Curvas algébricas sobre corpos finitos

Steve da Silva Vicentim

Curvas algébricas sobre corpo finitos

Steve da Silva Vicentim

Orientador: **Prof. Dr. Herivelto Martins Borges Filho**

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências - Matemática . *VERSÃO REVISADA*

USP – São Carlos
Maio de 2012

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

da Silva Vicentim, Steve
d633c Curvas algébricas sobre corpos finitos / Steve da Silva Vicentim; orientador Herivelto Martins Borges Filho. -- São Carlos, 2012.
136 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2012.

1. ÁLGEBRA ABSTRATA. 2. CURVAS ALGÉBRICAS. I. Borges Filho, Herivelto Martins, orient. II. Título.

"Keep walking."

Johnnie Walker.

Agradecimentos

Primeiramente a minha mãe, que mesmo passando por uma série de momentos difíceis, sempre se mostrou forte e esteve ao meu lado, simplesmente sendo minha mãe e me apoiando.

Ao Professor Dr. Herivelto Martins Borges Filho, pela orientação, auxílio, confiança e paciência.

Aos professores da pós-graduação do ICMC-USP, por tudo o que me ensinaram.

Às garotas da secretaria da pós-graduação.

Aos colegas de mestrado, pelo apoio, amizade e boas lembranças.

Aos velhos e novos amigos de Araraquara e São Carlos, por toda a atenção, amizade e suporte emocional.

À minha família, em especial à minha prima Thamy e à nossa avó Lurdes.

À CAPES pelo suporte financeiro.

Muito obrigado.

Resumo

A Teoria das curvas algébricas sobre corpos finitos é de fundamental importância para a matemática e tem aplicações essenciais em muitas áreas, tais como Geometria Finita, Teoria dos Números, Teoria de Grafos e Teoria de Códigos.

Neste trabalho tratamos do segmento algébrico desta teoria, isto é, corpos de funções algébricas, inicialmente sobre qualquer corpo, apresentando propriedades fundamentais. Depois nos restringimos aos corpos de funções algébricas sobre corpos finitos, e são apresentados resultados referentes à estimativa do gênero e número de lugares racionais, além de propriedades que conectam estes dois números e a característica do corpo, sendo o principal resultado dado por: "Para q uma potência de um número primo e N inteiro não negativo, existe uma constante inteira não negativa g_0 (dependendo de q e N) tal que, para todo g maior ou igual a g_0, existe um corpo de funções sobre $\mathbb{F}_q$ de gênero g tendo exatamente N lugares racionais."

Palavras-chave: Curvas algébricas, Corpos de funções algébricas, Lugares racionais, Gênero.

Abstract

The Theory of algebraic curves over finite fields is of fundamental importance to mathematics and has essential applications in many areas, such Finite Geometry, Number Theory, Graph Theory and Coding Theory.

In this work we treat the algebraic part of this theory, ie, algebraic function fields, initially over any field, presenting fundamental properties. Then we restrict to algebraic function fields over finite fields, and presented results for the estimation of the genus and the number of racional places, as well as properties that connect these two numbers and the characteristic of the constant field, being the main result given by: "For q a prime power and N a non-negative integer, there is an integer non-negative g_0 (that depends of q and N) such that for all $g \geq g_0$, there exists a function field over $\mathbb{F}_q$ with genus g having exactly N racional places."

Key words: Algebraic curves, Algebraic function fields, Racional places, Genus.

Sumário

Introdução

A teoria das curvas algébricas sobre corpos finitos é de grande importância em várias áreas da matemática. Exemplo deste fato está na teoria de códigos, área esta onde Goppa (1981) mostrou em [3] como construir códigos a partir de curvas algébricas sobre $\mathbb{F}_q$, os chamados códigos AG ou códigos de Goppa:

Dados n lugares racionais distintos $P_1, ..., P_n$ de um corpo de funções $F/\mathbb{F}_q$ e um divisor G de F com suporte disjunto de $\{P_1, ..., P_n\}$, o código de Goppa $C_{\mathcal{L}}(D, G) \subseteq \mathbb{F}_q^n$ é definido por

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

onde $D = P_1 + ... + P_n$ e $\mathcal{L}(G)$ é o espaço de Riemann-Roch associado a G.

Ao considerarmos um corpo de funções F sobre um corpo finito $\mathbb{F}_q$, temos determinados os valores de seu gênero $g(F)$ e de seu número de lugares racionais $\mathrm{N}(F)$. Assim é natural perguntar quais são as relações entre q, $g(F)$ e $\mathrm{N}(F)$. E um dos principais resultados perante esta questão é a cota de Hasse-Weil [8]:

$$|\mathrm{N}(F) - (q+1)| \leq 2g(F)\sqrt{q},$$

mais tarde refinada para a cota de Serre:

$$|\mathrm{N}(F) - (q+1)| \leq g(F)\,\lfloor 2\sqrt{q} \rfloor .$$

Mas isso gera outras questões: Para determinados inteiros não negativos g e N, e

uma potência de primo q, existe um corpo de funções F sobre $\mathbb{F}_q$ tal que $g(F) = g$ e $\mathrm{N}(F) = N$? Quais são as condições necessárias para se garantir tal existência?

Uma forma de se pensar a respeito destas questões é fixar dois destes números e refletir quanto ao terceiro, o que equivale a estudar os seguintes conjuntos:

$$\mathcal{N}(q,g) := \{N;\ \text{existe um corpo de funções } F \text{ sobre } \mathbb{F}_q \text{ tal que } g(F) = g \text{ e } \mathrm{N}(F) = N\},$$

$$\mathcal{Q}(N,g) := \{q;\ \text{existe um corpo de funções } F \text{ sobre } \mathbb{F}_q \text{ tal que } g(F) = g \text{ e } \mathrm{N}(F) = N\},$$

$$\mathcal{G}(q,g) := \{g;\ \text{existe um corpo de funções } F \text{ sobre } \mathbb{F}_q \text{ tal que } g(F) = g \text{ e } \mathrm{N}(F) = N\}.$$

Das cotas de Serre e Hasse-Weil segue:

$$\mathcal{N}(q,g) \subseteq \left[q + 1 - g\left\lfloor 2\sqrt{q}\right\rfloor, q + 1 + g\left\lfloor 2\sqrt{q}\right\rfloor\right],$$

$$\mathcal{Q}(N,g) \subseteq \left[N + 2g^2 - 1 - 2g\sqrt{g^2+N-1}, N + 2g^2 - 1 + 2g\sqrt{g^2+N-1}\right].$$

Mas e quanto ao conjunto $\mathcal{G}(q,N)$? O que podemos dizer a seu respeito?

O objetivo deste trabalho é tratar desta última questão.

No Capítulo 1 vamos desde a definição de um corpo de funções algébricas sobre um corpo dado, apresentamos uma série de propriedades fundamentais e resultados importantes, como o Teorema de Riemann-Roch.

No Capítulo 2 tratamos de extensões de corpos de funções e o seus respectivos gêneros (Fórmula do gênero de Hurwitz). Vemos também como se corporta a ramificação dos lugares nestas extensões em algumas situações, resultando no Teorema de Kummer e extensões de Artin-Schreier.

Já no Capítulo 3, tratamos de corpos de funções sobre $\mathbb{F}_q$ com um número prescrito de lugares racionais, discorrendo sobre o conjunto $\mathcal{G}(q,N)$ e apresentando como principal resultado o fato dele não ser limitado, diferente de $\mathcal{N}(q,g)$ e $\mathcal{Q}(N,g)$.

Este trabalho foi baseado nas referências [8] e [9].

Capítulo

1

Fundamentos da teoria de corpos de funções algébricas

1.1 Lugares

Definição 1.1.1. Um corpo de funções algébricas F/K de uma variável sobre K é uma extensão de corpos $F \supset K$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.
Por simplicidade, chamaremos F/K de corpo de funções.

O conjunto $\tilde{K} = \{z \in F; z \text{ é algébrico sobre } K\}$ é um subcorpo de F, pois a soma, produto e inverso de elementos algébricos são também algébricos. $\tilde{K}$ é chamado corpo de constantes de F/K.

Assim, temos $K \subseteq \tilde{K} \subset F$; além disso $F/\tilde{K}$ é um corpo de funções sobre $\tilde{K}$. De fato: $K \subseteq \tilde{K} \Rightarrow K(x) \subseteq \tilde{K}(x) \subset F \Rightarrow [F : \tilde{K}(x)][\tilde{K}(x) : K(x)] = [F : K(x)] = n \in \mathbb{N}$ (finito) $\Rightarrow [F : \tilde{K}(x)] \leq n$.

Dizemos que K é algebricamente fechado sobre F se $\tilde{K} = K$, isto é, quando K é todo corpo de funções constantes de F.

Observação 1.1.2. Os elementos de F que são transcendentes sobre K podem ser caracterizados como: $z \in F$ é transcendente sobre K se, e somente se,

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

De fato:

($\Leftarrow$) se $[F : K(z)] < \infty \Rightarrow [K(z) : K] = \infty \Rightarrow z$ não é algébrico ($[K(z) : K] < \infty \Leftrightarrow z$ algébrico).

($\Rightarrow$) se z é transcendente, então $trdegK(z)/K = 1$, mas temos $trdegK(x)/K = 1$ e $[F : K(x)] < \infty$, donte temos $[K(x, z) : K(x)] < \infty$, logo extensão algébrica. Assim $trdegK(x, z)/K(x) = 0$, e pelo carácter somativo do grau de transcendência temos $trdegK(x, z)/K = 1$, implicando que $trdegK(x, z)/K(z) = 0$ e portanto temos x algébrico sobre $K(z)$, destarte finita. Logo, $[F : K(z)] < \infty$.

Exemplo 1.1.3. O corpo de funções racionais.

F/K é dito o corpo de funções racionais se $F = K(x)$ para algum $x \in F$ transcendente sobre K. Todo elemento $z \in K(x)$ não nulo tem uma única representação da forma:

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

em que a é não nulo, $p_i(x) \in K[x]$ são mônicos, todos distintos e irredutíveis e $n_i \in \mathbb{Z}$.

Para tal observe:

$$K(x) = \left\{ \tfrac{f(x)}{g(x)}; f(x), g(x) \in K[x] \text{ e } g(x) \neq 0 \right\}$$
$$\Rightarrow z = \tfrac{f(x)}{g(x)}, \text{ onde } f(x), g(x) \in K[x] \text{ e } g(x) \neq 0$$

Veja que $K[x]$ não é corpo, pois se o fosse, teríamos $K(x) = K[x] \Leftrightarrow x$ algébrico. Gerando uma contradição.

Assim, faz sentido considerar elementos irredutíveis em $K[x]$.

Logo temos:

$$f(x) = \alpha.p_{f1}(x)^{n_{f1}} \dots p_{fp}(x)^{n_{fp}}$$
$$g(x) = \beta.p_{g1}(x)^{n_{g1}} \dots p_{gq}(x)^{n_{gq}}$$

onde $\alpha, \beta \in K^*$ e $p_{fi}(x)$ e p_{gi} são polinômios mônicos irredutíveis dois a dois distintos e os expoentes de todos são naturais.

$$\Rightarrow z = \tfrac{f(x)}{g(x)} = a \textstyle\prod_i p_i(x)^{n_i}.$$

Um corpo de funções arbitrário é frequentemente representado como uma extensão algébrica simples de uma corpo de funções racionais $K(x)$, isto é, $F = K(x, y)$ onde $\varphi(y) = 0$ para algum $\varphi(T) \in K(x)[T]$ irredutível.

Veremos decomposições de elementos de um corpo de funções qualquer similar a que fizemos acima. Mas para tal, serão introduzidos os conceitos de aneis de valorização e lugares do corpo de funções. Além dos conceitos de zeros e pólos dos elementos de um corpo de funções racionais.

Definição 1.1.4. Um anel de valorização do corpo de funções F/K é um anel $O \subset F$ que satisfaz as seguintes propriedades:

1. $K \subsetneq O \subsetneq F$;

2. $\forall z \in F, z \in O$ ou $z^{-1} \in O$.

Tal definição motiva a construção do seguinte conjunto em $F = K(x)$:

Seja $p(x) \in K[x]$ irredutível, defina:

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}.$$

Veja que $\frac{f(x)}{p(x)}$, onde $f(x), p(x)$ são elementos não nulos de $K[x]$, pertence a $K(x)$, mas tal elemento não pertence a $O_{p(x)}$ se $p(x)$ não divide $f(x)$. Além disso, seja $g(x) \in K[x]$ tal que $g(x)$ é irredutível e $mdc(p(x), g(x)) = 1$, então $\frac{1}{g(x)} \in O_{p(x)} \backslash K$.

Portanto, $K \subsetneq O_{p(x)} \subsetneq F$.

Seja $z = \frac{f(x)}{g(x)} \in F = K(x)$ não nulo, então se $z \notin O_{p(x)} \Rightarrow p(x) | g(x)$. E, como já podemos supor que $f(x)$ e $g(x)$ são relativamente primos, temos que $p(x)$ não divide $f(x)$; logo, $z^{-1} = \frac{g(x)}{f(x)} \in O_{p(x)}$.

Portanto, $O_{p(x)}$ é um anel de valorização de $K(x)$.

Note ainda que se $p(x)$ e $g(x)$ são polinômios irredutíveis de $K[x]$ distintos, temos $O_{p(x)} \neq O_{g(x)}$, pois $\frac{1}{g(x)} \in O_{p(x)}$ e $\frac{1}{g(x)} \notin O_{g(x)}$.

Proposição 1.1.5. *Seja O um anel de valorização do corpo de funções F/K. Então:*

1. *O tem um único ideal maximal $P = O \backslash O^*$, onde*

$$O^* = \{x \in O; \exists z \in O \text{ } onde \text{ } x.z = 1\};$$

2. *Para $x \in F$, não nulo, temos: $x \in P \Leftrightarrow x^{-1} \notin O$;*

3. *Para $\tilde{K}$ o corpo de constantes de F/K, temos $\tilde{K} \subseteq O$ e $\tilde{K} \cap P = \{0\}$.*

Demonstração. 1. Primeiro, seja $x \in P$ e $z \in O$, se $zx \in O^* \Rightarrow \exists w \in O$ onde $xzw = 1 \Rightarrow x(zw) = 1 \Rightarrow x \in O$.

Agora, sejam $x, y \in P$. Considere $\frac{x}{y} \in F$, então $\frac{x}{y} \in O$ ou $\frac{y}{x} \in O$.

Se $\frac{x}{y} \in O \Rightarrow 1 + \frac{x}{y} \in O \Rightarrow x + y = y(1 + \frac{x}{y}) \in P$. Se $\frac{y}{x} \in O$, é análogo.

Portanto, $x + y \in P$, donde temos que P é um ideal.

Mostremos agora que P é maximal.

Seja J um ideal onde $P \subsetneq J \subseteq O$. Tome $x \in J \backslash P$. Então $x \in O^*$, pois $P = O \backslash O^*$, assim $xx^{-1} \in J$, pois J é ideal. Logo $1 \in J \Rightarrow O \subset J \Rightarrow J = O$. Portanto P é maximal.

P é o único ideal maximal de O: Seja J ideal maximal de O. Se J não contém unidades de O, então $J \subseteq P \Rightarrow J = P$, pois J é maximal. Agora se J possui uma unidade, então $J = O$.

Portanto, P é o único ideal maximal próprio de O.

2. $x \in P \Leftrightarrow x \in O \backslash O^* \Leftrightarrow x \notin O^* x^{-1} \notin O$.

3. Seja $z \in \tilde{K}$:

Se $z = 0 \Rightarrow z \in O$, pois O é anel.

Se $z \neq 0$:

Suponha $z \notin O \underbrace{\Rightarrow}_{2} z^{-1} \in O$.

Como $\tilde{K}$ é corpo, então $z^{-1} \in \tilde{K} \Rightarrow \exists a_1, ..., a_r \in K$ onde $a_r(z^{-1})^r + ... + a_1 z^{-1} + 1 = 0$, pois $z^{-1} \Rightarrow p_{z^{-1}}(x) \neq x^n$.

Assim:

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

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

$$\Rightarrow -(a_r(z^{-1})^{r-1} + ... + a_1) = z \in K[z^{-1}] \subset O.$$

Logo $z \in O$, absurdo.

Portanto, temos $z \in O$, daí $\tilde{K} \subset O$.

Seja, novamente, $z \in \tilde{K}, z \neq 0$. Como $\tilde{K}$ é corpo, então $z^{-1} \in \tilde{K}$; donde temos $z \in O^*$, pois $\tilde{K} \subset O$.

Portanto $z \notin P$ e $\tilde{K} \cap P = \{0\}$.

□

Teorema 1.1.6. *Seja O um anel de valorização do corpo de funções F/K e P o único ideal maximal de O. Então:*

1. *P é ideal principal;*
2. *Se $P = tO$, então $\forall z \in F$ $(z \neq 0)$, existe uma única representação da forma $z = t^n u$, para algum $n \in \mathbb{Z}$ e $u \in O^*$;*
3. *O é um domínio de ideais principais. Mais que isso: se $P = tO$ e $\{0\} \neq I \subseteq O$ é um ideal, então $I = t^n O$, para algum $n \in \mathbb{Z}$.*

Para provar tal teorema precisamos do lema:

Lema 1.1.7. *Sejam O um anel de valorização de F/K, P o ideal maximal de O e $x \in P$, tal que $x \neq 0$. Sejam $x_1, ..., x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, ..., n-1$. Então $n \leq [F : K(x)] < \infty$.*

Demonstração. Pela Proposição 1.1.5, temos que $\tilde{K} \cap P = \{0\}$. Como $x \neq 0$, então $x \notin \tilde{K}$, logo x é transcendente sobre K. Assim pela observação 1.1.2, temos $[F : K(x)] < \infty$.

Logo, é suficiente mostrar que $\{x_1, ..., x_n\}$ é um conjunto l.i. em F sobre $K(x)$.

Suponha que $\{x_1, ..., x_n\}$ é l.d. sobre $K(x)$, então $\exists \varphi_i \in K(x), i = 1, .., n$, não todos nulos tais que:

$$\sum_{i=1}^{n} \varphi_i x_i = 0.$$

Como $\varphi_i \in K(x)$, então podemos supor $\varphi_i \in K[x]$ e tal que x não divide todos eles.

Tome $a_i := \varphi_i(0) \in K$ o termo constante de φ_i, e defina $j \in \{1, .., n\}$ tal que $a_j \neq 0$ mas $a_i = 0, \forall j < i$.

Assim:

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

com $\varphi_i \in O$ para $i = 1, .., n$ (pois $x \in P$), $x_i \in x_j P$ para $i < j$ e $\varphi_i = x g_i$ para $i > j$, onde g_i são polinômios em x.

Dividindo $(\star)$ por x_j, temos:

$$-\varphi_j = \sum_{i<j} \varphi_i \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i x_i. \ (\star\star)$$

Como $(\star\star) \in P$ então $\varphi_j \in P$. Além disso $\varphi_j = a_j + x g_j$, onde $g_j \in K[x] \subset O$ e $x \in P$, donde temos $a_j = \varphi_j - x g_j \in P$.

Assim $a_j \in P \cap K$ e $a_j \neq 0$, contrariando a Proposição 1.1.5 item 3.

□

Demonstração. (teorema)

1. Suponha que P não é principal e escolha $x_1 \in P$ não nulo. Como $P \neq x_1 O$, então existe $x_2 \in P \backslash x_1 O$. Então $x_2 x_1^{-1} \notin O$, pois $x_2 x_1^{-1} \in O \Rightarrow x_2 x_1^{-1} = o \Rightarrow x_2 = o x_1 \Rightarrow x_2 \in x_1 O$.

   Isso implica que $x_2^{-1} x_1 \in P$ (pela Proposição 1.1.5 item 2), donde temos $x_1 \in x_2 P$. Por indução temos então uma sequencia infinita $x_1, x_2, ... \in P$ tal que $x_i \in x_{i+1} P, \forall i \geq 1$, contrariando o Lema 1.1.7.

2. Seja $z \in F$ $(z \neq 0)$, como $z \in O$ ou $z^{-1} \in O$, então podemos supor que $z \in O$, pois caso contrário basta fazer o mesmo raciocínio para $z^{-1} \in O$.

   Se $z \in O^* \Rightarrow z = t^0 z$.

   Se $z \notin O^* \Rightarrow z \in P$.

   Como $z \in P = tO$, então $A := \{m \geq 1; z \in t^m O\} \neq \emptyset$.

Seja $m := \max A$. Veja que $m < \infty$, pois caso contrário, ao construir a sequência $x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-2}, ..., x_m = t$, temos que ela é limitado, pois se não o fosse, contrariaríamos o Lema 1.1.7.

Assim $z \in t^m O \Rightarrow z = t^m u$, onde $u \in O^*$, pois se $u \notin O^*$, teríamos $u \in P \Rightarrow u = tw$, onde $w \in O \Rightarrow z = t^{m+1}w \in t^{m+1}O$. Contrariando a maximalidade de m.

Suponha agora que $z = t^m u = t^n v$, onde $m, n \in \mathbb{Z}$ e $u, v \in O^*$. Temos:

$$t^m u = t^n v \Rightarrow t^n(u - t^{n-m}v) = 0$$
$$\Rightarrow u = t^{n-m}v \Rightarrow t^{n-m} = uv^{-1} \in O^*$$

Portanto se $m \neq m$, temos $t \in O^*$ e assim $t \notin P$, gerando um absurdo. Assim $m = n$, e também $u = v$. Donde temos a unicidade da representação.

3. Seja $\{0\} \neq I \subset O$ um ideal.

   O conjunto $A := \{r \in \mathbb{N}; t^r \in I\} \neq \emptyset$, pois se $0 \neq x \in I$, então $x = t^r u$ com $u \in O^*$, assim $t^r = xu^{-1} \in I$.

   Defina $n := \min A$. Temos $I = t^n O$:

   $I \supset t^n O$**:** Como $t^n \in I \Rightarrow t^n O \subset I$.

   $I \subset t^n O$**:** Seja $y \in I$ não nulo, então $y = t^s w$, onde $w \in O^*$ e $s \geq 0$. Assim $t^s = yu^{-1} \in I$, logo $s \geq n$. Portanto $y = t^n t^{s-n} w \in t^n O$.

□

Definição 1.1.8. 1. Um lugar P de um corpo de funções F/K é o ideal maximal de algum anel de valorização O de F/K. Todo $t \in P$ tal que $P = tO$ é chamado de um elemento primo de P (outras notações são parâmetro local ou variável uniforme).

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

Pela Proposição 1.1.5 item 2, temos que dado O um anel de valorização de F/K e P seu ideal maximal, O é unicamente determinado por P: $O = \{z \in F; z^{-1} \notin P\}$. Assim $O_P := O$ é chamado de anel de valorização do lugar P.

Definição 1.1.9. Uma valorização discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

1. $v(x) = \infty \Leftrightarrow x = 0$;
2. $v(xy) = v(x) + v(y), \forall x, y \in F$;
3. $v(x + y) \geq \min\{v(x), v(y)\}, \forall x, y \in F$;
4. $\exists z \in F$ tal que $v(z) = 1$;
5. $v(a) = 0, \forall a \in K$ não nulo.

Neste contexto, o símbolo ∞ designa um elemento não inteiro ($\notin \mathbb{Z}$) tal que $\infty + \infty = \infty + n = \infty$ e $\infty > m$, $\forall n, m \in \mathbb{Z}$.

Dos itens 2 e 4 acima, temos que $v : F \to \mathbb{Z} \cup \{\infty\}$ é sobrejetora.

De fato, seja $j \in \mathbb{Z} \cup \{\infty\}$. Se $j = 0$ ou $j = \infty$, como $\{0, 1\} \subset K$, então acabou.

Se $j \in \mathbb{Z}$ e $j \neq 0$, por 4, $\exists z \in F$ tal que $v(z) = 1$, assim:

$$j > 0 \Rightarrow v(z^j) = jv(z) = j.$$

$j < 0$, fazendo $q = -j, q > 0$, temos $0 = v(1) = v(zz^{-1}) = v(z) + v(z^{-1}) = 1 + v(z^{-1})$

$$\Rightarrow 0 = 1 + v(z^{-1}) \Rightarrow v(z^{-1}) = -1 \Rightarrow v((z^{-1})^q) = -q = j \Rightarrow v(z^j) = j.$$

A propriedade 3 é chamada desigualdade triangular. Uma forte versão dessa desigualdade pode ser derivada a partir dos axiomas e é frequentemente muito útil:

Lema 1.1.10. *(DESIGUALDADE TRIANGULAR ESTRITA)*

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

Demonstração. Veja que $v(ay) = v(y), \forall a \in K$ $(a \neq 0)$, como $-1 \in K$, então, por 2, $v(-y) = v(-1y) = 0 + v(y)$. Por hipótese $v(x) \neq v(y)$, assim podemos supor sem perda de generalidade $v(x) < v(y)$.

Se $v(x + y) \neq \min\{v(x), v(y)\} = v(x)$, então por 3, $v(x + y) > v(x)$. Assim $v(x) = v(x+y-y) \geq \min\{v(x+y), v(-y)\} = \min\{v(x+y), v(y)\} > v(x) \Rightarrow v(x) > v(x)$, gerando um absurdo.

□

Definição 1.1.11. Para todo lugar $P \in \mathbb{P}_F$ associamos uma função $v_P : F \to \mathbb{Z} \cup \infty$ que provaremos ser uma valorização discreta de F/K: Escolha t um elemento primo de P. Então para todo $z \in F$ não nulo, temos uma única representação $z = t^n u$, com $u \in O^*$ e $n \in \mathbb{Z}$. Defina $v_P(z) := n$ e $v_P(0) := \infty$.

Veja que tal definição depende apenas de P, e não do t escolhido. De fato, se t' é primo em P, então $P = tO = t'O$, donde temos $t = t'w$, onde $w \in O^*$, assim $t^n u = (t'w)^n u = t'^n w^n u = t'^n(w^n u)$, com $w^n u \in O^*$.

Teorema 1.1.12. *Seja F/K um corpo de funções:*

1. *Para todo lugar $P \in \mathbb{P}_F$, a função v_P acima definida é uma valorização discreta de F/K. Mais que isso:*

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

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

2. *Reciprocamente, se v é uma valorização discreta de F/K, então o conjunto $P = \{z \in F; v(z) > 0\}$ é um lugar de F/K, e $O_P = \{z \in F; v(z) \geq 0\}$ é o seu anel de valorização correspondente.*

3. *Qualquer anel de valorização O de F/K é um subanel maximal próprio de F.*

Demonstração. 1. Pelo que observamos logo acima, temos a boa definição de v_P. A propriedade 1 de valorização discreta segue d definição de v_P: $v_P(0) := \infty$.

A propriedade 2 de valorização discreta vem de: $v_P(xy) = v_P(t^n u_1 t^m u_2) = v_P(t^{n+m} \underbrace{(u_1 u_2)}_{\in O^*}) = n + m = v_P(x) + v_P(y)$.

Agora a propriedade 3 de valorização discreta: sejam $x, y \in F$ com $v_P(x) = n$ e $v_P(y) = m$. Sem perda de generidade podemos supor $n \leq m < \infty$. Assim, temos: $x = t^n u_1$ e $y = t^m u_2$, com $u_1, u_2 \in O_P^*$.

Então $x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n}u_2) = t^n z$, com $z \in O_P$.

Se $z = 0$: $v_P(x + y) = \infty > \min\{n, m\} = \min\{v_P(x), v_P(y)\}$.

Se $z \neq 0$: $z = t^k u$, com $0 \leq k \in \mathbb{Z}$ e $u \in O^*$. Então:

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

Agora se $x = 0$ ou $y = 0$, então $v_P(x+y) = v_P(y) = \min\{v_P(x), v_P(y)\}$, no caso em que $y \neq 0$, e $v_P(x + y) = v_P(x) = \min\{v_P(x), v_P(y)\}$.

Quanto a propriedade 4 de valorização discreta, observe que $v_P(t) = 1$.

