*$ e z, $w \in M$. A dimensão de M^* sobre M é um e assim cada $\lambda \in M^*$ possui uma única representação na forma $\lambda = z\,.\,Tr_{M/L}$, com $z \in M$.

Para um elemento fixo $v \in V$, definamos a função $\lambda_v : M \to L$ por $\lambda_v(a) = \mu(av)$. Então λ_v é uma transformação linear sobre L, donde $\lambda_v = z_v\,.\,Tr_{M/L}$ para um

único elemento $z_v \in M$. Definamos $\mu'(v) = z_v$. Assim, temos que

$$\begin{aligned}\mu(av) &= \lambda_v(a)\\ &= (z_v \,.\, Tr_{M/L})(a)\\ &= (\mu'(v) \,.\, Tr_{M/L})(a)\\ &= Tr_{M/L}(a \,.\, \mu'(v)),\end{aligned}$$

para todos $a \in M$ e $v \in V$. Ainda, $\mu'(v)$ é unicamente determinado pela unicidade de z_v. Utilizando as igualdades anteriores, podemos mostrar que $\mu' : V \to M$ é $M-$linear. Escrevendo $a = 1$, obtemos que $\mu = Tr_{M/L} \circ \mu'$, o que mostra a existência de $\mu' : V \to M$ com as propriedades desejadas.

Suponhamos agora que exista uma outra $\mu^* : V \to M$ tal que $Tr_{M/L} \circ \mu' = Tr_{M/L} \circ \mu^*$ e $\mu^* \neq \mu'$. Como os únicos subespaços de M (visto aqui como um espaço vetorial sobre M) são os conjuntos $\{0\}$ e M, e $\mu' - \mu^*$ não é a transformação linear identicamente nula, temos que sua imagem, que é um subespaço vetorial de M, deve ser o conjunto M inteiro. Mas, como $Tr_{M/L}(\mu' - \mu^*) = 0$, teríamos uma contradição, pois $Tr_{M/L}$ não é a função identicamente nula já que M/L é uma extensão separável. ■

Teorema 4.4.10. *Para cada diferencial de Weil w de F/K, existe um único diferencial de Weil w' de F'/K' tal que*

$$Tr_{K'/K}(w'(\alpha)) = w(Tr_{F'/F}(\alpha)),$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Esse diferencial de Weil é chamado cotraço de w em F'/F e denotado por $Cotr_{F'/F}(w)$. Se $w \neq 0$ e $(w) \in Div(F)$ é o divisor de w, então

$$(Cotr_{F'/F}(w)) = Con_{F'/F}((w)) + Diff(F'/F).$$

Demonstração. Em primeiro lugar, queremos mostrar a existência de um diferencial de Weil w' tal que

$$Tr_{K'/K}(w'(\alpha)) = w(Tr_{F'/F}(\alpha)),$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Para $w = 0$, definamos $w' = 0$. Suponhamos agora que $w \neq 0$. Definamos também

$$W' = Con_{F'/F}((w)) + Diff(F'/F).$$

A construção de w' será desenvolvida em três etapas.

Etapa 1. A transformação $K-$linear $w_1 : \mathcal{A}_{F'/F} \to K$, definida por $w_1 = w \circ Tr_{F'/F}$, possui as seguintes propriedades:

a.1) $w_1(\alpha) = 0$ sempre que $\alpha \in \mathcal{A}_{F'/F}(W') + F'$.

b.1) Se $B' \in Div(F')$ é um divisor com $B' \not\leqslant W'$, então existe um adele $\beta \in \mathcal{A}_{F'/F}(B')$ com $w_1(\beta) \neq 0$.

Demonstração da Etapa 1. *a*.1) Temos que w_1 é $K-$linear, pois é a composição de aplicações que podem ser consideradas $K-$lineares, e w_1 se anula em F' já que w se anula em F. Agora, seja $\alpha \in \mathcal{A}_{F'/F}(W')$. Com o intuito de mostrarmos que $w_1(\alpha) = 0$, temos que verificar que, para todos $P \in \mathbb{P}_F$ e $P'|P$,

$$v_P(Tr_{F'/F}(\alpha_{P'})) \geqslant -v_P(w),$$

pois isso nos dá que $Tr_{F'/F}(\alpha_{P'}) \in \mathcal{A}_F((w))$ e, pela definição do divisor (w), temos que w se anula em $\mathcal{A}_F((w))$. Escolhamos um elemento $x \in F$ tal que $v_P(x) = v_P(w)$. Então

$$\begin{aligned} v_{P'}(x\alpha_{P'}) &= v_{P'}(x) + v_{P'}(\alpha_{P'}) \\ &= e(P'|P)v_P(x) + v_{P'}(\alpha_{P'}) \\ &= e(P'|P)v_P(w) + v_{P'}(\alpha_{P'}) \\ &\geqslant e(P'|P)v_P(w) - v_{P'}(W') \text{ (pois } \alpha \in \mathcal{A}_{F'}(W')) \\ &= v_{P'}(Con_{F'/F}((w)) - W') \\ &= -v_{P'}(Diff(F'/F)) = -d(P'|P). \end{aligned}$$

Pela Observação 4.4.4, temos que $x\alpha_{P'} \in \mathcal{C}_P$ e assim $v_P(Tr_{F'/F}(x\alpha_{P'})) \geqslant 0$. Como $Tr_{F'/F}(x\alpha_{P'}) = x \,.\, Tr_{F'/F}(\alpha_{P'})$ e $v_P(x) = v_P(w)$, temos que

$$v_P(Tr_{F'/F}(\alpha_{P'})) \geqslant -v_P(w),$$

para todos $P \in \mathbb{P}_F$ e $P'|P$.

b.1) Seja B' um divisor tal que $B' \nleqslant W'$, isto é, tal que existe $P_0 \in \mathbb{P}_F$ tal que, para algum $P^*|P_0$,

$$\begin{aligned} v_{P^*}(B') &> v_{P^*}(W') \\ &= v_{P^*}(Con_{F'/F}((w)) + Diff(F'/F)) \\ &= v_{P^*}(Con_{F'/F}((w))) + v_{P^*}(Diff(F'/F)), \end{aligned}$$

o que implica que $-v_{P^*}(Diff(F'/F)) > v_{P^*}(Con_{F'/F}((w)) - B')$, isto é,

$$-d(P^*|P_0) > v_{P^*}(Con_{F'/F}((w)) - B').$$

Sejam ${\mathcal{O}'}_{P_0}$ e $\mathcal{C}_{P_0}$ o fecho integral de $\mathcal{O}_{P_0}$ em F' e o módulo complementar sobre $\mathcal{O}_{P_0}$, respectivamente. Consideremos o conjunto

$$J = \{z \in F';\, v_{P^*}(z) \geqslant v_{P^*}(Con_{F'/F}((w)) - B'),\ \text{para todo } P^*|P_0\}.$$

Pelo Teorema da Aproximação, existe um elemento $u \in J$ satisfazendo

$$v_{P^*}(u) = v_{P^*}(Con_{F'/F}((w)) - B'),$$

para todo $P^*|P_0$. Isso nos dá, juntamente com a Observação 4.4.4, que $J \nsubseteq \mathcal{C}_{P_0}$. Como $J \,.\, {\mathcal{O}'}_{P_0} \subseteq J$, temos que

$$Tr_{F'/F}(J) \nsubseteq \mathcal{O}_{P_0}.$$

Escolhamos $t \in F$ tal que $v_{P_0}(t) = 1$. Para algum $r \geqslant 0$, temos que $t^r \,.\, J \subseteq {\mathcal{O}'}_{P_0}$, donde $t^r \,.\, Tr_{F'/F}(J) = Tr_{F'/F}(t^r J) \subseteq \mathcal{O}_{P_0}$. Ainda, $t^r \,.\, Tr_{F'/F}(J)$ é um ideal de $\mathcal{O}_{P_0}$. Consequentemente, $t^r \,.\, Tr_{F'/F}(J) = t^s \,.\, \mathcal{O}_{P_0}$, para algum $s \geqslant 0$, e assim obtemos que $Tr_{F'/F}(J) = t^m \,.\, \mathcal{O}_{P_0}$, para algum $m \in \mathbb{Z}$. Como $J \nsubseteq \mathcal{C}_{P_0}$, temos que $m \leqslant -1$, de modo que

$$t^{-1} \,.\, \mathcal{O}_{P_0} \subseteq Tr_{F'/F}(J).$$

Pela Proposição 3.5.3 (a), podemos encontrar um elemento $x \in F$ com

$$v_{P_0}(x) = -v_{P_0}(w) - 1 \text{ e } w_{P_0}(x) \neq 0.$$

Escolhamos $y \in F$ com $v_{P_0}(y) = v_{P_0}(w)$. Então $xy \in t^{-1} \,.\, \mathcal{O}_{P_0}$. Como

$$t^{-1} \,.\, \mathcal{O}_{P_0} \subseteq Tr_{F'/F}(J),$$

existe $z \in J$ tal que $Tr_{F'/F}(z) = xy$. Consideremos, um adele $\beta \in \mathcal{A}_{F'/F}$ dado por

$$\beta_{P'} = \begin{cases} 0, & \text{se } P' \nmid P_0 \\ y^{-1}z, & \text{se } P'|P_0. \end{cases}$$

Daí, segue da definição de J que, para $P'|P_0$,

$$\begin{aligned} v_{P'}(\beta) &= -v_{P'}(y) + v_{P'}(z) \\ &\geqslant -v_{P'}(Con_{F'/F}((w)) + v_{P'}(Con_{F'/F}((w)) - B') \\ &= -v_{P'}(B'). \end{aligned}$$

Logo, $\beta \in \mathcal{A}_{F'/F}(B')$. Por último, temos que $w_1(\beta) = w(Tr_{F'/F}(\beta)) = w_{P_0}(x) \neq 0$. Com efeito,

$$\begin{aligned} (Tr_{F'/F}(\beta))_{P_0} &= Tr_{F'/F}(\beta_{P'}), \text{ onde } P'|P_0 \\ &= Tr_{F'/F}(y^{-1}z) \\ &= y^{-1}Tr_{F'/F}(z) \\ &= y^{-1}(xy) = x \end{aligned}$$

e

$$\begin{aligned} (Tr_{F'/F}(\beta))_P &= Tr_{F'/F}(\beta_{P'}), \text{ onde } P'|P, \ P \neq P_0 \\ &= Tr_{F'/F}(0) = 0. \end{aligned}$$

Isso conclui a demonstração do item $b.1)$.

Etapa 2. Definamos $w_2 : \mathcal{A}_{F'/F} \to K$ como a seguir: para $\alpha \in \mathcal{A}_{F'}$ existem adeles $\beta \in \mathcal{A}_{F'/F}$ e $\gamma \in \mathcal{A}_{F'/F}(W')$ tais que $\alpha = \beta + \gamma$, pelo Lema 4.4.8. Escrevamos

$$w_2(\alpha) = w_1(\beta).$$

Então w_2 está bem definido. Com efeito, se $\beta + \gamma$ e $\beta_1 + \gamma_1$ são duas representações para um mesmo elemento α, com β, $\beta_1 \in \mathcal{A}_{F'/F}$ e γ, $\gamma_1 \in \mathcal{A}_{F'}(W')$, então

$$\beta_1 - \beta = \gamma - \gamma_1 \in \mathcal{A}_{F'/F} \cap \mathcal{A}_{F'}(W') = \mathcal{A}_{F'/F}(W').$$

Logo $w_1(\beta_1) - w_1(\beta) = w_1(\beta_1 - \beta) = 0$ por $a.1)$. A função w_2 é $K-$linear e, por $a.1)$ e $b.1)$, ela possui as seguintes propriedades:

$a.2)$ $w_2(\alpha) = 0$, para $\alpha \in \mathcal{A}_{F'}(W') + F'$.

$b.2)$ Se $B' \in Div(F')$ é um divisor com $B' \nleqslant W'$, então existe um adele $\beta \in \mathcal{A}_{F'}(B')$ com $w_2(\beta) \neq 0$.

Dessa forma, construímos uma transformação $K-$linear $w_2 : A_{F'} \to K$ que se anula em $\mathcal{A}_{F'}(W') + F'$. Contudo, w_2 não é um diferencial de Weil de F'/K' se $K \subsetneq K'$. Isso nos leva à próxima etapa.

Etapa 3. Pelo Lema 4.4.9, existe uma transformação $K'-$linear $w' : \mathcal{A}_{F'} \to K'$ tal que $Tr_{K'/K} \circ w' = w_2$. Das definições de w_1 e w_2 obtemos, para $\alpha \in \mathcal{A}_{F'/F}$, que

$$Tr_{K'/K}(w'(\alpha)) = w_2(\alpha) = w_1(\alpha) = w(Tr_{F'/F}(\alpha)).$$

Resta-nos mostrar que:

$a.3)$ $w'(\alpha) = 0$, para $\alpha \in \mathcal{A}_{F'}(W') + F'$.

$b.3)$ Se $B' \in Div(F')$ é um divisor com $B' \nleqslant W'$, então existe um adele $\beta \in \mathcal{A}_{F'}(B')$ com $w'(\beta) \neq 0$.

Demonstração de $a.3$). Como w' é $K'-$linear, a imagem de $\mathcal{A}_{F'}(W') + F'$ sob w' é $\{0\}$ ou K'. Se o último caso ocorresse, então existiria $\alpha \in \mathcal{A}_{F'}(W') + F'$ tal que $Tr_{K'/K}(w'(\alpha)) \neq 0$, já que $Tr_{K'/K}$ não é a transformação identicamente nula. Pela construção de w', temos que $w_2 = Tr_{K'/K} \circ w'$. Logo $w_2(\alpha) \neq 0$, o que é uma contradição com $a.2$).

Demonstração de $b.3$). Por $b.2$), existe um adele $\beta \in \mathcal{A}_{F'}(B')$ com a propriedade de $w_2(\beta) \neq 0$. Daí $Tr_{K'/K}(w'(\beta)) \neq 0$ e assim a afirmação segue.

Com as etapas anteriores conseguimos estabelecer a existência de um diferencial de Weil w' satisfazendo $Tr_{K'/K}(w'(\alpha)) = w(Tr_{F'/F}(\alpha))$ e também mostramos que

$$(w') = W' = Con_{F'/F}((w)) + Diff(F'/F).$$

Com o intuito de mostrarmos a unicidade, suponhamos que w^* seja um outro diferencial de Weil de F'/K' tal que

$$Tr_{K'/K}(w^*(\alpha)) = Tr_{K'/K}(w'(\alpha)) = w(Tr_{F'/F}(\alpha)),$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Definindo $\eta = w^* - w'$, obtemos

$$Tr_{K'/K}(\eta(\alpha)) = 0,$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Ainda, η é um diferencial de Weil de F'/K', donde η se anula em $\mathcal{A}_{F'}(C')$, para algum $C' \in Div(F')$. Pelo Lema 4.4.8, temos que $Tr_{K'/K}(\eta(\alpha)) = 0$, para todo $\alpha \in \mathcal{A}_{F'}$. Isso implica que $\eta = 0$ e assim $w^* = w'$. ■

Teorema 4.4.11 (Fórmula do Gênero de Hurwitz)**.** *Sejam F/K um corpo de funções de gênero g e F'/F uma extensão finita e separável. Seja K' o corpo de constantes de F' e g' o gênero de F'/K'. Então*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + deg(Diff(F'/F)).$$

Demonstração. Escolhamos um diferencial de Weil $w \neq 0$ de F/K. Segue do Teorema 4.4.10 que

$$(Cotr_{F'/F}(w)) = Con_{F'/F}((w)) + Diff(F'/F).$$

Recordemos que, pelo Corolário 3.4.20, o grau de um divisor canônico de F/K é $2g - 2$ e de F'/K' é $2g' - 2$. Assim, obtemos da igualdade anterior e do Corolário 4.1.16 que

$$\begin{aligned} 2g' - 2 &= deg(Con_{F'/F}((w))) + deg(Diff(F'/F)) \\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + deg(Diff(F'/F)). \end{aligned}$$

■

4.5 A DIFERENTE

Ao longo dessa seção, consideremos uma extensão finita e separável F'/F, onde F/K e F'/K' são corpos de funções com corpos de constantes K e K', respectivamente. Ainda, consideraremos K e K' corpos perfeitos.