Por fim a propridade 5: seja $0 \neq a \in K \subset O^* \subset O$. Então $v_P(a) = v_P(t^0 a) = 0$.

Agora quanto aos conjuntos:

$O_P = \{z \in F; v_P(z) \geq 0\}$: se $z \in O_P$, então: se z é nulo temos $v_P(z) = \infty > 0$, e se z é não nulo temos $v_P(z) = v_P(t^n u) = n$, onde $0 \leq n \in \mathbb{Z}$ e $u \in O^*$. Se $z \in F$ e $v_P(z) \geq 0$, temos:

$$(\star) \text{ se } v_P(z) = 0 \Leftrightarrow z \in O^*$$

$$(\star\star) \text{ se } v_P(z) = \infty \Leftrightarrow z = 0 \in P \subset O_P \text{ e se } v_P(z) = n > 0 \Leftrightarrow z = t^n u,$$
$$0 < n \in \mathbb{Z} \text{ e } u \in O^* \Leftrightarrow z \in tO = P \subset O_P.$$

Observe que $O_P^* = \{z \in F; v_P(z) = 0\}$ segue de $(\star)$.

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

Se $x \in F$ é primo e P, então vimos que q definição independe do primo t, donde temos que $v_P(x) = v_P(t) = 1$.

2. Segue da verificação das propriedades destes conjuntos e usando que se $x \in F$ então $v(x) = -v(x_{-1})$.

3. Sejam O um anel de valorização, P seu ideal maximal, v_P a valorização discreta de P e $z \in F \backslash O$.

Seja também $y \in F$. Como $z \notin O \Rightarrow z^{-1} \in O$, além disso $z^{-1} \notin O^* \Rightarrow v_P(z^{-1}) > 0$. Veja que $v_P(yz^{-k}) = \underbrace{v_P(y)}_{\in \mathbb{Z} \cup \{\infty\}} + k \underbrace{v_P(z^{-1})}_{>0}$.

Assim para $k \geq 0$ suficientemente grande, $v_P(yz^{-k}) \geq 0 \Rightarrow yz^{-k} \in O$. Defina $w := yz^{-k} \in O$, temos assim $y = wz^k \Rightarrow F = O[z]$.

Portanto O é maximal.

□

Seja P um lugar de F/K e O_P seu respectivo anel de valorização. Como P é maximal, então o anel das classes residuais $\frac{O_P}{P}$ é um corpo. Para $x \in O_P$, definimos $x(P) \in \frac{O_P}{P}$ como a classe residual de x módulo P, para $x \in F - O_P$, fazemos $x(P) := \infty$.

Da Proposição 1.1.5, temos que $K \subset O_P$ e $\tilde{K} \cap P = \{0\}$, assim $K \subset O_P$ e $K \cap P = \{0\}$.

Então a aplicação $\varphi : O_P \to \frac{O_P}{P}$, onde $x \mapsto x(P)$, induz um mergulho canônico de K em $\frac{O_P}{P}$.

De fato, se $x, y \in K$ e $x(P) = y(P) \Rightarrow x - y \in P \Rightarrow x - y \in P \cap K \Rightarrow x - y = 0 \Rightarrow x = y$.

Assim, podemos ver K como subcorpo de $\frac{O_P}{P}$, pois φ se torna isomorfismo quando restrita a K. Como $\tilde{K} \subset O_P$ e $\tilde{K} \cap P = \{0\}$, podemos extender este raciocínio para $\tilde{K}$. Ou seja, ver $\tilde{K}$ como subcorpo de $\frac{O_P}{P}$.

Definição 1.1.13. Seja $P \in \mathbb{P}_F$.

1. $F_P := \frac{O_P}{P}$ é o corpo das classes residuais módulo P. A aplicação $x \mapsto x(P)$ de F e $F_P \cup \{\infty\}$ é chamada aplicação classe residual com respeito a P. E também podemos denotar $x + P := x(P), \forall x \in O_P$.

2. $\deg P := [F_P : K]$ é chamado de grau de P.

Proposição 1.1.14. *Se P é um lugar de F/K e $0 \neq x \in P$, então:*

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

Demonstração. Da observação 1.1.2, tendo que $x \in P$ não nulo é transcendente, pois $\tilde{K} \cap P = \{0\}$, segue que $[F : K(x)] < \infty$.

Sejam $z_1, ..., z_n \in O_P$ tais que $z_1(P), ..., z_n(P) \in \frac{O_P}{P}$ sejam l.i. sobre K. Mostremos que $z_1, ..., z_n \in F$ são l.i. sobre $K(x)$.

Suponhamos que sejam l.d., assim tomemos a combinação linear não trivial:

$$0 = \sum_{i=1}^{n} \varphi_i z_i, \text{ onde } \varphi \in K(x), i = 1, ..., n.$$

Sem perda de generalidade, podemos supor que $\varphi_i \in K[x], \forall i$, e que x nnão divide $\varphi_i, \forall i$, ou seja, $\exists j \in \{1, ..., n\}$ onde $\varphi_j = a_j + xg_j$, com $a_j \in K$ não nulo.

Como $x \in P$ e $g_i \in K[x] \subset O_P$, então, $\forall i$, temos:

$$\varphi_i(P) = a_i(P) + xg_i(P) = a_i(P) + 0(P) = a_i(P) = a_i.$$

Assim:

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

onde os a_i's não são todos nulos.

Donde temos que $z_1(P), ..., z_n(P)$ são l.d. sobre K, gerando uma contradição.

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

□

Corolário 1.1.15. *O corpo das constantes $\tilde{K}$ de F/K é uma extensão de corpos finita de K, ou seja, $[\tilde{K} : K] < \infty$.*

Demonstração. A frente mostraremos que $\mathbb{P}_F \neq \emptyset$. Portanto vamos assumí-lo verdadeiro, por enquanto.

Seja $P \in \mathbb{P}_F$. Pela proposição anterior, temos: $[F_P : K] < \infty$. Mas, observamos acima que podemos megulhar $\tilde{K}$ em F_P, assim:

$$\begin{gathered}[F_P : \tilde{K}][\tilde{K} : K] = [F_P : K] < \infty \\ \Rightarrow [\tilde{K} : K] \leq [F_P : K] < \infty \\ \Rightarrow [\tilde{K} : K] < \infty\end{gathered}$$

□

Observação 1.1.16. No caso em que $\deg P = 1$ temos que $F_P = K$, e a aplicação classe residual leva F em $K \cup \{\infty\}$. Em particular, se K é algebricamente fechado, então todo lugar de F tem grau 1. De fato, se K é algebricamente fechado, então toda extensão algébrica é trivial $\Rightarrow [F_P : K] = 1, \forall P \in \mathbb{P}_F$.

Assim, podemos ver $z \in F$ como a função:

$$z : \mathbb{P}_F \to K \cup \{\infty\}, \text{ tal que } P \mapsto z(P)$$

Daí o porquê F/K é chamado corpo de funções. Os elementos de K visto como funções do tipo acima são funções constantes, pois se $P_1, P_2 \in \mathbb{P}_F$ e $k \in K$, então $k(P_1) = k(P_2) = k$. Por isso K é chamado de corpo de constantes de F.

Definição 1.1.17. Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se, e somente se, $v_P(z) > 0$; P é um pólo de z se, e somente se, $v_P(z) < 0$. Se $v_P(z) = m > 0$, P é dito um zero de z de ordem m; se $v_P(z) = -m < 0$, P é dito um pólo de z de ordem m.

Teorema 1.1.18. *Seja F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq O_P$.*

Demonstração. Considere o conjunto:

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

Por definição IS é o conjunto de todas as somas finitas $\sum a_\nu s_\nu$ com $a_\nu \in I$ e $s_\nu \in S$, isto é um ideal de S.

Λ é não vazio, pois $R \in \Lambda$. Além disso a relação de inclusão induz uma ordem parcial em Λ.

Seja $H \subseteq \Lambda$ uma cadeia, assim defina:

$$T := \bigcup \{S; S \in H\}$$

Temos que T é um subanel de F e $R \subset T$. Verifiquemos agora que $IT \neq T$. Suponha que $T = IT$, então:

$$1 \in IT \Rightarrow 1 = \textstyle\sum_{\nu=1}^{n} a_\nu s_\nu.$$

Como H é uma cadeia, então $\exists S_0 \in H$ tal que $s_\nu \in S_0, \forall \nu = 1, ..., n \Rightarrow 1 \in IS_0 \Rightarrow S_0 \subset IS_0 \Rightarrow S_0 = IS_0$. Gerando uma contradição.

Portanto $T \in \Lambda$. Observe que T é um limitante superior de H, assim, pelo lema de Zorn, temos que Λ possui um elemento maximal, isto é, $\exists O \subseteq F$ subanel tal que $R \subseteq O \subseteq F$ e $IO \neq O$ e O é maximal com esta propriedade.

Mostremos que O é um anel de valorização de F/K:

Como $I \neq \{0\}$ e $IO \neq O$, então $O \subsetneq F$ e $I \subseteq O \backslash O^*$. De fato: Se $\exists u \in O^*$ tal que $u \in I$, teríamos $uu^{-1} = 1 \in IO \Rightarrow IO = O$, contrariando as propriedades apresentadas por O. Se $O = F$, seja $u \in I \Rightarrow u^{-1} \in F \Rightarrow 1 \in IF \Rightarrow F = IF \Rightarrow IO = O$, gerando novamente uma contradição.

Suponha agora $z \in F$ tal que $z, z^{-1} \notin O \Rightarrow O \subsetneq O[z]$, que é um anel de F onde $R \subset O \subset O[z]$. Como O é maximal, então $IO[z] = O[z]$. Analogamente $IO[z^{-1}] = O[z^{-1}]$. Assim $1 \in IO[z] \cap IO[z^{-1}]$, logo $\exists a_0, ..., a_n, b_0, ..., b_m \in IO$ onde:

$$\underbrace{a_0 + a_1 z + ... + a_n z^n}_{(i)} = 1 = \underbrace{b_0 + b_1 z^{-1} + ... + b_m z^{-m}}_{(ii)} (\star)$$

Veja que se $n = 0 \Rightarrow a_0 = 1 \Rightarrow OI = O$, absurdo! Portanto $n \geq 1$ e analogamente $m \geq 1$.

Tomemos n e m mínimos satisfazendo $(\star)$. Sem perda de generalidade, suponha $m \leq n$ (caso contrário basta fazer $z^{-1} = y$ e $y^{-1} = z$).

Multiplicando (i) por $(1 - b_0)$ e (ii) por $a_n z^n$ temos:

$$(1 - b_0)a_0 + (1 - b_0)a_1 z + ... + (1 - b_0)a_n z^n = 1 - b_0$$

e

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

Somando estas duas expressões temos:

$$1 = c_0 + ... + c_{n-1} z^{n-1}, \text{ com } c_i \in IO, \forall i.$$

Contrariando a minimalidade de n. Logo $z \in O$ ou $z^{-1} \in O$.

Portanto O é anel de valorização de F/K e $I \subseteq P = O \backslash O^*$.

□

Corolário 1.1.19. *Sejam F/K corpo de funções e $z \in F$ transcendente sobre K. Então z tem pelo menos um zero e um pólo. Em particular $\mathbb{P}_F \neq \emptyset$.*

Demonstração. Tome $R = K[z]$ e $I = zK[z]$. Então $\exists P$ lugar de F/K tal que $z \in P$ (teorema anterior). Como $z \in P = tO \subset O_P$, temos que $z = t^n u$, onde $1 \leq n \in \mathbb{Z}$ e $u \in O_P^*$. Daí $v_P(z) = n > 0 \Rightarrow P$ é um zero de z. Veja que $z^{-1} = t^{-n}u^{-1} \Rightarrow P$ é um pólo de z^{-1}.

Fazendo o mesmo raciocínio para z^{-1}, temos que $\exists Q \in \mathbb{P}_F$ onde Q é zero de z^{-1} e Q é pólo de z. Portanto, $\forall z \in F$ transcendente sobre K, temos que z possui zero e pólo em $\mathbb{P}_F$.

□

Observemos que $0 \neq z \in \tilde{K} \subset O$, então $v_P(z) \geq 0$; como $\tilde{K} \cap P = \{0\} \Rightarrow z \in O^* \Rightarrow v_P(z) = 0$. E se $z \notin \tilde{K}$, então sempre existem lugares P e Q tais que $v_P(z) > 0$ e $v_Q(z) < 0$. Assim, na observação 1.1.16, se $z \notin \tilde{K}$, conseguimos uma função, no sentido alí descrito, não constante.

1.2 Corpo de funções racionais

Será investigado aqui o cropo de funções racionais $F = K(x)$, onde x é transcendente sobre K.

Dado um polinômio arbitrário, mônico e irredutível $p(x) \in K[x]$, considere o anel de valorização:

$$O_{p(x)} = \left\{ \tfrac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}$$

de $K(x)/K$ com seu ideal maximal:

$$P_{p(x)} = \left\{ \tfrac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) | f(x) \text{ e } p(x) \text{ não divide } g(x) \right\}.$$

No caso de $p(x)$ for linear, isto é, $p(x) = x - \alpha$ com $\alpha \in K$ escrevemos $P_\alpha := P_{p(x)} \in \mathbb{P}_F$.

Existe outro anel de valorização de $K(x)/K$:

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

com ideal maximal:

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

P_∞ é chamado de lugar infinito de $K(x)$.

Observe que este rótulo depende especificamente da escolha de elemento gerador $x \in K(x)$. Por exemplo, $K(x) = K(\frac{1}{x})$, pois $x^{-1} = \frac{1}{x}$, e o lugar infinito com respeito a $\frac{1}{x}$ é o lugar P_0 com respeito a x.

Proposição 1.2.1. *Seja $F = K(x)$ um corpo de funções racionais.*

1. *Seja $P = P_{p(x)} \in \mathbb{P}_F$ um lugar como o explicitado acima, onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é primo para P e a correspondente valorização discreta v_P pode ser escrita como segue:*

   Se $z \in K(x)\backslash\{0\}$ é escrito da forma $z = p(x)^n \frac{f(x)}{g(x)}$, com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$ onde $p(x)$ não divide nem $f(x)$ e nem $g(x)$, então $v_P(z) = n$.

   O corpo de classes residuais $K(x)_P = \frac{O_P}{P}$ é isomorfo a $\frac{K[x]}{(p(x))}$; um isomorfismo é dado por: $\varphi : \frac{K[x]}{(p(x))} \to \frac{O_P}{P}$, onde $f(x) \bmod(p(x)) \mapsto f(x)(P)$.

   Consequentemente $\deg P = \deg p(x)$.

2. *Quando $p(x) = x - \alpha$ com $\alpha \in K$, o grau de $P = P_\alpha$ é 1, e a aplicação classe residual é dada por: $z(P) = z(\alpha), \forall z \in K(x)$, onde $z(\alpha)$ é definido como se segue: escrevendo $z = \frac{f(x)}{g(x)}$, com $f(x), g(x) \in K[x]$ relativamente primos, então: $z(\alpha) = \frac{f(\alpha)}{g(\alpha)}$ se $g(\alpha) \neq 0$, e, $z(\alpha) = \infty$ se $g(\alpha) = 0$.*

3. *Seja $P = P_\infty$ o lugar infinito de $K(x)/K$. Então* $\deg P = 1$. *Um elemento primo de P_∞ é $t = \frac{1}{x}$. A correspondente valorização discreta v_∞ é dada por: $v_\infty(\frac{f(x)}{g(x)}) = \deg g(x) - deg f(x)$, onde $f(x), g(x) \in K[x]$. A aplicação classe residual de P_∞ é determinada por: $z(P_\infty) = z(\infty), \forall z \in K(x)$, onde $z(\infty)$ é definido como: se $z = \frac{a_n x^n + \ldots + a_0}{b_m x^m + \ldots + b_0}$, com a_n e b_m não nulo, então $z(\infty) = \frac{a_n}{b_m}$ se $n = m$, $z(\infty) = 0$ se $n < m$, e, $z(\infty) = \infty$ se $n > m$.*

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

Demonstração. 1. Seja $P = P_{p(x)} \in \mathbb{P}_F$, $p(x) \in K[x]$ irredutível. O ideal $P_{p(x)} \subset O_{p(x)}$ é gerado por $p(x)$, de fato, veja que se $\frac{f(x)}{g(x)} \in P_{p(x)} \Rightarrow p(x)|f(x)$ e $p(x)$ não divide $g(x) \Rightarrow \frac{f(x)}{g(x)} = \underbrace{\frac{\mu(x)}{g(x)}}_{\in O_{p(x)}} p(x) \in O_{p(x)}p(x)$.

Portanto $P_{p(x)} \subset p(x)O_{p(x)}$.

Como $p(x) \in P_{p(x)}$, então $P_{p(x)} = p(x)O_{p(x)}$.

Agora defina $\phi : K[x] \to K(x)_P$, de forma que $f(x) \mapsto f(x)(P)$. Temos que ϕ está bem definida, pois $f(x) = \frac{f(x)}{1} \Rightarrow f(x) \in O_{p(x)}$. Além disso, ϕ é homomorfismo e $f(x) \in \ker\phi \Leftrightarrow f(x)(P) = (P) \Leftrightarrow p(x)|f(x) \Leftrightarrow f(x) \in (p(x))$. Logo $(p(x)) = \ker\phi$.

ϕ é sobrejetora: seja $z \in O_{p(x)} \Rightarrow z = \frac{u(x)}{v(x)}$ onde $p(x)$ não divide $v(x)$. Como $p(x)$ é irredutível temos $\text{mdc}(p(x), v(x)) = 1$, assim $\exists a(x), b(x) \in K[x]$ onde $a(x)p(x) + b(x)v(x) = 1$, então:

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

$$= \tfrac{u(x)}{v(x)}a(x)p(x) + b(x)u(x)$$

$$\Rightarrow z(P) = (b(x)u(x))(P), \text{ onde } b(x)u(x) \in K[x]$$

$$\Rightarrow \phi(b(x)u(x)) = z(P)$$

Portanto ϕ é sobrejetora. Donde temos $\frac{K[x]}{(p(x))}$ e $K(x)_P$ são isomorfos.

Como $[\frac{K[x]}{(p(x))} : K] = [K(x)_P : K] \Rightarrow \deg P = \deg p(x)$.

2. Agora $P = P_\alpha$, com $\alpha \in K$.

Se $f(x) \in K[x] \Rightarrow (x - \alpha)|(f(x) - f(\alpha))$. Assim,

$$f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = \underbrace{f(\alpha)}_{\in K}(P) = f(\alpha).$$

Seja agora $z \in O_P \Rightarrow z = \frac{f(x)}{g(x)}$, onde $p(x)$ não divide $g(x)$ $(g(\alpha) \neq 0)$, então $z(P) = \frac{f(x)}{g(x)}(P)$, onde $g(x)(P) \neq (P)$, e assim:

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

Se $z \notin O_P \Rightarrow z = \frac{f(x)}{g(x)}$, onde $p(x)|g(x)$ $(g(\alpha) = 0) \Rightarrow z(P) = \infty = z(\alpha)$.

3. Seja $z \in P_\infty \Rightarrow z = \frac{f(x)}{g(x)}$, onde $\deg f(x) < \deg g(x) \Rightarrow z = \frac{1}{x}\frac{xf(x)}{g(x)}$, onde $\deg xf(x) \leq \deg g(x)$, ou seja $\frac{xf(x)}{g(x)} \in O_\infty$. Logo $P_\infty = \frac{1}{x}O_\infty \Rightarrow \frac{1}{x}$ é primo de P_∞.

   Como P_∞ com respeito a x é P_0 com respeito a $\frac{1}{x}$, então $\frac{K(x)}{P_\infty} \cong \frac{K(\frac{1}{x})}{P_0} \cong \frac{K[\frac{1}{x}]}{(\frac{1}{x})}$ $\Rightarrow \deg P_0 = 1 \Rightarrow \deg P_\infty = 1$.

4. Tome um lugar P de $K(x)/K$ com grau 1, $P = P_\alpha$ com $\alpha \in K$ por exemplo.

   Podemos mergulhar $\tilde{K} \subset K(x)$ em $K(x)_P$, assim:

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

□

Teorema 1.2.2. *Não existe lugares do corpo de funções racionais $K(x)/K$ que não sejam da forma $P_{p(x)}$ ou P_∞.*

Demonstração. Seja $P \in \mathbb{P}_{K(x)}$, considere o anel de valorização correspondente a P, O_P.

CASO I: $x \in O_P$.

$x \in O_P \Rightarrow K[x] \subset O_P \Rightarrow I := K[x] \cap P$ é ideal de $K[x]$, e como P é ideal maximal de O_P, então I é maximal de $K[x]$, e portanto $\frac{K[x]}{I}$ é corpo.

Assim, podemos mergulhar $\frac{K[x]}{I} \hookrightarrow K(x)_P$, $z(I) \mapsto z(P)$. De fato, $z_1(P) = z_2(P) \Rightarrow (z_1 - z_2)(P) = (P) \Rightarrow z_1 - z_2 \in I \Rightarrow z_1(I) = z_2(I)$.

Veja ainda que $I \neq \{0\}$, pois se $I = \{0\}$ então $K[x] = \frac{K[x]}{I} = K \Rightarrow K[x]$ é um corpo $\Leftrightarrow x$ é algébrico, o que não é verdade.

Portanto I é ideal maximal não nulo de $K[x]$.

Como K é corpo, então $K[x]$ é domínio de ideais principais, logo existe $p(x) \in K[x]$ irredutível e mônico tal que $I = (p(x)) \Rightarrow I = K[x] \cap P = p(x)K[x]$.

Assim $\forall g(x) \in K[x]$ com $p(x)$ não dividindo $g(x)$, temos $g(x) \notin I \Rightarrow g(x) \notin P \Rightarrow \frac{1}{g(x)} \in O_P$ (Proposição 1.1.5).

Considere:

$$O_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \text{ não divide } g(x) \right\}.$$

Seja $\frac{f(x)}{g(x)} \in O_{p(x)}$. Como $p(x)$ não divide $g(x) \Rightarrow g(x)^{-1} \in O_P \underbrace{\Rightarrow}_{K[x] \subset O_P} \frac{f(x)}{g(x)} \in O_P$.

Portanto, $O_{p(x)} \subseteq O_P$. Como $O_{p(x)}$ é anel de valorização, então $O_{p(x)}$ é maximal, donde temos $O_{p(x)} = O_P \Rightarrow P_{p(x)} = P$.

CASO II: $x \notin O_P$.

Como $x \notin O_P$ então temos $x^{-1} \in O_P$ e $x^{-1} \in P$.

$x^{-1} \in O_P \Rightarrow K[x^{-1}] \subset O_P \Rightarrow x^{-1} \in P \cap K[x^{-1}] \Rightarrow x^{-1}K[x^{-1}] \subset P \cap K[x^{-1}]$ ideais de $K[x^{-1}]$. Como x^{-1} é irredutível em $K[x^{-1}] \Rightarrow x^{-1}K[x^{-1}]$ é maximal $\Rightarrow x^{-1}K[x^{-1}] = P \cap K[x^{-1}]$.

Assim, como no caso I:

$$O_P \supseteq \left\{ \tfrac{f(x^{-1})}{g(x^{-1})}; f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \text{ não divide } g(x^{-1}) \right\} =$$
$$= \{ \tfrac{a_0+a_1x^{-1}+\ldots+a_nx^{-n}}{b_0+b_1x^{-1}+\ldots+b_mx^{-m}}; b_0 \neq 0 \} = \{ \tfrac{(a_0x^n+a_1x^{n-1}+\ldots+a_n)/x^n}{(b_0x^m+b_1x^{m-1}+\ldots+b_m)/x^m}; b_0 \neq 0 \} =$$
$$= \{ \tfrac{a_0x^{n+m}+a_1x^{n-1+m}+\ldots+a_nx^m}{b_0x^{m+n}+b_1x^{m-1+n}+\ldots+b_mx^n}; b_0 \neq 0 \} =$$
$$= \{ \tfrac{u(x)}{v(x)}; u(x), v(x) \in K[x] \text{ e } \deg v(x) \geq \deg u(x) \} = O_\infty.$$

Como O_∞ é maximal, então $O_\infty = O_P$. Logo $P = P_\infty$.

□

Corolário 1.2.3. *Os lugares de $K(x)/K$ com grau 1 são 1-1 correspondentes com $K \cup \{\infty\}$.*

Demonstração. Seja $\Lambda = \{\text{lugares de } K(x)/K \text{ com grau } 1\}$. Pelo teorema anterior $\Lambda = \{P_\alpha; \alpha \in K \cup \{\infty\}\}$. Defina $x : \Lambda \to K \cup \{\infty\}$, tal que $P_\alpha \mapsto x(P_\alpha) = x(\alpha) = \alpha$.

□

1.3 Independência de valorização

Teorema 1.3.1. *(Teorema da aproximação fraca ou Teorema de independência) Sejam F/K um corpo de funções, $P_1, ..., P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K,*

$x_1, ..., x_n \in F$ e $r_1, ..., r_n \in \mathbb{Z}$. Então existe $x \in F$ tal que $v_{P_i}(x - x_i) = r_i$, $i = 1, ..., n$.

Demonstração. $v_{P_i} = v_i$

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

Indução sobre n:

Para $n = 2$: veja que O_{P_1} não está contido em O_{P_2} e O_{P_2} não está contido em O_{P_1}, por conta da maximalidade dos anéis de valorização. Assim podemos tomar $y_1 \in O_{P_1} \backslash O_{P_2}$ e $y_2 \in O_{P_2} \backslash O_{P_1}$. Então $v_1(y_1) \geq 0$, $v_2(y_1) < 0$, $v_1(y_2) < 0$ e $v_2(y_2) \geq 0$. Tome $u = \frac{y_1}{y_2}$.

Para $n > 2$: pela hipótese de indução, $\exists y \in F$ tal que $v_1(y) > 0$ e $v_2(y), ..., v_{n-1}(y) < 0$.

Se $v_n(y) < 0$, acabou!

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

$$v_1(u) \geq \min\{v_1(y), rv_1(z)\} > 0 \text{ e}$$
$$v_i(u) = \min\{v_i(y), rv_i(z)\} < 0, \text{ para } i = 2, ..., n.$$

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

Tome u do passo anterior. Defina $w = (1 + u^s)^{-1}$. Temos que para $s \in \mathbb{N}$ suficientemente grande:

$$v_1(w - 1) = v_1((1 + u^s)^{-1} - 1) = v_1(\tfrac{1}{1+u^s} - 1) = v_1(\tfrac{1-1-u^s}{1+u^s}) =$$
$$= v_1(-u^s(1 + u^s)^{-1}) = v_1(-u^s) + v_1((1 + u^s)^{-1}) = v_1(-u^s) - v_1(1 + u^s) =$$
$$= v_1(-u^s) - \underbrace{\min\{v_1(1), v_1(u^s)\}}_{=0} = v_1(u^s) = sv_1(u) > r_1, \text{ e}$$
$$v_i(w) = v_i((1 + u^s)^{-1}) = -v_i(1 + u^s) = -sv_i(u) > r_i, \text{ para } i = 2, ..., n.$$

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

Escolha $s \in \mathbb{Z}$ de forma que $v_i(y_j) \geq s, \forall i, j \in \{1, ..., n\}$.

Pelo passo 2, existem $w_1, ..., w_n \in F$ tais que: $v_i(w_i - 1) > r_i - s$ e $v_i(w_j) > r_i - s$ quando $i \neq j$.

Tomando $z := \sum_{j=1}^{n} y_j w_j$, temos:

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

Agora o teorema: pelo passo 3, $\exists z \in F$, onde $v_i(z - x_i) > r_i$, $\forall i = 1, ..., n$. Depois tome z_i's $\in F$ de forma que $v_i(z_i) = r_i$ (potências dos primos dos lugares em questão, por exemplo). De novo, pelo passo 3, $\exists z' \in F$ tal que $v_i(z' - z_i) > r_i$, $i = 1, ..., n$. Assim $v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i$, $\forall i = 1, ..., n$.

Tome $x := z + z'$. Temos:

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

□

Corolário 1.3.2. *Todo corpo de funções tem uma quantidade infinita de lugares.*

Demonstração. Suponha que existe apenas uma quantidade finita de lugares, digamos $P_1, ..., P_n$. Pelo teorema anterior, existe $0 \neq x \in F$ tal que $v_{P_i}(x) > 0$, $\forall i = 1, ..., n$. Donde temos que x é transcendente sobre K, mas não tem nenhum pólo, contrariando o Corolário 1.1.19.

□

Proposição 1.3.3. *Seja F/K um corpo de funções e $P_1, ..., P_r$ zeros de um elemento $x \in F$. Então:*

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

Demonstração. Redefinindo inicialmente $v_i := v_{P_i}$, $f_i := \deg P_i$ e $e_i := v_i(x)$.

Para cada $i = 1, ..., r$, $\exists t_i \in F$ onde $v_i(t_i) = 1$ e $v_k(t_i) = 0$ quando $i \neq k$ (isto pelo teorema anterior, fazendo $x_i = 0, i = 1, ..., r$ e, $r_i = 1$ e $r_k = 0$ se $i \neq k$).

Agora, escolha $s_{i1}, ..., s_{if_i} \in O_{P_i}$ tal que $s_{i1}(P_i), ..., s_{if_i}(P_i)$ constitua uma base para F_{P_i} sobre K. Pelo teorema de independência, temos que para todo i, j, $\exists z_{ij} \in F$ onde $v_i(s_{ij} - z_{ij}) > 0$ e $v_k(z_{ij}) \geq e_k, k \neq i$, bastando tomar $x_i = s_{ij}$ e $x_k = 0, k \neq i$.

Afirmamos que os elementos $t_i^a z_{ij}$, onde $1 \leq i \leq r$, $1 \leq j \leq f_i$ e $0 \leq a < e_i$, são linearmente independentes em F sobre $K(x)$. O conjunto destes vetores soma $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \deg P_i$ elementos, donde temos a proposição.

Suponhamos por absurdo que existe uma combinação linear não trivial sobre $K(x)$:

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

Sem perda de generalidade, podemos assumir $\varphi_{ija} \in K[x]$ e nem todos os φ_{ija} são divisíveis por x. Então existe um índice $k \in \{1, ..., r\}$ e $c \in \{0, ..., e_k - 1\}$ onde $x|\varphi_{ija}$, $\forall a < c$ e $\forall j \in \{1, ..., f_k\}$ e x não divide φ_{kjc}, para algum $j \in \{1, ..., f_k\}$.

Multiplicando $(\star)$ por t_k^{-c}, temos:

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

Veja agora que:

$i \neq k$: $v_k(\varphi_{ija}t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}) + v_k(t_i^a) + v_k(t_k^{-c}) + v_k(z_{ij}) \geq \geq -c + e_k > 0$;

$i = j$ e $a < c$: $(\Rightarrow x|\varphi_{kja} \Rightarrow v_k(\varphi_{kja}) \geq e_k)$ $v_k(\varphi_{kja}t_k^a t_k^{-c} z_{kj}) \geq \geq e_k + a - c > e_k - c > 0$;

$i = j$ e $a > c$: $v_k(\varphi_{kja}t_k^a t_k^{-c} z_{kj}) \geq a - c > 0$.

Pois veja que $v_k(z_{kj}) \geq 0$, já que $s_{kj} \in O_{P_k}$.

Assim temos:

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

Como P_k é um zero de x, então $\varphi_{kjc}(P_k) \in K, \forall j \in \{1, ..., f_k\}$ e $\exists j \in \{1, ..., f_k\}$ tal que $\varphi_{kjc}(P_k) \neq 0$.

Assim:

$$\sum_{j=1}^{f_k}\varphi_{kjc}(P_k) z_{kj}(P_k) = 0(P_k)$$

é uma combinação linear não trivial sobre K identicamente nula . Contradição, pois $z_{k1}(P_k), ..., z_{kf_k}(P_k)$ constituem uma base de F_{P_k} sobre K.

□

Corolário 1.3.4. *Em um corpo de funções F/K, qualquer elemento $0 \neq x \in F$ tem uma quantidade finita de zeros e pólos.*

Demonstração. Se x é constante, então x não tem zeros e nem pólos. Se x é transcendente sobre K, então o número de zeros de x é $\leq [F : K(x)]$ (proposição anterior) que é finito. Pelo mesmo argumento x^{-1} tem finitos zeros, donde temos que x tem também finitos pólos.

□

1.4 Divisores

O corpo de constantes $\tilde{K}$ de F/K é uma extensão finita de K (Corolário 1.1.15), e F pode ser visto como corpo de funções sobre $\tilde{K}$. Logo, a seguinte hipótese não é crucial para a teoria:

A partir de agora, F/K denota sempre um corpo de funções de um variável tal que $K = \tilde{K}$.

Definição 1.4.1. O grupo de divisores de F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K, denotado por $\mathrm{Div}(F)$. Os elementos de $\mathrm{Div}(F)$ são chamados de divisores de F/K. Ou seja, um divisor é uma soma

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

com $n_P \in \mathbb{Z}$, quase todos nulos.

O suporte de D é definido como

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

Também é conveniente escrever

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

onde $S \subseteq \mathbb{P}_F$ é finito com $\mathrm{supp}(D) \subseteq S$.

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado um divisor primo. Dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ são somados pelos coeficientes: $D = \sum (n_P + n'_P)P$.

O elemento neutro do grupo de divisores $\mathrm{Div}(F)$ é o divisor $0 := \sum_{P \in \mathbb{P}_F} r_P P$, onde $r_P = 0$.

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P \in \mathbb{P}_F} n_P P \in \mathrm{Div}(F)$, definimos $v_Q(D) := n_Q$. Assim $\mathrm{supp}(D) = \{P \in \mathbb{P}_F / v_P(D) \neq 0\}$ e $D = \sum_{P \in \mathbb{P}_F} v_P(D) P$.

Uma ordem parcial é definida em $\mathrm{Div}(F)$:

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

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

Um divisor $D \geq 0$ é chamado positivo ou efetivo.

O grau de um divisor é definido por $\deg D := \sum_{P \in \mathbb{P}_F} v_P(D) \deg P$

Observemos que $\deg : \mathrm{Div}(F) \to \mathbb{Z}$ é um homomorfismo.

Pelo Corolário 1.3.4, um elemento $x \in F$ não nulo tem somente uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Assim podemos definir:

Definição 1.4.2. Sejam $0 \neq x \in F$ e Z (respectivamente N) o conjunto de zeros (respectivamente pólos) de x em $\mathbb{P}_F$. Definimos:

$$(x)_0 := \sum_{P \in Z} v_P(x)P \text{ o divisor de zeros de } x,$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x))P \text{ o divisor de pólos de } x \text{ e}$$

$$(x) := (x)_0 - (x)_\infty \text{ o divisor principal de } x.$$

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

O elemento $0 \neq x \in K$ pode ser visto como:

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

pois estamos assumindo $K = \tilde{K}$ e já temos que $\tilde{K} \subset O_P^*, \forall P \in \mathbb{P}_F$.

Definição 1.4.3. O conjunto dos divisores $\mathrm{Princ}(F) := \{(x)/0 \neq x \in F\}$ é chamado de grupo de divisores principais de F/K.

Veja que $(xy) = (x) + (y) \forall x, y \in F$ não nulos, donde temos $\mathrm{Princ}(F)$ é subgrupo de $\mathrm{Div}(F)$.

O grupo de fatoração $\mathrm{Cl}(F) := \frac{\mathrm{Div}(F)}{\mathrm{Princ}(F)}$ é chamado de grupo das classes de divisores de F/K. Para $D \in \mathrm{Div}(F)$, o elemento correspondente no grupo de fatoração $\mathrm{Cl}(F)$ é denotado $[D]$, a classe de divisores de D.

Dois elementos $D, D' \in \mathrm{Div}(F)$ são equivalentes ($D \equiv D'$) se $[D] = [D']$, ou seja, $D = D' + (x)$ para algum $(x) \in \mathrm{Princ}(F)$ (ou seja, para algum $0 \neq x \in F$).

Definição 1.4.4. Para um divisor $A \in \mathrm{Div}(F)$, definimos o espaço de Riemann-Roch associado a A por:

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

Esta definição pode ser interpretada como:

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

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

2. x pode ter pólos somente em P_i, com ordem limitada por $n_i, i = 1, ..., r$.

Observação 1.4.5. Veja ainda que para cada $A \in \mathrm{Div}(F)$, temos:

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

2. $\mathcal{L}(A) \neq \{0\} \Leftrightarrow \exists A' \in \mathrm{Div}(F)$ onde $A' \equiv A$ com $A' \geq 0$.

Lema 1.4.6. *Seja $A \in \mathrm{Div}(F)$, então:*

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

2. *Se A' é um divisor equivalente a A, então $\mathcal{L}(A) \cong \mathcal{L}(A')$, (isomorfos como espaços vetoriais sobre K).*

Demonstração. 1. Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$, temos $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A)$ e $v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A), \forall P \in \mathbb{P}_F$, logo $x + y \in \mathcal{L}(A)$ e $ax \in \mathcal{L}(A)$.

2. Como $A \equiv A' \Rightarrow A - A' \in \mathrm{Princ}(F)$, logo existe $z \in F$ não nulo onde $A = A' + (z)$. Assim considere a aplicação $\varphi : \mathcal{L}(A) \to F$, onde $x \mapsto \varphi(x) = xz$. Veja que se $x, y \in \mathcal{L}(A)$ e $a \in K$, então $\varphi(x + ay) = (x + ay)z = xz + ayz = \varphi(x) + a\varphi(y)$. Logo φ é K-linear.

Veja ainda que $\varphi(x) \in \mathcal{L}(A')$. De fato:

$$x \in \mathcal{L}(A) \Rightarrow (x) \geq -A \Rightarrow (x) \geq -(A' + (z)) \Rightarrow (x) \geq -A' - (z) \Rightarrow$$

$$v_P(x) \geq -v_P(A' + (z)), \forall P \in \mathbb{P}_F \Rightarrow v_P(x) \geq -v_P(A') - v_P(z), \forall P \in \mathbb{P}_F.$$

Logo, $v_P(xz) = v_P(x) + v_P(z) \geq -v_P(A') - v_P(z) + v_P(z) = -v_P(A')$, $\forall P \in \mathbb{P}_F$.

Portanto, $xz \in \mathcal{L}(A')$.

De forma análoga, definindo $\varphi' : \mathcal{L}(A') \to F$, tal que $x \mapsto xz^{-1}$, temos φ' $K-$linear e $\varphi'(\mathcal{L}(A')) \subset \mathcal{L}(A)$. Como φ e φ' são uma a inversa da outra, temos que φ estabelece um isomorfismo entre $\mathcal{L}(A)$ e $\mathcal{L}(A')$.

□

Lema 1.4.7. *1.* $\mathcal{L}(0) = K$*;*

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

Demonstração. 1. Veja que $\forall x \in K$ não nulo, $(x) = 0 \Rightarrow (x) \geq -0 = 0 \Rightarrow x \in \mathcal{L}(0) \underbrace{\Rightarrow}_{0 \in \mathcal{L}(0)} K \subset \mathcal{L}(0)$.

Seja agora $0 \neq x \in \mathcal{L}(0) \Rightarrow (x) \geq -0 = 0$, ou seja, $v_P(x) \geq 0, \forall P \in \mathbb{P}_F \Rightarrow x$ não tem pólos, isto é, $x \in \tilde{K} = K \Rightarrow \mathcal{L}(0) \subset K$ (Corolário 1.1.19).

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

2. Suponha por absurdo que $\exists x \in \mathcal{L}(A)$ não nulo. Assim $(x) \geq -A \Rightarrow (x) > 0$. Daí, $v_P(x) > 0, \forall P \in \mathbb{P}_F$, ou seja, x tem zeros mas não tem pólos, contrariando o Corolário 1.1.19.

□

Lema 1.4.8. *Sejam* $A, B \in \mathrm{Div}(F)$ *com* $A \leq B$*. Então* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e* $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A$.

Demonstração. Seja $x \in \mathcal{L}(A) \Rightarrow (x) \geq -A \geq -B \Rightarrow x \in \mathcal{L}(B)$. Portanto, $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.

Mostremos agora o que falta para o caso $B = A + P$, onde $P \in \mathbb{P}_F$, os demais casos seguirão por indução.

Tome $t \in F$ onde $v_P(t) = v_P(B) = v_P(A) + 1$. Seja $x \in \mathcal{L}(B)$, veja que: $v_P(x) \geq -v_P(B) = -v_P(t) \Rightarrow v_P(x) + v_P(t) \geq 0 \Rightarrow v_P(xt) \geq 0 \Rightarrow xt \in O_P$.

Defina: $\psi : \mathcal{L}(B) \to F_P = O_P/P$, onde $x \mapsto \psi(x) = (xt)(P)$.

Seja agora $x \in \mathcal{L}(B)$, observemos que $x \in \ker\psi \Leftrightarrow (xt)(P) = 0(P) \Leftrightarrow xt \in P \Leftrightarrow v_P(xt) > 0 \Leftrightarrow v_P(x) + v_P(t) > 0 \Leftrightarrow v_P(x) > -v_P(t) \Leftrightarrow v_P(x) \geq 1 - v_P(t) = 1 - v_P(B) = -v_P(A) \Leftrightarrow x \in \mathcal{L}(A)$. Portanto, $\ker\psi = \mathcal{L}(A)$.

Donde temos que ψ induz uma aplicação $K-$linear injetora de $\mathcal{L}(B)/\mathcal{L}(A)$ em $O_P/P = F_P$.

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

No caso $B = A+P+Q$, temos, fazendo $A' = A+P$ e $B = A'+Q$: $\dim(\mathcal{L}(B)/\mathcal{L}(A')) < \infty$ e $\dim(\mathcal{L}(A')/\mathcal{L}(A)) < \infty$, além disso $(\mathcal{L}(B)/\mathcal{L}(A))/(\mathcal{L}(A')/\mathcal{L}(A)) \cong \mathcal{L}(B)/\mathcal{L}(A')$, donde temos que $\mathcal{L}(B)/\mathcal{L}(A)$ tem dimensão finita e $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim(\mathcal{L}(B)/\mathcal{L}(A'))+ \dim(\mathcal{L}(A')/\mathcal{L}(A))$.

Para o caso $B = A + D$, onde $0 \leq D \in \mathrm{Div}(F)$, podemos escrever $B = \sum_{i=1}^{n} Q_i + Q_{n+1} + A$. Tomar a hipótese de indução para $B\sum_{i=1}^{n} Q_i + A'$ e $A' = A + Q_{n+1}$ e repitir o argumento do caso anterior.

□

Proposição 1.4.9. *Para cada divisor $A \in \mathrm{Div}(F), \mathcal{L}(A)$ é um espaço vetorial de dimensão finita sobre K. Mais precisamente, se $A = A_+ - A_-$, com A_+ e A_- divisores positivos, então:*

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

Demonstração. Veja que $A = A_+ - A_- \leq A_+ + 0 = A_+ \Rightarrow A \leq A_+ \Rightarrow \mathcal{L}(A) \subseteq \mathcal{L}(A_+)$.

Mostremos agora que $\dim \mathcal{L}(A) \leq \deg A_+ + 1$: temos $A_+ \geq 0$, assi pelo Lema 1.4.8, $\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq \deg A_+$. Além disso $\mathcal{L}(0) = K$, assim: $\dim \mathcal{L}(A_+) \leq \dim(\mathcal{L}(A_+)/\mathcal{L}(0))+ 1 \leq \deg A_+ + 1$. Portanto, $\dim \mathcal{L}(A) \leq \deg A_+ + 1$.

□

Definição 1.4.10. Seja $A \in \mathrm{Div}(F)$, o inteiro $\ell(A) := \dim \mathcal{L}(A)$ é chamado de dimensão

do divisor A.

Teorema 1.4.11. *Todo divisor principal tem grau zero. Mais precisamente: seja $x \in F\backslash K$ e $(x)_0$, respectivamente $(x)_\infty$, o divisor de zeros, respectivamente o divisor de pólos, de x. Então:* $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

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

$$\deg B = \deg(x)_\infty = \sum_{i=1}^{r} v_i(x)_\infty \deg P_i = \sum_{i=1}^{r} -v_i(x) \deg P_i = \sum_{i=1}^{r} v_i(x^{-1}) \deg P_i.$$

Logo pela Proposição 1.3.3, temos $\deg B = \sum_{i=1}^{r} v_i(x^{-1}) \deg P_i \leq [F : K(x^{-1})] = [F : K(x)] = n$.

Portanto $\deg B \leq n$.

Mostremos agora que $n \leq \deg B$.

Seja $\{u_1, ..., u_n\}$ uma base de F sobre $K(x)$ e $0 \leq C \in \mathrm{Div}(F)$ tal que $(u_j) \geq -C$, $j = 1, ..., n$.

Temos: $\ell(\lambda B + C) = \dim(\mathcal{L}(\lambda B + C)) \geq n(\lambda + 1), \forall \lambda \geq 0$, inteiro.

De fato, seja $0 \leq i \leq \lambda$ e $1 \leq j \leq n$, considere o elemento $x^i u_j$, veja que $(x^i u_j) = (x^i) + (u_j) = i(x) + (u_j) \geq -iB - C \geq -\lambda B - C = -(\lambda B + C)$. Logo $x^i u_j \in \mathcal{L}(\lambda B + C)$.

Temos também que o conjunto $\{x^i u_j; 0 \leq i \leq \lambda \text{ e } 1 \leq j \leq n\}$ é l.i. De fato, se não fosse, teríamos: $\sum_{i,j} a_{ij} x^i u_j = 0, a_{ij} \in K$ não todos nulos. Daí $\sum_j (\sum_i a_{ij} x^i) u_j = 0, \sum_i a_{ij} x^i \in K(x)$ não todos nulos. E assim teríamos $\{u_1, ..., u_n\}$ l.d. sobre $K(x)$, gerando o absurdo. Logo $\ell(\lambda B + C) \geq n(\lambda + 1)$, $\forall \lambda \geq 0$.

Agora definindo $c := \deg C$, temos: $n(\lambda + 1) \leq \ell(\lambda B + C) \leq \deg(\lambda B + C)_+ + 1 = \deg(\lambda B)_+ + \deg C_+ + 1 = \lambda \deg B + \deg C + 1$, pois $B \geq 0$ e $C \geq 0$. Ou seja, $n(\lambda + 1) \leq \lambda \deg B + \deg C + 1, \forall \lambda \geq 0$.

Assim, $n\lambda + n \leq \lambda \deg B + \deg C + 1 = \lambda \deg B + c + 1 \Rightarrow n - c - 1 \leq \lambda(\deg B - n), \forall \lambda \in \mathbb{N}$.

Veja agora que se $\deg B < n \Rightarrow \deg B - n < 0$, e assim para λ suficientemente grande teríamos $\lambda(\deg B - n) < n - c - 1$, pois $n - c - 1$ não depende de λ, gerando uma contradição. Logo $\deg B \geq n$.

Portanto, $\deg(x)_\infty = n$, ou seja, $\deg(x)_\infty = [F : K(x)]$. E, como $(x)_0 = (x^{-1})_\infty$, temos $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$ e assim $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

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

□

Corolário 1.4.12. *1. Sejam $A, A' \in \mathrm{Div}(F)$ tais que $A \equiv A'$, então temos $\ell(A) = \ell(A')$ e $\deg A = \deg A'$;*

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

3. Para $A \in \mathrm{Div}(F)$, onde $\deg A = 0$, são equivalentes:

(a) A é principal;

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

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

Demonstração. 1. $A \equiv A'$, assim pelo Lema 1.4.6, temos $\mathcal{L}(A) \cong \mathcal{L}(A')$, daí $\ell(A) = \ell(A')$. Além disso, $A \equiv A' \Rightarrow \exists x \in F$ não nulo onde $A - A' = (x)$, e, pelo Teorema 1.4.11, $\deg(x) = \deg(A - A') \Rightarrow \deg A = \deg A'$.

2. Seja $A \in \mathrm{Div}(F)$ tal que $\ell(A) > 0$, pela observação 1.4.5, $\exists A' \geq 0$ onde $A \equiv A'$. Assi pelo item anterior $\deg A = \deg A' \geq 0$. Logo, $\ell(A) > 0 \Rightarrow \deg A \geq 0$ e portanto $\deg A < 0 \Rightarrow \ell(A) = 0$.

3. $(a) \Rightarrow (b)$: Se $A = (x)$, então $(x^{-1}) = -(x) = -A$. Logo $x^{-1} \in \mathcal{L}(A) \Rightarrow \ell(A) \geq 1$.

   $(b) \Rightarrow (c)$: $\ell(A) \geq 0$ e $\deg A = 0 \Rightarrow \exists A' \geq 0$ onde $A' \equiv A \Rightarrow A' \geq 0$ e $\deg A' = 0 \Rightarrow A' = 0$. Assim, $\mathcal{L}(A) \cong \mathcal{L}(A') = \mathcal{L}(0) = K \Rightarrow \ell(A) = 1$.

   $(c) \Rightarrow (a)$: Se $\ell(A) = 1$ e $\deg A = 0$, tome $z \in \mathcal{L}(A)$ não nulo, então $(z) + A \geq 0$, assim $\deg((z) + A) = 0$ e $(z) + A \geq 0 \Rightarrow (z) + A = 0 \Rightarrow A = (z^{-1}) \Rightarrow A$ é principal.

□

Exemplo 1.4.13. Seja $F = K(x)$ um corpo de funções racionais. Seja $z \in K(x)$ não nulo, podemos escrever $z = a\frac{f(x)}{g(x)}$, com $a \in K$ e $f(x), g(x) \in K[x]$ mônicos e relativamente

primos. Sejam $f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}$ e $g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$ as decomposições em fatores primos de $f(x)$ e $g(x)$.

Então o divisor principal de z em $\mathrm{Div}(K(x))$ é dado por:

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

onde P_i e Q_j são os lugares correspondentes a $p_i(x)$ e $q_j(x)$, respectivamente.

Da Proposição 1.4.9, temos $\ell(A) \leq \deg A + 1, \forall A \geq 0$. Afim de verificar isso tome $\ell(A) > 0$. Daí $A \equiv A'$ para algum $A' \geq 0 \Rightarrow \ell(A) = \ell(A') \leq \deg A' + 1 = \deg A + 1$, pelo Corolário 1.4.12.

Proposição 1.4.14. *Existe $\gamma \in \mathbb{Z}$ tal que $\forall A \in \mathrm{Div}(F)$ vale: $\deg A - \ell(A) \leq \gamma$, onde γ não depende de A, dependendo apenas de F/K.*

Demonstração. Observe inicialmente que se $A_1 \leq A_2$, então $\dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leq \deg A_2 - \deg A_1$ e assim:

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

pelo Lema 1.4.8 ($\star\star\star$).

Seja $x \in F \backslash K$ fixado. Considere o divisor $B := (x)_\infty$. Como feito na demonstração do Teorema 1.4.11, $\exists C \geq 0$ divisor onde C depende de x e $\ell(\lambda B + C) \geq (\lambda + 1)\deg B, \forall \lambda \geq 0$.

Mas pelo Lema 1.4.8, temos:

$$\deg C \geq \dim(\mathcal{L}(\lambda B + C)/\mathcal{L}(\lambda B)) = \ell(\lambda B + C) - \ell(\lambda B)$$

$$\Rightarrow \ell(\lambda B + C) \leq \ell(\lambda B) + \deg C.$$

Assim, $\ell(\lambda B) + \deg C \geq (\lambda+1)\deg B \Rightarrow \ell(\lambda B) \geq (\lambda+1)\deg B - \deg C = \lambda \deg B + \deg B - \deg C = \lambda \deg B + (\underbrace{\deg B}_{=[F:K(x)]} - \deg C) \Rightarrow \ell(\lambda B) \geq \lambda \deg B + \underbrace{([F : K(x)] - \deg C)}_{-\gamma}, \forall \lambda \geq 0.$

$$\Rightarrow \ell(\lambda B) \geq \lambda \deg B - \gamma, \forall \lambda \geq 0$$

$$\Rightarrow \deg \lambda B - \ell(\lambda B) \leq \gamma, \forall \lambda \geq 0 (\star\star).$$

Mostremos que podemos substituir λB por $A \in \mathrm{Div}(F)$, sem alterar γ.

Dado $A \in \mathrm{Div}(F)$, existem $A_1, D \in \mathrm{Div}(F)$ e $\lambda \in \mathbb{Z}$, tais que $A \leq A_1$, $A_1 \equiv D$ e $D \leq \lambda B$.

De fato, tome $A_1 \geq A$ tal que $A_1 \geq 0$, então $\lambda B - A_1 \leq A_1$, logo pelo Lema 1.4.8 temos $\dim(\lambda B / \lambda B - A_1) \leq \deg(\lambda B) - \deg(\lambda B - A_1) \Rightarrow \ell(\lambda B) - \ell(\lambda B - A_1) \leq \deg(\lambda B) - \deg(\lambda B - A_1) = \deg A_1$. Portanto, $\ell(\lambda B - A_1) \geq \ell(\lambda B) - \deg A_1 (\star)$.

Temos então:

$$\ell(\lambda B - A_1) \underbrace{\geq}_{(\star)} \ell(\lambda B) - \deg A_1 \underbrace{\geq}_{(\star\star)} \lambda \deg(B) - \gamma - \deg A_1.$$

Assim, para λ suficientemente grande $\ell(\lambda B - A_1) > 0$. Tome $0 \neq z \in \mathcal{L}(\lambda B - A_1)$, defina $D := A_1 - (z)$, então $A_1 \equiv D$ e $D = A_1 - (z) \leq A_1 + (\lambda B - A_1) = \lambda B$.

Logo, $\deg A - \ell(A) \underbrace{\leq}_{(\star\star\star)} \deg A_1 - \ell(A_1) \underbrace{=}_{Cor.1.4.12} \deg D - \ell(D) \underbrace{\leq}_{(\star\star\star)} \deg \lambda B - \ell(\lambda B) \leq \gamma$.

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

□

Definição 1.4.15. O gênero g de F/K é definido por:

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

Corolário 1.4.16. *O gênero de F/K é não negativo.*

Demonstração. Veja que $\deg 0 - \ell(0) + 1 = 0 \Rightarrow g \geq 0$.

□

Teorema 1.4.17. *(Teorema de Riemann)*

Seja F/K um corpo de funções de gênero g. Temos então:

1. $\forall A \in \mathrm{Div}(F), \ell(A) \geq \deg A + 1 - g$;
2. $\exists c \in \mathbb{Z}$, *dependendo somente de* F/K *tal que* $\ell(A) = \deg A + 1 - g, \forall A \in \mathrm{Div}(F)$ *com* $\deg A \geq c$.

Demonstração. 1. Segue direto da definição de gênero.

2. Seja $A_0 \in \mathrm{Div}(F)$ tal que $g = \deg A_0 - \ell(A_0) + 1$. Defina $c := g = \deg A_0 + g$. Assim se $\deg A \geq c$, temos $\ell(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g = 1$. Tome $z \in \mathcal{L}(A - A_0)$ não nulo. Defina $A' = A + (z) \geq A_0$. Temos $A \equiv A'$, e assim $\deg A - \ell(A) = \deg A' - \ell(A') \geq \deg A_0 - \ell(A_0) = g - 1$. Logo, $\deg A - \ell(A) \geq g - 1 \Rightarrow \ell(A) \leq \deg A + 1 - g$. Portato, pelo item anterior, $\ell(A) = \deg A + 1 - g$.

□

Exemplo 1.4.18. Em um corpo de funções racionais $K(x)/K$, temos que o gênero é $g = 0$.