Lema 4.5.1. *Sejam F^*/F uma extensão algébrica de corpos de funções, $P \in \mathbb{P}_F$ e $P^* \in \mathbb{P}_{F^*}$ com $P^*|P$. Consideremos um automorfismo σ de F^*/F. Então $\sigma(P^*) = \{\sigma(z);\ z \in P^*\}$ é um lugar de F^* e temos que:*

a) $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y))$, *para todo* $y \in F^*$.

b) $\sigma(P^*)|P$.

c) $e(\sigma(P^*)|P) = e(P^*|P)$ *e* $f(\sigma(P^*)|P) = f(P^*|P)$.

Demonstração. Como σ é um automorfismo, temos que $\sigma(\mathcal{O}_{P^*})$ é um anel de valorização de F^* e $\sigma(P^*)$ é o seu ideal maximal. Dessa forma, $\sigma(P^*)$ é um lugar de F^*, com anel de valorização correspondente $\mathcal{O}_{\sigma(P^*)} = \sigma(\mathcal{O}_{P^*})$. Ainda, se t^* é um elemento primo para P^*, então $\sigma(t^*)$ é um elemento primo para $\sigma(P^*)$. Com isso, mostremos as afirmações *a*), *b*) e *c*).

a) Dado $0 \neq y \in F^*$, temos que $y = \sigma(z)$, para algum $z \in F^*$. Escrevendo $z = t^{*r}u$, onde $r = v_{P^*}(z)$ e $u \in \mathcal{O}_{P^*}^{\times} = \mathcal{O}_{P^*} \backslash P^*$, obtemos que

$$y = \sigma(z) = \sigma(t^{*r}u) = \sigma(t^*)^r \sigma(u),$$

onde $\sigma(u) \in \mathcal{O}_{\sigma(P^*)}^{\times} = \mathcal{O}_{\sigma(P^*)} \backslash \sigma(P^*)$ e $\sigma(t^*)$ é um elemento primo para $\sigma(P^*)$. Isso nos dá que $v_{\sigma(P^*)}(y) = r = v_{P^*}(z) = v_{P^*}(\sigma^{-1}(y))$, como queríamos mostrar.

b) $\sigma(P^*)|P$, pois $\sigma(P^*) \supseteq \sigma(P) = P$.

c) Seja $x \in F$ um elemento primo para P. Então

$$e(\sigma(P^*)|P) = v_{\sigma(P^*)}(x) = v_{P^*}(\sigma^{-1}(x)) = v_{P^*}(x) = e(P^*|P).$$

Ainda, o automorfismo σ de F^*/F induz um isomorfismo

$$\begin{array}{rccc} \overline{\sigma}: & F_{P^*}^* & \to & F_{\sigma(P^*)}^* \\ & z + P^* & \mapsto & \sigma(z) + \sigma(P^*) \end{array}$$

cuja restrição à F_P é a identidade. Portanto

$$f(P^*|P) = [F_{P^*}^* : F_P] = [F_{\sigma(P^*)}^* : F_P] = f(\sigma(P^*)|P).$$

■

Lema 4.5.2. *Sejam* $P \in \mathbb{P}_F$ *e* $P_1, \ldots, P_r$ *todas as extensões de* P *em* F'/F. *Denotemos por* $k = \mathcal{O}_P/P$, $k_i = \mathcal{O}_{P_i}/P_i \supseteq k$ *e consideremos as respectivas projeções*

$\pi : \mathcal{O}_P \to k$ e $\pi_i : \mathcal{O}_{P_i} \to k_i$, para todo $i = 1, \ldots, r$. Então, para todo $u \in \mathcal{O'}_P$, onde $\mathcal{O'}_P$ é o fecho integral de $\mathcal{O}_P$ em F', temos que

$$\pi(Tr_{F'/F}(u)) = \sum_{i=1}^{r} e(P_i|P) \, . \, Tr_{k_i/k}(\pi_i(u)).$$

Demonstração. Pode ser encontrada em [16] (Lema 3.5.3). ■

Teorema 4.5.3 (Teorema da Diferente de Dedekind)**.** *Seguindo a notação apresentada no início dessa seção, temos, para todo $P'|P$, que:*

a) $d(P'|P) \geqslant e(P'|P) - 1$.

b) $d(P'|P) = e(P'|P) - 1$ *se, e somente se, $e(P'|P)$ não é divisível por $char(K)$. Em particular, se $char(K) = 0$, então $d(P'|P) = e(P'|P) - 1$.*

Demonstração. a) Como antes, sejam $\mathcal{O'}_P$ o fecho integral de $\mathcal{O}_P$ em F' e $\mathcal{C}_P$ o módulo complementar sobre $\mathcal{O}_P$. Queremos mostrar que

$$Tr_{F'/F}(t \, . \, \mathcal{O'}_P) \subseteq \mathcal{O}_P,$$

isto é, que $t \in \mathcal{C}_P$, para todo $t \in F'$ satisfazendo

$$v_{P'}(t) = 1 - e(P'|P),$$

para todo $P'|P$. Pela Observação 4.4.4, isso nos daria que $1 - e(P'|P) \geqslant -d(P'|P)$ e assim $d(P'|P) \geqslant e(P'|P) - 1$.

Com o intuito de provarmos a afirmação inicial, consideremos uma extensão de Galois finita F^*/F tal que $F \subseteq F' \subseteq F^*$ e escolhamos $n = [F' : F]$ automorfismos $\sigma_1, \ldots, \sigma_n$ de F^*/F cujas restrições à F' sejam duas a duas distintas. Para $z \in \mathcal{O'}_P$ temos que

$$Tr_{F'/F}(t \, . \, z) = \sum_{i=1}^{n} \sigma_i(t \, . \, z).$$

Fixemos um lugar P^* de F^* que é uma extensão de P e definamos $P_i^* = \sigma_i^{-1}(P^*)$ e $P_i' = P_i^* \bigcap F'$. Notemos que $\sigma_i(z)$ é integral sobre $\mathcal{O}_P$. Com efeito, seja

$$\varphi(T) = a_0 + a_1 T + \ldots + a_{r-1} T^{r-1} + T^r \in \mathcal{O}_P[T]$$

tal que $\varphi(z) = 0$. Então $a_0 + a_1 z + \ldots + a_{r-1} z^{r-1} + z^r = 0$, implica que

$$\begin{aligned} 0 &= \sigma_i(a_0 + a_1 z + \ldots + a_{r-1} z^{r-1} + z^r) \\ &= a_0 + a_1 \sigma_i(z) + \ldots + a_{r-1} \sigma_i(z)^{r-1} + \sigma_i(z)^r \\ &= \varphi(\sigma_i(z)), \end{aligned}$$

isto é, $\sigma_i(z)$ é integral sobre $\mathcal{O}_P$. Logo, $v_{P^*}(\sigma_i(z)) \geqslant 0$ e assim

$$\begin{aligned} v_{P^*}(\sigma_i(t\,.\,z)) &= v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z)) \\ &\geqslant v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) \text{ (\textit{pelo Lema} 4.5.1)} \\ &= e(P_i^*|P_i') v_{P_i'}(t) \\ &= e(P_i^*|P_i')(1 - e(P_i'|P)) \\ &> -e(P_i^*|P_i') e(P_i'|P) \\ &= -e(P_i^*|P) \\ &= -e(P^*|P) \text{ (\textit{pelo Lema} 4.5.1).} \end{aligned}$$

Pela Desigualdade Triangular,

$$-e(P^*|P) < v_{P^*}(Tr_{F'/F}(t\,.\,z)) = e(P^*|P)\,.\,v_P(Tr_{F'/F}(t\,.\,z)),$$

o que nos dá que $v_P(Tr_{F'/F}(t\,.\,z)) \geqslant 0$, como queríamos mostrar.

b) Sigamos a notação do Lema 4.5.2 e abreviemos $e_i = e(P_i|P)$. Sejam $P' = P_1$ e $e = e(P'|P)$. Devemos mostrar que

$$d(P'|P) = e - 1 \text{ se, e somente se, } char(K) \nmid e.$$

($\Leftarrow$) Assumamos que $char(K) \nmid e$ e suponhamos que $d(P'|P) \geqslant e > e - 1$. Então $-d(P'|P) \leqslant -e$ e existe $w \in F'$ tal que $-d(P'|P) \leqslant v_{P'}(w) \leqslant -e$, donde, pela Observação 4.4.4, $w \in \mathcal{C}_P$, isto é, $Tr_{F'/F}(w\,.\,\mathcal{O}'_P) \subseteq \mathcal{O}_P$. Como K é um corpo perfeito, temos que k_1/k é uma extensão separável, donde $Tr_{k_1/k}$ não é a tranformação linear identicamente nula e assim podemos encontrar $y_0 \in \mathcal{O}_{P'}$ tal que $Tr_{k_1/k}(\pi_1(y_0)) \neq 0$. Pelo Teorema da Aproximação Fraca, existe $y \in F'$ tal que

$$v_{P'}(y - y_0) > 0$$

e

$$v_{P_i}(y) \geqslant max\{1,\, e_i + v_{P_i}(w)\}$$

para $i = 2, \ldots, r$. Logo, $y \in \mathcal{O}'_P$ e, pelo Lema 4.5.2,

$$\begin{aligned} \pi(Tr_{F'/F}(y)) &= e\,.\,Tr_{k_1/k}(\pi_1(y)) + \sum_{i=2}^{r} e_i\,.\,Tr_{k_i/k}(\pi_i(y)) \\ &= e\,.\,Tr_{k_1/k}(\pi_1(y_0)) \neq 0 \end{aligned}$$

onde as igualdades anteriores seguem do fato de $v_{P_i}(y) \geqslant 1$ implicar que $y \in P_i$, para todo $i = 2, \ldots, r$, donde $\pi_i(y) = 0$ e assim $Tr_{k_i/k}(\pi_i(y)) = 0$, bem como o fato de $char(K)$ não dividir e. Dessa forma, temos que $v_P(Tr_{F'/F}(y)) = 0$.

Escolhamos $x \in F$ tal que $v_P(x) = 1$. Então

$$Tr_{F'/F}(x^{-1}y) = x^{-1}\,.\,Tr_{F'/F}(y) \notin \mathcal{O}_P,$$

pois $v_P(x^{-1}y) = -1$. Por outro lado, $x^{-1}yw^{-1} \in \mathcal{O}'_P$, já que

$$\begin{aligned} v_{P'}(x^{-1}yw^{-1}) &= v_{P'}(x^{-1}) + v_{P'}(y) + v_{P'}(w^{-1}) \\ &= e\,.\,v_P(x^{-1}) + v_{P'}(y) + v_{P'}(w^{-1}) \\ &= -e + v_{P'}(y) + v_{P'}(w^{-1}) \\ &\geqslant 0 \end{aligned}$$

e

$$\begin{aligned} v_{P_i}(x^{-1}yw^{-1}) &= v_{P_i}(x^{-1}) + v_{P_i}(y) + v_{P_i}(w^{-1}) \\ &= e_i\,.\,v_P(x^{-1}) + v_{P_i}(y) + v_{P_i}(w^{-1}) \\ &= v_{P_i}(y) - (e_i + v_{P_i}(w)) \\ &\geqslant 0, \end{aligned}$$

para $i = 2, \ldots, r$. Daí $x^{-1}y \in w\,.\,\mathcal{O}'_P$, donde $Tr_{F'/F}(x^{-1}y) \in \mathcal{O}_P$, o que é uma contradição. Portanto $d(P'|P) = e - 1$, como queríamos mostrar.

($\Rightarrow$) Assumamos que $char(K)|e$. Queremos mostrar que $d(P'|P) \geqslant e$. Escolhamos $u \in F'$ tal que

$$v_{P'}(u) = -e \text{ e } v_{P_i}(u) \geqslant -e_i + 1, \text{ para } i = 2, \ldots, r.$$

Seja x um elemento primo para P. Para cada $z \in \mathcal{O}'_P$, temos que

$$v_{P'}(xuz) = v_{P'}(x) + v_{P'}(u) + v_{P'}(z) = e - e + v_{P'}(z) \geqslant 0$$

e

$$v_{P_i}(xuz) = v_{P_i}(x) + v_{P_i}(u) + v_{P_i}(z) \geqslant e_i - e_i + 1 + v_{P_i}(z) \geqslant 1 > 0,$$

para todo $i = 2, \ldots, r$. Dessa forma, $xuz \in \mathcal{O}'_P$ e, pelo Lema 4.5.2,

$$\begin{aligned} \pi(Tr_{F'/F}(xuz)) &= e \,.\, Tr_{k_1/k}(\pi_1(xuz)) + \sum_{i=2}^{r} e_i \,.\, Tr_{k_i/k}(\pi_i(xuz)) \\ &= e \,.\, Tr_{k_1/k}(\pi_1(xuz)) = 0, \end{aligned}$$

onde as igualdades anteriores podem ser explicadas de forma análoga ao que foi feito em ($\Leftarrow$). Assim, concluímos que $x \,.\, Tr_{F'/F}(uz) = Tr_{F'/F}(xuz) \in P = x\mathcal{O}_P$, donde $Tr_{F'/F}(uz) \in \mathcal{O}_P$ para todo $z \in \mathcal{O}'_P$. Isso mostra que $u \in \mathcal{C}_P$ e $-e = v_{P'}(u) \geqslant -d(P'/P)$, pela Observação 4.4.4. ■

Teorema 4.5.4. *Suponhamos que $F' = F(y)$ seja uma extensão finita e separável de um corpo de funções F de grau $[F' : F] = n$. Seja $P \in \mathbb{P}_F$ tal que o polinômio minimal $\varphi(T)$ de y sobre F possua coeficientes em $\mathcal{O}_P$, isto é, y seja integral sobre $\mathcal{O}_P$, pela Proposição 4.3.1. Sejam ainda $P_1, \ldots, P_r \in \mathbb{P}_{F'}$ todos os lugares de F' que são extensão de P. Então:*

a) $d(P_i|P) \leqslant v_{P_i}(\varphi'(y))$, *para todo* $i = 1, \ldots, r$.

b) $\{1, y, \ldots, y^{n-1}\}$ *é uma base integral de* F'/F *no lugar* P *se, e somente se,* $d(P_i|P) = v_{P_i}(\varphi'(y))$, *para* $i = 1, \ldots, r$, *onde* $\varphi'(T)$ *denota a derivada de* $\varphi(T)$ *em* $F[T]$.

Demonstração. A base dual de $\{1, y, \ldots, y^{n-1}\}$ está diretamente relacionada com os expoentes diferentes $d(P_i|P)$, pela Proposição 4.4.2. Assim, o nosso primeiro objetivo será determinar essa base dual. Como $\varphi(y) = 0$, o polinômio $\varphi(T)$ fatora-se em $F'[T]$ como

$$\varphi(T) = (T - y)(c_{n-1}T^{n-1} + \ldots + c_1T + c_0),$$

com $c_0, \ldots, c_{n-1} \in F'$ e $c_{n-1} = 1$. Afirmamos que

$$\left\{ \frac{c_0}{\varphi'(y)}, \ldots, \frac{c_{n-1}}{\varphi'(y)} \right\}$$

é a base dual de $\{1, y, \ldots, y^{n-1}\}$. Notemos ainda que $\varphi'(y) \neq 0$, uma vez que y é separável sobre F. Pela definição de base dual a afirmação anterior é equivalente a

$$Tr_{F'/F}\left(\frac{c_i}{\varphi'(y)} . y^l \right) = \delta_{il},$$

para todo $0 \leqslant i, l \leqslant n-1$. Com o intuito de provarmos isso, consideremos n mergulhos distintos $\sigma_1, \ldots, \sigma_n$ de F'/F em Φ, onde Φ denota uma extensão algebricamente fechada de F (tais mergulhos existem pelo Teorema 2.5.8). Definamos $y_j = \sigma_j(y)$, de modo que

$$\varphi(T) = \prod_{j=1}^{n} (T - y_j),$$

por uma explicação análoga à desenvolvida na Observação 4.7.8. Para cada $\nu \in \{1, \ldots, n\}$, podemos escrever

$$\varphi'(T) = \prod_{\substack{j=1 \\ j \neq \nu}}^{n} (T - y_j) + (T - y_\nu) \left(\prod_{\substack{j=1 \\ j \neq \nu}}^{n} (T - y_j) \right)',$$

donde

$$\varphi'(y_\nu) = \prod_{\substack{j=1 \\ j \neq \nu}}^{n} (y_\nu - y_j).$$

Para $0 \leqslant l \leqslant n-1$ consideremos o polinômio

$$\varphi_l(T) = \left(\sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)} \right) - T^l \in \Phi[T].$$

O grau desse polinômio é no máximo $n-1$ e, para $1 \leqslant \nu \leqslant n$ temos que

$$\varphi_l(y_\nu) = \left(\prod_{i \neq \nu} (y_\nu - y_i) \right) \cdot \frac{y_\nu^l}{\varphi'(y_\nu)} - y_\nu^l = 0.$$

Agora, um polinômio de grau menor ou igual a $n-1$ tendo n raízes distintas deve ser o polinômio identicamente nulo. Logo $\varphi_l(T) = 0$, isto é,

$$T^l = \sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)},$$

para $0 \leqslant l \leqslant n-1$. Os mergulhos $\sigma_i : F' \to \Phi$ se estendem a mergulhos $\sigma_i : F'(T) \to \Phi(T)$ definindo $\sigma_i(T) = T$, de modo que

$$\begin{aligned}
T^l &= \sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)} \\
&= \sum_{j=1}^{n} \frac{\sigma_j(\varphi(T))}{T - \sigma_j(y)} \cdot \frac{\sigma_j(y)^l}{\varphi'(\sigma_j(y))} \\
&= \sum_{j=1}^{n} \sigma_j \left(\frac{\varphi(T)}{T - y} \cdot \frac{y^l}{\varphi'(y)} \right) \\
&= \sum_{j=1}^{n} \sigma_j \left(\sum_{i=0}^{n-1} c_i T^i \cdot \frac{y^l}{\varphi'(y)} \right) \\
&= \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n} \sigma_j \left(\frac{c_i}{\varphi'(y)} \cdot y^l \right) \right) T^i \\
&= \sum_{i=0}^{n-1} \left(Tr_{F'/F} \left(\frac{c_i}{\varphi'(y)} \cdot y^l \right) \right) T^i.
\end{aligned}$$

Comparando os coeficientes de ambos os lados da igualdade anterior, obtemos que

$$Tr_{F'/F} \left(\frac{c_i}{\varphi'(y)} \cdot y^l \right) = \delta_{il}$$

como desejado.

O próximo passo agora é mostrar que

$$c_j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i,$$

para $j = 0, \ldots, n-1$. O polinômio minimal $\varphi(T)$ de y sobre F possui a forma

$$\varphi(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0,$$

com $a_i \in \mathcal{O}_P$. Assim chegamos às seguintes expressões

$$c_{n-1} = 1,\ c_0 y = -a_0 \text{ e } c_i y = c_{i-1} - a_i \text{ para } i = 1, \ldots, n-1.$$

Já temos que $c_{n-1} = 1 \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$. Agora, supondo que $c_j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$ para algum $j \in \{1, \ldots, n-1\}$, temos que

$$c_j = \sum_{i=0}^{n-1} s_i y^i,$$

com $s_i \in \mathcal{O}_P$. Utilizando as relações anteriores para os coeficientes, obtemos que

$$\begin{aligned} c_{j-1} &= a_j + c_j y = a_j + \sum_{i=0}^{n-2} s_i y^{i+1} + s_{n-1} y^n \\ &= a_j + \sum_{i=0}^{n-2} s_i y^{i+1} - s_{n-1} \sum_{i=0}^{n-1} a_i y^i \in \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, y^i. \end{aligned}$$

De modo similar, podemos mostrar que $y^j \in \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, c_i$, para $j = 0, \ldots, n-1$. De fato, $y^0 = 1 \in \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, c_i$. Se

$$y^j = \sum_{i=0}^{n-1} r_i c_i,$$

com $r_i \in \mathcal{O}_P$, para algum $j \geqslant 0$, então

$$\begin{aligned} y^{j+1} &= \sum_{i=0}^{n-1} r_i c_i y = \sum_{i=1}^{n-1} r_i (c_{i-1} - a_i) - r_0 a_0 \\ &= \sum_{i=0}^{n-2} r_{i+1} c_i - \left(\sum_{i=0}^{n-1} r_i a_i \right) . 1 \\ &= \sum_{i=0}^{n-2} r_{i+1} c_i - \left(\sum_{i=0}^{n-1} r_i a_i \right) . c_{n-1} \in \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, c_i. \end{aligned}$$

Mostremos agora as letras a) e b) deste teorema.

a) Sejam $\mathcal{C}_P$ o módulo complementar e $\mathcal{O}'_P$ o fecho integral de $\mathcal{O}_P$ em F'. Queremos mostrar que $d(P_i|P) \leqslant v_{P_i}(\varphi'(y))$, o que é equivalente, pela Observação 4.5.5, à seguinte afirmação

$$z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geqslant -v_{P_i}(\varphi'(y)) \text{ para } i = 1, \ldots, r.$$

O elemento $z \in \mathcal{C}_P$ pode ser escrito como

$$z = \sum_{i=0}^{n-1} r_i \,.\, \frac{c_i}{\varphi'(y)},$$

com $r_i \in F$. Como y^l é integral sobre $\mathcal{O}_P$, pois z o é e $\mathcal{O}'_P$ é um subanel de F', e $z \in \mathcal{C}_P$, temos que $Tr_{F'/F}(z \,.\, y^l) \in \mathcal{O}_P$. Agora,

$$Tr_{F'/F}(z \,.\, y^l) = Tr_{F'/F} \left(\sum_{i=0}^{n-1} r_i \,.\, \frac{c_i}{\varphi'(y)} \,.\, y^l \right) = r_l,$$

donde $r_l \in \mathcal{O}_P$. Isso nos dá que

$$z = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} r_i c_i \text{ pertence a } \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i \subseteq \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P,$$

o que mostra a afirmação inicial e conclui a demonstração da letra a) do teorema.

b) Já mostramos que

$$\sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i = \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i.$$

Suponhamos inicialmente que $\{1, y, \ldots, y^{n-1}\}$ seja uma base integral no lugar P. Pela Proposição 4.4.2, temos que

$$\begin{aligned} \mathcal{C}_P &= \sum_{i=0}^{n-1} \mathcal{O}_P \cdot \frac{c_i}{\varphi'(y)} = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i \\ &= \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P. \end{aligned}$$

Consequentemente $d(P_i|P) = v_{P_i}(\varphi'(y))$, pela Definição 4.4.3. Reciprocamente, temos que mostrar que as condições

$$d(P_i|P) = v_{P_i}(\varphi'(y)), \text{ para } i = 1, \ldots, r,$$

implicam que $\mathcal{O}'_P \subseteq \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$ (notemos que a outra inclusão segue das definições). Seja $z \in \mathcal{O}'_P$ e escrevamos

$$z = \sum_{i=0}^{n-1} t_i y^i,$$

com $t_i \in F$. Observemos que $c_j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i \subseteq \mathcal{O}'_P$ e $\mathcal{C}_P = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P$ pela hipótese inicial e pela Proposição 4.4.2. Logo

$$Tr_{F'/F}\left(\frac{1}{\varphi'(y)} \cdot c_j \cdot z\right) \in \mathcal{O}_P.$$

Como

$$Tr_{F'/F}\left(\frac{1}{\varphi'(y)} \cdot c_j \cdot z\right) = Tr_{F'/F}\left(\sum_{i=0}^{n-1} \frac{c_j}{\varphi'(y)} \cdot y^i\right) = t_j,$$

concluímos que $t_j \in \mathcal{O}_P$, como queríamos mostrar. ■

Observação 4.5.5. Nesta observação, queremos mostrar a equivalência entre as seguintes afirmações, nas quais estamos utilizando as mesmas notações do Teorema 4.5.4:

a) $d(P_i|P) \leqslant v_{P_i}(\varphi'(y))$, para todo $i = 1, \ldots, r$.

b) $z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geqslant -v_{P_i}(\varphi'(y))$, para todo $i = 1, \ldots, r$.

De fato: *a)* $\Rightarrow$ *b)* Fixemos $i = 1, \ldots, r$. Se $d(P_i|P) \leqslant v_{P_i}(\varphi'(y))$, então $-d(P_i|P) \geqslant -v_{P_i}(\varphi'(y))$, donde para todo $z \in \mathcal{C}_P$, $v_{P_i}(z) \geqslant -d(P_i|P) \geqslant -v_{P_i}(\varphi'(y))$, pela Observação 4.4.4, o que mostra a letra *b*).
b) $\Rightarrow$ *a)* Fixemos $i = 1, \ldots, r$. Se $z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geqslant -v_{P_i}(\varphi'(y))$, em particular escrevendo $\mathcal{C}_P = t \,.\, \mathcal{O}'_P$, temos que $-d(P_i|P) = v_{P_i}(t) \geqslant -v_{P_i}(\varphi'(t))$, o que mostra a letra *a*).

Proposição 4.5.6. *Sejam F'/F uma extensão finita e separável de corpos de funções, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$, com $P'|P$. Suponhamos que $P'|P$ seja totalmente ramificado, isto é, que $e(P'|P) = [F' : F] = n$. Seja $t \in F'$ um elemento primo para P' e consideremos o polinômio minimal $\varphi(T) \in F[T]$ de t sobre F. Então $d(P'|P) = v_{P'}(\varphi'(t))$ e $\{1, \ldots, t^{n-1}\}$ é uma base integral de F'/F em P.*

Demonstração. Primeiramente, mostremos que $1, t, \ldots, t^{n-1}$ são linearmente independentes sobre F. De fato, assumamos o contrário. Então existem $r_0, \ldots, r_{n-1} \in F$ não todos nulos tais que

$$\sum_{i=0}^{n-1} r_i t^i = 0.$$

Para $r_i \neq 0$, temos que

$$v_{P'}(r_i t^i) = v_{P'}(t^i) + e(P'|P) v_P(r_i) = i \,.\, v_{P'}(t) + n \,.\, v_P(r_i) = i + n \,.\, v_P(r_i) \equiv i \pmod{n}.$$

Assim, $v_{P'}(r_i t^i) \neq v_{P'}(r_j t^j)$ se $i \neq j$, $r_i \neq 0$ e $r_j \neq 0$. Pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que

$$v_{P'}\left(\sum_{i=0}^{n-1} r_i t^i\right) = min\{v_{P'}(r_i t^i);\, r_i \neq 0\} < \infty,$$

o que é uma contradição, pois $\sum_{i=0}^{n-1} r_i t^i = 0$ implica que $v_{P'}\left(\sum_{i=0}^{n-1} r_i t^i\right) = \infty$. Ainda, pela Igualdade Fundamental (Teorema 4.1.12), P' é a única extensão em $\mathbb{P}_{F'}$ de P, donde $\mathcal{O}_{P'}$ é o fecho integral de $\mathcal{O}_P$ em F'. Desse modo, para concluirmos a demonstração, precisamos mostrar que

$$\mathcal{O}_{P'} = \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, t^i.$$

A inclusão $\mathcal{O}_{P'} \supseteq \sum_{i=0}^{n-1} \mathcal{O}_P \,.\, t^i$ segue do fato de t ser um elemento primo para P' e do fato de $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Para a outra inclusão, consideremos $z \in \mathcal{O}_{P'}$. Escrevamos

$$z = \sum_{i=0}^{n-1} x_i t^i,$$

com $x_i \in F$. Como $0 \leqslant v_{P'}(z) = min\{n \,.\, v_P(x_i) + i;\ 0 \leqslant i \leqslant n-1\}$ pelo argumento acima, temos que $v_P(x_i) \geqslant 0$, para todo $i = 0, \ldots, n-1$. A igualdade $d(P'|P) = v_{P'}(\varphi'(t))$ segue então do Teorema 4.5.4, o que conclui a demonstração. ■

4.6 EXTENSÕES POR CONSTANTES

Consideraremos nessa seção um corpo de funções F/K com corpo de constantes K, onde K é um corpo perfeito. Essa última hipótese é essencial para a validade da maioria dos resultados aqui apresentados. Recordemos que $\Phi \supseteq F$ denota um corpo algebricamente fechado fixo.

Seja K' uma extensão algébrica de K. O compósito $F' = FK'$ é um corpo de funções sobre K' e o seu corpo de constantes é dessa forma um extensão finita de K', pelo Corolário 3.1.23. Contudo, não é claro, a princípio, se K' é o corpo de constantes de FK'. Essa questão será melhor discutida na Proposição 4.6.2, cuja demonstração necessitará do lema a seguir.