Sejam P_∞ pólo de x e $r \geq 0$ inteiro, considere o espaço vetorial $\mathcal{L}(rP_\infty)$. Veja que $\{1, x, ..., x^r\} \subset \mathcal{L}(rP_\infty)$, daí $1 + r \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$, para r suficientemente grande. Donde temos $g \leq 0$, e portanto pelo Corolário 1.4.16 temos $g = 0$.

1.5 O Teorema de Riemann-Roch

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

Definição 1.5.1. Para $A \in \mathrm{Div}(F)$, o inteiro

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

é chamado de índice de especialidade de A.

O Teorema 1.4.17 (Teorema de Riemann) nos diz que $i(A)$ é um inteiro não negativo e que $i(A) = 0$ para $\deg A$ suficientemente grande.

Definição 1.5.2. Um adele de F/K é uma aplicação $\alpha : \mathbb{P}_F \to F$, $P \mapsto \alpha_P$, tal que $\alpha_P \in O_P$ para quase todo $P \in \mathbb{P}_F$.

Consideramos um adele como um elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$ e portanto usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$, ou, ainda menor, $\alpha = (\alpha_P)$.

O conjunto $\mathcal{A}_F := \{\alpha; \alpha \text{ é um adele de } F/K\}$ é chamado de espaço adele de F/K. Este conjunto é considerado um espaço vetorial sobre K de forma óbvia.

O adele principal de um elemento $x \in F$ é o adele cuja totalidade das componentes são iguais a x, o que faz sentido, pois x tem no máximo finitos pólos.

A definição de adele principal nos fornece um mergulho $F \hookrightarrow \mathcal{A}_F$, e a função valorização v_P de F/K é naturalmente extendida para $\mathcal{A}_F$ por $v_P(\alpha) := v_P(\alpha_P)$, onde α_P é a $P-$componente do adele α. Por definição, temos $v_P(\alpha) \geq 0$, para quase todo $P \in \mathbb{P}_F$.

Definição 1.5.3. Para $A \in \mathrm{Div}(F)$ definimos:

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

o $K-$espaço de $\mathcal{A}_F$.

Teorema 1.5.4. *Para cada $A \in \mathrm{Div}(F)$, o índice de especialidade de A é dado por:*

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

Demonstração. Vamos dividir a demonstração em passos:

1. Sejam $A_1, A_2 \in \mathrm{Div}(F)$ e $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e $\dim(A_2/A_1) = \deg A_2 - \deg A_1$.

   De fato, se $A_1 \leq A_2 \Rightarrow -A_2 \leq -A_1$. Assim se $\alpha \in \mathcal{A}_F(A_1) \Rightarrow v_P(\alpha) \geq -v_P(A_1) \geq -v_P(A_2), \forall P \in \mathbb{P}_F \Rightarrow \alpha \in \mathcal{A}_F(A_2)$. Portanto, $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.

   Falta agora mostramos que $\dim(A_2/A_1) = \deg A_2 - \deg A_1$. Mostremos para o caso em que $A_2 = A_1 + P$, e o caso geral segue por indução, como no Lema 1.4.8.

   Escolha $t \in F$ tal que $v_P(t) = v_P(A_1) + 1$ e considere a aplicação $K-$linear: $\varphi : \mathcal{A}_F(A_2) \to F_P, \alpha \mapsto (t\alpha_P)(P)$. Como no Lema 1.4.8, φ está bem definida e $\ker \varphi = \mathcal{A}_F(A_1)$. Temos também que φ é sobrejetora, pois seja $\beta \in O_P$, tome $\alpha \in \mathcal{A}_F$ tal que $\alpha = (\alpha_Q)$, onde $\alpha_Q = t_Q^{1-v_Q(A_2)}$, t_Q é primo de $Q, \forall Q \in \mathbb{P}_F$ e $Q \neq P$, e $\alpha_P = \frac{\beta}{t}$. Logo, $\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \cong F_P \Rightarrow \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = [F_P : K] = \deg P = \deg A_2 - \deg A_1$.

2. Sejam $A_1, A_2 \in \mathrm{Div}(F)$ e $A_1 \leq A_2$ como antes, então:

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

De fato, temos a sequência exata de aplicações lineares:

$$\{0\} \to \mathcal{L}(A_2)/\mathcal{L}(A_1) \stackrel{\varphi_1}{\to} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \stackrel{\varphi_2}{\to} (\mathcal{A}_F(A_2)+F)/(\mathcal{A}_F(A_1)+F) \to \{0\},$$

onde $\varphi_1 : \mathcal{L}(A_2)/\mathcal{L}(A_1) \to \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1), a+\mathcal{L}(A_1) \mapsto a+\mathcal{A}_F(A_1)$, é injetora e $\varphi_2 : \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \to \mathcal{A}_F(A_2)+F/\mathcal{A}_F(A_1)+F, a+\mathcal{A}_F(A_1) \mapsto a+\mathcal{A}_F(A_1)+F$, é sobrejetora.

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

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

Seja B_1 divisor tal que $B_1 \geq B$, então pelo Lema 1.4.8: $\ell(B_1) \leq \deg B_1 + \ell(B) - \deg(B) = \deg B_1 + \deg B + 1 - g - \deg B = \deg B_1 + 1 - g$. Mas pelo primeiro item do teorema de Riemann: $\ell(B_1) \geq \deg B_1 + 1 - g$.

Assim $\ell(B_1) = \deg B_1 + 1 - g, \forall B_1 \geq B$. Seja agora $\alpha \in \mathcal{A}_F$, tome $B_1 \geq B$ tal que $\alpha \in \mathcal{A}_F(B_1)$ então pelo passo anterior, temos:

$\dim((\mathcal{A}_F(B_1)+F)/(\mathcal{A}_F(B)+F)) = (\deg B_1 - \ell(B_1)) - (\deg B - \ell(B)) = (g-1) - (g-1) = 0$, logo $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$, daí $\alpha\mathcal{A}_F(B_1) = \mathcal{A}_F(B) + F$.

Portanto, $\mathcal{A}_F \subset \mathcal{A}_F(B) + F$, e como $\mathcal{A}_F(B) + F \subset \mathcal{A}_F$, temos por fim que $\mathcal{A}_F(B) + F = \mathcal{A}_F$.

Demosntremos agora o teorema.

Seja $A \in \mathrm{Div}(F)$, pelo segundo item do teorema de Riemann, existe $A_1 \geq A$ tal que $\ell(A_1) = \deg A_1 + 1 - g$, donde temos pelo terceiro passo temos $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$. Logo:

$$\dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) = \dim((\mathcal{A}_F(A_1)+F)/(\mathcal{A}_F(A)+F)) =$$

$$= (\deg A_1 - \ell(A_1)) - (\deg A - \ell(A)) = (g-1) + \ell(A) - \deg A = i(A).$$

□

Corolário 1.5.5. $g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Demonstração.

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

□

Podemos, a partir do Teorema 1.5.4, escrever:

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

Definição 1.5.6. Um diferencial de Weil de F/K é uma aplicação $K-$linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A) + F$ para algum divisor $A \in \mathrm{Div}(F)$. E chamamos:

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

o conjunto de diferenciais de Weil de F/K.

Para cada $A \in \mathrm{Div}(F)$ temos:

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

Podemos considerar Ω_F um $K-$espaço vetorial. De fato, se ω_1 se anula em $\mathcal{A}_F(A_1)+F$ e ω_2 se anula em $\mathcal{A}_F(A_2) + F$, tome $A_3 \in \mathrm{Div}(F)$ tal que $A_3 \leq A_1$ e $A_3 \leq A_2$, assim $\mathcal{A}_F(A_3)+F \subset \mathcal{A}_F(A_1)+F$ e $\mathcal{A}_F(A_3)+F \subset \mathcal{A}_F(A_2)+F$. Logo $\mathcal{A}_F(A_3)+F \subset (\mathcal{A}_F(A_1)+F) \cap (\mathcal{A}_F(A_2) + F)$. Portanto, $\omega_1 + \omega_2$ se anula em $\mathcal{A}_F(A_3) + F$.

Lema 1.5.7. *Para $A \in \mathrm{Div}(F)$, temos* $\dim \Omega_F(A) = i(A)$.

Demonstração. Seja $(\mathcal{A}_F/(\mathcal{A}_F(A)+F))^*$ conjunto dos funcionais $K-$lineares de $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$. Defina $\varphi : \Omega_F \to (\mathcal{A}_F/(\mathcal{A}_F(A) + F))^*$, $\omega \mapsto \overline{\omega}$, onde $\overline{\omega}$ é aplicação dada por

$\overline{\omega}(a + \mathcal{A}_F(A) + F) = \omega(a)$. Temos que φ é $K-$linear e bijetora. Donde temos $\Omega_F \cong \mathcal{A}_F/(\mathcal{A}_F(A) + F)^*$, e assim:

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

□

Definição 1.5.8. Para $x \in F$ e $\omega \in \Omega_F$, definimos $x\omega : \mathcal{A}_F \to K$ por $(x\omega)(a) = \omega(xa)$.

Veja que $x\omega \in \Omega_F$, pois temos $\omega \in \Omega_F$, então $\exists A \in \mathrm{Div}(F)$ onde ω se anula em $\mathcal{A}_F(A) + F$. Seja agora $a \in \mathcal{A}_F(A + (x)) + F$, então $a = \alpha + f$ onde $\alpha \in \mathcal{A}_F(A + (x))$ e $f \in F$, destarte $xa = x\alpha + xf$, onde $\alpha \in \mathcal{A}_F(A + (x))$ e $xf \in F$.

Mostremos que $x\alpha \in \mathcal{A}_F(A)$.

Para quase todo $P \in \mathbb{P}_F, v_P(\alpha_P) \geq -v_P(A+(x)) = -v_P(A) - v_P(x)\ v_P(x) + v_P(\alpha_P) \geq -v_P(A)$, para quase todo $P \in \mathbb{P}_F$, assim $v_P(x\alpha_P) \geq -v_P(A) \Rightarrow v_P(x\alpha) \geq -v_P(A)$ para quase todo $P \in \mathbb{P}_F$. Logo, $x\alpha \in \mathcal{A}_F(A)$ e portanto $xa \in \mathcal{A}_F(A) + F$, assim temos que $x\omega$ se anula em $\mathcal{A}_F(A + (x))$. Concluimos então que $x\omega \in \Omega_F$.

Logo, Ω_F é um $F-$espaço vetorial, com esta definição.

Proposição 1.5.9. *Ω_F é um espaço vetorial de dimensão 1 sobre F.*

Demonstração. Seja $\omega_1 \in \Omega_F$ não nulo. Mostremos que para todo $\omega_2 \in \Omega_F$, $\exists z \in F$ tal que $\omega_2 = z\omega_1$.

Sendo então $\omega_2 \in \Omega_F$, se $\omega_2 = 0$, tome $z = 0$. Agora, se $\omega_2 \neq 0$, tome $A_1, A_2 \in \mathrm{Div}(F)$ tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$.

Seja $B \in \mathrm{Div}(F)$, considere as aplicações $K-$lineares injetoras:

$$\varphi_i : \mathcal{L}(A_i + B) \to \Omega_F(-B), x \mapsto x\omega_i.$$

Como $xb \in \mathcal{A}_F(A_i) + F$ e $\omega \in \Omega_F(A_i)$, temos a boa definição das aplicações.

Afirmação: Para uma escolha apropriada de B, temos:

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

Com esta afirmação, temos que existem $x_i \in \mathcal{L}(A_i + B)$, não nulos, onde $x_1\omega_1 = x_2\omega_2$ e por fim $\omega_2 = x_2^{-1}x_1\omega_1$, como queríamos. Provemos agora a afirmação com o seguinte fato: se V é espaço vetorial tal que $dimV < \infty$ e $U_1, U_2 \leq V$, então:

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

Seja então $B > 0$ divisor com grau suficientemente grande tal que $\ell(A_i+B) = \deg(A_i+B) + 1 - g$, para $i = 1, 2$ (teorema de Riemann). Pela boa definição de φ_i, temos que $U_i := \varphi_i(\mathcal{L}(A_i + B)) \subset \Omega_F(-B)$. Além disso, $\dim \Omega_F(-B) = i(-B) = \dim \mathcal{L}(-B) - \deg(-B) + g - 1 = \deg B + g - 1$.

Logo, $\dim U_1 + \dim U_2 - \dim \Omega_F(-B) = \deg B + (\deg A_1 + \deg A_2 + 3(1 - g))$.

Tomando grau de B suficientemente grande, temos:

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

Portanto, $\dim(U_1 \cap U_2) > 0 \Rightarrow U_1 \cap U_2 \neq \{0\}$.

□

Agora para fixado diferencial de Weil ω, consideremos o conjunto de divisores:

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

Lema 1.5.10. *Seja $\omega \in \Omega_F$ não nulo. Então existe um único divisor $W \in M(\omega)$ tal que $A \leq W, \forall A \in M(\omega)$.*

Demonstração. Pelo teorema de Riemann, existe uma constante c que depende apenas de F/K, onde $i(A) = 0, \forall A \in \mathrm{Div}(F)$ tal que $\deg A \geq c$. E, pelo Teorema 1.5.4, temos $\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$, e, como estamos tomando $\omega \neq 0$, temos $\mathcal{A}_F \neq \mathcal{A}_F(A) + F \Rightarrow i(A) \neq 0 \Rightarrow \deg A < c, \forall A \in M(\omega)$.

Tome W com grau máximo. Suponha que W não satisfaz a propriedade do lema, então existe $A_0 \in M(\omega)$ tal que não vale $A_0 \leq W$, isto é, $\exists Q \in \mathbb{P}_F$ onde $v_Q(A_0) > v_Q(W)$. Mostremos que $W + Q \in M(\omega)$, contrariando a maximalidade de W.

Considere o adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W+Q)$. Podemos escreve $\alpha = \alpha' + \alpha''$, onde $\alpha'_P = \alpha_P$ se $P \neq Q$ e $\alpha'_Q = 0$, e, $\alpha''_P = 0$ se $P \neq Q$ e $\alpha''_Q = \alpha_Q$. Assim $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in \mathcal{A}_F(A_0)$, portanto $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Logo ω se anula em $\mathcal{A}_F(W+Q) + F$, assim $W + Q \in M(\omega)$.

A unicidade segue da propriedade.

□

Definição 1.5.11. 1. O divisor (ω) de um diferencial de Weil $\omega \neq 0$ é o divisor unicamente determnado de F/K satisfazendo:

   (a) ω se anula em $\mathcal{A}_F((\omega)) + F$;

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

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

3. Um lugar P é dito ser zero (respectivamente pólo) de ω se $v_P(\omega) > 0$ (respectivamente $v_P(\omega) < 0$). O diferencial de Weil ω é dito regular em P se $v_P(\omega) \geq 0$, e ω é dito regular (ou holomorfo) se é regular $\forall P \in \mathbb{P}_F$;

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

Observação 1.5.12. Veja que:

$$\Omega_F(A) = \{\omega \in \Omega_F; \omega \text{ se anula em } \mathcal{A}_F(A) + F\} = \{\omega \in \Omega_F; \omega = 0 \text{ ou } (\omega) \geq A\}$$

e

$$\Omega_F(0) = \{\omega \in \Omega_F; \omega = 0 \text{ ou } (\omega) \geq 0\} = \{\omega \in \Omega_F; \omega = 0 \text{ ou } v_P(\omega) \geq 0, \forall P \in \mathbb{P}_F\}$$

$$= \{\omega \in \Omega_F; \omega = 0 \text{ ou } \omega \text{ é regular}\}.$$

Temos ainda pelo Lema 1.5.7 e pela Definição 1.5.1:

$$\dim \Omega_F(0) = i(0) = \ell(0) - \deg 0 + g - 1 = g.$$

Proposição 1.5.13. *1. Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$, temos $(x\omega) = (x) + (\omega)$;*

2. Quaisquer dois divisores canônicos de F/K são equivalentes.

Demonstração. 1. Se ω se anula em $\mathcal{A}_F(A) + F$, vimos que $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$, assim $A + (x) \leq (x\omega)$. Como ω anula $\mathcal{A}_F((\omega)) + F$, então $(\omega) + (x) \leq (x\omega)$. Analogamente, $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Daí, $(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (x) + (\omega)$ e portanto $(x\omega) = (x) + (\omega)$.

2. Sejam $(\omega_1), (\omega_2)$ divisores canônicos de F/K, então pela Proposição 1.5.9, existe $x \in F$ tal que $\omega_1 = x\omega_2$, assim $(\omega_1) = (x\omega_2) = (x) + (\omega_2) \Rightarrow (\omega_1) \equiv (\omega_2)$.

□

Teorema 1.5.14. *(Teorema da Dualidade)*

Seja $A \in \mathrm{Div}(F)$ e $W = (\omega)$ divisor canônico de F/K. Então a aplicação $\mu : \mathcal{L}(W - A) \to \Omega_F(A), x \mapsto x\omega$ é um isomorfismo de $K-$espaços vetoriais. Em particular $i(A) = \ell(W - A)$.

Demonstração. Seja $x \in \mathcal{L}(W - A) \Rightarrow (x\omega) = (x) + (\omega) \geq -(W - A) + W = A \Rightarrow (x\omega) \in \Omega_F(A)$. Portanto, μ está bem definida.

Como μ é $K-$linear e injetora, falta mostrar que μ é sobrejetora.

Seja $\omega_1 \in \Omega_F(A)$, pela Proposição 1.5.9 existe $x \in F$ tal que $x\omega = \omega_1$. Agora veja que $x \in \mathcal{L}(W - A)$:

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A \Rightarrow (x) \geq -W + A \Rightarrow x \in \mathcal{L}(W - A).$$

Portanto, $x \in \mathcal{L}(W - A)$ e $\mu(x) = \omega_1$, ou seja, μ é sobrejetora.

Portanto, $\dim \Omega_F(A) = \dim \mathcal{L}(W - A) = \ell(W - A)$ e pelo Lema 1.5.7, $\dim \Omega_F(A) = i(A) \Rightarrow \ell(W - A) = i(A)$.

□

Teorema 1.5.15. *(Teorema de Riemann-Roch)*

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

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

Demonstração. Pela definição de índice de especiabilidade, $i(A) = \ell(A) - \deg A + g - 1$. Assim pelo teorema anterior $\ell(A) - \deg A + g - 1 = \ell(W - A)$, e portanto, $\ell(A) = \deg A - g + 1 + \ell(W - A)$.

□

Corolário 1.5.16. *Para cada divisor canônico W, temos $\deg W = 2g - 2$ e $\ell(W) = g$.*

Demonstração. Fazendo $A = 0$, temos $\mathcal{L}(A) = K$ (Lema 1.4.7). Assim, $1 = \ell(0) = \deg 0 + 1 - g + \ell(W - 0)$, e portanto, $\ell(W) = g$.

Fazendo $A = W$, temos $\ell(W) = \deg W + 1 - g + \ell(W - W) = \deg W + 2 - g$. Assim, $g = \deg W + 2 - g$, e portanto, $\deg W = 2g - 2$.

□

Pelo teorema de Riemann, sabemos que existe uma constante c tal que $i(A) = 0, \forall A \in \mathrm{Div}(F)$ com $\deg A \geq c$. Mas podemos escolher de forma mais precisa esta constante.

Teorema 1.5.17. *Se $A \in \mathrm{Div}(F)$ é tal que $\deg A \geq 2g - 1$, então $\ell(A) = \deg A + 1 - g$.*

Demonstração. Pelo teorema de Riemann-Roch temos $\ell(A) = \deg A + 1 - g + \ell(W - A)$, onde W é qualquer divisor canônico. Tome $\deg A \geq 2g - 1$ e pelo corolário anterior temos $\deg W = 2g - 2$, assim $\deg(W - A) = \deg W - \deg A \leq 2g - 2 - 2g + 1 = -1 < 0$. E assim temos $\deg(W - A) < 0 \Rightarrow \ell(W - A) = 0$ e portanto, $\ell(A) = \deg A + 1 - g$.

□

O limite $2g - 1$ é o melhor possível, pois pelo Corolário 1.5.16, para W divisor canônico temos $\ell(W) = g > g - 1 = 2g - 2 + 1 - g = \deg W + 1 - g$, logo, $\ell(W) > \deg W + 1 - g$, e, $0 > \deg(W - A) = \deg W - \deg A$ $\deg A > \deg W = 2g - 2$. Portanto, $\deg A \geq 2g - 1$.

1.6 Algumas consequências do Teorema de Riemann-Roch

Proposição 1.6.1. *Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in \mathrm{Div}(F)$ satisfazem $\ell(A) = \deg A + 1 - g_0 + \ell(W_0 - A), \forall A \in \mathrm{Div}(F)$. Então $g_0 = g$ e W_0 é um divisor canônico.*

Demonstração. Fazendo $A = 0$ e respectivamente $A = W_0$, temos, como feito anteriormente, $\ell(W_0) = g_0$ e $\deg W_0 = 2g_0 - 2$.

Seja W um divisor canônico de F/K. Tome $A \in \mathrm{Div}(F)$ tal que $\deg A > \max\{2g - 2, 2g_0 - 2\} \Rightarrow \deg A \geq 2g - 1$. Logo pelo Teorema 1.5.17, temos $\ell(A) = \deg A + 1 - g$. Mas pela hipótese $\ell(A) = \deg A + 1 - g_0 + \ell(W_0 - A)$, onde $\deg A > \deg W_0$, e assim $\ell(A) = \deg A + 1 - g_0$. Daí $\deg A + 1 - g = \deg A + 1 - g_0 \Rightarrow g = g_0$.

Agora fazendo $A = W$, temos:

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

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

Veja agora que $\deg W_0 = \deg W = 2g - 2 \Rightarrow \deg(W_0 - W) = 0$. Assim, pelo Corolário 1.4.12, temos $W_0 - W$ é principal. Portanto $W \equiv W_0 \Rightarrow W_0 = (\omega) + (x) = (x\omega)$. Portanto W_0 é canônico.

□

Proposição 1.6.2. *Um divisor B é canônico se e somente se* $\deg B = 2g - 2$ *e* $\ell(B) \geq g$.

Demonstração. Suponha que $\deg B = 2g - 2$ e $\ell(B) \geq g$, tome W divisor cvanônico. Então:

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

$$\Rightarrow 1 \leq \ell(W - B).$$

Veja que $\deg(W - B) = 2g - 2 - 2g - 2 = 0$. Assim, pelo Corolário 1.4.12, temos $W - B$ é principal, logo $\exists x \in F$ não nulo tal que $W - B = (x) \Rightarrow (\omega) - B = (x)$ $\Rightarrow B - (\omega) = (x^{-1}) \Rightarrow B = (\omega) + (x^{-1}) = (x^{-1}\omega)$. Portanto B é divisor canônico.

□

Proposição 1.6.3. *Para um corpo de funções F/K as seguintes condições são equivalentes:*

1. *F/K é racional, isto é, $F = K(x)$ para algum $x \in F$ que é transcendente sobre K;*

2. F/K tem gênero 0, e existe $A \in \mathrm{Div}(F)$ com $\deg A = 1$.

Demonstração. $1 \Rightarrow 2$: Basta tomar $A = P_\infty$ e seguir o exemplo 1.4.18.

$2 \Rightarrow 1$: Se $g = 0$ e $\deg A = 1$, então $\deg A \geq 2g - 1$, logo $\ell(A) = \deg A + 1 - g = 2 \Rightarrow \mathcal{L}(A) \neq \{0\} \Leftrightarrow \exists A' \geq 0$ tal que $A' \equiv A \Rightarrow \ell(A') = 2$.

Como $A' \geq 0 \Rightarrow K \subset \mathcal{L}(A')$ e $\ell(A') = 2$, seja então $\{1, x\}$ base de $\mathcal{L}(A')$ sobre K, temos que $x \in \mathcal{L}(A')\backslash K$, e assim, $(x) \neq 0$ e $-A' \leq (x) \Rightarrow (x) + A' \geq 0$.

Agora pelo Corolário 1.4.12, temos $A' \geq 0$ e $\deg A' = 1$, o que nos implicará $A' = (x)_\infty$.

De fato, $A' \geq 0 \Rightarrow v_P(A') \geq 0, \forall P \in \mathbb{P}_F$, logo $\sum_{P \in \mathbb{P}_F} \underbrace{v_P(A')}_{\geq 0} \underbrace{\deg P}_{\geq 1} = 1 \Rightarrow A' = P \in \mathbb{P}_F$ com $\deg P = 1$.

Assim, $x \in \mathcal{L}(P) \Rightarrow (x) \geq -P \Rightarrow v_Q(x) \geq -v_Q(P), \forall Q \in \mathbb{P}_F$, donde temos $v_Q(x) \geq 0, \forall Q \in \mathbb{P}_F\backslash\{P\}$, e, $v_P(x) \geq -1$.

Se $v_P(x) \geq 0 \Rightarrow x$ não tem pólos $\Rightarrow x \in K$, gerando um absurdo.

Portanto, $v_P(x) = -1$ e $v_Q(x) \geq 0, \forall Q \in \mathbb{P}_F\backslash\{P\}$.

Daí, $(x)_\infty = -v_P(x)P = P \Rightarrow A' = (x)_\infty$.

Logo, pelo Teorema 1.4.11, temos $1 = \deg A' = \deg P = \deg(x)_\infty = [F : K(x)]$.

Portanto, $F = K(x)$.

□

Observação 1.6.4. Existe corpo de de funções não racionais de gênero 0 (estes não podem ter divisores de grau 1 pela proposição anterior). No entanto, se K é um corpo algebricamente fechado ou finito, sempre existe um divisor de grau 1 (para o caso algebricamente fechado, observação 1.1.16, já para o caso finito, será visto futuramente), portanto nestes casos teremos $g = 0 \Leftrightarrow F/K$ é racional.

Teorema 1.6.5. *(Teorema da aproximação forte)*

Seja $S \subsetneq \mathbb{P}_F$ subconjunto próprio de $\mathbb{P}_F$ e $P_1, ..., P_r \in S$. Suponha dados os elementos $x_1, ..., x_r \in F$ e os números inteiros $n_1, ..., n_r \in \mathbb{Z}$. Então existe um elemento $x \in F$ tal que:

1. $v_{P_i}(x - x_i) = n_i, i = 1, ..., r$;

2. $v_P(x) \geq 0, \forall P \in S\backslash\{P_1, ..., P_r\}$.

Demonstração. Considere o adele $\alpha = (\alpha_P)$ com $\alpha_P = x_i$ para $P = P_i, i = 1, ..., r$, e $\alpha_0 = 0$ caso contrário. Tome $Q \in \mathbb{P}_F \backslash S$. Pelos teoremas de Riemann e Teorema 1.5.4, para $m \in \mathbb{N}$ suficientemente grande,temos:

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

Logo $\alpha = \alpha' + z$ onde $\alpha' \in \mathcal{A}_F(mQ - \sum_{i=1}^{r}(n_i + 1)P_i)$ e $z \in F$, donde temos $z - \alpha \in \mathcal{A}_F(mQ - \sum_{i=1}^{r}(n_i + 1)P_i)$.

Assim, $v_{P_i}(z - x_i) = v_{P_i}(z - \alpha_{P_i}) = v_{P_i}(z - \alpha) \geq n_i + 1 > n_i$. Portanto, $v_{P_i}(z - x_i) > n_i, i = 1, ..., r$.

Para $P \in S\backslash\{P_1, ..., P_r\}$, temos $v_P(z) = v_P(z - 0) = v_P(z - \alpha_P) = v_P(z - \alpha) \geq -v_P(mQ - \sum_{i=1}^{r}(n_i + 1)P_i) = 0$. Portanto, $v_P(z) \geq 0, \forall P \in S\backslash\{P_1, ..., P_r\}$.

Tome agora $y_1, ..., y_r \in F$ tais que $v_{P_i}(y_i) = n_i$. De forma análoga, $\exists y \in F$ tal que $v_{P_i}(y - y_i) > n_i, i = 1, ..., r$ e $v_P(y) > 0, \forall P \in S\backslash\{P_1, ..., P_r\}$.