Lema 4.6.1. *Suponhamos que $\alpha \in \Phi$ seja algébrico sobre K. Então*

$$[K(\alpha) : K] = [F(\alpha) : F].$$

Demonstração. Inicialmente, consideremos os polinômios $irr(\alpha, K)$ e $irr(\alpha, F)$. Como $irr(\alpha, K) \in F[T]$ e este anula α, temos que $irr(\alpha, F)|irr(\alpha, K)$, de modo

que $[F(\alpha) : F] \leqslant [K(\alpha) : K]$. Para mostrarmos a outra desigualdade, devemos mostrar que $irr(\alpha, K)$ é irredutível em $F[T]$. Suponhamos que o contrário seja verdade, isto é, que $irr(\alpha, K) = g(T) \, . \, h(T)$, onde $g(T)$, $h(T)$ são polinômios mônicos em $F[T]$ de grau $\geqslant 1$. Como cada raiz de $g(T)$, $h(T)$ em Φ é também uma raiz de $irr(\alpha, K)$, temos que cada uma dessas raízes é um elemento algébrico sobre K. Dessa forma, cada um dos coeficientes de $g(T)$, $h(T)$ são algébricos sobre K, pois estes são expressões polinomiais das raízes. Por outro lado, esses coeficientes são elementos de F e, como K é algebricamente fechado em F, temos que $g(T)$, $h(T) \in K[T]$, o que é uma contradição com o fato de $irr(\alpha, K)$ ser irredutível em $K[T]$. ■

Proposição 4.6.2. *Seja $F' = FK'$ uma extensão algébrica por constantes de F/K (de grau finito ou infinito). Então, temos que K' é o corpo de constantes de F'.*

Demonstração. Consideremos um elemento $\gamma \in F'$ que é algébrico sobre K'. Então γ é algébrico sobre K, pois K'/K é uma extensão algébrica, e existe um número finito de elementos $\alpha_1, \ldots, \alpha_r \in K'$ tais que $\gamma \in F(\alpha_1, \ldots, \alpha_r)$ (isso ocorre pela definição do compósito). Ainda a extensão $K(\alpha_1, \ldots, \alpha_r)/K$ é finita e separável, pois K'/K é uma extensão algébrica, de modo que podemos utilizar o Teorema 2.1.9 para garantir a finitude da extensão, e K é um corpo perfeito. Daí $K(\alpha_1, \ldots, \alpha_r) = K(\alpha)$ para algum $\alpha \in K'$, pelo Teorema 2.5.11. Como γ é um elemento algébrico sobre K, é possível encontrarmos $\beta \in F'$ algébrico sobre K tal que $K(\alpha, \gamma) = K(\beta)$ (aqui estamos empregando um argumento análogo ao utilizado anteriormente). Desse modo, temos que $F(\beta) = F(\alpha, \gamma) = F(\alpha)$, já que $\gamma \in F(\alpha_1, \ldots, \alpha_r) = F(\alpha)$. Ainda, pelo Lema 4.6.1, obtemos que

$$[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K].$$

Isso nos dá que $K(\alpha) = K(\beta)$, donde $\gamma \in K(\alpha) \subseteq K'$. ■

Teorema 4.6.3. *Seja $F' = FK'$ uma extensão por constantes algébrica de F/K. Então F'/F é não ramificada, isto é, $e(P'|P) = 1$, para todo $P \in \mathbb{P}_F$ e todo $P' \in \mathbb{P}_{F'}$ com $P'|P$.*

Demonstração. Suponhamos que $K' = K(\alpha)$ é uma extensão finita de K. Neste caso, $F' = F(\alpha)$ e o polinômio minimal $irr(\alpha, K) = \varphi(T)$ permanece irredutível em

$F[T]$, pelo Lema 4.6.1. Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$. O expoente diferente $d(P'|P)$ satisfaz $0 \leqslant d(P'|P) \leqslant v_{P'}(\varphi'(\alpha))$, pelo Teorema 4.5.4. Notemos que α é separável sobre K, pois estamos sob a hipótese de que K é um corpo perfeito, donde $\varphi'(\alpha) \neq 0$. Como $\varphi'(\alpha) \in K'$, temos que $v_{P'}(\varphi'(\alpha)) = 0$ e, desse modo, $d(P'|P) = v_{P'}(\varphi'(\alpha)) = 0$. Pelo Teorema da Diferente de Dedekind (Teorema 4.5.3), concluímos que $P'|P$ é não ramificado, isto é, $e(P'|P) = 1$, para todos $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$.

A partir de agora, suponhamos que K' seja uma extensão algébrica arbitrária de K. Seja $P' \in \mathbb{P}_{F'}$ uma extensão de P. Escolhamos $t \in F'$ um elemento primo para P'. Então existe um corpo intermediário $K \subseteq K_1 \subseteq K'$ tal que o grau de $[K_1 : K]$ é finito e $t \in F_1 = FK_1$. Seja $P_1 = P' \bigcap F_1$. Então $1 = v_{P'}(t) = e(P'|P_1)\,.\,v_{P_1}(t)$ e assim $e(P'|P_1) = 1$. Pelo caso inicial, mostramos que $e(P_1|P) = 1$, de modo que $e(P'|P) = e(P'|P_1)\,.\,e(P_1|P) = 1$, pela Proposição 4.1.7. ■

4.7 EXTENSÕES DE GALOIS

Definição 4.7.1. Uma extensão F'/K' de um corpo de funções F/K é dita uma extensão de Galois se F'/F é uma extensão de Galois finita.

Teorema 4.7.2. *Seja F'/K' uma extensão de Galois de F/K e sejam P_1, $P_2 \in \mathbb{P}_{F'}$ extensões de $P \in \mathbb{P}_F$. Então $P_2 = \sigma(P_1)$, para algum $\sigma \in Gal(F'/F)$.*

Demonstração. Suponhamos que $\sigma(P_1) \neq P_2$, para todo $\sigma \in G = Gal(F'/F)$. Pelo Teorema da Aproximação Fraca (Teorema 3.2.1), existe um elemento $z \in F'$ tal que $v_{P_2}(z) > 0$ e $v_Q(z) = 0$ para todo $Q \in \mathbb{P}_{F'}$ tal que Q é uma extensão de P e $Q \neq P_2$. Seja $N_{F'/F} : F' \to F$ a aplicação norma (ver Seção 2.7). Então obtemos

$$\begin{aligned} v_{P_1}(N_{F'/F}(z)) &= v_{P_1}\left(\prod_{\sigma \in G} \sigma(z)\right) \\ &= \sum_{\sigma \in G} v_{P_1}(\sigma(z)) \\ &= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) \text{ (\textit{pelo Lema} 4.5.1)} \\ &= \sum_{\sigma \in G} v_{\sigma(P_1)}(z) \\ &= 0, \end{aligned}$$

já que P_2 não pertence ao conjunto $\{\sigma(P_1);\ \sigma \in G\}$. Por outro lado,

$$v_{P_2}(N_{F'/F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0,$$

visto que $id \in G$. Mas, como $N_{F'/F}(z) \in F$, temos que

$$v_{P_1}(N_{F'/F}(z)) = 0 \Leftrightarrow v_P(N_{F'/F}(z)) = 0 \Leftrightarrow v_{P_2}(N_{F'/F}(z)) = 0,$$

donde obtemos uma contradição. ■

Corolário 4.7.3. *Consideremos a notação como no Teorema 4.7.2. Sejam $P_1, \ldots, P_r$ todas as extensões de P em $\mathbb{P}_{F'}$. Então:*

a) $e(P_i|P) = e(P_j|P)$ *e* $f(P_i|P) = f(P_j|P)$, *para todos* i, j. *Dessa forma, escreveremos*

$$e(P_i|P) = e(P) \text{ e } f(P_i|P) = f(P)$$

e chamaremos $e(P)$ o índice de ramificação de P em F'/F e $f(P)$ o grau relativo de P em F'/F.

b) $e(P) \,.\, f(P) \,.\, r = [F' : F]$. *Em particular, $e(P)$, $f(P)$ e r dividem o grau $[F' : F]$.*

c) $d(P_i|P) = d(P_j|P)$, *para todos* i, j.

Demonstração. *a*) Segue do Teorema 4.7.2 e do Lema 4.5.1.

b) Segue do Teorema 4.1.12 e da letra *a*).

c) Consideremos o fecho integral de $\mathcal{O}_P$ em F'

$$\mathcal{O'}_P = \bigcap_{i=1}^{r} \mathcal{O}_{P_i}$$

e o módulo complementar

$$\mathcal{C}_P = \{z \in F';\ Tr_{F'/F}(z \,.\, \mathcal{O'}_P) \subseteq \mathcal{O}_P\}.$$

Dado $\sigma \in Gal(F'/F)$, temos que $\sigma(\mathcal{O'}_P) = \mathcal{O'}_P$ e $\sigma(\mathcal{C}_P) = \mathcal{C}_P$, onde a última igualdade segue do fato de $Tr_{F'/F}(\sigma(u)) = Tr_{F'/F}(u)$, para todo $u \in F'$. Escrevendo $\mathcal{C}_P = t \,.\, \mathcal{O'}_P$, obtemos $\sigma(t) \,.\, \mathcal{O'}_P = \sigma(\mathcal{C}_P) = \mathcal{C}_P = t \,.\, \mathcal{O'}_P$, de modo que

$$-d(P_i|P) = v_{P_i}(t) = v_{P_i}(\sigma(t)),$$

para todo $1 \leqslant i \leqslant r$, pela Proposição 4.4.2 e pela definição do expoente diferente. Consideremos agora dois lugares P_i e P_j extensões de P e escolhamos $\sigma \in Gal(F'/F)$ tal que $\sigma(P_j) = P_i$. Então $-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j|P)$, como queríamos mostrar. ■

Teorema 4.7.4 (Teorema de Hilbert)**.** *Sejam F/K uma extensão cíclica de grau n com grupo de Galois G, σ um gerador de G, $\beta \in F$, $N_{F/K}$ a norma de F em K e $Tr_{F/K}$ o traço de F em K. Então:*

a) $N_{F/K}(\beta) = 1$ se, e somente se, existe um elemento $0 \neq \alpha \in F$ tal que $\beta = (\sigma(\alpha))^{-1}\alpha$.

b) (Forma Aditiva) $Tr_{F/K}(\beta) = 0$ se, e somente se, existe um elemento $\alpha \in F$ tal que $\beta = \alpha - \sigma(\alpha)$.

Demonstração. *a*) Este resultado pode ser encontrado em [12] (Teorema 6.1, Cap. VI).

b) Este resultado pode ser encontrado em [12] (Teorema 6.3, Cap. VI). ■

Teorema 4.7.5 (Artin-Schreier)**.** *Seja K um corpo de característica $p > 0$.*

a) Seja F uma extensão cíclica de K de grau p. Então existe $\alpha \in F$ tal que $F = K(\alpha)$ e α satisfaz uma equação da forma $T^p - T - k = 0$, para algum $k \in K$.

b) Reciprocamente, dado $k \in K$, o polinômio $f(T) = T^p - T - k$ possui uma raiz em K, de modo que todas as suas raízes também estão em K, ou é irredutível. No último caso, dada uma raiz α de $f(T)$, temos que $K(\alpha)$ é uma extensão cíclica de K de grau p.

Demonstração. *a*) Seja F/K uma extensão cíclica de grau $p > 0$. Então $Tr_{F/K}(-1) = 0$, pois $Tr_{F/K}(-1) = p \,.\, (-1)$. Seja σ um gerador do grupo de Galois G. Pela forma aditiva do Teorema de Hilbert (Teorema 4.7.4 - b)), temos que existe um elemento $\alpha \in F$ tal que $\sigma(\alpha) - \alpha = 1$. Logo $\sigma^i(\alpha) = \alpha + i \,.\, 1$, para todo $i = 1, \ldots, p$, e assim

α possui p elementos conjugados distintos. Daí, $[K(\alpha) : K] \geqslant p$ e assim $K(\alpha) = F$. Notemos ainda que

$$\sigma(\alpha^p - \alpha) = (\sigma(\alpha))^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Logo $\alpha^p - \alpha$ é fixado por σ e assim é fixado por qualquer potência de σ. Isso nos dá que $\alpha^p - \alpha$ pertence ao corpo fixo de G, de modo que, chamando $k = \alpha^p - \alpha$, concluímos a demonstração.

b) Sejam $k \in K$ e α uma raiz de $f(T) = T^p - T - k$. Então $\alpha + i \,.\, 1$ é também uma raiz de $f(T)$, para todo $i = 1, \ldots p$, e, neste caso, $f(T)$ possui p raízes distintas. Se uma delas pertencer a K, então temos que todas as demais também pertencem. Agora, consideremos o caso em que $f(T)$ não possui raízes em K. Afirmamos que $f(T)$ é irredutível em $K[T]$. De fato, suponhamos $f(T) = g(T)h(T)$, com $g(T)$, $h(T) \in K[T]$ tais que $1 \leqslant deg(g(T))$, $deg(h(T)) < p$. Como $f(T) = \prod_{i=1}^{p}(T - \alpha - i \,.\, 1)$, temos que $g(T)$ é o produto sobre certos inteiros i. Seja $d = deg(g(T))$. Então o coeficiente de T^{d-1} em $g(T)$ é igual a soma de termos $-(\alpha + i \,.\, 1)$ para precisamente d inteiros i. Logo este coeficiente é da forma $-d\alpha + j \,.\, 1$, para algum inteiro j. Como $d \,.\, 1 \neq 0$ em K, temos que $-d\alpha + j \,.\, 1 \in K$ implica que $\alpha \in K$, o que é uma contradição. Isso mostra que $f(T)$ é irredutível. Como todas as raízes de $f(T)$ pertencem a $K(\alpha)$ e $f(T)$ não possui raízes múltiplas, temos que $K(\alpha)/K$ é uma extensão normal e separável. Logo $K(\alpha)$ é uma extensão de Galois sobre K. Isso nos dá que existe um automorfismo σ de $K(\alpha)$ sobre K tal que $\sigma(\alpha) = \alpha + 1$. Como as potências de σ são tais que $\sigma^i(\alpha) = \alpha + i \,.\, 1$, temos que $\sigma^i \neq \sigma^j$ se $i \neq j$. Portanto o grupo de Galois associado a $K(\alpha)/K$ é cíclico, fato que conclui a demonstração deste resultado. ■

Lema 4.7.6. *Seja F/K um corpo de funções de característica $p > 0$. Dados um elemento $u \in F$ e um lugar $P \in \mathbb{P}_F$, temos que:*

a) *Ou existe um elemento $z \in F$ tal que $v_P(u - (z^p - z)) \geqslant 0$.*

b) *Ou para algum $z \in F$, tem-se*

$$v_P(u - (z^p - z)) = -m < 0, \text{ com } m \not\equiv 0 \pmod{p}.$$

No último caso, o inteiro m é unicamente determinado por u e P, a saber

$$-m = max\{v_P(u - (w^p - w)); w \in F\}.$$

Demonstração. Comecemos a demonstração com a seguinte afirmação

Sejam x_1, $x_2 \in F\backslash\{0\}$ tais que $v_P(x_1) = v_P(x_2)$. Então existe $y \in F$ satisfazendo

$$v_P(y) = 0 \text{ e } v_P(x_1 - y^p x_2) > v_P(x_1).$$

De fato, como $v_P(x_1) = v_P(x_2)$, temos que $v_P(x_1/x_2) = 0$, donde $x_1/x_2 \in \mathcal{O}_P\backslash P$ e assim $(x_1/x_2)(P) \neq 0$ em $\mathcal{O}_P/P$. Daí, podemos escrever que $(x_1/x_2)(P) = y(P)^p$, para algum $y \in \mathcal{O}_P\backslash P$, onde aqui estamos utilizando a hipótese de que $\mathcal{O}_P/P$ é um corpo perfeito. Logo, $v_P(y) = 0$ e $v_P((x_1/x_2) - y^p) > 0$, de modo que

$$\begin{aligned} v_P(x_1 - y^p x_2) &= v_P(x_2((x_1/x_2) - y^p)) \\ &= v_P(x_2) + v_P((x_1/x_2) - y^p) \\ &= v_P(x_1) + v_P((x_1/x_2) - y^p) \\ &> v_P(x_1). \end{aligned}$$

Agora mostremos que

Se $v_P(u - (z_1^p - z_1)) = -lp < 0$, então existe um elemento $z_2 \in F$ com

$$v_P(u - (z_2^p - z_2)) > -lp.$$

Com efeito, escolhamos $t \in F$ tal que $v_P(t) = -l$. Então

$$v_P(u - (z_1^p - z_1)) = v_P(t^p).$$

Pela afirmação inicial, é possível encontrarmos $y \in F$ com $v_P(y) = 0$ e

$$v_P(u - (z_1^p - z_1) - (yt)^p) > -lp.$$

Como $v_P(yt) = v_P(t) = -l > -lp$, temos que

$$v_P(u - (z_1^p - z_1) - ((yt)^p - yt)) > -lp.$$

Definindo $z_2 = z_1 + yt$, temos que o resultado segue.