Assim, pela desigualdade triangular estrita:

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = n_i, i = 1, ..., r.$$

Defina $x := y + z$.

Temos $v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = n_i$, $i = 1, ..., r$ .E para $P \in S\backslash\{P_1, ..., P_r\}$, $v_P(x) = v_P(y + z) \geq \min\{v_P(y), v_P(z)\} \geq 0, \forall P \in S\backslash\{P_1, ..., P_r\}$.

□

Proposição 1.6.6. *Seja $P \in \mathbb{P}_F$. Então para cada $n \geq 2g$ inteiro, existe um elemento $x \in F$ com divisor de pólos $(x)_\infty = nP$.*

Demonstração. Considere os divisores $(n - 1)P$ e nP, veja que o grau destes divisores são $\geq 2g - 1$. Assim, pelo Teorema 1.5.17, temos $\ell((n - 1)P) = (n - 1)\deg P + 1 - g$ e $\ell(nP) = n \deg P + 1 - g$. Logo, $\ell((n - 1)P) < \ell(nP)$ e assim, $\mathcal{L}((n - 1)P) \subsetneq \mathcal{L}(nP)$. Tome $x \in \mathcal{L}(nP)\backslash\mathcal{L}((n - 1)P)$.

Temos que $(x)_\infty = nP$. De fato, temos 2 casos:

CASO I: $n = 0$

$x \in \mathcal{L}(0) = K$ e $\deg((n-1)P) < 0 \Rightarrow \mathcal{L}((n-1)P) = \{0\}$. Portanto, $x \in K\backslash\{0\}$. Logo $(x) = 0$ e assim, $(x)_\infty = 0 = 0P = nP$.

CASO II: $n > 0$

$x \in \mathcal{L}(nP)$, então x só pode ter pólo em P e de no máximo ordem n. Como $n > 0$ então $n - 1 \geq 0$ e assim $K \subset \mathcal{L}((n-1)P)$, donde temos $x \in F\backslash K$. Assim, x tem pelo menos um pólo. Portanto P é pólo de x de no máximo ordem n.

Veja agora que se a ordem do pólo P com respeito a x for menor que n, então $v_P(x) \geq -(n-1) = -v_P((n-1)P)$, o que implica $x \in \mathcal{L}((n-1)P)$, gerando um absurdo. Logo $v_P(x) = -n$ e portanto $(x)_\infty = nP$.

□

1.7 Componentes locais de diferenciais de Weil

Definição 1.7.1. Seja $P \in \mathbb{P}_F$.

1. Para cada $x \in F$, defina $i_P(x) \in \mathcal{A}_F$ o adele cuja $P-$componente é x, e todas as outras componentes são 0;

2. Para um diferencial de Weil $\omega \in \Omega_F$, definimos a componente local $\omega_P : F \to K$ por $\omega_P(x) := \omega(i_P(x))$.

Como $\omega \in \Omega_F$ é $K-$linear e i_P é $K-$linear, então ω_P é $K-$linear.

Proposição 1.7.2. *1. Seja $\omega \neq 0$ um diferencial de Weil de F/K e $P \in \mathbb{P}_F$, então $v_P(\omega) = \max\{r \in \mathbb{Z}; \omega_P(x) = 0, \forall x \in F$ com $v_P(x) \geq -r\}$. Em particular, ω_P não é identicamente nulo;*

2. Se $\omega, \omega' \in \Omega_F$ e $\omega_P = \omega'_P$ para algum lugar $P \in \mathbb{P}_F$, então $\omega = \omega'$.

Demonstração. 1. Por definição, $v_P(\omega) = v_P(W)$, onde $(\omega) = W$ é o divisor de ω. Seja $s := v_P(\omega)$.

Para $x \in F$ com $v_P(x) \geq -s$ temos $i_P(x) \in \mathcal{A}_F(W)$, então $\omega_P(x) = \omega(i_P(x)) = 0$. Logo, $s \in \{r \in \mathbb{Z}; \omega_P(x) = 0, \forall x \in F$ com $v_P(x) \geq -r\}$.

Suponha agora que $\omega_P(x) = 0, \forall x \in F$ tal que $v_P(x) \geq -s-1$. Seja $\alpha \in \mathcal{A}_F(W+P)$. Então $\alpha = (\alpha - i_P(\alpha_P)) + i_P(\alpha_P)$, onde $\alpha - i_P(\alpha_P) \in \mathcal{A}_F(W)$ e $v_P(\alpha_P) \geq -s-1$.

Logo, $\omega(\alpha) = \omega(\alpha - i_P(\alpha_P)) + \omega_P(\alpha_P) = 0$. Assim, ω anula $\mathcal{A}_F(W+P)$ e $W < W+P$, contrariando a definição de W. Logo, $s+1 \notin \{r \in \mathbb{Z}; \omega_P(x) = 0, \forall x \in F \text{ com } v_P(x) \geq -r\}$;

2. Se $\omega_P = \omega'_P \Rightarrow \omega_P - \omega'_P = 0 \Rightarrow \omega(i_P) - \omega'(i_P) = 0 \Rightarrow (\omega - \omega')(i_P) = 0 = (\omega - \omega')_P$. Assim, pelo item anterior $(\omega - \omega') = 0 \Rightarrow \omega = \omega'$.

□

Capítulo

2

Extensões de corpos de funções algébricas

Aqui, F/K é um corpo de funções algébricas com corpo constante K, onde K é um corpo perfeito, F'/K' é um corpo de funções algébricas com corpo constante K' tal que $F \subseteq F'$ e $K \subseteq K'$, e Φ é um corpo algebricamente fechado tal que $F' \subseteq \Phi$.

2.1 Extensões algébricas de corpos de funções

Definição 2.1.1. 1. Um corpo de funções algébricas F'/K' é chamado extensão algébrica de F/K se a extensão F'/F é algébrica;

2. Uma extensão algébrica F'/K' de F/K é chamada extensão por constantes se $F' = FK'$, o compósito de F e K';

3. Uma extensão algébrica F'/K' de F/K é dita extensão finita se $[F' : F] < \infty$.

Em todo este capítulo, F'/K' será uma extensão algébrica de F/K.

Lema 2.1.2. *Se F'/K' é extensão algébrica de F/K, temos:*

1. *K'/K é algébrica e $F \cap K' = K$;*

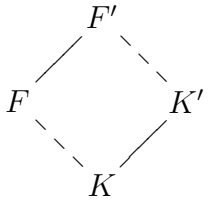
2. *F'/K' é uma extensão finita de F/K se, e somente se, $[K' : K] < \infty$;*

3. *Seja $F_1 = FK'$. Então F_1/K' é uma extensão constante de F/K, e F'/K' é uma extensão finita de F_1/K' (tendo o mesmo corpo de constantes).*

Demonstração. 1. F'/K' é extensão algébrica de F/K , ou seja, $F \subseteq F'$ é algébrica. Assim a extensão F'/K tem grau de transcendência 1 e $K \subseteq K'$. Como K' é o corpo constante de F'/K', então o F'/K' tem grau de transcendência 1. Logo K'/K tem grau de transcendência 0, e portanto K'/K é algébrica.

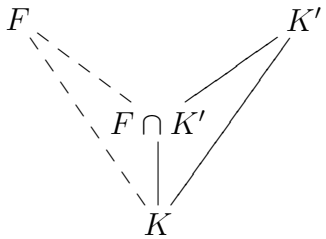
Isso pode ser observado no diagrama abaixo, onde as linha tracejadas representam extensões com grau de transcendência 1 e as contínuas, algébricas.

Diagrama 1.



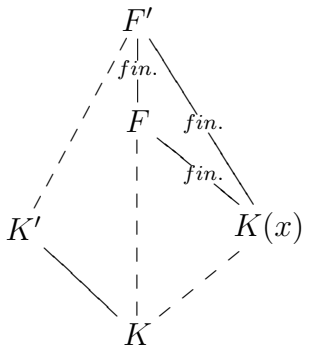
Para mostrar que $F \cap K' = K$, veja que os elementos de $F \cap K'$ são algébricos sobre K (pois K'/K é algébrica) e estão em F, logo são elementos de F algébricos sobre K. Como K é o corpo constante de F/K, temos que $F \cap K' \subseteq K$.

Diagrama 2.



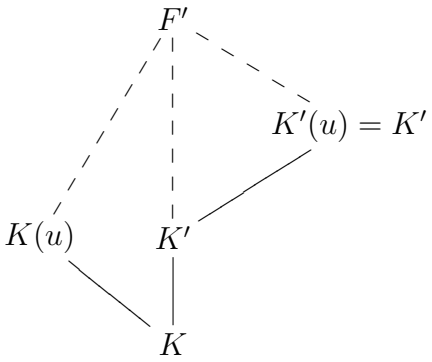
2. Se $[F' : F]$ é finito, pelos diagramas abaixo, F' pode ser visto como corpo de funções algébricas sobre K, cujo corpo de constantes é K'.

Diagrama 3.



O corpo constante de F'/K é K' pois tomando $u \in F'$ algébrico sobre K, temos que u é algébrico sobre K' e assim $u \in K'$.

Diagrama 4.



Logo, pelo Corolário 1.1.15, $[K' : K]$ é finito. Se $[K' : K]$ é finito, seja $x \in F \backslash K$, então $x \in F' \backslash K'$. Veja que x é transcendente sobre K', pois caso contrário, seria algébrico sobre K; logo $[F' : K'(x)]$ é finito. Além disso, $[K'(x) : K(x)]$ é finito, como pode ser visto no Lema 2.1.10. Assim, $[F' : K(x)]$ é finito, e portanto $[F' : F]$ é finito.

3. Fazendo $F_1 = FK'$, então K' é corpo de constantes de F_1. Como F' é extensão algébrica de F, Então FK' também o é. Logo, F_1/K' é estensão algébrica de F/K, portanto F_1/K' é extensão constante. E, como $[K' : K] = 1$, segue pelo item 2 que $[F' : F_1]$ é finito.

□

Definição 2.1.3. Considere uma extensão algébrica F'/K' de F/K. Um lugar $P' \in \mathbb{P}_{F'}$ é dito uma extensão de $P \in \mathbb{P}_F$ se $P \subseteq P'$ e, neste caso, escrevemos $P'|P$.

Proposição 2.1.4. *Seja F'/K' uma extensão algébrica de F/K. Suponha que P (resp. P') é um lugar de F/K (resp. F'/K'), $O_P \subseteq F$ (resp. $O_{P'} \subseteq F'$) o seu respectivo anel de valorização e v_P (resp. $v_{P'}$) a correspondente valorização discreta. Então, são equivalentes:*

1. *$P'|P$;*

2. *$O_P \subseteq O_{P'}$;*

3. *Existe um número inteiro $e \geq 1$ tal que $v_{P'}(x) = ev_P(x), \forall x \in F$.*

Além isso, se $P'|P$, então $P = P' \cap F$ e $O_P = O_{P'} \cap F$. Por esta razão P é chamado de restrição de P' em F.

Demonstração. $1 \Rightarrow 2$: Suponha que $P'|P$ e que existe $u \in O_P \backslash O_{P'}$. Logo $v_P(u) \geq 0$ e $v_{P'}(u) < 0$, e, assim, $v_P(u) = 0$, (se $v_P(u) > 0$, então $u \in P \subseteq P'$, e assim $v_{P'}(u) > 0$). Seja t um parâmetro local de P, então defina $r := v_{P'}(t) > 0$. Considere o elemento $u^r t$, temos $v_P(u^r t) = 1$ e $v_{P'}(u^r t) \leq 0$, ou seja, $u^r t \in P \backslash P'$. Gerando uma contradição.

$2 \Rightarrow 1$: Seja $y \in P$, então $y^{-1} \notin O_P$. Observe que $y^{-1} \notin O_{P'}$, pois caso contrário $y^{-1} \in O_P$. Logo $y \in P'$.

$2 \Rightarrow 3$: Seja $u \in F$ tal que $v_P(u) = 0$, ou seja,$u, u^{-1} \in O_P \subseteq O_{P'}$. Logo, $v_{P'}(u) = 0$.

Seja t um parâmetro local de P, defina $e = v_{P'}(t)$, então $e \geq 1$. Seja $x \in F$ não nulo, defina $r := v_P(x)$, então $v_P(xt^{-r}) = 0$, e assim $v_{P'}(xt^{-r}) = 0$, daí: $v_{P'}(x) - rv_{P'}(t) = 0$ e $v_{P'}(x) = ev_P(x)$.

$3 \Rightarrow 2$: Segue direto.

Portanto $1 \Leftrightarrow 2 \Leftrightarrow 3$.

Veja ainda que $O_P \subseteq O_{P'} \Rightarrow O_P = F \cap O_{P'}$.

De fato, considere o subanel $F \cap O_{P'}$ de F.

Claramente $O_P \subseteq F \cap O_{P'}$, e como O_P é maximal (Teorema 1.1.12) então $O_P = F \cap O_{P'}$ ou $F = F \cap O_{P'}$. Suponha que $F = F \cap O_{P'}$, ou seja, $F \subseteq O_{P'}$, e considere $z \in F' \backslash O_{P'}$. Como F' é algébrico sobre F, então extistem $c_0, ..., c_{n-1} \in F$ tais que:

$$z^n + c_{n-1}z^{n-1} + ... + c_0 = 0$$

Veja que por hipótese temos $v_{P'}(nz) = nv_{P'}(z) < iv_{P'}(z) \leq v_{P'}(c_i) + iv_{P'}(z) = v_{P'}(c_i z^i), i = 0, ..., n-1$.

E, pela desigualdade triangular estrita:

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

Logo não vale $z^n + c_{n-1}z^{n-1} + ... + c_0 = 0$. Gerando uma contradição. Portanto $O_P = F \cap O_{P'}$.

Falta, por fim, mostrar que $P = P' \cap F$.

Se $x \in P$ não nulo, então pelo item 3, $x \in P'$; agora se $x \in P' \cap F$, então, também pelo item 3, $x \in P$. Logo $P = P' \cap F$.

□

Nas mesmas condições da proposição anterior, seja $P'|P$ extensão de P e defina $\varphi : O_P/P \to O_{P'}/P'$, onde $\varphi(x(P)) = x(P')$. Então, se $x \in O_P$ é tal que $\varphi(x(P)) = 0$, temos, pela Proposição 2.1.4:

$$x(P') = \varphi(x(P)) = 0 \Rightarrow x \in P' \Rightarrow x \in P' \cap F = P \Rightarrow x(P) = 0.$$

Logo φ é bem definida e injetora, e temos então um mergulho $O_P/P \hookrightarrow O_{P'}/P'$. Ou seja, podemos ver O_P/P como subcorpo de $O_{P'}/P'$.

Definição 2.1.5. Sejam F'/K' extensão algébrica de F/K, e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$.

1. O inteiro $e(P'|P) = e$, onde $v_{P'}(x) = ev_P(x), \forall x \in F$, é chamado de índice de ramificação de P' sobre P. Dizemos que $P'|P$ é ramificada se $e(P'|P) > 1$, e $P'|P$ é não ramificada se $e(P'|P) = 1$.

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

Proposição 2.1.6. *Seja F'/K' extensão algébrica de F/K e seja $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$. Então:*

1. *$f(P'|P)$ é finito se, e somente se, $[F' : F]$ é finito;*

2. *Se F''/K'' é uma extensão algébrica de F'/K' e P'' é uma extensão de P', então:*

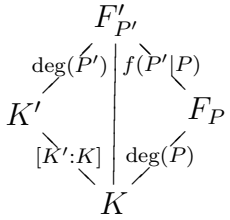
$$e(P''|P) = e(P''|P')e(P'|P)$$

$$e$$

$$f(P''|P) = f(P''|P')f(P'|P).$$

Demonstração. 1. Pelo Lema 2.1.2, $[F' : F]$ é finito se, e somente se, $[K' : K]$ é finito. Temos também que $[F'_{P'} : K'] = \deg(P')$ é finito e $[F_P : K] = \deg(P)$ é finito, donte temos que $[F_{P'} : F_P] < \infty \Leftrightarrow [K' : K] \Leftrightarrow [F' : F]$. De fato:

Diagrama 5.



Observe pelo diagrama acima que:

$$\deg(P')\,[K' : K] = \deg(P)f(P'|P) \Rightarrow f(P'|P) = \frac{\deg(P')}{\deg(P)}\,[K' : K]\,.$$

Assim temos:

$$[K' : K] < \infty \Rightarrow \infty > [F'_{P'} : K']\,[K' : K] = [F'_{P'} : K] = [F'_{P'} : F_P]\,[F_P : K]$$

$$\Rightarrow [F'_{P'} : F_P] < \infty.$$

$$[F'_{P'} : F_P] < \infty \Rightarrow \infty > [F'_{P'} : F_P]\,[F_P : K] = [F'_{P'} : K] = [F'_{P'} : K']\,[K' : K]$$

$$\Rightarrow [K' : K] < \infty$$

2. $\forall x \in F$ temos $v_{P'}(x) = e(P'|P)v_P(x)$ e $\forall y \in F'$ temos $v_{P''}(y) = e(P''|P')v_{P'}(y)$, logo $\forall x \in F$ temos $v_{P''}(x) = e(P''|P')e(P'|P)v_P(x)$, daí o resultado.

   A propriedade $f(P''|P) = f(P''|P')f(P'|P)$ segue direto da definição de grau relativo:

$$f(P''|P) = [F''_{P''} : F_P] = [F''_{P''} : F'_{P'}]\,[F'_{P'} : F_P] = f(P''|P')f(P'|P).$$

□

Proposição 2.1.7. *Seja F'/K' extensão algébrica de F/K.*

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

2. *Todo lugar $P \in \mathbb{P}_F$ tem pelo menos uma, mas somente uma quantidade finita, de extensões $P' \in \mathbb{P}_{F'}$.*

Demonstração. Afirmamos inicialmente que existe $z \in F$ não nulo tal que $v_{P'}(z) \neq 0$.

Suponha que a afirmação seja falsa, então $\forall z \in F^*, v_{P'}(z) = 0$. Escolha $t \in F'$ tal que $v_{P'}(t) > 0$. Como F'/F é algébrica então existe um polinômio não nulo com coeficientes em F, e que tem t como uma de sua raízes, ou seja:

$$t^n + c_{n-1}t^{n-1} + ... + c_0 = 0, \text{ onde } c_0 \neq 0 \text{ e } c_i \in F, \forall i = 0, ..., n-1.$$

Pelo que assumimos, $v_{P'}(c_i) = 0, i = 0, ..., n-1$, então:

$$v_{P'}(t^n) > v_{P'}(c_i t^i) > v_{P'}(c_j t^j), 0 \leq j < i \leq n-1.$$

E pela desigualdade triangular estrita, $v_{P'}(0) = v_{P'}(t^n + c_{n-1}t^{n-1} + ... + c_0) = v_{P'}(c_0) = 0$, gerando uma contradição.

1. Defina $O := O_{P'} \cap F$ e $P := P' \cap F$. Veja que $K \subset O$.

   Pela afirmação anterior, $\exists z \in F$, tal que $v_{P'}(z) > 0$, o que implica $K \subsetneq O$, e além disso, como $v_{P'}(z^{-1}) < 0$, temos $O \subsetneq F$.

Agora veja que $x \in P$ se, e somente se, $x^{-1} \notin O$ se, e somente se, $x \in \tilde{P}$, onde $\tilde{P}$ é o lugar de O. Portanto, $P = \tilde{P}$ (ideal maximal de O), logo P é lugar de F/K e $P'|P$.

Suponha que $P'|P_1$, então $P_1 \subseteq P \subseteq O$, e como P é maximal, temos $P_1 = P$. Nos dando a unicidade.

2. Seja $P \in \mathbb{P}_F$. Pela Proposição 1.6.6, se $n > 2g$, então $\exists x \in F \backslash K$ onde $(x^{-1})_\infty = nP$, ou seja, $(x)_0 = nP$ e P é o único zero de x. Assim, veja que se $P' \in \mathbb{P}_{F'}$, então $P'|P \Leftrightarrow v_{P'}(x) > 0$.

   Como x tem finitos zeros em $\mathbb{P}_{F'}$, concluímos o que desejávamos.

□

Definição 2.1.8. Seja F'/K' extensão algébrica de F/K. Para cada $P \in \mathbb{P}_F$, definimos sua conorma com respeito a F'/F por:

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P)P',$$

onde a soma corre sobre todos os lugares $P' \in \mathbb{P}_{F'}$ que estendem P. Podemos estender a aplicação conorma a um homomorfismo de grupos de $\mathrm{Div}(F)$ para $\mathrm{Div}(F')$:

$$\mathrm{Con}_{F'/F}(\textstyle\sum n_P P) := \sum n_P \,\mathrm{Con}_{F'/F}(P).$$

A conorma comporta-se bem em torres de corpos de funções $F \subseteq F' \subseteq F''$. De fato, pela Proposição 2.1.6, item 2, temos $e(P''|P) = e(P''|P')e(P'|P)$, assim $\forall A \in \mathrm{Div}(F)$, temos:

$$\mathrm{Con}_{F''/F}(A) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(A)).$$

Proposição 2.1.9. *Seja F'/K' extensão algébrica de F/K. Para $x \in F$, não nulo, sejam $(x)_0^F, (x)_\infty^F, (x)^F$ e respectivamente $(x)_0^{F'}, (x)_\infty^{F'}, (x)^{F'}$ os divisores de zeros, de pólos e principal de x em $\mathrm{Div}(F)$ e respectivamente $\mathrm{Div}(F')$. Então:*

$$\mathrm{Con}_{F'/F}((x)_0^F) = (x)_0^{F'}, \mathrm{Con}_{F'/F}((x)_\infty^F) = (x)_\infty^{F'} \text{ e } \mathrm{Con}_{F'/F}((x)^F) = (x)^{F'}.$$

Demonstração. Pela definição de divisor principal de x segue que:

$$(x)^{F'} = \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x)P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P)v_P(x)P' =$$
$$\sum_{P \in \mathbb{P}_F} v_P(x) \sum_{P'|P} e(P'|P)P' = \sum_{P \in \mathbb{P}_F} v_P(x) \operatorname{Con}_{F'/F}(P) = \operatorname{Con}_{F'/F}(\sum_{P \in \mathbb{P}_F} v_P(x)P) =$$
$$\operatorname{Con}_{F'/F}((x)^F).$$

Fazendo o mesmo para $(x)_0^{F'}$ e $(x)_\infty^{F'}$, obtemos o resultado.

□

Pela Proposição 2.1.9, podemos definir o homomorfismo $\operatorname{Con}_{F'/F} : \operatorname{Cl}(F) \to \operatorname{Cl}(F)$, onde $[D] \mapsto \left[\operatorname{Con}_{F'/F}(D)\right]$.

De fato, tal homomorfismo está bem definido, pois se A é B são divisores de F tais que $[A] = [B]$, então $A = B + (x)^F$, para algum x de F não nulo. Logo

$$\operatorname{Con}_{F'/F}([A]) = \left[\operatorname{Con}_{F'/F}(A)\right] = \left[\operatorname{Con}_{F'/F}(B + (x)^F)\right] =$$

$$= \left[\operatorname{Con}_{F'/F}(B) + (x)^{F'}\right] = \left[\operatorname{Con}_{F'/F}(B)\right] = \operatorname{Con}_{F'/F}([B]).$$

Veja ainda que enquanto $\operatorname{Con}_{F'/F} : \operatorname{Div}(F) \to \operatorname{Div}(F')$ é injetora, $\operatorname{Con}_{F'/F} : \operatorname{Cl}(F) \to \operatorname{Cl}(F')$, em geral, não é nem injetora e nem sobrejetora.

Lema 2.1.10. *Sejam K'/K uma extensão finita e x transcendente sobre K. Então $[K'(x) : K(x)] = [K' : K]$.*

Demonstração. Como $[K' : K]$ é finito, então podemos escrever $K' = K(\alpha)$, onde $\alpha \in K'$ e α é raiz de $p(T) \in K[T]$, irredutível e $\deg(p(T)) = [K' : K]$. Assim, $K'(x) = K(x)(\alpha)$, o que implica $[K'(x) : K(x)] \leq [K' : K]$.

Para mostrar que $[K'(x) : K(x)] \geq [K' : K]$, basta mostrar que $p(T)$ é irredutível sobre $K(x)$.

Suponha falso, então $p(T) = f(T)g(T)$, onde $f(T), g(T) \in K(x)[T]$ e têm grau menor que o grau de $p(T)$.

Como $p(\alpha) = 0$, então sem perda de generalidade, podemos supor que $g(\alpha) = 0$. Podemos escrever:

$$g(T) = T^r + c_{r-1}(x)T^{r-1} ... + c_0(x)$$

com $c_i(x) \in K(x)$ e $r < \deg(p(T))$. Assim $\alpha^r + c_{r-1}(x)\alpha^{r-1} ... + c_0(x) = 0$. E assim temos $g_r\alpha^r + g_{r-1}(x)\alpha^{r-1} ... + g_0(x) = 0$, para certos $g_i(x) \in K[x]$ e $g_i(x) = 0 \mod x$ para algum i. Tomando então $x = 0$, obtemos uma combinação linear não trivial identicamente nula de potência de α com coeficientes em K de grau menor que o grau de $p(T)$, gerando uma contradição.

□

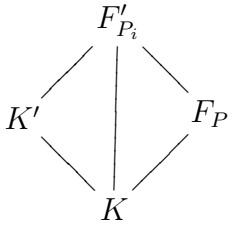
Teorema 2.1.11. *(Igualdade Fundamental)*

Sejam F'/K' extensão finita de F/K, $P \in \mathbb{P}_F$ e $P_1, ..., P_m \in \mathbb{P}_{F'}$ todos os lugares que estendem P. Sejam $e_i = e(P_i|P)$ o índice de ramificação e $f_i = f(P_i|P)$ o grau relativo de $P_i|P$. Então:

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Demonstração. Seja $x \in F$ tal que P é o único zero de x (Proposição 1.6.6) e defina $r := v_P(x) > 0$. Então pela Proposição 2.1.7, temos que os únicos zeros de x em F'/K' são $P_1, ..., P_m$. Agora veja que como F'/K' é uma extensão finita de F/K, temos:

Diagrama 6.



$$\left[F'_{P_i} : K'\right][K' : K] = \left[F'_{P_i} : F_P\right][F_P : K]$$

Assim:

$$[F' : K(x)] = [F' : K'(x)]\,[K'(x) : K(x)] = \left(\sum_{i=1}^{m} v_{P_i}(x)\deg(P_i)\right)[K' : K] = \sum_{i=1}^{m} v_{P_i}(x)\left[F'_{P_i} : K'\right][K' : K] = r\deg(P)\sum_{i=1}^{m} e_i f_i$$

por conta do Teorema 1.4.11 e do Lema 2.1.10.

Por outro lado,

$$[F' : K(x)] = [F' : F]\,[F : K(x)] = [F' : F]\,r\deg(P).$$

Assim, das duas igualdades temos o resultado.

□

Definição 2.1.12. Sejam F'/K' uma extensão finita de F/K de grau $[F' : F] = n$ e $P \in \mathbb{P}_F$.

1. P se decompõe completamente em F'/F se existem exatamente n lugares distintos $P' \in \mathbb{P}_{F'}$ tais que $P'|P$;

2. P é totalmente ramificado em F'/F se existe um lugar $P' \in \mathbb{P}_{F'}$ com $P'|P$ e $e(P'|P) = n$.

Veja que P se decompõe completamente se, e somente se, $e(P'|P) = f(P'|P) = 1$, para toda extensão $P'|P$. E, além disso P ser totalmente ramificando implica que existe um único $P' \in \mathbb{P}_{F'}$ tal que P' é uma extensão de P.

Corolário 2.1.13. *Seja F'/K' uma extensão finita de F/K. Então para cada divisor $A \in \mathrm{Div}(F)$, temos:*

$$\deg(\mathrm{Con}_{F'/F}(A)) = \frac{[F' : F]}{[K' : K]} \deg(A).$$

Demonstração. Se $A = P \in \mathbb{P}_F$, então, pelo que observamos no Diagrama 5, temos:

$$[F'_{P'} : K'] = \frac{f(P'|P) \deg(P)}{[K' : K]},$$

portanto:

$$\deg(\mathrm{Con}_{F'/F}(P)) = \deg(\textstyle\sum_{P'|P} e(P'|P)P') = \sum_{P'|P} e(P'|P) \, [F'_{P'} : K'] = \frac{\deg(P)}{[K':K]} \sum_{P'|P} e(P'|P) f(P'|P) = \frac{[F':F]}{[K':K]} \deg(P).$$

Para o caso em que A é um divisor qualquer, basta escrever $A = \sum n_P P$, pois $\mathrm{Con}_{F'/F}(\sum n_P P) = \sum n_P \, \mathrm{Con}_{F'/F}(P)$ e $\deg(\sum n_P P) = \sum n_P \deg(P)$, e temos o resultado.

□

2.2 Subanéis de corpos de funções

Definição 2.2.1. Um subanel de F/K é um anel R tal que $K \subsetneq R \subsetneq F$, e R não é um corpo.

Um exemplo de subanel de F/K é o anel de valorização O_P, para $P \in \mathbb{P}_F$.

Outro exemplo de subanel é $K[x_1, ..., x_n]$, onde $x_1, ..., x_n$ são elementos transcendentes de F sobre K. De fato, se P é um lugar de F tal que $v_P(x_i) \geq 0, i = 1, ..., n$, defina $x := x_1$ e $d := \deg(P)$. Temos que $1, x(P), x^2(P), ..., x^d(P) \in F_P$ são linearmente dependentes sobre K, e portanto existem $\alpha_0, ..., \alpha_d \in K$ tais que $\alpha_0 + \alpha_1 x(P) + ... + \alpha_d x^d(P) = 0$, ou seja, $\alpha_0 + \alpha_1 x + ... + \alpha_d x^d = z \in P$, e como x é transcendente, temos $z \neq 0$. Logo $v_P(z^{-1}) < 0$ e daí $z^{-1} \notin K[x_1, ..., x_n]$, pois $K[x_1, ..., x_n] \subseteq O_P$.

Definição 2.2.2. Para $\emptyset \neq S \subsetneq \mathbb{P}_F$, considere o anel:

$$O_S = \{z \in F; v_P(z) \geq 0, \forall P \in S\} = \bigcap_{P \in S} O_P,$$

a interseção de todos os anéis de valorização O_P, com $P \in S$. Um anel $R \subseteq F$ tal que $R = O_S$, para algum $\emptyset \neq S \subsetneq \mathbb{P}_F$, é chamado anel holomórfico de F/K.

O anel $K[x]$ é um anel holomórfico do corpo de funções racionais $K(x)/K$. Pois, $K[x] = \bigcap_{P \neq P_\infty} O_P$.

Lema 2.2.3. *1. Todo anel de valorização O_P é um anel holomórfico, a saber $O_P = O_S$, com $S = \{P\}$;*

2. Todo anel holomórfico O_S é um subanel de F/K;

3. Para $P \in \mathbb{P}_F$ e $\emptyset \neq S \subsetneq \mathbb{P}_F$, temos $O_S \subseteq O_P \Leftrightarrow P \in S$. Consequentemente, $O_S = O_T \Leftrightarrow S = T$.

Demonstração. 1. Trivial.

2. Basta mostrar que O_S não é um corpo.

   Seja $P_1 \in S$, pelo teorema da aproximação forte $\exists x \in F$ não nulo, tal que $v_{P_1}(x) > 0$ e $v_P(x) \geq 0, \forall P \in S$. Logo pela definição de O_S, temos que $x \in O_S$ e $x^{-1} \notin O_S$.

3. Se $P_1 \in S$, então claramente $O_S \subseteq O_{P_1}$.

   Mostremos $P \notin S \Rightarrow O_S \nsubseteq O_P$.

   (a) Se $S \cup \{P\} \neq \mathbb{P}_F$, então pelo teorema de aproximação forte, existe $z \in F$ (não nulo) tal que $v_P(z) < 0$ e $v_Q(z) \geq 0, \forall Q \in S$, ou seja $z \notin O_P$ e $z \in O_S$.

   (b) Se $S \cup \{P\} = \mathbb{P}_F$, então também pelo teorema da aproximação forte, existe $z \in F$ (não nulo) tal que para $P_1 \in S$ fixado, $v_{P_1}(z) > 0$ e $v_Q(z) \geq 0, \forall Q \in S \setminus \{P_1\}$. Logo $z \notin K$, assim z tem pelo menos um pólo. Logo P é pólo de z, e portanto, $z \notin O_P$ e $z \in O_P$

   Se $O_S \subseteq O_T$, então, pela definição de O_T, temos $O_S \subset O_P, \forall P \in T \Rightarrow P \in S \Rightarrow T \subseteq S$.

□

Definição 2.2.4. Seja R um subanel de F/K.

1. Um elemento $z \in F$ é dito ser integral sobre R se $f(z) = 0$ para algum polinômio mônico $f(T) \in R[T]$, isto é, se existem $a_0, ..., a_{n-1} \in R$ tais que $z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0 = 0$. Uma equação deste tipo é chamada equação integral para z sobre R.

2. O conjunto $\mathrm{ic}_F(R) := \{z \in F; z \text{ é integral sobre } R\}$ é chamado de o fecho integral de R sobre F;

3. Seja $F_0 \subseteq F$ o corpo de frações de R. O anel R é dito integralmente fechado se $\mathrm{ic}_{F_0}(R) = R$, isto é, todo elemento $z \in F_0$ tal que z é integral sobre R, está na verdade em R.

Proposição 2.2.5. *Seja O_S anel holomórfico de F/K. Então:*

1. *F é o corpo de frações de O_S;*

2. *O_S é integralmente fechado.*

Demonstração. 1. Seja $x \in F$, não nulo. Seja $P_0 \in S$, pelo teorema da aproximação forte existe $z \in F$, não nulo, onde $v_{P_0}(z) = \max\{0, v_{P_0}(x^{-1})\}$ e $v_P(z) \geq \max\{0, v_P(x^{-1})\}, \forall P \in S$.

De fato, se $x \in O_S$, então $v_P(x^{-1}) \leq 0$, para todo $P \in S$, e pelo teorema da aproximação forte existe $z \in F$, não nulo, onde $v_{P_0}(z) = \max\{0, v_{P_0}(x^{-1})\}$ e $v_P(z) \geq 0 \geq \max\{0, v_P(x^{-1})\}, \forall P \in S \setminus \{P_0\}$. Se $x \notin O_S$, então existem $P_1, ..., P_t \in S$ tais que $v_{P_i}(x) < 0, i = 1, ..., t$ e $v_P(x) \geq 0$, para $P \in S \setminus \{P_1, ..., P_t\}$,e pelo teorema da apriximação forte existe $z \in F$, não nulo onde $v_{P_i}(z) = \max\{0, v_{P_i}(x^{-1})\}, i = 0, 1, ..., t$ e $v_P(z) \geq 0 \geq \max\{0, v_P(x^{-1})\}, \forall P \in S \setminus \{P_0, P_1, ..., P_t\}$.

Logo $z \in O_S$.

Defina $y := zx$. Temos que $y \in O_S$, pois $v_P(y) = v_P(z) + v_P(x) \geq 0, \forall P \in S$ e, além disso $x = yz^{-1}$, onde $y, z \in O_S$, ou seja, x pertence ao corpo de frações de O_S. Logo F está contido no corpo de frações de O_S, e portanto são iguais.

2. Pelo item anterior, vimos que o corpo de frações de O_S é todo o corpo F, e pela definição de fecho algébrico temos que $\mathrm{ic}_F(O_S) \supset O_S$. Seja agora $u \in F$ integral sobre O_S, considere a equação integral para u sobre O_S: $u^n + a_{n-1}u^{n-1} + ... + a_1u + a_0 = 0$. Mostremos que $v_P(u) \geq 0, \forall P \in S$.

   Suponha que existe $P \in S$ tal que $v_P(u) < 0$. Como $v_P(a_i) \geq 0, i = 0, ..., n-1$, temos $v_P(u^n) < v_P(a_iu^i) = v_P(a_i) + iv_P(u)$. Logo, pela desigualdade triangular estrita, $0 > v_P(u^n) = v_P(u^n + a_{n-1}u^{n-1} + ... + a_1u + a_0) = v_P(0) = \infty$, gerando uma contradição.

□

Teorema 2.2.6. *Seja R subanel de F/K e $S(R) := \{P \in \mathbb{P}_F; R \subseteq O_P\}$. Então:*

1. *$\emptyset \neq S(R) \subsetneq \mathbb{P}_F$;*
2. *O fecho integral de R em F é $\mathrm{ic}_F(R) = O_{S(R)}$. Em particular, $\mathrm{ic}_F(R)$ é subanel de F/K integralmente fechado com corpo de frações F.*

Demonstração. 1. Como R é subanel, então não é corpo, existe um ideal próprio $\{0\} \neq I \subsetneq R$. Assim pelo Teorema 1.1.18, $S(R) \neq \emptyset$.

Seja $x \in R$ transcedente sobre K, como x tem pelo menos um pólo $Q \in \mathbb{P}_F$, então $x \notin O_Q$, e portanto R não está contido em O_Q, o que implica $Q \notin S(R)$.

2. Como $R \subset O_{S(R)}$ e $O_{S(R)}$ é integralmente fechado e tem F como corpo de frações, pela Proposição 2.2.5, temos $O_{S(R)} = \mathrm{ic}_F(O_{S(R)}) \supseteq \mathrm{ic}_F(R)$.

   Seja $z \in O_{S(R)}$, então $z^{-1}R[z^{-1}] = R[z^{-1}]$, pois caso contrário $z^{-1}R[z^{-1}]$ seria um ideal próprio de $R[z^{-1}]$, e pelo Teorema 1.1.18, existiria $Q \in \mathbb{P}_F$ onde $z^{-1}R[z^{-1}] \subseteq Q$, $R[z^{-1}] \subseteq O_Q$ e $z^{-1} \in Q$. E, assim, teríamos $Q \in S(R)$ e $z \notin O_Q$, contrariando $z \in O_{S(R)}$.

   Como $1 \in R[z^{-1}] = z^{-1}R[z^{-1}]$, existem $a_0, ..., a_s \in R$ tais que $1 = z^{-1}(\sum_{i=0}^{s} a_i z^{-i})$.

   Multiplicando esta expressão por z^{s+1}, concluimos que $z \in \mathrm{ic}_F(R)$, e portanto $\mathrm{ic}_F(R) = O_{S(R)}$.

   Por fim, pelo Lema 2.2.3 e pela Proposição 2.2.5, obtemos que F é todo o corpo de frações de $\mathrm{ic}_F(R)$ e que $\mathrm{ic}_F(R)$ é subanel de F/K integralmente fechado.

□

Proposição 2.2.7. *Seja O_S anel holomórfico se F/K. Então existe uma correspondência 1-1 entre S e o conjunto de ideais maximais de O_S, dada por $P \mapsto M_P := P \cap O_S, (P \in S)$. Mais ainda, a aplicação $\varphi : O_S/M_P \to F_P$, onde $x + P \mapsto x + P$, é um isomorfismo.*

Demonstração. Seja $P \in S$, considere o homomorfismo $\phi : O_S \to F_P, x \mapsto x + P$. Como $O_S \subseteq O_P$, então ϕ está bem definida. Temos também que ϕ é sobrejetora, de fato, seja $z + P \in F_P$, pelo teorema da aproximação forte, existe $x \in F$ tal que $v_P(x - z) > 0$ e $v_Q(x) \geq 0, \forall Q \in S \setminus \{P\}$. Assim, $x \in O_S$. Além disso, como $x + P = z + P$.

Temos ainda que $\ker(\phi) = P \cap O_S$, pois $x \in \ker(phi) \Leftrightarrow x \in P$ e $x \in O_S$. Logo φ é um isomorfismo.

F_P é corpo, então M_P é ideal maximal de O_S.

Falta mostrar que a aplicação $P \mapsto M_P$ é bijetora.

Sejam $P, Q \in S$ distintos, então pelo teorema da aproximação forte existe $z \in F$ tal que $z \in O_S$, $z \in P$ e $z \notin Q$, ou seja, $M_P \neq M_Q$. O que significa $P \mapsto M_P$ injetora. Mostremos, então, a sobrejetividade.

Seja M ideal maximal de O_S, pelo Teorema 1.1.18, existe $P \in \mathbb{P}_F$ tal que $M \subseteq P$ e $O_S \subseteq O_P$, e, pelo Lema 2.2.3, temos $P \in S$. Logo $M \subseteq P \cap O_S$ com $P \in S$, e pela maximalidade de M segue que $M = P \cap O_S$.

□

Proposição 2.2.8. *Se $S \subset \mathbb{P}_F$ é um conjunto finito e não vazio de lugares de F/K, então O_S é um domínio de ideais principais.*

Demonstração. Sejam $S = \{P_1, ..., P_s\}$ e $\{0\} \neq I \subseteq O_S$ um ideal de O_S. Para cada $i = 1, ..., s$, escolha $x_i \in I$ tal que $v_{P_i}(x_i) =: n_i \leq v_{P_i}(u), \forall u \in I$.

Pelo teorema da aproximação forte, para cada $i = 1, ..., s$, existe $z_i \in F$ onde $v_{P_i}(z_i) = 0$ e $v_{P_j}(z_i) > n_j, i \neq j$. Logo, $z_i \in O_S, i = 1, ..., s$.

Defina $x := \sum_{i=1}^{s} x_i z_i \in I$.

Veja que $v_{P_i}(x_i z_i) = v_{P_i}(x_i) + v_{P_i}(z_i) = n_i$ e $v_{P_j}(x_i z_i) = v_{P_i}(x_i) + v_{P_i}(z_i) > n_i$, e assim, pela desigualdade triangular estrita temos que $v_{P_i}(x) = n_i$.

Seja, agora, $z \in I$, defina $y := x^{-1}z$. Observe que $v_{P_i}(y) \geq 0$, pois $v_{P_i}(y) = v_{P_i}(x^{-1}z) = v_{P_i}(z) - n_i \geq 0, i = 1, ..., s$, ou seja, $y \in O_S$. Assim, como $z = yx$, temos $I \subseteq xO_S$, e como $x \in I$, temos $xO_S = I$. Logo, O_S é domínio de ideais principais.

□

2.3 Bases integrais locais

Aqui, F/K é um corpo de funções com corpo de constantes K, e $F \subseteq F'$ é um extensão finita, com corpo de constantes K' podendo ser maior do que K.

Proposição 2.3.1. *Seja R subanel de F/K integralmente fechado com corpo de frações F, ou seja, anel holomorfo de F/K. Para $z \in F'$, seja $\varphi(T) \in F[T]$ seu polinômio minimal sobre F. Então z é integral sobre R se, e somente se, $\varphi(T) \in R[T]$.*

Demonstração. ($\Leftarrow$): segue direto da definição de um elemento ser integral sobre um anel.

($\Rightarrow$): $z \in F'$ é integral sobre R, ou seja, existe $f(T) \in R[T]$ tal que $f(z) = 0$. Como $\varphi(T)$ é minimal, então existe $\psi(T) \in F[T]$ tal que $f(T) = \varphi(T)\psi(T)$.

Sejam $F' \subseteq F''$ extensão finita de F' contendo todas as raízes de $\varphi(T)$ e $R'' = \mathrm{ic}_{F''}(R)$ o fecho integral de R em F''. Como todas as raízes de $\varphi(T)$ estão em F'', elas també estão em R''.

Os coeficientes de $\varphi(T)$ são expressões polinomiais de suas raízes, então $\varphi(T) \in R''[T]$.

Mas $\varphi(T) \in F[T]$ e $F \cap R'' = R$, pois R é integralmente fechado.

Assim, $\varphi(T) \in F[T] \cap R''[T] = (F \cap R'')[T] = R[T]$.

□

Corolário 2.3.2. *Nas condições da proposição anterior, sejam* $\mathrm{Tr}_{F'/F} : F' \to F$ *a aplicação traço de* F' *para* F *e* $x \in F'$ *integral sobre* R. *Então* $\mathrm{Tr}_{F'/F}(x) \in R$.

Proposição 2.3.3. *Seja* M/L *uma extensão finita separável, e considere* $\{z_1, ..., z_n\}$ *uma base de* M/L. *Então existem* $z_1^*, ..., z_n^* \in M$ *unicamente determinados tais que* $\mathrm{Tr}_{M/L}(z_i z_j^*) = \delta_{ij}$ *(símbolo de Kronecker). O conjunto* $\{z_1^*, ..., z_n^*\}$ *é uma base de* M/L *e é chamada base dual de* $\{z_1, ..., z_n\}$ *com respeito ao traço.*

Demonstração. Considere o espaço dual $\hat{M}$ de M sobre L, isto é, $\hat{M}$ é o espaço de todas as aplicações $L-$lineares de M em L. Então $\dim \hat{M} = n$.

Podemos ver $\hat{M}$ como um $M-$espaço vetorial definindo, para $z \in M$ e $\lambda \in \hat{M}$, $z\lambda \in \hat{M}$ por $z\lambda(w) := \lambda(zw), \forall w \in M$. E assim concluímos que $\dim_M(\hat{M}) = 1$.

Como M/L é separável, então $\mathrm{Tr}_{M/L}$ é não nula e está em $\hat{M}$, logo $\forall \lambda \in \hat{M}$, existe $z \in M$, tal que $\lambda = z\,\mathrm{Tr}_{M/L}$. Considere então as transformações lineares $\lambda_j \in \hat{M}$ tais que $\lambda_j(z_i) = \delta_{ij}$. Podemos escrever $\lambda_j = z_j^* \mathrm{Tr}_{M/L}$. Logo $\mathrm{Tr}_{M/L}(z_i z_j^*) = z_j^* \mathrm{Tr}_{M/L}(z_i) = \lambda_j(z_i) = \delta_{ij}$.

Como $\lambda_1, ..., \lambda_n$ são linearmente independentes, o mesmo vale para $z_1^*, ..., z_n^*$, ou seja, também constituem uma base de M/L.

□

Teorema 2.3.4. *Sejam* R *subanel integralmente fechado de* F/K *com corpo de frações* F, *e* F'/F *extensão finita separável de grau* n. *Considere* $R' = \mathrm{ic}_{F'}(R)$ *o fecho integral de* R *em* F'. *Então:*

1. *Para toda base* $\{x_1, ..., x_n\}$ *de* F'/F*, existem elementos* $a_i \in R\setminus\{0\}, i = 1, ..., n$*, tais que* $a_1x_1, ..., a_nx_n \in R'$*. Consequentemente, existe bases de* F'/F *contidas em* R'*;*

2. *Se* $\{z_1, ..., z_n\} \subset R'$ *é uma base de* F'/F *e* $\{z_1^*, ..., z_n^*\}$ *é sua base dual com respeito ao traço, então:*

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*;$$

3. *Se* R *é domínio de ideais principais, então existe uma base* $\{u_1, ..., u_n\}$ *de* F'/F *tal que:*

$$R' = \sum_{i=1}^{n} Ru_i.$$

Demonstração. 1. Seja $x \in F'$, com F'/F é algébrica e F é o corpo de frações de R, então existem $a_i, b_i \in R$, com $a_i \neq 0$, $i = 0, ..., r-1$, onde:

$$x^r + \tfrac{b_{r-1}}{a_{r-1}}x^{r-1} + ... + \tfrac{b_1}{a_1}x + \tfrac{b_0}{a_0} = 0.$$

Definindo $a := \prod_{i=0}^{r-1} a_i$ e multiplicando a equação acima por a^r, obtemos:

$$(ax)^r + c_{r-1}(ax)^{r-1} + ... + c_1(ax) + c_0 = 0,$$

onde $c_i \in R, i = 0, .., r$. Ou seja, $ax \in R'$.

Isso significa que $\forall x \in F'$ existe $a \in R\setminus\{0\}$ tal que ax é integral sobre R.

2. Sejam $\{z_1, ..., z_n\} \subseteq R'$ base de F'/F e $\{z_1^*, ..., z_n^*\}$ base dual induzida pela primeira. Então $\forall z \in F'$, existem $e_i \in F, i = 1, ..., n$, tais que $z = e_1z_1^* + ... + e_nz_n^*$.

Se $z \in R'$, então $zz_i \in R'$, e assim, pelo Corolário 2.3.2, $\mathrm{Tr}_{F'/F}(zz_i) \in R$. Além disso, pela Proposição 2.3.3 $\mathrm{Tr}_{F'/F}(zz_j) = \sum_{i=1}^{n} e_i \mathrm{Tr}_{F'/F}(z_i^*z_j) = e_j$, logo $e_j \in R, j = 1, .., n$. Portanto, $R' \subseteq \sum_{i=1}^{n} Rz_i^*$. Por fim, como $\{z_1, ..., z_n\} \subset R'$, temos:

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

3. Pelos itens anteriores, existe $\{w_1, ..., w_n\}$ base de F'/F tal que $R' \subseteq \sum_{i=1}^{n} Rw_i$. Então, para $1 \leq k \leq n$, defina:

$$R_k := R' \cap \sum_{i=1}^{k} Rw_i.$$

Vamos construir, recursivamente, $u_1, ..., u_n$ tais que $R_k = \sum_{i=1}^{k} Ru_i$, através do princípio de indução finita sobre k.

Para $k = 1$, considere o conjunto $I_1 := \{a \in F; aw_1 \in R'\}$. I_1 é um ideal de R, e portanto é da forma $I_1 = a_1R$, pois supomos que R é domínio de ideais principais.

Definindo $u_1 := a_1w_1$, como $R_1 = R' \cap Rw_1$, temos $R_1 = Ru_1$.

Suponha agora pela hipótese de indução que para $k \geq 2$, encontramos $u_1, ..., u_{k-1}$ tais que $R_{k-1} = \sum_{i=1}^{k-1} Ru_i$.

Seja $I_k = \left\{a \in F; \exists b_1, ..., b_{k-1} \in R \text{ tais que } (\sum_{i=1}^{k-1} b_iw_i) + aw_k \in R'\right\}$. I_k é um ideal de R, e como antes é da forma a_kR. Seja $u_k \in R'$ tal que $u_k = c_1w_1 + ... + c_{k-1}w_{k-1} + a_kw_k$.

Mostremos que $R_k = \sum_{i=1}^{k} Ru_i$.

Seja $w \in R_k$, então $w \in R'$ e existem $d_1, ..., d_k \in R$ tais que $w = d_1w_1 + ... + d_kw_k$, logo $d_k \in I_k \Rightarrow d_k = a_kd$, para algum $d \in R$.

Assim, $d_kw_k = da_kw_k = d(u_k - c_1w_1 - ... - c_{k-1}w_{k-1}) \Rightarrow w - du_k \in (\sum_{i=1}^{k-1} Rw_i) \cap R' = R_{k-1} = \sum_{i=1}^{k-1} Ru_i$. Por fim, fazendo $k = n$ e tendo que $\{u_1, ..., u_n\}$ é um conjunto linearmente independente, pois pelo primeiro item deste teorema, R' contém uma base de F'/F e o corpo de frações de R é todo o corpo F, temos o resultado.

□

Corolário 2.3.5. *Sejam F'/F extensão finita separável do corpo de funções F/K e $P \in \mathbb{P}_F$. Então o fecho integral O'_P de O_P em F' é dado por:*

$$O'_P = \bigcap_{P'|P} O_{P'}.$$

Existe uma base $\{u_1, ..., u_n\}$ *de* F'/F *tal que:*

$$O'_P = \sum_{i=1}^{n} O_P u_i.$$

Esse tipo de base $\{u_1, ..., u_n\}$ *é chamada uma base integral de* O'_P *sobre* O_P *(ou base integral local de* F'/F *para o lugar* P*).*

Demonstração. Pelo Teorema 2.2.6, item 2, temos:

$$O'_P = \mathrm{ic}_F(O_P) = O_{S(O_P)} = \textstyle\bigcap_{P' \in S(O_P)} O_{P'},$$

onde $S(O_P) = \{P' \in \mathbb{P}_{F'}; O_P \subseteq O_{P'}\} = \{P' \in \mathbb{P}_{F'}; P'|P\}$.

Portanto, $O'_P = \bigcap_{P'|P} O_{P'}$.

E, pelo Teorema 2.3.4, item 3, existe base $\{u_1, ..., u_n\}$ de F'/F tal que:

$$O'_P = \sum_{i=1}^{n} O_P u_i.$$

Isso acontece porque, pelo Teorema 1.1.6, O_P é um domínio de ideais principais.

□

Teorema 2.3.6. *Sejam* F/K *corpo de funções e* F'/F *extensão finita separável. Então cada base* $\{z_1, ..., z_n\}$ *de* F'/F *é uma base integral para quase todos os lugares* $P \in \mathbb{P}_F$*.*

Demonstração. Seja $\{z_1, ..., z_n\}$ base de F'/F, considere a base dual $\{z_1^*, ..., z_n^*\}$ referente a aplicação traço.

Os polinômios minimais de $z_1, ..., z_n, z_1^*, ..., z_n^*$ sobre F envolvem apenas uma quantidade finita de coeficientes. Sejam $S \subseteq \mathbb{P}_F$ o conjunto de todos os pólos destes coeficientes, $P \notin S$ um lugar e $z \in \{z_1, ..., z_n, z_1^*, ..., z_n^*\}$. Então $z \in O'_P = \mathrm{ic}_{F'}(O_P)$, pois P não é pólo de nenhum coeficiente do polinômio minimal de z, e assim, tais coeficientes estão em O_P. Logo, as duas bases estão contidas em O'_P.

Portanto, pelo teorema anterior, temos $\sum O_P z_i \subseteq O'_P \subseteq \sum O_P z_i^* \subseteq O'_P \subseteq \sum O_P z_i$, pois $\{z_1, ..., z_n\}$ é base dual de $\{z_1^*, ..., z_n^*\}$. Ou seja, $\sum O_P z_i = O'_p$. Logo $\{z_1, ..., z_n\}$ é base integral de O'_P sobre $O_P, \forall P \notin S$.

□

Para os próximos resultados, tomemos:

$\overline{F} := F_P$ é o corpo das classes residuais módulo P;

$\overline{a} := a(P) \in \overline{F}$ é a classe residual de $a \in O_P$;

Se $\psi(T) = \sum c_i T^i$ é um polinômio com coeficientes em O_P, definimos $\overline{\psi}(T) := \sum \overline{c_i} T^i \in \overline{F}\,[T]$.

Teorema 2.3.7. *(Kummer)*

Suponha $F' = F(y)$, onde y é integral sobre O_P, e considere $\varphi(T) \in O_P\,[T]$ 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 fatores irredutíveis sobre $\overline{F}$. Escolha polinômios mônicos $\varphi_i(T) \in O_P\,[T]$ com $\overline{\varphi_i}(T) = \gamma_i(T)$ e $\deg \varphi_i(T) = \deg \gamma_i(T)$.

Então para $1 \leq i \leq r$, existem lugares $P_i \in \mathbb{P}_{F'}$ satisfazendo:

$$P_i|P, \varphi_i(y) \in P_i \text{ e } f(P_i|P) \geq \deg \gamma_i(T).$$

Além disso, $P_i \neq P_j$ para $i \neq j$.

Supondo adicionalmente que pelo menos uma das hipóteses abaixo é satisfeita:

$(\star) \varepsilon_i = 1, i = 1, ..., r$;

$(\star\star)$ $\{1, y, ..., y^{n-1}\}$ *é base integral em P.*

Então existe, para $1 \leq i \leq r$, exatamente um lugar $P_i \in \mathbb{P}_{F'}$ com $P_i|P$ e $\varphi_i(y) \in P_i$. Os lugares $P_1, ..., P_r$ são todos os lugares de F' que estendem P, e temos:

$$\mathrm{Con}_{F'/F}(P) = \sum_{i=1}^{r} \varepsilon_i P_i,$$

isto é, $\varepsilon_i = e(P_i|P)$. O corpo de classes residuais $F'_{P_i} = O_{P_i}/P_i$ é isomorfo a $\overline{F}\,[T]\,/(\gamma_i(T))$, portanto $f(P_i|P) = \deg \gamma_i(T)$.