Agora, demonstremos o lema.

Se existir $z \in F$ tal que $v_P(u-(z^p-z)) \geqslant 0$, então $a)$ ocorre. Caso contrário, para todo $z \in F$, temos que $v_P(u-(z^p-z)) < 0$. Assim, fixemos $z \in F$. Se $v_P(u-(z^p-z)) = -m < 0$, onde $m \not\equiv 0 \pmod{p}$, então já vale a letra $b)$. Se, contudo, $v_P(u-(z^p-z)) = -lp < 0$, para algum $l > 0$, então, pela segunda afirmação, existe $z_1 \in F$ tal que $v_P(u-(z_1^p-z_1)) > -lp$. Se $v_P(u-(z_1^p-z_1)) = -m < 0$, onde $m \not\equiv 0 \pmod{p}$, então temos que o item $b)$ se cumpre. Caso contrário, procedemos como anteriormente e, como $v_P(u-(z^p-z)) < 0$, para todo $z \in F$, temos que em algum momento é possível obtermos um elemento como no item $b)$.

Resta-nos agora mostrar que se a letra $b)$ ocorre, então o inteiro m é unicamente determinado por u e P, a saber

$$-m = max\{v_P(u-(w^p-w)); w \in F\}.$$

Por hipótese, temos que existe $z \in F$ tal que $v_P(u-(z^p-z)) = -m < 0$, com $m \not\equiv 0 \pmod{p}$. Para todo $w \in F$, vale $p\,.\,v_P(w-z) \neq -m$, de modo que podemos considerar os seguintes casos:

1) $p\,.\,v_P(w-z) > -m$
   Neste caso temos que $v_P((w-z)^p) > -m$ e $v_P(w-z) > -m/p > -m$, donde pela Desigualdade Triangular $v_P((w-z)^p-(w-z)) > -m$. Assim, $v_P(u-(w^p-w)) = v_P(u-(z^p-z)-((w-z)^p-(w-z))) = -m$ pela Desigualdade Triangular Estrita (Lema 3.1.16).

2) $p\,.\,v_P(w-z) < -m$
   Neste caso obtemos

$$v_P(u-(w^p-w)) = v_P(u-(z^p-z)-((w-z)^p-(w-z))) < -m.$$

Como em qualquer um dos casos anteriores $v_P(u-(w^p-w)) \leqslant -m$, temos que o resultado segue. ■

Proposição 4.7.7 (Extensões de Artin-Schreier)**.** *Seja F/K um corpo de funções de característica $p > 0$. Suponhamos que $u \in F$ seja um elemento que satisfaça a seguinte condição*

$$u \neq w^p - w, \text{ para todo } w \in F.$$

Seja

$$F' = F(y), \text{ com } y^p - y = u.$$

A extensão F'/F é chamada uma extensão de Artin-Schreier de F. Para $P \in \mathbb{P}_F$ definimos o inteiro m_P por

$$m_P = \begin{cases} m, & \text{se existe } z \in F \text{ tal que } v_P(u - (z^p - z)) = -m < 0 \\ & \text{e } m \not\equiv 0 \pmod{p}. \\ -1, & \text{se } v_P(u - (z^p - z)) \geqslant 0 \text{ para algum } z \in F. \end{cases}$$

(Observemos que, pelo Lema 4.7.6, m_P está bem definido). Logo, temos que:

a) *F'/F é uma extensão de Galois cíclica de grau p. Os automorfismos de F'/F são dados por $\sigma(y) = y + \nu$, onde $\nu = 0, \ldots, p-1 \in \mathbb{F}_p$.*

b) *P é não ramificado em F'/F se, e somente se, $m_P = -1$.*

c) *P é totalmente ramificado em F'/F se, e somente se, $m_P > 0$. Neste caso, denotando por P' o único lugar de F' que é extensão de P, temos que $d(P'|P)$ é dado por*

$$d(P'|P) = (p-1)(m_P + 1).$$

d) *Se pelo menos um lugar $Q \in \mathbb{P}_F$ satisfaz $m_Q > 0$, então K é algebricamente fechado em F' e*

$$g' = p.g + \frac{p-1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1).deg(P)\right),$$

onde g' é o gênero de F'/K e g é o gênero de F/K.

Demonstração. *a*) Segue do Teorema 4.7.5.

b) e *c*) Suponhamos que $m_P = -1$, ou seja, que $v_P(u - (z^p - z)) \geqslant 0$ para algum $z \in F$. Sejam $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Então $F' = F(y_1)$ e $\varphi_1(T) = T^p - T - u_1$

é o polinômio minimal de y_1 sobre F. Como $v_P(u_1) \geqslant 0$, y_1 é integral sobre o anel de valorização $\mathcal{O}_P$ e o expoente diferente $d(P'|P)$ de uma extensão P' de P em F satisfaz

$$0 \leqslant d(P'|P) \leqslant v_{P'}(\varphi_1'(y_1)) = 0,$$

pelo Teorema 4.5.4, já que $\varphi_1'(T) = -1$. Logo $d(P'|P) = 0$ e $P'|P$ é não ramificada pelo Teorema da Diferente de Dedekind (Teorema 4.5.3).

Suponhamos agora que $m_P > 0$. Escolhamos $z \in F$ tal que $v_P(u-(z^p-z)) = -m_P$. Consideremos os elementos $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Como antes, temos que $F' = F(y_1)$ e que $\varphi_1(T) = T^p - T - u_1$ é o polinômio minimal de y_1 sobre F. Seja $P' \in \mathbb{P}_{F'}$ uma extensão de P em F'. Como $y_1^p - y_1 = u_1$, temos que:

$$v_{P'}(u_1) = e(P'|P)\,.\,v_P(u_1) = -m_P\,.\,e(P'|P)$$

e

$$v_{P'}(u_1) = v_{P'}(y_1^p - y_1) = p\,.\,v_{P'}(y_1),$$

onde a última igualdade segue da Desigualdade Triangular Estrita (Lema 3.1.16) e do fato de $v_{P'}(y_1) < 0$ (notemos que se o contrário ocorresse, teríamos que $v_{P'}(u_1) \geqslant 0$, fato que não ocorre uma vez que $v_{P'}(u_1) = -m_P < 0$). Como p e m_P são relativamente primos, temos que p divide $e(P'|P)$. Ainda $e(P'|P) \leqslant [F' : F] = p$, pelo Corolário 4.1.13, de modo que

$$e(P'|P) = p \text{ e } v_{P'}(y_1) = -m_P.$$

Em particular, isso nos mostra que P é totalmente ramificado em F'/F.

Seja $x \in F$ um elemento primo para P. Escolhamos inteiros i, $j \geqslant 0$ tais que $1 = ip - jm_P$ (notemos que isso é possível pois p e m_P são elementos primos entre si). Ainda, temos que $j \not\equiv 0 \pmod{p}$, pois caso contrário p seria invertível. Então, $t = x^i y_1^j$ é um elemento primo para P', uma vez que $v_{P'}(t) = i\,.\,v_{P'}(x) + j\,.\,v_{P'}(y_1) = i\,.\,e(P'|P)\,.\,v_P(x) - j\,.\,m_P = i\,.\,e(P'|P) - j\,.\,m_P = 1$. Pela Proposição 4.5.6, temos que o expoente diferente $d(P'|P)$ é dado por

$$d(P'|P) = v_{P'}(\psi'(t)),$$

onde $\psi(T) \in F[T]$ é o polinômio minimal de t sobre F. Seja $G = Gal(F'/F)$ o grupo de Galois da extensão F'/F. Então

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t) \,.\, h(T),$$

com $h(T) = \prod_{\sigma \neq id} (T - \sigma(t)) \in F'[T]$, pela Observação 4.7.8. Assim, $\psi'(T) = h(T) + (T - t) \,.\, h'(T)$ e $\psi'(t) = h(t)$. Concluímos dessa forma que

$$d(P'|P) = v_{P'} \left(\prod_{\sigma \neq id} (t - \sigma(t)) \right) = \sum_{\sigma \neq id} v_{P'}(t - \sigma(t)).$$

Cada $\sigma \in G \backslash \{id\}$ possui a forma $\sigma(y_1) = y_1 + \mu$ para algum $\mu \in \{1, \ldots, p-1\} \subseteq \mathbb{F}_p \subseteq K$, de modo que

$$t - \sigma(t) = x^i y_1^j - x^i (y_1 + \mu)^j = -x^i \,.\, \sum_{l=1}^{j} \binom{j}{l} y_1^{j-l} \mu^l.$$

Como $v_{P'}(y_1^{j-1}) < v_{P'}(y_1^{j-l})$ para $l \geqslant 2$, pela Desigualdade Triangular Estrita (Lema 3.1.16) temos que

$$v_{P'}(t - \sigma(t)) = v_{P'}(x^i) + v_{P'}((j\mu) y_1^{j-1})$$

$$= ip + (j-1) \,.\, (-m_P) = ip - jm_P + m_P = m_P + 1.$$

Portanto $d(P'|P) = (p-1)(m_P + 1)$.

d) Suponhamos agora que $m_Q > 0$ para pelo menos um lugar $Q \in \mathbb{P}_F$. Pela letra *c*), temos que Q é totalmente ramificado em F'/F. Escolhamos uma extensão Q' de Q em F' tal que $e(Q'|Q) = [F' : F] = p$. Suponhamos que $[K' : K] > 1$ e consideremos o corpo intermediário $F_1 = FK' \supsetneq F$ e o lugar $Q_1 = Q' \bigcap F_1$. Como $e(Q'|Q) = [F' : F] = p$ e $e(Q_1 : Q) = 1$ pelo Teorema 4.6.3, temos que $e(Q' : Q_1) = e(Q' : Q) = [F' : F]$ pela Proposição 4.1.7. Ainda, $e(Q' : Q_1) \leqslant [F' : F_1]$ pelo Corolário 4.1.13 e $[F' : F_1] \leqslant [F' : F]$, de modo que $[F' : F_1] \leqslant e(Q' : Q_1) \leqslant [F' : F_1]$, ou seja, $e(Q' : Q_1) = [F' : F_1]$. Logo, $[F_1 : F] = 1$, o que é uma contradição. Portanto, $[K' : K] = 1$.

Agora, pela Fórmula do Gênero de Hurwitz (Teorema 4.4.11), temos que

$$\begin{aligned}
2g'-2 &= [F':F](2g-2)+deg(Diff(F'/F)) \\
&= p(2g-2)+\sum_{P\in\mathbb{P}_F}\sum_{P'|P} d(P'|P)\,.\,deg(P') \\
&= p(2g-2)+\sum_{P\in\mathbb{P}_F}\sum_{P'|P}(p-1)(m_P+1)\,.\,deg(P') \\
&= p(2g-2)+(p-1)\sum_{P\in\mathbb{P}_F}\sum_{P'|P}(m_P+1)\,.\,\frac{e(P)}{e(P)}\,.\,deg(P') \\
&= p(2g-2)+(p-1)\sum_{P\in\mathbb{P}_F}\frac{m_P+1}{e(P)}\,.\,deg\left(\sum_{P'|P}e(P)P'\right) \\
&= p(2g-2)+(p-1)\sum_{P\in\mathbb{P}_F}\frac{m_P+1}{e(P)}\,.\,deg(Con_{F'/F}(P)) \\
&= p(2g-2)+(p-1)\sum_{\substack{P\in\mathbb{P}_F\\ m_P>0}}\frac{m_P+1}{e(P)}\,.\,deg(Con_{F'/F}(P)) \\
&= p(2g-2)+(p-1)\sum_{\substack{P\in\mathbb{P}_F\\ m_P>0}}\frac{m_P+1}{[F':F]}\,.\,deg(Con_{F'/F}(P)) \\
&= p(2g-2)+(p-1)\sum_{\substack{P\in\mathbb{P}_F\\ m_P>0}}(m_P+1)\,.\,deg(P),
\end{aligned}$$

onde a penúltima igualdade segue da letra c). Logo

$$\begin{aligned}
g' &= p.g+\frac{p-1}{2}\left(-2+\sum_{\substack{P\in\mathbb{P}_F\\ m_P>0}}(m_P+1)\,.\,deg(P)\right) \\
&= p.g+\frac{p-1}{2}\left(-2+\sum_{P\in\mathbb{P}_F}(m_P+1)\,.\,deg(P)\right).
\end{aligned}$$

■

Observação 4.7.8. Escrevamos $\psi(T)=a_0+a_1T+\ldots+a_nT^n$ e sejam $\alpha_1,\ldots,\alpha_n$ o conjunto de todas as raízes distintas de $\psi(T)$ em F'. Como $\psi(t)=0$, temos que $0=\sigma(0)=\sigma(\psi(t))=\sigma(a_0+a_1t+\ldots+a_nt^n)=a_0+a_1\sigma(t)+\ldots+a_n\sigma(t)^n$, para todo $\sigma\in G$, ou seja, $\sigma(t)$ é uma raiz de $\psi(T)$, para todo $\sigma\in G$. Isso nos dá que, para todo $\sigma\in G$, σ induz uma função do conjunto $\{\alpha_1,\ldots,\alpha_n\}$ nele mesmo. Como σ é

um automorfismo, temos que $\sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$ é injetor, donde, sendo $\{\alpha_1,\ldots,\alpha_n\}$ um conjunto finito, temos que $\sigma|_{\{\alpha_1,\ldots,\alpha_n\}}$ é uma bijeção. Daí é possível representarmos $\psi(T)$ como no Proposição 4.7.7.

Definição 4.7.9. Um polinômio da forma

$$a(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \ldots + a_1 T^p + a_0 T \in K[T],$$

onde $p = char(K) > 0$, é chamado um polinômio aditivo sobre K.

Proposição 4.7.10. *Consideremos um corpo de funções F/K com corpo de constantes K de característica $p > 0$, um polinômio separável aditivo $a(T) \in K[T]$ de grau p^n que possui todas as suas raízes em K e $u \in F$. Suponhamos que para cada $P \in \mathbb{P}_F$ existe um elemento $z \in F$ (dependendo de P) tal que*

$$v_P(u - a(z)) \geqslant 0$$

ou

$$v_P(u - a(z)) = -m, \text{ com } m > 0 \text{ e } m \not\equiv 0 \pmod{p}.$$

Definamos $m_P = -1$ se o primeiro caso acima ocorrer e $m_P = m$ se o segundo ocorrer. Então m_P está bem definido. Consideremos a extensão $F' = F(y)$ de F, onde y satisfaz a equação

$$a(y) = u.$$

Se existe pelo menos um lugar $Q \in \mathbb{P}_F$ com $m_Q > 0$, então:

a) F'/F é uma extensão de Galois, $[F' : F] = p^n$ e o grupo de Galois de F'/F é isomorfo ao grupo aditivo $\{\alpha \in K;\, a(\alpha) = 0\}$ e assim isomorfo à $(\mathbb{Z}_p)^n$. Um tal grupo é dito ser um grupo abeliano elementar de expoente p, donde F'/F é dita uma extensão abeliana elementar de expoente p e grau p^n.

b) K é algebricamente fechado em F'.

c) Cada $P \in \mathbb{P}_F$ com $m_P = -1$ é não ramificado em F'/F.

d) Cada $P \in \mathbb{P}_F$ com $m_P > 0$ é totalmente ramificado em F'/F e o expoente diferente $d(P'|P)$ da extensão P' de P em F' é

$$d(P'|P) = (p^n - 1)(m_P + 1).$$

e) Sejam g e g' os gêneros de F e F', respectivamente. Então

$$g' = p^n \,.\, g + \frac{p^n - 1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \,.\, deg(P)\right).$$

Demonstração. A demonstração desse resultado pode ser feita, de forma geral, como na Proposição 4.7.7. ■

5 CORPOS DE FUNÇÕES COM UM NÚMERO PRESCRITO DE LUGARES DE GRAU SUPERIOR

5.1 PRELIMINARES

Nesta seção trabalharemos com corpos de funções sobre $\mathbb{F}_q$ tais que o corpo de constantes seja $\mathbb{F}_q$. Ainda, para um corpo de funções $F/\mathbb{F}_q$ denotemos por:

$p = char(\mathbb{F}_q)$ a característica do corpo $\mathbb{F}_q$,

$g(F)$ o gênero de F,

$N(F)$ o número de lugares racionais de F sobre $\mathbb{F}_q$,

$B_r(F)$ o número de lugares de grau r de F sobre $\mathbb{F}_q$.