Demonstração. Defina $\overline{F_i} = \overline{F}[T]/(\gamma_i(T))$. Como γ_i é irredutível, então $\overline{F_i}$ é extensão de $\overline{F}$ com grau $\left[\overline{F_i} : \overline{F}\right] = \deg \gamma_i(T)$.

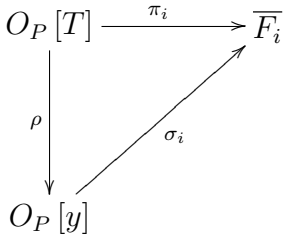
Considere o anel $O_P[y] = \sum_{j=0}^{n-1} O_P y^j$, onde $n = \deg \varphi(T) = [F' : F]$.

Existem homomorfismo de anéis: $\rho : O_P[T] \to O_P[y]$, onde $\sum c_j T^j \mapsto \sum c_j y^j$, e $\pi_i : O_P[T] \to \overline{F_i}$, onde $\sum c_j T^j \mapsto \sum \overline{c_j} T^j \bmod \gamma_i(T)$.

Temos $\ker(\rho) = (\varphi(T))$ e $\ker(\rho) \subseteq \ker(\pi_i)$. De fato, seja $p(T) \in (\varphi(T))$, então existe $\lambda(T) \in O_{P[T]}$ tal que $p(T) = \lambda(T)\varphi(T)$, assim $\rho(p(T)) = \rho(\lambda(T))\rho(\varphi(T)) = \rho(\lambda(T))\varphi(y) = 0$, logo $(\varphi(T)) \subseteq \ker(\rho)$. Agora, se $p(T) \in \ker(\rho)$, então $p(y) = 0$, o que implica $\varphi(T)$ divide $p(T)$, e assim $p(T) \in (\varphi(T))$, e temos $\ker(\rho) \subseteq (\varphi(T))$. Veja ainda que se $p(T) \in \ker(\rho)$, então $p(T) = \lambda(T)\varphi(T)$, para algum $\lambda(T) \in O_P[T]$, e assim $\pi_i(p(T)) = \pi_i(\lambda(T))\pi_i(\varphi(T)) = \pi_i(\lambda(T))\overline{\varphi}(T) \bmod \gamma_i(T)$, ou seja, $\ker(\rho) \subseteq \ker(\pi_i)$.

Assim, defina $\sigma_i : O_P[y] \to \overline{F_i}$, tal que $\sum_{j=0}^{n-1} c_j y^j \mapsto \sum_{j=0}^{n-1} \overline{c_j} T^j \bmod \gamma_i(T)$. Então σ_i é um epimorfismo e $\pi_i = \sigma_i \circ \rho$.

Diagrama 7.



Temos ainda $\ker \sigma_i = P \cdot O_P[y] + \varphi_i(y) \cdot O_P[y]$, e $\ker \sigma_i$ é um ideal próprio do anel $O_P[y] \subseteq F'$.

De fato, seja $z \in P \cdot O_P[y] + \varphi_i(y) \cdot O_P[y]$, então existe $p \in P$, $a_0, ..., a_{n-1}, b_0, ..., b_{n-1} \in O_P$ tais que:

$$z = p(a_0 + a_1 y + ... + a_{n-1} y^{n-1}) + \varphi_i(y)(b_0 + b_1 y + ... + b_{n-1} y^{n-1})$$

$$\Rightarrow \sigma_i(z) = \sigma i(p(a_0 + a_1 y + ... + a_{n-1} y^{n-1}) + \varphi_i(y)(b_0 + b_1 y + ... + b_{n-1} y^{n-1}))$$

$$= \sigma_i(p)(\sum_{j=0}^{n-1} \overline{a_j} T^j) \bmod \gamma_i(T) = 0,$$

ou seja, $P \cdot O_P[y] + \varphi_i(y) \cdot O_P[y] \subseteq \ker(\sigma_i)$.

Agora a inclusão contrária:

Seja $z \in \ker(\sigma_i) \subseteq O_P[y]$. Podemos escrever:

$$z = c_0 + c_1 y + ... + c_{n-1} y^{n-1},$$

assim

$$\sigma_i(z) = (\overline{c_0} + \overline{c_1} T + ... + \overline{c_{n-1}} T^{n-1}) \bmod \gamma_i(T) = 0,$$

ou seja, existe $\psi(T) \in O_P[T]$ tal que:

$$\overline{c_0} + \overline{c_1} T + ... + \overline{c_{n-1}} T^{n-1} = \gamma_i(T)\overline{\psi}(T) = \overline{\varphi_i}(T)\overline{\psi}(T)$$

$$\Rightarrow \overline{c_0} + \overline{c_1} T + ... + \overline{c_{n-1}} T^{n-1} - \overline{\varphi_i}(T)\overline{\psi}(T) = 0.$$

Logo:

$$c_0 + c_1 T + ... + c_{n-1} T^{n-1} - \varphi_i(T)\psi(T) \in PO_P[T]$$

$$\Rightarrow c_0 + c_1 T + ... + c_{n-1} T^{n-1} \in PO_P[T] + \varphi_i(T) O_P[T]$$

$$\Rightarrow z \in P \cdot O_P[y] + \varphi_i(y) \cdot O_P[y],$$

e portanto temos a igualdade dos conjuntos.

Temos que $\ker(\sigma_i)$ é um ideal próprio de $O_P[y]$, pois $\pi_i \neq 0 \Rightarrow \sigma_i \neq 0 \Rightarrow \ker(\sigma_i) \subsetneq O_P[y]$. Além disso, veja que $\varphi_i(y) \in \ker(\sigma_i)$, o que implica $\{0\} \subsetneq \ker(\sigma_i)$.

Logo, pelo Teorema 1.1.18, existe $P_i \in \mathbb{P}_{F'}$ de forma que $\ker \sigma_i \subseteq P_i$ e $O_P[y] \subseteq O_{P_i}$. E assim temos, $\varphi_i(y) \in P_i$ e $P_i | P$.

Como σ_i é epimorfismo então $O_P[y] / \ker \sigma_i \cong \overline{F_i}$ (e portanto $\ker(\sigma_i)$ é ideal maximal) e como $\ker \sigma_i \subseteq P_i$ e $O_P[y] \subseteq O_{P_i}$, temos $O_{P_i}/P_i \supseteq O_P[y] / \ker \sigma_i$, e então $f(P_i|P) = \left[F'_{P_i} : F_P\right] \geq \left[\overline{F_i} : \overline{F}\right] = \deg \gamma_i(T)$.

Se $i \neq j$, então os polinômios $\gamma_i(T)$ e $\gamma_j(T)$ são relativamente primos em $\overline{F}[T]$, o que implica que existem polinômios $\lambda_i(T), \lambda_j(T) \in O_P[T]$ tais que:

$$1 = \overline{\lambda_i}(T)\gamma_i(T) + \overline{\lambda_j}(T)\gamma_j(T)$$

$$\Rightarrow \overline{\varphi_i}(T)\overline{\lambda_i} + \overline{\varphi_j}(T)\overline{\lambda_j}(T) - 1 = 0$$

$$\Rightarrow \varphi_i(T)\lambda_i(T) + \varphi_j(T)\lambda_j(T) - 1 \in PO_P[T]$$

$$\Rightarrow \varphi_i(y)\lambda_i(y) + \varphi_j(y)\lambda_j(y) - 1 \in PO_P[y]$$

$$\Rightarrow 1 \in P \cdot O_P[y] + \varphi_i(y)O_P[y] + \varphi_j(y)O_P[y] = \ker\sigma_i + \ker\sigma_j$$

Logo, existem z_i em P_i tal que $1 - z_i \in P_j$.

Portanto, se $P_i = P_j$, teríamos $1 \in P_j$, gerando uma contradição ao fato de P_j ser um ideal próprio. Logo, $P_i \neq P_j, i \neq j$.

Suponhamos agora a hipótese adicional $(\star)$, ou seja:

$$\overline{\varphi}(T) = \sum_{i=1}^{r} \gamma_i(T).$$

Então, pela igualdade fundamental, podemos concluir que:

1. $\sum_{i=1}^{r} f(P_i|P) = \sum_{i=1}^{r} e(P_i|P)f(P_i|P) \Rightarrow e(P_i|P) = 1$;
2. $\sum_{i=1}^{r} \deg\varphi_i(T) = \sum_{i=1}^{r} f(P_i|P)$ e $\deg\varphi_i(T) \leq f(P_i|P), \forall i \Rightarrow \deg\varphi_i(T) = f(P_i|P), \forall i$;
3. $\sum_{i=1}^{r} e(P_i|P)f(P_i|P) = \sum_{P'|P} e(P'|P)f(P'|P) \Rightarrow P_1, ..., P_r$ são todos os lugares de F' que estendem P.

Assumiremos agora $(\star\star)$. Como antes, sejam $P_i \in \mathbb{P}_{F'}$ tais que $P_i|P$ e $\varphi_i(y) \in P_i$.

Mostremos que $P_1, ..., P_r$ são as únicas extensões de P em F'.

Temos $0 = \varphi(y) \equiv \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \bmod P \cdot O_P[y]$, logo $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in P \cdot O_P[y]$.

Como y é integral sobre $O_P \Rightarrow y \in O'_P = \bigcap_{P'|P} O_{P'} \Rightarrow O_P[y] \subset O_{P'}, \forall P'|P \Rightarrow \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in P', \forall P'|P$.

Seja $P'|P$.

Como P' é ideal primo, então $\varphi_i(y) \in P'$, para algum $1 \leq i \leq r$. E temos $\ker\sigma_i = P \cdot O_P[y] + \varphi_i(y)O_P[y] \subseteq P' \cap O_P[y]$, e pela maximalidade do núcleo, temos $P \cdot O_P[y] + \varphi_i(y)O_P[y] = P' \cap O_P.[y]$.

Além disso, como $\ker\sigma_i \subseteq P_i \Rightarrow P \cdot O_P[y] + \varphi_i(y)O_P[y] \subseteq P_i \cap O_P[y]$, temos novamente pela maximalidade $P \cdot O_P[y] + \varphi_i(y)O_P[y] = P_i \cap O_P[y]$, e daí $P_i \cap O_P[y] = P' \cap O_P[y]$.

Pela hipótese adicional, $\{1, y, ..., y^{n-1}\}$ é base integral de O'_P sobre $O_P \Rightarrow O'_P = O_P[y] = \bigcap_{i=1}^{r} O_{P_i}$ (Corolário 2.3.5). Logo pela Proposição 2.2.7, existe uma correspondência 1-1 entre os lugares $P'|P$ e os ideais maximais de $O_P[y]$, e assim $P' = P_i$.

Portanto $P_1, ..., P_r$ são as únicas extensões de P em F'.

Pelo teorema da aproximação existem $t_i \in F', i = 1, ..., r$, tais que $v_{P_i}(t_i) = 1$ e $v_{P_j}(t_i) = 0, i \neq j$.

Seja $t \in F$ um parâmetro local P.

Como $t_i \in O_P[y] \cap P_i = P \cdot O_P[y] + \varphi_i(y) O_P[y] = tO_P[y] + \varphi_i(y) O_P[y], i = 1, ..., r$, podemos escrever cada t_i como:

$$t_i = \varphi_i(y) a_i(y) + t b_i(y),$$

onde $a_i(y), b_i(y) \in O_P[y]$.

Logo:

$$\prod_{i=1}^{r} t_i^{\varepsilon_i} = \prod_{i=1}^{r} (\varphi_i(y) a_i(y) + t b_i(y))^{\varepsilon_i} = a(y) \prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} + t b(y),$$

onde $a(y), b(y) \in O_P[y]$.

Usando agora o fato que $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \equiv \varphi(y) \bmod tO_P[y]$, temos $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} \in tO_P[y]$, ou seja, $\prod_{i=1}^{r} \varphi_i(y)^{\varepsilon_i} = tu(y)$, onde $u(y) \in O_P[y]$.

Assim $\varepsilon_i = v_{P_i}(\prod_{i=1}^{r} t_i^{\varepsilon_i}) = v_{P_i}(a(y)tu(y) + tb(y)) \geq v_{P_i}(t) = e(P_i|P)$.

Falta mostrar que $f(P_i|P) = \deg \gamma_i(T)$.

Já vimos que:

1. $\left[\overline{F_i} : \overline{F}\right] = \deg \gamma_i(T)$;

2. $\ker \sigma_i = P_i \cap O_P[y]$.

Pela Proposição 2.2.7, temos então:

$$\frac{O_P[y]}{P_i \cap O_P[y]} \cong \frac{O_{P_i}}{P_i}.$$

Logo:

$$\deg(\gamma_i(T)) = \left[\overline{F_i} : \overline{F}\right] = \left[\frac{O_P[Y]}{\ker(\sigma_i)} : \overline{F}\right] = \left[\frac{O_{P_i}}{P_i} : \overline{F}\right] = f(P_i|P).$$

E assim concluimos $\deg \gamma_i(T) = f(P_i|P)$. Além disso, pela igualdade fundamental, $e(P_i|P) = \varepsilon_i$.

□

2.4 O cotraço de diferenciais de Weil e a fórmula do gênero de Hurwitz

Aqui F/K é um corpo de funções, F'/F extensão separável finita e K' corpo de constantes de F'.

Como F'/F é finita, então K'/K é finita e portanto K'/K é separável.

Queremos associar a cada diferencial de Weil de F/K um diferencial de Weil de F'/K'. O resultado será uma fórmula para o gênero de F', a fórmula do gênero de Hurwitz.

Como F'/F é separável, então $\mathrm{Tr}_{F'/F}$ não é identicamente nula.

Definição 2.4.1. Para $P \in \mathbb{P}_F$ seja $O'_P = \mathrm{ic}_{F'}(O_P)$ o fecho intgral de O_P em F'. Então o conjunto:

$$\mathcal{C}_P := \left\{z \in F'; \mathrm{Tr}_{F'/F}(zO'_P) \subseteq O_P\right\}$$

é chamado de módulo complementar sobre O_P.

Proposição 2.4.2. *Com a notação da definição anterior, vale:*

1. *$\mathcal{C}_P$ é um O'_P-módulo e $O'_P \subseteq \mathcal{C}_P$;*

2. *Se $\{z_1, ..., z_n\}$ é uma base integral de O'_P sobre O_P, então $\mathcal{C}_P = \sum_{i=1}^{n} O'_P z_i^*$, onde $\{z_1^*, ..., z_n^*\}$ é a base dual de $\{z_1, ..., z_n\}$;*

3. *Existe $t \in F'$ (dependendo de P) tal que $\mathcal{C}_P = tO'_P$. Além disso, $v_{P'}(t) \leq 0, \forall P'|P$, e, $\forall t' \in F'$, temos: $\mathcal{C}_P = t'O'_P \Leftrightarrow v_{P'}(t') = v_{P'}(t), \forall P'|P$;*

4. $\mathcal{C}_P = O'_P$ *para quase todo* $P \in \mathbb{P}_F$.

Demonstração. 1. Seja $z \in \mathcal{C}_P$ e $\alpha, \beta \in O'_P$, então $\mathrm{Tr}_{F'/F}(z\alpha\beta) = \mathrm{Tr}_{F'/F}(z\alpha)\,\mathrm{Tr}_{F'/F}(\beta) \in O_P$. Portanto $\mathcal{C}_P$ é um O'_P-módulo. Além disso, pelo Corolário 2.3.2, segue que $O'_P \subseteq \mathcal{C}_P$.

2. Seja $\{z_1, ..., z_n\}$ base integral de O'_P sobre O_P, considere sua base dual $\{z_1^*, ..., z_n^*\}$, e $z \in \mathcal{C}_P$. Logo existem $x_1, ..., x_n \in F$ tais que $z = \sum x_i z_i^*$ e $\mathrm{Tr}_{F'/F}(zz_j) \in O_P, 1 \leq j \leq n$.

   Veja ainda que $\mathrm{Tr}_{F'/F}(zz_j) = x_j$. Portanto $x_j \in O_P$ e $z \in \sum O_P z_i^*$, ou seja, $\mathcal{C}_P \subseteq \sum O_P z_i^*$.

   Seja $z \in \sum O_P z_i^*$ e $u \in O'_P$, então $z = \sum x_i z_i^*$ e $u = \sum y_j z_j$, onde $x_i, y_j \in O_P$. E assim temos $\mathrm{Tr}_{F'/F}(zu) = \sum_{i,j} x_i y_j \,\mathrm{Tr}_{F'/F}(z_i^* z_j) = \sum x_i y_i \in O_P$. Logo $\sum O_P z_i^* \subseteq \mathcal{C}_P$.

3. Do item 2, $\mathcal{C}_P = \sum O_P u_i$, para alguma base $\{u_1, ..., u_n\}$ de F'/F apropriada.

   Seja $x \in F$ tal que $v_P(x) \geq -v_{P'}(u_i), \forall P'|P$ e $i = 1, ..., n$. Assim, $v_{P'}(xu_i) \geq 0, \forall P'|P$ e $i = 1, ..., n$. Como $O_P \subseteq O'_P$, então $x \cdot \mathcal{C}_P \subseteq O'_P$, e, pelo item 1, $\mathcal{C}_P$ é um O'_P-módulo, logo $x \cdot \mathcal{C}_P$ é um ideal de O'_P.

   Pela Proposição 2.2.8, O'_P é um domínio de ideais principais, o que implica $x \cdot \mathcal{C}_P = yO'_P$, para algum $y \in O'_P$.

   Definindo $t = x^{-1}y$, temos $\mathcal{C}_P = tO'_P$. E, por $O'_P \subseteq \mathcal{C}_P$, temos $v_{P'}(t) \leq 0, \forall P'|P$. De fato, $1 = tz$, para algum $z \in O'_P$, e assim $v_{P'}(t) = -v_{P'}(z) \leq 0, \forall P'|P$.

   Por fim, se $t' \in F'$:

$$tO'_P = t'O'_P \Leftrightarrow tt'^{-1}, t^{-1}t' \in O'_P \Leftrightarrow v_{P'}(tt'^{-1}) = 0, \forall P'|P$$

$$\Leftrightarrow v_{P'}(t) = v_{P'}(t'), \forall P'|P.$$

4. Seja $\{z_1, ..., z_n\}$ base de F'/F. Então $\{z_1, ..., z_n\}$ é base integral para quase todo $P \in \mathbb{P}_F$ e $\{z_1^*, ..., z_n^*\}$ é base integral para quase $P \in \mathbb{P}_F$, pelo Teorema 2.3.6. Logo, pelo item 2, $O'_P = \mathcal{C}_P$, para quase todo $P \in \mathbb{P}_F$.

□

Definição 2.4.3. Considere um lugar $P \in \mathbb{P}_F$ e o fecho integral O'_P de O_P em F'. Seja $\mathcal{C}_P = tO'_P$ o módulo complementar sobre O_P. Então definimos para $P'|P$ o expoente da diferente de P' sobre P por $d(P'|P) = -v_{P'}(t)$.

Pela Proposição 2.4.2, $d(P'|P)$ está bem definido e $d(P'|P) \geq 0$. Além disso, como $\mathcal{C}_P = O'_P$ para quase todo $P \in \mathbb{P}_F$, então $t = 1$, para quase todo $P \in \mathbb{P}_F$, ou seja, $d(P'|P) = 0$ para quase todo $P \in \mathbb{P}_F$ e $P'|P$.

Portanto, podemos definir o divisor:

$$\mathrm{Diff}(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P)P'.$$

Este divisor é chamado o divisor da diferente de F'/F.

Observe que $\mathrm{Diff}(F'/F)$ é divisor de F' onde $\mathrm{Diff}(F'/F) \geq 0$.

Observação 2.4.4. Outra característica importante do módulo complementar é que $\forall z \in F'$:

$$z \in \mathcal{C}_P \Leftrightarrow v_{P'}(z) \geq -d(P'|P), \forall P'|P$$

(isso segue do teorema da aproximação).

Seja $z \in \mathcal{C}_P$, então $z \in tO'_P$, ou seja, existe $\alpha \in O'_P$ tal que $z = t\alpha$. Assim, para todo $P' \in \mathbb{P}_{F'}$ tal que $P'|P$, $v_{P'}(z) = v_{P'}(t) + v_{P'}(\alpha)$, e temos $v_{P'}(z) = v_{P'}(\alpha) - d(P'|P) \geq -d(P'|P)$.

Agora, seja $z \in F'$ tal que $v_{P'}(z) \geq -d(P'|P), \forall P'|P$, então $v_{P'}(z) + d(P'|P) \geq 0, \forall P'|P$ (podemos supor que $z \neq 0$, pois, caso contrário, segue trivialmente). Pelo teorema da aproximação forte, existe $\alpha \in F'$ (não nulo) onde $v_{P'}(\alpha) = v_{P'}(z) + d(P'|P) \geq 0, \forall P'|P$. Logo $\alpha \in O'_P$ e $v_{P'}(t\alpha) = v_{P'}(z)$, o que implica $t\alpha = kz$, onde k é invertível em O'_P, e por fim $z = \alpha k^{-1} t \in tO'_P = \mathcal{C}_P$.

Definição 2.4.5. Seja $\mathcal{A}_{F'/F} := \{\alpha \in \mathcal{A}_{F'}; \alpha_{P'} = \alpha_{Q'}$ sempre que $P' \cap F = Q' \cap F\}$.

Tal conjunto é um $F'-$subespaço de $\mathcal{A}_{F'}$.

Observemos que como $\mathrm{Tr}_{F'/F} : F' \to F$ é $F-$linear, podemos extendê-la a uma aplicação $F-$linear (també denotada por $\mathrm{Tr}_{F'/F}$) de $\mathcal{A}_{F'/F}$ a $\mathcal{A}_F$ definida por:

$$(\mathrm{Tr}_{F'/F}(\alpha))_P := \mathrm{Tr}_{F'/F}(\alpha_{P'}),$$

para $\alpha \in \mathcal{A}_{F'/F}$, onde P' é um lugar de F' estendendo P.

Como $\alpha_{P'} \in O_{P'}$, para quase todo $P' \in \mathbb{P}_{F'}$, então $\mathrm{Tr}_{F'/F}(\alpha_{P'}) \in O_P$ para quase todo $P \in \mathbb{P}_F$ (Corolário 2.3.2), assim $\mathrm{Tr}_{F'/F}(\alpha) \in \mathcal{A}_F$.

Veja ainda que o traço do adele principal $z \in F'$ é o adele principal de $\mathrm{Tr}_{F'/F}(z)$. E, se $A' \in \mathrm{Div}(F')$, definimos:

$$\mathcal{A}_{F'/F}(A') := \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}.$$

Teorema 2.4.6. *Na situação acima, para todo diferencial de Weil $\omega \in \Omega_F$ existe um único diferencial de Weil $\omega' \in \Omega_{F'}$ tal que:*

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega(\mathrm{Tr}_{F'/F}(\alpha)),$$

$\forall \alpha \in \mathcal{A}_{F'/F}$. Este diferencial de Weil é chamado cotraço de ω em F'/F, e é denotado por $\mathrm{Cotr}_{F'/F}(\omega)$. Se $\omega \neq 0$ e $(\omega) \in \mathrm{Div}(F)$ é o divisor canônico de ω, então:

$$(\mathrm{Cotr}_{F'/F}(\omega)) = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F).$$

Para demonstrar o teorema, precisamos de dois lemas:

Lema 2.4.7. *Para cada $C' \in \mathrm{Div}(F')$, temos $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$.*

Demonstração. Seja $\alpha = (\alpha_{P'})_{P'} \in \mathcal{A}_{F'}$. Para cada $P \in \mathbb{P}_F$, existe $x_P \in F'$ tal que $v_{P'}(\alpha_{P'} - x_P) \geq -v_{P'}(C'), \forall P'|P$ (teorema da aproximação).

Defina $\beta = (\beta_{P'})_{P'}$ com $\beta_{P'} := x_P, \forall P'|P$. Logo $\beta \in \mathcal{A}_{F'/F}$ e $\alpha - \beta \in \mathcal{A}_{F'}(C')$. Como $\alpha = \beta + (\alpha - \beta)$, segue o resultado.

□

Lema 2.4.8. *Sejam M/L extensão finita separável de corpos, 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 $\mathrm{Tr}_{M/L} \circ \mu' = \mu$.*

Demonstração. Considere $\hat{M} := \{\lambda : M \to L; \lambda \text{ é } L-\text{linear}\}$ um espaço vetorial sobre M definindo $(z\lambda)(w) = \lambda(zw)$, $\lambda \in \hat{M}$ e $z, w \in M$, então $\dim_M(\hat{M}) = 1$, logo se $\lambda \in \hat{M}$, existe um único $z \in M$ tal que $\lambda = z \,\mathrm{Tr}_{M/L}$.

Para fixado $v \in V$, defina $\lambda_v : M \to L$, onde $\lambda_v(a) = \mu(av), \forall a \in M$. E, como antes, existe um único $z_v \in M$ tal que $\lambda_v = z_v \,\mathrm{Tr}_{M/L}$.

Definindo $\mu' : V \to M$, dada por $\mu'(v) = z_v$, temos $\mu(av) = \mathrm{Tr}_{M/L}(a\mu'(v)), \forall v \in V, \forall a \in M$, e μ' é $M-$linear.

Fazendo $a = 1$, temos $\mu(v) = \mathrm{Tr}_{M/L}(\mu'(v)), \forall v \in V$. Ou seja, $\mathrm{Tr}_{M/L} \circ \mu' = \mu$ $(\star)$.

Para a unicidade, suponha μ^*, diferente de μ', satisfazendo também $(\star)$. Então $\mu' - \mu^*$ é $M-$linear não nula. Mas por $(\star)$ temos $\mathrm{Tr}_{M/L} \circ (\mu' - \mu^*) = 0 \Rightarrow \mathrm{Tr}_{M/L} = 0$, absurdo, pois M/L é separável finita.

□

Demonstração. (do Teorema 2.4.6)

Primeiro mostremos que existe um diferencial de Weil $\omega' \in \Omega_{F'}$ tal que $\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega(\mathrm{Tr}_{F'/F}(\alpha)), \forall \alpha \in \mathcal{A}_{F'/F}$.

Se $\omega = 0$, basta tomar $\omega' := 0$.

Podemos agora tomar ω não nulo.

Defina $W' := \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$. A construção de ω' será dada em 3 passos:

1. A aplicação $K-$linear $\omega_1 : \mathcal{A}_{F'/F} \to K$, dada por $\omega_1 = \omega \circ \mathrm{Tr}_{F'/F}$ tem as seguintes propriedades:

   (a) $\omega_1(\alpha) = 0, \forall \alpha \in \mathcal{A}_{F'/F}(W') + F'$;

   (b) Se $B' \in \mathrm{Div}(F')$ é um divisor com onde **não vale** $B' \leq W'$, então existe um adele $\beta \in \mathcal{A}_{F'/F}(B')$ com $\omega_1(\beta) \neq 0$.

   Demonstração. (a) Seja $z \in F'$, então $\mathrm{Tr}_{F'/F}(z) \in F$, logo $\omega_1(z) = 0$, pois ω se anula em F.

Seja, agora, $\alpha \in \mathcal{A}_{F'/F}(W')$. Observe que se $\forall P \in \mathbb{P}_F$ e $P'|P$ tivermos $v_P(\mathrm{Tr}_{F'/F}(\alpha_{P'})) \geq -v_P(\omega)$, então, pela definição do divisor canônico (ω), $\omega_1(\alpha) = 0$.

Assim, seja $P \in \mathbb{P}_F$, seja $x \in F$ tal que $v_P(x) = v_P(\omega)$, então:

$$v_{P'}(x\alpha_{P'}) \geq e(P'|P)v_P(\omega) - v_{P'}(W') = -d(P'|P),$$

e, pela observação 2.4.4, $x\alpha_{P'} \in \mathcal{C}_P$. O que significa $\mathrm{Tr}_{F'/F}(x\alpha_{P'}) \in O_P$, e assim temos o resultado.