Consideremos ainda os seguintes conjuntos

$\mathcal{M}_q = \{(N,\, g);$ existe um corpo de funções $F/\mathbb{F}_q$ tal que $g(F) = g$ e $N(F) = N\}$ e

$\mathcal{M}_q(g) = \{N \in \mathbb{N};$ existe um corpo de funções $F/\mathbb{F}_q$ tal que $g(F) = g$ e $N(F) = N\}$.

Os resultados a seguir serão importantes para o desenvolvimento das próximas seções.

Lema 5.1.1. *Sejam $F/\mathbb{F}_q$ um corpo de funções sobre $\mathbb{F}_q$ e $z \in F$ um elemento com divisor de polos dado por $(z)_\infty = P_1 + \ldots + P_n$, onde os lugares P_i são dois a dois distintos. Seja $E = F(y)$, onde o elemento y satisfaz a equação*

$$y^{p^r} - y = z,\ com\ r \geqslant 1.$$

Então:

a) A extensão E/F é uma extensão de Galois e possui grau $[E : F] = p^r$.

b) Os lugares $P_1, \ldots, P_n$ são totalmente ramificados e todos os demais lugares de F são não ramificados em E.

c) *Denotando por $\tilde{P}_i$ a extensão do lugar P_i em E, temos que $d(\tilde{P}_i|P_i) = 2(p^r-1)$, para todo $i = 1, \ldots, n$. Logo, o grau da diferente de E/F é*

$$deg(Diff(E/F)) = 2(p^r - 1)\sum_{i=1}^{n} deg(P_i).$$

Demonstração. A demonstração deste resultado segue da Proposição 4.7.10. ■

Apresentaremos a seguir o enunciado de um resultado fundamental para a teoria dos corpos de funções sobre corpos finitos: o Teorema de Hasse-Weil. Esse resultado é equivalente a determinar o valor absoluto das raízes da função zeta de um corpo de funções $F/\mathbb{F}_q$, o que é a célebre Hipótese de Riemann nesse cenário. Além disso, sabe-se que para corpos de funções $F/\mathbb{F}_q$ com gênero $g \leqslant (q - \sqrt{q})/2$, a cota apresentada nesse teorema é, em geral, a melhor possível. Para maior apronfudamento sobre o assunto, sugerimos as referências [9] (Seção 9.2) e [16] (Seção 5.2).

Teorema 5.1.2 (Hasse-Weil)**.** *O número $N = N(F)$ de lugares de $F/\mathbb{F}_q$ de grau 1 satisfaz a desigualdade*

$$|N - (q + 1)| \leqslant 2g\sqrt{q},$$

onde $g = g(F)$.

Demonstração. A demonstração deste teorema pode ser encontrada em [16] (Teorema 5.2.3). ■

Notemos que, com o Teorema de Hasse-Weil, temos que

$$\mathcal{M}_q(g) \subseteq [-2g\sqrt{q} + (q + 1),\ 2g\sqrt{q} + (q + 1)].$$

Lema 5.1.3. *Sejam F um corpo de funções sobre $\mathbb{F}_q$ de gênero $g(F) \geqslant 2$ e r um inteiro tal que $r > 2g(F)$. Então existe um lugar $P \in \mathbb{P}_F$ de grau r.*

Demonstração. Este resultado pode ser encontrado em [5] (Lema 2.1). ■

5.2 DEMONSTRAÇÃO DO TEOREMA 1.1.2

Lema 5.2.1. *Dado um corpo de funções $E/\mathbb{F}_q$ de gênero $g(E) \geqslant 2$, seja N um inteiro com $0 \leqslant N \leqslant N(E)$ e escrevamos $N(E) = N + s$. Denotemos por $P_1, \ldots, P_N, Q_1, \ldots, Q_s$ os distintos lugares racionais de E e sejam r um inteiro com $r \geqslant 2g(E) + 1 + s$ e $\alpha \in \mathbb{F}_q$. Então existe um elemento $x \in E$ e um lugar $P \in \mathbb{P}_F$ com as seguintes propriedades:*

a) $deg(P) = r$.

b) *x possui polos simples em $P, P_1, \ldots, P_N$ e x não possui outros polos.*

c) $x(Q_i) = \alpha$, *para todo* $i = 1, \ldots, s$.

Demonstração. Aplicando o Lema 5.1.3, é possível escolhermos um lugar $P \in \mathbb{P}_E$ de grau r, visto que $g(E) \geqslant 2$ e $r \geqslant 2g(E) + 1 + s \geqslant 2g(E) + 1 > 2g(E)$.

Seja $A = P - \sum_{i=1}^{s} Q_i$. Então

$$\begin{aligned} deg(A) &= deg(P) - \sum_{i=1}^{s} deg(Q_i) \\ &= r - s \\ &= 2g(E) + 1 \\ &> 2g(E) - 1 \end{aligned}$$

de modo que, pelo Teorema 3.4.21,

$$\begin{aligned} \ell(A) &= deg(A) + 1 - g(E) \\ &\geqslant 2g(E) + 1 + 1 - g(E) \\ &= g(E) + 2 \\ &> 0, \end{aligned}$$

donde existe $0 \neq u \in \mathcal{L}(A)$. Percebamos que, como todo elemento em E transcendente sobre $\mathbb{F}_q$ possui pelo menos um polo pelo Corolário 3.1.27, $v_Q(u) \geqslant 0$, para todo $Q \in \mathbb{P}_E \backslash \{P, Q_1, \ldots, Q_s\}$, $v_{Q_i}(u) \geqslant 1$, para todo $i = 1, \ldots, s$, e $v_P(u) \geqslant -1$,

temos que $v_P(u) = -1$.

Chamando $A_j = P + P_j - \sum_{i=1}^{s} Q_i$, para $j = 1, \ldots, N$, temos que $A \leqslant A_j$, de modo que $\mathcal{L}(A) \subseteq \mathcal{L}(A_j)$. Ainda, a última inclusão é estrita. Com efeito, como

$$deg(A_j) = deg(A) + deg(P_j) = deg(A) + 1 > deg(A) > 2g(E) - 1,$$

pelo Teorema 3.4.21 segue que

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

Logo, existe $x_j \in \mathcal{L}(A_j)\backslash\mathcal{L}(A)$, para todo $j = 1, \ldots, N$. Notemos que, neste caso,

$$v_Q(x_j) \begin{cases} \geqslant -1, & \text{se } Q = P \\ = -1, & \text{se } Q = P_j \text{ (pois } x_j \notin \mathcal{L}(A)) \\ \geqslant 1, & \text{se } Q = Q_i, \text{ para algum } i = 1, \ldots, s \\ \geqslant 0, & \text{se } Q \in \mathbb{P}_E\backslash\{P, P_j, Q_1, \ldots, Q_s\}. \end{cases}$$

Seja agora $w = \sum_{j=1}^{N} x_j$. Então, pela Desigualdade Triangular, temos que

$$v_Q(w) \begin{cases} \geqslant -1, & \text{se } Q = P \\ = -1, & \text{se } Q = P_j, \text{ para algum } j = 1, \ldots, N \text{ (pelo Lema 3.1.16)} \\ \geqslant 1, & \text{se } Q = Q_i, \text{ para algum } i = 1, \ldots, s \\ \geqslant 0, & \text{se } Q \in \mathbb{P}_E\backslash\{P, P_1, \ldots, P_N, Q_1, \ldots, Q_s\}. \end{cases}$$

Podemos perceber pelas relações anteriores que $P_1, \ldots, P_N$ são polos simples de w e $Q_1, \ldots, Q_s$ são zeros de w. Definamos agora

$$\tilde{x} = \begin{cases} w, & \text{se } P \text{ é um polo de } w \\ w + u, & \text{caso contrário} \end{cases}$$

e escrevamos $x = \tilde{x} + \alpha$. Então x é o elemento que procuramos. De fato

1) Se P é um polo de w, isto é, $v_P(w) < 0$, então pela Desigualdade Triangular e pela Desigualdade Triangular Estrita (Lema 3.1.16), temos que $v_Q(x) =$

$v_Q(\tilde{x}+\alpha) = v_Q(w+\alpha) \geqslant min\{v_Q(w),\, v_Q(\alpha)\} = min\{v_Q(w),\, 0\}$, valendo a igualdade se $v_Q(w) \neq v_Q(\alpha)$. Assim

$$v_Q(x) \begin{cases} = -1, & \text{se } Q = P \text{ (pois } -1 \leqslant v_P(w) < 0) \\ = -1, & \text{se } Q = P_j, \text{ para algum } j = 1, \ldots, N \\ = 0, & \text{se } Q = Q_i, \text{ para algum } i = 1, \ldots, s \\ \geqslant 0, & \text{se } Q \in \mathbb{P}_E \backslash \{P, P_1, \ldots, P_N, Q_1, \ldots, Q_s\}, \end{cases}$$

de modo que $x(Q_i) = w(Q_i) + \alpha(Q_i) = \alpha(Q_i) = \alpha$, para todo $i = 1, \ldots, s$, pois $w \in Q_i \Rightarrow w(Q_i) = 0$, e x possui polos simples em $P, P_1, \ldots, P_N$, sendo estes seus únicos polos.

2) Se P não é um polo de w, isto é, $v_P(w) \geqslant 0$, então pela Desigualdade Triangular, temos que $v_Q(x) = v_Q(\tilde{x}+\alpha) = v_Q(w+u+\alpha) \geqslant min\{v_Q(w),\, v_Q(u),\, v_Q(\alpha)\}$ $= min\{v_Q(w),\, v_Q(u),\, 0\}$. Ainda, pela Desigualdade Triangular Estrita (Lema 3.1.16), temos, por exemplo, que $v_Q(x) = min\{v_Q(u),\, v_Q(w+\alpha)\}$, se $v_Q(u) \neq v_Q(w+\alpha)$. Assim, recordando que $v_P(u) = -1$ e $v_Q(u) \geqslant 0$, para todo $Q \in \mathbb{P}_E \backslash \{P\}$, temos que

$$v_Q(x) \begin{cases} = v_P(u + (w+\alpha)) = -1, & \text{se } Q = P \text{ (pelo Lema 3.1.16)} \\ = v_Q(w + (u+\alpha)) = -1, & \text{se } Q = P_j, \text{ para algum } j = 1, \ldots, N \\ \geqslant 0, & \text{se } Q = Q_i, \text{ para algum } i = 1, \ldots, s \\ \geqslant 0, & \text{se } Q \in \mathbb{P}_E \backslash \{P, P_1, \ldots, P_N, Q_1, \ldots, Q_s\}, \end{cases}$$

de modo que $x(Q_i) = w(Q_i) + u(Q_i) + \alpha(Q_i) = \alpha(Q_i) = \alpha$, para todo $i = 1, \ldots, s$, pois $w,\, u \in Q_i \Rightarrow w(Q_i) = u(Q_i) = 0$, e x possui polos simples em $P, P_1, \ldots, P_N$, sendo estes seus únicos polos.

■

Proposição 5.2.2. *Sejam $E/\mathbb{F}_q$ um corpo de funções de gênero $h = g(E) \geqslant 2$ e N um inteiro com $0 \leqslant N \leqslant N(E)$. Suponhamos que g seja um inteiro satisfazendo as seguintes condições:*

a) $g \equiv h \pmod{p-1}$ *e*

b) $g \geqslant (3p-2)h + (p-1)N(E)$.

Então $(N,\, g) \in \mathcal{M}_q$.

Demonstração. Denotemos por $P_1, \ldots, P_N$, $Q_1, \ldots, Q_s$ todos os lugares racionais de E, onde $s = N(E) - N$. Escolhamos $\alpha \in \mathbb{F}_q \backslash Im(\wp)$, onde $\wp$ é o mapa de Artin-Schreier de $\mathbb{F}_q$ em $\mathbb{F}_q$ dado por $\beta \mapsto \beta^p - \beta$ (a existência desse elemento α será explicada na Observação 5.2.3). Podemos escrever

$$g = (3p-2)h + (p-1)N(E) + j(p-1),$$

com $j \geqslant 0$. De fato, $g \geqslant (3p-2)h + (p-1)N(E)$ implica que

$$g = (3p-2)h + (p-1)N(E) + l,$$

para algum inteiro $l \geqslant 0$. Como $g \equiv h \pmod{p-1}$ e

$$g - h = 3(p-1)h + (p-1)N(E) + l,$$

temos que $(p-1)$ divide l, donde $l = j(p-1)$, para algum $j \geqslant 0$. Pelo Lema 5.2.1, existem $x \in E$ e um lugar $P \in \mathbb{P}_E$ de grau $2h + 1 + s + j$ tal que $(x)_\infty = P + P_1 + \ldots + P_N$ e $x(Q_i) = \alpha$, para todo $i = 1, \ldots, s$. Definamos $F = E(y)$, onde $y^p - y = x$. Notemos que $y \notin E$. Com efeito, se $y \in E$, então $v_{Q_i}(y) \geqslant 0$, pois $y^p - y = x$ e $x \in \mathcal{O}_{Q_i}$. Como $1 = deg(Q_i) = [\mathcal{O}_{Q_i}/Q_i : \mathbb{F}_q]$, temos que $\mathcal{O}_{Q_i}/Q_i = \mathbb{F}_q$, de modo que $y(Q_i)^P - y(Q_i) = x(Q_i) = \alpha$, com $y(Q_i) \in \mathbb{F}_q$, o que nos daria uma contradição. Ainda, pelo Lema 5.1.1, a extensão F/E é uma extensão de Galois de grau $[F : E] = p$, e possui as seguintes propriedades:

1) Os lugares $P_1, \ldots, P_N$ e P são totalmente ramificados e todos os outros lugares de E são não ramificados em F/E.

2) O expoente diferente dos lugares $P_1, \ldots, P_N$ e P em F/E é $d = 2(p-1)$.

3) Os lugares $Q_1, \ldots, Q_s$ são inertes em F/E, isto é, não possuem extensões racionais em F/E.

Os itens 1) e 2) seguem do Lema 5.1.1. Já o item 3) segue das considerações a seguir: como o polinômio $T^p - T - x$ não possui raízes em E, pelo Teorema 4.7.5 temos que este é o polinômio minimal de y. Ainda, $T^p - T - x(Q_i) = T^p - T - \alpha$ não possui raízes em $\mathbb{F}_q = \mathcal{O}_{Q_i}/Q_i$, de modo que todos os seus fatores irredutíveis possuem grau maior ou igual a 2. Assim, temos que, para todo $i = 1, \ldots, s$, qualquer extensão de Q_i possui grau estritamente maior que 1, pois se $Q|Q_i$, então

$$\begin{aligned} deg(Q) &= [\mathcal{O}_Q/Q : \mathbb{F}_q] = [\mathcal{O}_Q/Q : \mathcal{O}_{Q_i}/Q_i] \,.\, [\mathcal{O}_{Q_i}/Q_i : \mathbb{F}_q] \\ &= [\mathcal{O}_Q/Q : \mathcal{O}_{Q_i}/Q_i] \,.\, deg(Q_i) = [\mathcal{O}_Q/Q : \mathcal{O}_{Q_i}/Q_i] \\ &= j(Q|Q_i) \geqslant 2, \end{aligned}$$

onde última desigualdade segue do Teorema de Kummer (Teorema 4.3.7).

De 1) e 3), temos que $N(F) = N$ e obtemos, pela Fórmula do Gênero de Hurwitz (Teorema 4.4.11) e pelo Lema 5.1.1, que

$$\begin{aligned} 2g(F) - 2 &= p(2h-2) + deg(Diff(F/E)) \\ &= p(2h-2) + 2(p-1)\left(deg(P) + \sum_{i=1}^{N} deg(P_i)\right) \\ &= p(2h-2) + 2(p-1)((2h+1+s+j) + N). \end{aligned}$$

Logo

$$g(F) - 1 = p(h-1) + (p-1)((2h+1+s+j) + N)$$

e

$$\begin{aligned} g(F) &= 1 + p(h-1) + (p-1)((2h+1+s+j) + N) \\ &= 1 + ph - p + 2ph + p + ps + pj + pN - 2h - 1 - s - j - N \\ &= (3p-2)h + (p-1)s + (p-1)N + (p-1)j \\ &= (3p-2)h + (p-1)(s+N) + (p-1)j \\ &= (3p-2)h + (p-1)N(E) + (p-1)j \\ &= g, \end{aligned}$$

como queríamos demonstrar. ■

Observação 5.2.3. Escrevamos $q = p^m$. Então:

a) $\mathbb{F}_q/\mathbb{F}_p$ é uma extensão de Galois. Em particular, $\mathbb{F}_q/\mathbb{F}_p$ é uma extensão separável.

Com efeito, $\mathbb{F}_{p^n}$ é o corpo de decomposição de $x^{p^n} - x$ sobre $\mathbb{F}_p$ e esse é um polinômio separável pelo Teorema 2.14 da referência [13]. Portanto, o resultado segue pelo Teorema 2.6.4.

b) (Teorema 90 de Hilbert) $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$ se, e somente se, existe $\beta \in \mathbb{F}_q$ tal que $\beta^p - \beta = \alpha$.

As afirmações anteriores nos garantem, pela Proposição 2.7.3 (f), que existe $\alpha \in \mathbb{F}_q$ tal que $\alpha \neq \beta^p - \beta$, para todo $\beta \in \mathbb{F}_q$.

Estamos agora em posição de demonstrar o Teorema 1.1.2.

Teorema 1.1.2. Para toda potência q de um número primo, existem constantes a_q, $b_q > 0$ tais que

$$\{(N,\, g);\, g \geqslant a_q \,.\, N + b_q\} \subseteq \mathcal{M}_q.$$

Demonstração do Teorema 1.1.2. Definamos a_q, b_q por

$$a_q = \gamma_q^{-1}(3p - 2 + 2(p-1)\sqrt{q})$$

e

$$b_q = (p-1)(q + 2(p-1)\sqrt{q} + 3p - 1),$$

onde γ_q é a constante introduzida no Teorema 1.1.1. Dados N, g com

$$g \geqslant a_q \,.\, N + b_q,$$

temos que construir um corpo de funções $F/\mathbb{F}_q$ tal que $g(F) = g$ e $N(F) = N$. Seja h o único inteiro tal que $g \equiv h \pmod{p-1}$ e

$$\frac{N}{\gamma_q} \leqslant h < \frac{N}{\gamma_q} + (p-1).$$

Então $N \leqslant \gamma_q \,.\, h$ e pelo Teorema 1.1.1 podemos encontrar um corpo de funções $E/\mathbb{F}_q$ de gênero $g(E) = h$ com $N(E) \geqslant \gamma_q \,.\, h \geqslant N$. Ainda

$$\begin{aligned}
g &\geqslant a_q \,.\, N + b_q \\
&= (\gamma_q^{-1}(3p - 2 + 2(p-1)\sqrt{q})) \,.\, N + (p-1)(q + 2(p-1)\sqrt{q} + 3p - 1) \\
&= \gamma_q^{-1} \,.\, N \,.\, (3p - 2 + 2(p-1)\sqrt{q}) + (p-1)(q + 2(p-1)\sqrt{q} + 3p - 1) \\
&> (h - (p-1)) \,.\, (3p - 2 + 2(p-1)\sqrt{q}) + (p-1)(q + 2(p-1)\sqrt{q} + 3p - 1) \\
&= (h - (p-1)) \,.\, (3p - 2 + 2(p-1)\sqrt{q}) + (p-1)(3p - 2 + 2(p-1)\sqrt{q} + q + 1) \\
&= h \,.\, (3p - 2 + 2(p-1)\sqrt{q}) + (p-1)(q+1) \\
&= h \,.\, (3p-2) + (p-1)(2\sqrt{q} + q + 1) \\
&\geqslant h \,.\, (3p-2) + (p-1)N(E),
\end{aligned}$$

onde a última desigualdade segue do Teorema 5.1.2. Agora, pela Proposição 5.2.2, temos que existe um corpo de funções F sobre $\mathbb{F}_q$ com $N(F) = N$ e $g(F) = g$. Isso conclui a demonstração do Teorema 1.1.2.

Definição 5.2.4. Definimos a constante de Ihara $A(q) = \limsup_{g \to \infty} N_q(g)/g$.

Como uma consequência da cota de Drinfel'd-Vlâdut (DRINFEL'D e VLÂDUT, 1983)

$$A(q) \leqslant \sqrt{q} - 1$$

e do Teorema 1.1.2, temos o resultado a seguir.

Corolário 5.2.5. *Existe uma constante $\epsilon > 0$ (dependendo somente de q) tal que para g suficientemente grande*

$$[0,\, \epsilon_q \,.\, g] \cap \mathbb{N} \subseteq \mathcal{M}_q(g) \subseteq [0,\, \sqrt{q} \,.\, g] \cap \mathbb{N}.$$

As constantes a_q e b_q introduzidas no Teorema 1.1.2 podem ser melhoradas em alguns casos. Sem o intuito de aprofundarmos nessa questão, apresentaremos aqui apenas alguns comentários acerca desse assunto.

No artigo de ANBAR e STICHTENOTH (2013), os autores estudam o caso em que q é um quadrado, baseados na torre sobre $\mathbb{F}_q$ apresentada por GARCIA e STICHTENOTH (1995).

Ainda, no mesmo artigo, é abordado o caso no qual $q = 2$. Neste, temos, por exemplo, que o corpo de funções $F = \mathbb{F}_2(x, y)$, com $y^2 + y = x^{2g}(x + 1) + 1$ e $g \geqslant 1$, possui gênero g e apenas 1 lugar racional. Porém, tomando a_2 e b_2 como no Teorema 1.1.2 e $N = 1$, vemos que a cota de g para garantir que $(1,\, g) \in \mathcal{M}_2$ é estritamente maior que 1. Um caso análogo ocorre para o corpo de funções sobre $\mathbb{F}_2$ descrito por $y^2 + y = x^{2g-1} + 1/(x + 1)$, o qual possui gênero g e apenas 2 lugares racionais.

Por último, utilizando a torre de corpos de funções $\mathcal{F} = (F_0,\, F_1, \ldots)$ sobre $\mathbb{F}_2$ apresentada por DUURSMA e MAK (2013), para a qual temos $g(F_0) = 0$, $g(F_1) = 2$ e, para todo $n \geqslant 0$, $N(F_n) = 3 \,.\, 2^n$ e $g(F_n) \leqslant \gamma \,.\, N(F_n)$, com $\gamma = 3.1546\ldots$, podemos melhorar as constantes do Teorema 1.1.2 como segue.

Sejam dados N, g inteiros não negativos satisfazendo $N \geqslant 3$ e $g \geqslant (8\gamma+2)N$ (notemos que essa cota para g é melhor que a obtida no Teorema 1.1.2). Escolhamos i tal que

$$3 \,.\, 2^i \leqslant N \leqslant 3 \,.\, 2^{i+1}$$

e seja $E = F_{i+1}$. Temos então que $g(E) \geqslant 2$ e $N \leqslant N(E)$. Dessa forma, obtemos

$$\begin{aligned}(3p - 2)\, g(E) + (p - 1)\, N(E) &= 4g(E) + N(E) \\ &\leqslant (4\gamma + 1)\, N(E) \\ &\leqslant (4\gamma + 1) \,.\, 2N \\ &\leqslant g.\end{aligned}$$

Pela Proposição 5.2.2, segue que $(N,\, g) \in \mathcal{M}_2$, o que significa que, para todos (N, g) tais que $N \geqslant 3$ e $g \geqslant 27.237\, N$, existe um corpo de funções $F/\mathbb{F}_2$ com gênero g e exatamente N lugares racionais.

5.3 CORPOS DE FUNÇÕES COM UM NÚMERO PRESCRITO DE LUGARES DE GRAU SUPERIOR

Nesta seção, faremos a demonstração do Teorema 1.1.4. Para isso, necessitaremos de três lemas, que serão apresentados na sequência. Recordemos ainda que $B_r(F)$ denota o número de lugares de grau r do corpo de funções $F/\mathbb{F}_q$, notando que $B_1(F) = N(F)$.

Lema 5.3.1. *Para todo $h \in \{0, \ldots, q-2\}$ e para todo $c > 0$ existe um corpo de funções $F/\mathbb{F}_q$ tal que $g(F) \equiv h \pmod{q-1}$ e $B_1(F) \geqslant c$.*

Demonstração. Fixemos $h \in \{0, \ldots, q-2\}$ e $c > 0$, e consideremos $N \geqslant c > 0$. Pelo Teorema 1.1.2, temos que existem constantes a_q, $b_q > 0$ tais que para cada $g \geqslant a_q \,.\, N + b_q$ existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) = g$ e $B_1(F) = N(F) = N \geqslant c$. Em particular, considerando $g \geqslant a_q \,.\, N + b_q$ tal que $g \equiv h \pmod{q-1}$, o que é sempre possível, temos o resultado desejado. ■

Lema 5.3.2. *Para todo $h \in \{0, \ldots, q-2\}$ e para toda $m-$upla $(c_1, \ldots, c_m) \in \mathbb{N}^m$ existe um corpo de funções $F/\mathbb{F}_q$ tal que $g(F) \equiv h \pmod{q-1}$ e $B_r(F) \geqslant c_r$, para todo $r = 1, \ldots, m$.*

Demonstração. Façamos a demonstração deste resultado por indução. O caso $m = 1$ está estabelecido pelo Lema 5.3.1. Suponhamos agora que o lema seja válido para $m - 1 \geqslant 1$. Seja $(c_1, \ldots, c_m) \in \mathbb{N}^m$. Se $c_i = 0$, para todo $i = 1, \ldots, m$, então qualquer corpo de funções $F/\mathbb{F}_q$ com gênero $g \equiv h \pmod{q-1}$ satisfaz as condições do enunciado. Agora, suponhamos que pelo menos um c_i seja positivo e seja $c = max\{c_1, \ldots, c_m\}$. Pela hipótese de indução, existe um corpo de funções $E/\mathbb{F}_q$ com $g(E) \equiv h \pmod{q-1}$ e $B_i(E) \geqslant c$, para todo $i = 1, \ldots, m-1$. Seja

$$S = \{P \in \mathbb{P}_E;\, deg(P) \leqslant m-1\}.$$

Notemos que S é um conjunto finito pela Observação 5.3.3. Escolhamos ainda $Q \in \mathbb{P}_E$ com grau suficientemente grande e $x \in \mathcal{L}\left(Q - \sum_{P \in S} P\right)$. Consideremos agora uma extensão F/E definida pela equação

$$y^{q^m} - y = x.$$

Pelo Lema 5.1.1 e pela Fórmula do Gênero de Hurwitz (Teorema 4.4.11) temos que $g(F) \equiv g(E) \pmod{q-1}$. Com efeito, escrevendo $q = p^k$ e notando que $(x)_\infty = Q$ por uma justificativa análoga à apresentada na demonstração do Lema 5.2.1, obtemos

$$\begin{aligned} 2g(F) - 2 &= p^{km}(2g(E) - 2) + deg(Diff(F/E)) \\ &= p^{km}(2g(E) - 2) + 2(p^{km} - 1)deg(Q) \end{aligned}$$

donde

$$g(F) - 1 \;=\; p^{km}(g(E) - 1) + (p^{km} - 1)deg(Q)$$

e assim

$$\begin{aligned} g(F) - g(E) &= 1 - g(E) + p^{km}(g(E) - 1) + (p^{km} - 1)deg(Q) \\ &= (p^{km} - 1)(g(E) - 1) + (p^{km} - 1)deg(Q). \end{aligned}$$

Como $k|km$, temos que $(p^k - 1)|(p^{km} - 1)$, ou seja, $(q - 1)|(p^{km} - 1)$. Assim $(q - 1)|(g(F) - g(E))$, como queríamos mostrar.

Além disso, todo lugar $P \in S$ é um zero de x em E, de modo que o polinômio $T^{q^m} - T - x(P) = T^{q^m} - T$ pertence a $\mathbb{F}_q[T] \subseteq (\mathcal{O}_P/P)[T]$, para todo $P \in S$, e este fatora-se em polinômios irredutíveis distintos sobre $\mathbb{F}_q$. Recordando que $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ e que todos os elementos de $\mathbb{F}_{q^m}$ são raízes do polinômio $T^{q^m} - T$, vemos que este último possui fatores irredutíveis de grau 1 sobre $\mathbb{F}_q$. Pelo Teorema de Kummer (Teorema 4.3.7), temos que existem lugares $R \in \mathbb{P}_F$ que estão acima de P com grau relativo $f(R/P) = 1$, donde $deg(R) = deg(P)$. Isso mostra que $B_j(F) \geqslant B_j(E) \geqslant c \geqslant c_j$, para todo $j = 1, \ldots, m - 1$. Sabendo que um polinômio irredutível $f(T) \in \mathbb{F}_q$ de grau n divide $T^{q^m} - T \in \mathbb{F}_q$ se, e somente se, $n|m$, pelo Lema 2.13 da referência [13], e que, para todo $n \in \mathbb{N}$, existe um polinômio irredutível de grau n, temos que $T^{q^m} - T$ possui um fator irredutível de grau m em $\mathbb{F}_q$. Isso nos dá, pelo Teorema de Kummer, que, para cada lugar $P \in S$ de grau 1, caso em que $\mathbb{F}_q = \mathcal{O}_P/P$, existe uma extensão $R \in \mathbb{P}_F$ de P tal que $deg(R) = j(R|P)deg(P) = m \,.\, 1 = m$. Dessa forma, $B_m(F) \geqslant B_1(E) \geqslant c \geqslant c_m$, o que conclui a demonstração do lema. ■

Observação 5.3.3. Na demonstração do Lema 5.3.2, utilizamos o seguinte resultado que pode ser encontrado em [16] (Lema 5.1.1):

Para todo $n \geqslant 0$ existe somente um número finito de divisores positivos de grau n.

Lema 5.3.4. *Para todo $h \in \{0, \ldots, q-2\}$ e para toda $m-$upla $(c_1, \ldots, c_m) \in \mathbb{N}^m$, existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) \equiv h \pmod{q-1}$ e $B_r(F) = c_r$, para todo $r = 1, \ldots, m$.*

Demonstração. Fixemos $h \in \{0, \ldots, q-2\}$ e $(c_1, \ldots, c_m) \in \mathbb{N}^m$. Pelo Lema 5.3.2 existe um corpo de funções $F_0/\mathbb{F}_q$ com $g(F_0) \equiv h \pmod{q-1}$ e $B_j(F_0) \geqslant c_j$, para todo $j = 1, \ldots, m$.

Escolhamos um conjunto $S_1 \subseteq \mathbb{P}_{F_0}$ constituído por c_1 lugares de grau 1, c_2 lugares de grau 2, $\ldots$, c_m lugares de grau m e definamos

$$S_2 = \{R \in \mathbb{P}_{F_0};\, deg(R) \leqslant m \text{ e } R \notin S_1\}.$$

Para cada $R \in S_2$, escolhamos um elemento $a_R \in \mathcal{O}_R/R$ tal que a equação

$$T^q - T = a_R$$

não possua solução em $\mathcal{O}_R/R$. Isso é possível pois a transformação $\mathbb{F}_q-$linear $\alpha \mapsto \alpha^q - \alpha$ de $\mathcal{O}_R/R$ em $\mathcal{O}_R/R$ possui núcleo não trivial, a saber $\mathbb{F}_q$, de modo que não é sobrejetora pelo Teorema do Núcleo e da Imagem.

Escolhamos um lugar $Q \in \mathbb{P}_{F_0}$ de grau $deg(Q) > m$ e tal que $deg\left(Q - \sum_{R \in S_2} R\right) \geqslant 2g(F_0)$. Ainda, escolhamos para cada $P \in S_1$ um elemento primo $t_P \in F_0$ para P. Então, definindo a transformação $\mathbb{F}_q-$linear como a seguir

$$\begin{array}{rccl} \psi: & \mathcal{L}\left(Q + \sum_{P \in S_1} P\right) & \to & \bigoplus_{P \in S_1} \mathcal{O}_P/P \oplus \bigoplus_{R \in S_2} \mathcal{O}_R/R \\ & u & \mapsto & ((t_P \,.\, u \pmod P)_{P \in S_1}, (u \pmod R)_{R \in S_2}) \end{array}$$

temos que o núcleo de ψ é o espaço $\mathcal{L}\left(Q - \sum_{R \in S_2} R\right)$. Logo, o posto de ψ é

$$\begin{aligned} \text{Posto}\,(\psi) &= \ell\left(Q + \sum_{P \in S_1} P\right) - \ell\left(Q - \sum_{R \in S_2} R\right) \\ &= deg\left(Q + \sum_{P \in S_1} P\right) - deg\left(Q - \sum_{R \in S_2} R\right) \\ &= \sum_{P \in S_1} deg(P) + \sum_{R \in S_2} deg(R) \end{aligned}$$

pelo Teorema 3.4.21, pois $deg\left(Q + \sum_{P \in S_1} P\right) \geqslant deg\left(Q - \sum_{R \in S_2} R\right) \geqslant 2g(F_0)$. Assim, temos que ψ é sobrejetora, de modo que existe $x_1 \in \mathcal{L}\left(Q + \sum_{P \in S_1} P\right)$ tal que

x_1 possui polos simples em todos os lugares $P \in S_1$ e $x_1 \pmod R = a_R$, para todo $R \in S_2$.

Se Q também for um polo de x_1, definamos $x = x_1$. Caso contrário, definamos $x = x_1 + z$, para algum $0 \neq z \in Ker(\psi) = \mathcal{L}\left(Q - \sum_{R \in S_2} R\right)$. Assim, temos as seguintes situações possíveis:

1) Q é um polo de x_1
   Neste caso, temos que $x = x_1$ e assim $v_A(x) = v_A(x_1)$, para todo $A \in \mathbb{P}_{F_0}$, de modo que
   $$v_A(x) = \begin{cases} -1, & \text{se } A \in S_1 \\ -1, & \text{se } A = Q \end{cases}$$
   isto é, x possui polos simples em Q e em todos os lugares $P \in S_1$. Além disso, $x(R) = x_1(R) = a_R$, para todo $R \in S_2$.

2) Q não é um polo de x_1
   Neste caso, $x = x_1 + z$ e assim $v_A(x) = v_A(x_1 + z) \geqslant min\{v_A(x_1), v_A(z)\}$, valendo a igualdade se $v_A(x_1) \neq v_A(z)$ (Lema 3.1.16). Como $v_P(x_1) = -1$ e $v_P(z) \geqslant 0$, para todo $P \in S_1$, temos que $v_P(x_1) \neq v_P(z)$, donde $v_P(x) = -1$. Ainda, Q deve ser o único polo de z, donde $v_Q(z) = -1$, e por hipótese Q não é um polo de x_1, o que nos dá $v_Q(x_1) \geqslant 0$ e assim $v_Q(x) = -1$. Em resumo, temos que
   $$v_A(x) = \begin{cases} -1, & \text{se } A \in S_1 \\ -1, & \text{se } A = Q. \end{cases}$$
   Por último, $x(R) = x_1(R) + z(R) = x_1(R) = a_R$, para todo $R \in S_2$, pois $v_R(z) \geqslant 1$, para todo $R \in S_2$.

Na extensão $F_1 = F_0(y)$, com $y^q - y = x$, notemos que $y \notin F_0$, uma vez que $a_R \in \mathcal{O}_R/R$ é tal que a equação $T^q - T = a_R$ não possui solução em $\mathcal{O}_R/R$ e $v_R(y) \geqslant 0$, para todo $R \in S_2$. Ainda, pelo Lema 5.1.1, temos que todos os lugares $P \in S_1$ são totalmente ramificados em F_1/F_0, de modo que obtemos c_j lugares de grau j em F_1, para todo $j = 1, \ldots, m$ (a explicação para esse fato segue do Teorema de Kummer por um argumento análogo ao utilizado no Lema 5.3.2). Ainda, para todo lugar $R_1 \in \mathbb{P}_{F_1}$ que seja extensão de um lugar $R \in S_2$, o grau

de R_1 é estritamente maior que o grau de R. Isso segue também do Teorema de Kummer, notando-se que, como $T^q - T = a_R$ não possui solução em $\mathcal{O}_R/R$, este polinômio fatora-se em polinômios irredutíveis de grau maior ou igual a dois em $\mathcal{O}_R/R$, o que nos dá que $f(R_1|R) \geqslant 2$. Todos os demais lugares de F_1 possuem grau estritamente maior que m. Podem ainda existir lugares de F_1 que são extensão de lugares em S_2 com grau menor ou igual a m. Contudo, repetindo a construção anterior, obtemos, após um número finito de passos, um corpo de funções $F \supseteq F_0$ com $g(F) \equiv h \pmod{q-1}$ e $B_j(F) = c_j$, para todo $j = 1, \ldots, m$. ■

Agora, temos todos os resultados necessários para poder demonstrar o Teorema 1.1.4.

Teorema 1.1.4. Sejam $\mathbb{F}_q$ um corpo finito e $b_1, \ldots, b_m$ inteiros não negativos. Então existe um inteiro $g_0 \geqslant 0$ com a seguinte propriedade: para todo $g \geqslant g_0$ existe um corpo de funções $F/\mathbb{F}_q$ com gênero g tal que $F/\mathbb{F}_q$ possui exatamente b_r lugares de grau r, para $r = 1, \ldots, m$.

Demonstração do Teorema 1.1.4. Mostremos que para todo $h \in \{0, \ldots, q-2\}$ existe um inteiro positivo $g^{(h)} \equiv h \pmod{q-1}$ com a seguinte propriedade: para todo inteiro $g \geqslant g^{(h)}$ com $g \equiv g^{(h)} \pmod{q-1}$, existe um corpo de funções $F/\mathbb{F}_q$ de gênero g e com exatamente b_j lugares de grau j, para todo $j = 1, \ldots, m$. Com isso demonstramos o teorema, pois, considerando $g_0 = max\{g^{(h)};\ h = 0, \ldots, q-2\}$, temos que, para todo $g \geqslant g_0$, $g \equiv h \pmod{q-1}$ para algum $h \in \{0, \ldots, q-2\}$ e $g \geqslant g^{(h)}$, donde existe um corpo de funções $F/\mathbb{F}_q$ com gênero g e exatamente b_j lugares de grau j.

Fixemos $h \in \{0, \ldots, q-2\}$ e seja F_0 um corpo de funções sobre $\mathbb{F}_q$ de gênero $g(F_0) \equiv h \pmod{q-1}$ e com $B_j(F_0) = b_j$, para todo $j = 1, \ldots, m$. Notemos que isso é possível pelo Lema 5.3.4. Para cada inteiro $r \geqslant 2g(F_0) + 1$ existe, pelo Lema 5.1.3, um lugar $Q \in \mathbb{P}_{F_0}$ com $deg(Q) = r$. Sejam

$$S = \{P \in \mathbb{P}_{F_0};\ deg(P) \leqslant m\} \text{ e } D = \sum_{P \in S} P$$

e definamos

$$g^{(h)} = g(F_0) + (q-1)(deg(D) + 3g(F_0)).$$

Então $g^{(h)} \equiv h \pmod{q-1}$, para isto bastando notar que $q-1$ divide $g^{(h)} - g(F_0)$. Queremos agora construir para cada $g = g^{(h)} + (q-1)r_1$, com $r_1 \geqslant 0$, um corpo de funções $F/\mathbb{F}_q$ de gênero g, com $B_j(F) = b_j$, para todo $j = 1, \ldots, m$.

Escolhamos um lugar $Q \in \mathbb{P}_{F_0}$ de grau $r = 2g(F_0) + 1 + r_1$. Para todo $P \in S$, temos que

$$\begin{aligned} deg(Q+P) &= deg(Q) + deg(P) \\ &\geqslant deg(Q) + 1 \\ &> deg(Q) \\ &= 2g(F_0) + 1 + r_1 \\ &> 2g(F_0) - 1, \end{aligned}$$

donde, pelo Teorema 3.4.21,

$$\begin{aligned} \ell(Q+P) &= deg(Q+P) + 1 - g(F_0) = deg(Q) + deg(P) + 1 - g(F_0) \\ &\geqslant 1 + deg(Q) + 1 - g(F_0) \\ &> \ell(Q) = deg(Q) + 1 - g(F_0) = 2g(F_0) + 1 + r_1 + 1 - g(F_0) \\ &= g(F_0) + 2 + r_1 \\ &> 1. \end{aligned}$$

Escolhamos $x_P \in \mathcal{L}(P+Q) \backslash \mathcal{L}(Q)$ e definamos $x_1 = \sum_{P \in S} x_P$. Então todos os lugares $P \in S$ são polos simples de x_1. Se Q também for um polo de x_1, definimos $x = x_1$. Caso contrário, definamos $x = x_1 + z$, para algum $0 \neq z \in \mathcal{L}(Q) \backslash \mathbb{F}_q$. Em qualquer um dos casos, x possui polos simples em Q e em todos os lugares $P \in S$, e estes são os seus únicos polos por um argumento análogo ao apresentado nos Lemas 5.2.1 e 5.3.2.

Seja $F = F_0(y)$, com $y^q - y = x$. Então todos os lugares $P \in S$ são totalmente ramificados em F/F_0, pelo Lema 5.1.1, donde $B_j(F) = B_j(F_0) = b_j$, para todo $j = 1, \ldots, m$. Ainda, o gênero de F pode ser calculado pela Fórmula do Gênero de Hurwitz (Teorema 4.4.11) como segue

$$\begin{aligned} 2g(F) - 2 &= q(2g(F_0) - 2) + deg(Diff(F/F_0)) \\ &= q(2g(F_0) - 2) + 2(q-1)(deg(D) + deg(Q)) \end{aligned}$$

donde

$$g(F) - 1 \;=\; q(g(F_0) - 1) + (q-1)(deg(D) + deg(Q))$$

e

$$\begin{aligned} g(F) &= q(g(F_0) - 1) + (q-1)(deg(D) + deg(Q)) + 1 \\ &= g(F_0) - g(F_0) + qg(F_0) - q + (q-1)deg(D) \\ &+ (q-1)(2g(F_0) + 1 + r_1) + 1 \\ &= g(F_0) + (q-1)deg(D) + (q-1)(3g(F_0) + r_1) \\ &= g(F_0) + (q-1)(deg(D) + 3g(F_0) + r_1) \\ &= g^{(h)} + (q-1)r_1. \end{aligned}$$

Isso conclui a demonstração do Teorema 1.1.4.

REFERÊNCIAS

[1] ANBAR, N.; STICHTENOTH, H. Curves of every genus with a prescribed number of rational points. *Bulletin of the Brazilian Mathematical Society, New Series*, v. 44, n. 2, p. 173-193, 2013.

[2] BEACHY, J. A.; BLAIR, W. D. *Abstract Algebra*. 3. ed. Long Grove: Waveland Press, 2006.

[3] DRINFEL'D, V. G.; VLÂDUT, S. G. Number of points of an algebraic curve. *Functional Analysis and Its Applications*, v. 17, n. 1, p. 53-54, 1983.

[4] DUURSMA, I.; MAK, K. -H. On lower bounds for the Ihara constants A(2) and A(3). *Compositio Mathematica*, v. 149, n.7, p. 1108-1128, 2013.

[5] ELKIES, N. D. *et al*. Curves of every genus with many points, II: Asymptotically good families. *Duke Mathematical Journal*, v. 122, n. 2, p. 399-422, 2004.

[6] GARCIA, A. L. P.; LEQUAIN, Y. A. E. *Elementos de álgebra*. 6. ed. Rio de Janeiro: IMPA, 2012.

[7] GARCIA, A. L. P.; STICHTENOTH, H. A tower of Artin-Schreier extensions of function fields attaining the Drinfel'd-Vlâdut bound. *Inventiones Mathematicae*, v. 121, n. 1, p. 211-222, 1995.

[8] GONÇALVES, A. *Introdução à Álgebra*. 5. ed. Rio de Janeiro: IMPA, 2011.

[9] HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. *Algebraic Curves over a Finite Field*. 1. ed. Princeton: Princeton University Press, 2008.

[10] HUCZYNSKA, S.; NEUNHÖFFER, M. *Finite Fields*. Disponível em `http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf`. Acesso em: 29 jan. 2015.

[11] HUNGERFORD, T. W. *Algebra*. New York: Springer-Verlag, 1974.

[12] LANG, S. *Algebra*. 3. ed. New York: Springer-Verlag, 2002.

[13] LIDL, R.; NIEDERREITER, H. *Introduction to Finite Fields and their Applications*. Cambridge: Cambridge University Press, 1986.

[14] NIEDERREITER, H. *et al*. A new construction of algebraic-geometry codes. *Applicable Algebra in Engineering, Communication and Computing*, v. 9, n. 5, p. 373-381, 1999.

[15] STEWART, I. *Galois Theory*. 1. ed. London: Chapman and Hall, 1973.

[16] STICHTENOTH, H. *Algebraic Function Fields and Codes*. 2. ed. New York: Springer-Verlag, 2009.

[17] STICHTENOTH, H. Curves with a prescribed number of rational points. *Finite Fields and Their Applications*, v. 17, n. 6, p. 552–559, 2011.