(b) Seja $B' \in \mathrm{Div}(F')$ tal que existe $P^* \in \mathbb{P}_{F'}$ tal que $v_{P^*}(B') > v_{P^*}(W')$, então existe $P_0 \in \mathbb{P}_F$ tal que $P^*|P_0$ e $v_{P^*}(\mathrm{Con}_{F'/F}((\omega)) - B') < -d(P^*|P)$.

Considere O'_{P_0} o fecho integral e $\mathcal{C}_{P_0}$ o módulo complementar de O_{P_0} em F', e defina o conjunto:

$$J := \left\{z \in F'; v_{P^*}(z) \geq v_{P^*}(\mathrm{Con}_{F'/F}((\omega)) - B'), \forall P^*|P_0\right\}.$$

Pela teorema da aproximação, existe $u \in J$ tal que $v_{P^*}(z) = v_{P^*}(\mathrm{Con}_{F'/F}((\omega)) - B'), \forall P^*|P_0$. E, pela observação 2.4.4, $u \notin \mathcal{C}_{P_0}$, ou seja, J não está contido em $\mathcal{C}_{P_0}$. Observe que $J \cdot O_{P_0} \subseteq J$, e assim $\mathrm{Tr}_{F'/F}(J)$ não está contido em O_{P_0}.

Seja t um parâmetro local de P_0 e seja:

$$r \geq \max_{P^*|P_0} \left\{\left|v_{P^*}(\mathrm{Con}_{F'/F}((\omega)) - B')\right|\right\}.$$

Temos $t^r J \subseteq O'_{P_0}$, e consequentemente $t^r \,\mathrm{Tr}_{F'/F}(J) \subseteq O_{P_0}$ é um ideal de O_{P_0}. Assim existe um inteiro $s \geq 0$ tal que $t^r \,\mathrm{Tr}_{F'/F}(J) = t^s O_{P_0}$, e assim obtemos $\mathrm{Tr}_{F'/F}(J) = t^m O_{P_0}$, e como $\mathrm{Tr}_{F'/F}(J)$ não está contido em O_{P_0}, resulta $m \leq -1$.

Pela Proposição 1.7.2, item 1, temos $v_P(\omega) = \max\{r \in \mathbb{Z}; \omega_P(x) = 0, \forall x \in F \text{ com } v_P(x) \geq -r\}$. Então tomando $x \in F$ tal que $v_{P_0}(x) = -v_{P_0}(\omega) - 1$, faz sentido escolher x de forma que $\omega_{P_0}(x) \neq 0$. Tomando $y \in F$ tal que $v_{P_0}(y) = v_{P_0}(\omega)$, temos $v_{P_0}(xy) = -1 \Rightarrow xy \in t^{-1}O_{P_0} \Rightarrow \exists z \in J$ tal que $\mathrm{Tr}_{F'/F}(z) = xy$, pois $t^{-1}O_{P_0} \subseteq \mathrm{Tr}_{F'/F}(J)$.

Defina agora o adele $\beta \in \mathcal{A}_{F'/F}$ onde $\beta_{P'} = 0$ se P' não é extensão de P_0 e $\beta_{P'} = y^{-1}z$ se $P'|P_0$. Temos $\beta \in \mathcal{A}_{F'/F}(B')$. Por fim, veja que $\omega_1(\beta) \neq 0$, isto é, existe $\beta \in \mathcal{A}_{F'/F}(B')$ tal que $\omega_1(\beta) \neq 0$.

□

2. Defina $\omega_2 : \mathcal{A}_{F'} \to K$ como segue:

   Para cada $\alpha \in \mathcal{A}_{F'}$, existem $\beta \in \mathcal{A}_{F'/F}$ e $\gamma \in \mathcal{A}_{F'}(W')$ tal que $\alpha = \beta + \gamma$ (Lema 2.4.7). Defina $\omega_2(\alpha) := \omega_1(\beta)$.

   Temos que ω_2 é uma aplicação $K-$linear e satisfaz:

   (a) $\omega_2(\alpha) = 0, \forall \alpha \in \mathcal{A}_{F'}(W') + F'$;

   (b) Se $B' \in \mathrm{Div}(F')$ é tal que $B' \leq W'$ **não vale**, então existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\omega_2(\beta) \neq 0$.

   Demonstração. (a) Seja $\alpha \in \mathcal{A}_{F'}(W') + F'$, então

   $$\alpha = \underbrace{\beta}_{\in \mathcal{A}_{F'}(W')} + \underbrace{f}_{\in F'} = \underbrace{\beta}_{\in \mathcal{A}_{F'}(W')} + \underbrace{(0+f)}_{\in \mathcal{A}_{F'/F}(W')+F' \subseteq \mathcal{A}_{F'/F}}.$$

   (b) Seja $B'\,\mathrm{Div}(F')$ tal que não vale $B' \leq W'$, então pelo item (b) do passo 1, existe $\beta \in \mathcal{A}_{F'/F}(B')$ tal que $\omega_1(\beta) \neq 0$. Como $\mathcal{A}_{F'/F}(B') \subseteq \mathcal{A}_{F'}(B')$, então $\omega_2(\beta) = \omega_1(\beta) \neq 0$.

   Temos que ω_2 é $K-$linear e se anula em $\mathcal{A}_{F'}(W') + F'$, mas como $\omega_2 : \mathcal{A}_{F'} \to K$ temos que se $K \subsetneq K'$, então ω_2 não é um diferencial de Weil de F'/K'.

   □

3. Temos $\omega_2 : \mathcal{A}_{F'} \to K$, é $K-$linear, e $\mathcal{A}_{F'}$ é $K'-$espaço vetorial. Logo, pelo Lema 2.4.8, existe uma única $\omega' : \mathcal{A}_{F'} \to K'$ aplicação $K'-$linear tal que $\mathrm{Tr}_{K'/K} \circ \omega' = \omega_2$, e pela forma que ω_1 e ω_2 foram definidas, temos que se $\alpha \in \mathcal{A}_{F'/F}$, então $\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega(\mathrm{Tr}_{F/F}(\alpha))$.

   Além disso:

(a) $\omega'(\alpha) = 0, \forall \alpha \in \mathcal{A}_{F'}(W') + F'$;

(b) Se $B' \in \mathrm{Div}(F')$ é tal que $B' \leq W'$ **não vale**, então existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\omega'(\beta) \neq 0$.

Demonstração. (a) Como ω' é $K'-$linear, então a imagem de $\mathcal{A}_{F'}(W') + F'$ por ω' é $\{0\}$ ou K'. Caso $\omega'(\mathcal{A}_{F'}(W') + F') = K'$, como $\mathrm{Tr}_{K'/K}$ é não nula, então existe $\alpha \in \mathcal{A}_{F'}(W') + F'$ tal que $0 \neq \mathrm{Tr}_{K'/K}(\omega(\alpha)) = \omega_2(\alpha)$, contrariando o item (a) do passo 2.

(b) Pelo item (b) do passo 2, existe $\beta \in \mathcal{A}_{F'}(B')$ tal que $\omega_2(\beta) \neq 0$, então $\mathrm{Tr}_{K'/K}(\omega(\beta)) \neq 0 \Rightarrow \omega'(\beta) \neq 0$.

□

Falta mostrar que $(\omega') = W'$.

Seja $A \in M(\omega')$, veja que se não tivemos $A \leq W'$, então existe $\alpha \in \mathcal{A}_{F'}(A)$ tal que $\omega'(\alpha) \neq 0 \Rightarrow A \notin M(\omega')$, ou seja, $\forall A \in M(\omega')$ então $A \leq W'$. Portanto, $(\omega') = W' = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$.

Por fim, a unicidade de ω': suponha $\omega^* \in \Omega_{F'}$ tal que $\mathrm{Tr}_{K'/K}(\omega^*(\alpha)) = \omega(\mathrm{Tr}_{F'/F}(\alpha)), \forall \alpha \in \mathcal{A}_{F'/F}$.

Defina $\eta := \omega^* - \omega'$, então $\mathrm{Tr}_{K'/K}(\eta(\alpha)) = 0, \forall \alpha \in \mathcal{A}_{F'/F}$. Além disso, como $\eta \in \Omega_{F'}$, existe $C' \in \mathrm{Div}(F')$ tal que η anula $\mathcal{A}_{F'}(C') + F'$, logo, pelo Lema 2.4.7, $\mathrm{Tr}_{K'/K} \circ \eta \equiv 0 \Rightarrow \eta \equiv 0$, portanto $\omega' = \omega^*$.

Notação: $\omega' = \mathrm{Cotr}_{F'/F}(\omega)$.

□

Teorema 2.4.9. *(Fórmula do gênero de Hurwitz)*

Sejam F/K um corpo de funções algébricas de gênero g e F'/F uma extensão finita separável, com K' o corpo de constantes de F' e g' é o gênero de F'/K'. Então:

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg(\mathrm{Diff}(F'/F)).$$

Demonstração. Seja $0 \neq \omega \in \Omega_F$. Pelo Teorema 2.4.6, temos: $(\mathrm{Cotr}_{F'/F}(\omega)) = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$.

Como o gênero de F/K é g e o de F'/K' é g', então $\deg(\mathrm{Cotr}_{F'/F}(\omega)) = 2g' - 2$, o que implica $2g' - 2 = \deg(\mathrm{Cotr}_{F'/F}(\omega)) = \deg(\mathrm{Con}_{F'/F}((\omega))) + \deg(\mathrm{Diff}(F'/F))$. Pelo Corolário 2.1.13, temos:

$$2g' - 2 = \frac{[F' : F]}{[K' : K]} \deg((\omega)) + \deg(\mathrm{Diff}(F'/F)),$$

e assim temos o resultado.

□

2.5 A diferente

Aqui F'/F é extensão algébrica finita separável, onde F/K e F'/K' são corpos de funções algébricas com corpo de constantes K e K', respectivamente, onde K é perfeito.

Estudaremos como o índice de ramificação $e(P|P)$ e o expoente da diferente $d(P'|P)$ se relacionam.

Teorema 2.5.1. *(Teorema da diferente de Dedekind)*

Para toda $P'|P$, temos:

1. $d(P'|P) \geq e(P'|P) - 1$;
2. $d(P'|P) = e(P'|P) - 1$ *se, e somente se,* $e(P'|P)$ *não é divisível por* $\mathrm{char}\, K$. *Em particular, se* $\mathrm{char}\, K = 0$, $e(P'|P) - 1 = d(P'|P)$.

Para demonstrar o item 1 do teorema precisamos do seguinte lema:

Lema 2.5.2. *Sejam F^*/F uma extensão algébrica de corpos de funções algébricas, $P \in \mathbb{P}_F$ e P^* lugar de F^* extensão de P. Considere um automorfismo σ de F^*/F. Então $\sigma(P^*) := \{\sigma(z); z \in P^*\}$ é um lugar de F^* e:*

1. $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y)), \forall y \in F^*$;
2. $\sigma(P^*)|P$;
3. $e(\sigma(P^*)|P) = e(P'|P)$ *e* $f(\sigma(P^*)|P) = f(P'|P)$.

Demonstração. Seja σ automorfismo. Como O_{P^*} é anel de valorização de P^*, então $\sigma(O_{P^*})$ também o é, e $\sigma(P^*)$ é ideal maximal de $\sigma(O_{P^*})$. Assim, $\sigma(P^*)$ é lugar de F^*, com anel de valorização $O_{\sigma(P^*)} = \sigma(O_{P^*})$. Além disso, se t^* for um parâmetro local de P^*, então $\sigma(t^*)$ será parâmetro local de $\sigma(P^*)$.

De fato, como $O_{P^*} \subsetneq F^*$, então $\sigma(O_{P^*}) \subsetneq F^*$, e como $K^* \subsetneq O_{P^*}$, então $\sigma(O_{P^*})$ contém uma cópia isomorfa de K^*.

Seja $z \in F^*$, então existe $y \in F^*$ tal que $z = \sigma(y)$. Se $y \in O_{P^*}$, então $z \in \sigma(O_{P^*})$, e se $y \notin O_{P^*}$, então $z^{-1} = \sigma(y^{-1}) \in \sigma(O_{P^*})$.

Temos também que como P^* é um ideal maximal de O_{P^*}, então $\sigma(P^*)$ é um ideal maximal de $\sigma(O_{P^*})$.

Além disso, se t^* é um parâmetro local de P^*, então $t^*O_{P^*} = P^*$, e temos $\sigma(P^*) = \sigma(t^*O_{P^*}) = \sigma(t^*)\sigma(O_{P^*})$, ou seja, $\sigma(t^*)$ é um parâmetro local de $\sigma(P^*)$.

1. Mostremos que $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y)), \forall y \in F^*$.

   Se $y = 0$, o resultado segue trivialmente. Então seja $y \in F^*$ não nulo, logo existe $z \in F^*$ não nulo, onde $y = \sigma(z)$. Escrevendo $z = (t^*)^r u$, onde u é uma unidade de O_{P^*}; e assim temos que podemos escrever $y = (\sigma(t^*))^r \sigma(u)$, onde $\sigma(u)$ é uma unidade de $O_{\sigma(P^*)}$, logo $v_{\sigma(P^*)}(y) = r = v_{P^*}(z) = v_{P^*}(\sigma^{-1}(y))$.

2. Como σ é automorfismo de F^*/F, então $\sigma(a) = a, \forall a \in F$, o que implica $\sigma(P) = P$. E, como $P^*|P$, então $P = \sigma(P) \subseteq \sigma(P^*) \Rightarrow \sigma(P^*)|P$.

3. Seja $x \in F$ um parâmetro local de P, então $e(\sigma(P^*)|P) = v_{\sigma(P^*)}(x) = v_{P^*}(\sigma^{-1}(x)) = v_{P^*}(x) = e(P^*|P)$.

   Agora definindo $\overline{\sigma} : F^*_{P^*} \to F^*_{\sigma(P^*)}$, onde $\overline{\sigma}(z + P^*) = \sigma(z) + \sigma(P^*)$, temos que $\overline{\sigma}$ é um isomorfismo.

   Além disso, $\overline{\sigma}$ quando restito a F_P é igual a identidade Id, ou seja, $\overline{\sigma}$ é F_P-linear.

   Portanto $[F^*_{P^*} : F_P] = \left[F^*_{\sigma(P^*)} : F_P\right]$, isto é, $f(P^*|P) = f(\sigma(P^*)|P)$

□

Demonstração. (do Teorema 2.5.1, item 1)

Seja O'_P o fecho integral de O_P em F', e $\mathcal{C}_P$ o módulo complementar sobre O_P.

Veja que se $\mathrm{Tr}_{F'/F}(tO_{P'}) \in\subseteq O_P, \forall t \in F'$ tal que $v_{P'}(t) = 1 - e(P'|P), \forall P'|P$, então pela observação 2.4.4 temos $d(P'|P) \geq e(P'|P) - 1, \forall P'|P$.

Basta então mostrar este fato.

Seja F^*/F extensão de Galois finita tal que $F \subseteq F' \subseteq F^*$. Escolha $n = [F' : F]$ automorfismos distintos $\sigma_1, ..., \sigma_n$ de F^*/F, tais que suas restrições a F' são distintas.

Para $z \in O'_P$, temos:

$$\mathrm{Tr}_{F'/F}(tz) = \sum_{i=1}^{n} \sigma_i(tz).(\star)$$

Fixe P^* lugar de F^* tal que $P^*|P$ e defina: $P_i^* := \sigma_i^{-1}(P^*)$ e $P'_i = P_i^* \cap F'$.

Como $z \in O'_P$, então $\sigma_i(z)$ é também integral sobre O_P, assim, $v_{P^*}(\sigma_i(z)) \geq 0$. Agora, pelo Lema 2.5.2, temos: $v_{P^*}(\sigma_i(tz)) > -e(P^*|P)(\star\star)$.

Por $(\star)$, temos:

$$\begin{gathered}
\mathrm{Tr}_{F'/F}(tz) = \textstyle\sum_{i=1}^{n} \sigma_i(tz) \Rightarrow \\
e(P^*|P)v_P(\mathrm{Tr}_{F'/F}(tz)) = v_{P^*}(\mathrm{Tr}_{F'/F}(tz)) = v_{P^*}(\textstyle\sum_{i=1}^{n} \sigma_i(tz)) \geq \\
\min\{v_{P^*}(\sigma_i(tz))\} \underbrace{>}_{(\star\star)} -e(P^*|P) \Rightarrow \\
\mathrm{Tr}_{F'/F}(tO'_P) \subseteq O_P.
\end{gathered}$$

□

Para demonstar o item 2 do Teorema 2.5.1, precisaremos do seguinte lema:

Lema 2.5.3. *Sejam P lugar de F, $P_1, ..., P_r$ todas as extensões de P em F'/F. Considere os corpos $k := O_P/P$ e $k_i := O_{P_i}/P_i \supseteq k$ e as correspondentes aplicações de classe residual $\pi : O_P \to k$ e $\pi_i : O_{P_i} \to k_i (i = 1, ..., r)$. Então $\forall u \in O'_P$, temos:*

$$\pi(\mathrm{Tr}_{F'/F}(u)) = \sum_{i=1}^{r} e(P_i|P)\, \mathrm{Tr}_{k_i/k}(\pi_i(u)).$$

Demonstração. (do Teorema 2.5.1, item 2)

Vamos manter as mesmas notações do Lema 2.5.3 e abreviarmos $e_i := e(P_i|P)$. Seja $P' = P_1$ e $e := (P'|P)$, deve ser demonstrado que $d(P'|P) = e - 1 \Leftrightarrow \mathrm{char}\, K$ não divide e.

Primeiro assuma que e não é divisível por $\mathrm{char}\, K$.

Suponha por absurdo que $d(P'|P) \geq e$. Seja $w \in F'$ tal que $v_{P_i}(w) \leq -e, i = 1, ..., r$, logo $v_{P'}(w) \leq -e$ e $w \in \mathcal{C}_P$.

Como K é perfeito, então k_i/k é separável, e podemos tomar $y_0 \in O_{P'}$ tal que $\mathrm{Tr}_{k_1/k}(\pi_1(y_0)) \neq 0$.

Pelo teorema da aproximação, existe $y \in F'$ tal que $v_{P'}(y - y_0) > 0$ e $v_{P_i}(y) \geq \max\{1, e_i + v_{P_i}(w)\}, i = 2, ..., r$ (I). Logo $y \in O'_P$, e pelo Lema 2.5.3, temos: $\pi(\mathrm{Tr}_{F'/F}(y)) = e\,\mathrm{Tr}_{k_1/k}(\pi_1(y)) + \sum_{i=2}^{r} e_i\,\mathrm{Tr}_{k_i/k}(\pi_i(y))(\star)$.

Obeserve que y foi tomado de forma que $y \in P_i, i = 2, ..., r$, assim $\mathrm{Tr}_{k_i/k}(\pi_i(y)) = 0$, e $\pi_1(y) = \pi_1(y_0)$; portanto, por $(\star)$, $\pi(\mathrm{Tr}_{F'/F}(y)) = e\,\mathrm{Tr}_{k_1/k}(\pi_1(y_0)) \neq 0$, pois $\mathrm{char}\,K$ não divide e.

Assim, $\pi(\mathrm{Tr}_{F'/F}(y)) \neq 0 \Rightarrow v_P(\mathrm{Tr}_{F'/F}(y)) = 0$.

Agora seja $x \in F$ um parâmetro local de P, então $\mathrm{Tr}_{F'/F}(x^{-1}y) \notin O_P$.(II)

Mas, considerando o elemento $x^{-1}yw^{-1}$, temos, por (I), $v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geq 0$ e $v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P_i}(w)) \geq 0, i = 2, ..., r$, e portanto $x^{-1}y \in wO'_P \Rightarrow \mathrm{Tr}_{F'/F}(x^{-1}y) \in O_P$, absurdo por (II).

Falta mostrar a outra implicação, que é equivalente a $\mathrm{char}\,K$ divide $e \Rightarrow d(P'|P) \geq e$.

Pelo teorema da aproximação, podemos tomar $u \in F'$ tal que $v_{P'}(u) = -e$ e $v_{P_i}(u) \geq -e_i + 1, i = 2, ..., r$. Como antes, seja $x \in F$ um parâmetro local de P. Então para cada $z \in O'_P$, temos $v_{P'}(xuz) \geq 0$ e $v_{P_i}(xuz) > 0, i = 2, ..., r$ $(\Rightarrow xuz \in O'_P)$, e pelo Lema 2.5.3 segue que $\pi(\mathrm{Tr}_{F'/F}(xuz)) = e\,\mathrm{Tr}_{k_1/k}(\pi_1(xuz)) = 0$. Logo:

$$\mathrm{Tr}_{F'/F}(xuz) = x\,\mathrm{Tr}_{F'/F}(uz) \in P = xO_P \Rightarrow \mathrm{Tr}_{F'/F}(uz) \in O_P, \forall z \in O'_P,$$

ou seja, $u \in \mathcal{C}_P$ e $v_{P'}(u) = -e$, e pela observação 2.4.4, temos $-e = v_{P'}(u) \geq -d(P'|P)$, isto é, $d(P'|P) \geq e$.

□

Demonstração. (do Lema 2.5.3)

O traço $\mathrm{Tr}_{F'/F}(u)$ pode ser calculado como o traço de uma aplição $F-$linear $\mu : F' \to F'$ dada por $\mu(z) = uz$.

Primeiro mostremos que $\pi(\mathrm{Tr}_{F'/F}(u))$ tem uma interpretação como o traço de uma certa aplicação $k-$linear $\overline{\mu} : V \to V$ (onde V é um $k-$espaço ainda a ser definido);

decompondo V em subespaços invariantes, teremos o resultado.

Seja $t \in F$ um parâmetro local de P. O quociente $V = O'_P/tO'_P$ pode ser considerado um $k-$espaço definindo $(x + P)(z + tO'_P) := xz + (tO'_P), (x \in O_P \text{ e } z \in O'_P)$. Seja $\{z_1, ..., z_n\}$ uma base integral de O'_P sobre O_P. Então $\{z_1 + tO'_P, ..., z_n + tO'_P\}$ constitui ums base de V sobre k, em particular, $\dim_k V = n$.

Definimos a aplicação $k-$linear $\overline{\mu} : V \to V$ por $\overline{\mu}(z + tO'_P) = uz + tO'_P$.

Seja $A = (a_{i,j})_{1 \leq i,j \leq n}$ a matriz de μ com respeito a base $\{z_1, ..., z_n\}$. Como esta é uma base integral, então $O'_P = \sum_{i=1}^n O_P z_i$, e como $u \in O'_P$, então $uz_i \in O'_P = \sum_{i=1}^n O_P z_i$, logo os coeficientes de $A = (a_{i,j})_{1 \leq i,j \leq n}$ estão em O_P.

Veja que $\overline{\mu}(z_j + tO'_P) = (a_{1j} + P)(z_1 + tO'_P) + ... + (a_{nj} + P)(z_n + tO'_P)$, logo $\overline{A} := (\pi(a_{i,j}))_{1 \leq i,j \leq n}$ é a representação de $\overline{\mu}$ na base $\{z_1 + tO'_P, ..., z_n + tO'_P\}$. Assim:

$$\pi(\mathrm{Tr}_{F'/F}(u)) = \pi(\mathrm{Tr}(A)) = \mathrm{Tr}(\overline{A}) = \mathrm{Tr}(\overline{\mu}).(\star)$$

P_i é ideal maximal (único) de $O_{P_i} \Rightarrow \forall z \in O_{P_i}$ e $\forall x \in P_i$ temos $zx \in P_i$, e assim segue que $P_i^{e_i}$ é ideal.

Para $1 \leq i \leq r$, induza os quocientes $V_i := O_{P_i}/P_i^{e_i}$ e as aplicações $\mu_i : V_i \to V_i$ dadas por $\mu_i(z + P_i^{e_i}) := uz + P_i^{e_i}$. Temos que V_i são $k-$espaços vetoriais e μ_i são $k-$lineares.

Assim podemos construir o isomorfismo:

$$f : V \to \bigoplus_{i=1}^{r} V_i,$$

dado por $f(z+tO'_P) := (z+P_1^{e_1}, ..., z+P_r^{e_r})$. Veja que a sobrejetividade segue do teorema da aproximação; já a injetividade, basta observar que $f(z + tO'_P) = 0 \Rightarrow v_{P_i}(z) \geq e_i, i = 1, ..., r \Rightarrow zt^{-1} \in O'_P \Rightarrow z + tO'_P = 0$.

Existe um diagrama comutativo de aplicações $k-$lineares:

Diagrama 8.

$$\begin{array}{ccc} V & \xrightarrow{\quad\overline{\mu}\quad} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \bigoplus_{i=1}^{r} V_i & \xrightarrow{(\mu_1,...,\mu_r)} & \bigoplus_{i=1}^{r} V_i \end{array}$$

onde $(\mu_1, ..., \mu_r)(v_1, ..., v_r) = (\mu_1(v_1), ..., \mu_r(v_r)), v_i \in V_i$.

Como f é isomorfismo, temos que $(\mu_1, ..., \mu_r) = f^{-1} \circ \overline{\mu} \circ f$, além disso $(\mu_1, ..., \mu_r) = \sum_{i=1}^{r} (0, ..., 0, \mu_i, 0, ..., 0)$, portanto $\mathrm{Tr}(\overline{\mu}) = \sum_{i=1}^{r} \mathrm{Tr}(\mu_i)$. Daí, por $(\star)$, temos $\pi(\mathrm{Tr}_{F'/F}(u)) = \sum_{i=1}^{r} \mathrm{Tr}(\mu_i)$.

Falta agora mostrar que $\mathrm{Tr}(\mu_i) = e_i \, \mathrm{Tr}_{k_i/k}(\pi_i(u))$.

Considere a seguinte cadeia de $k-$espaços:

$$V_i = V_i^{(0)} \supseteq V_i^{(1)} \supseteq ... \supseteq V_i^{(e_i)} = \{0\},$$

onde $V_i^{(j)} := P_i^j / P_i^{e_i} \subseteq V_i$.

Observemos que V_i^j são espaços μ_i-invariantes.

Agora defindo $\sigma_{ij} : V_i^j / V_i^{j+1} \to V_i^j / V_i^{j+1}$ onde $[z + P_i^{e_i}] \mapsto uz + P_i^{e_i}$, para $j = 0, ..., e_i - 1$, onde $[z + P_i^{e_i}]$ representa a classe de $z + P_i^{e_i}$ em V_i^j / V_i^{j+1}. Então $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i - 1} \mathrm{Tr}(\sigma_{ij})$ (representando μ_i por uma matriz com respeito a uma base de V_i composta de bases de V_i^j módulo V_i^{j+1}, para $0 \leq j \leq e_i - 1$).

Sabemos que $\mathrm{Tr}_{k_i/k}(\pi_i(u)) = \mathrm{Tr}(\gamma_i)$, onde $\gamma_i : k_i \to k_i$ é $k-$linear e $\gamma_i(z + P_i) = uz + P_i$.

Agora para $0 \leq j \leq e_i - 1$, etabelecemos o isomorfismo $h : k_i \to V_i^j / V_i^{j+1}$ de $k-$espaços vetoriais tal que o seguinte diagrama comute:

Diagrama 9.

$$\begin{array}{ccc} k_i & \xrightarrow{\quad\gamma_i\quad} & k_i \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ V_i^j / V_i^{j+1} & \xrightarrow[\quad\sigma_{ij}\quad]{} & V_i^j / V_i^{j+1} \end{array}$$

Como h é isomorfismo, então $\mathrm{Tr}(\gamma_i) = \mathrm{Tr}(\sigma_{ij})$. Podemos definir h por: t_i um parâmetro local de P_i de F' e $h(z + P_i) = \left[t_i^j z + P_i^{e_i}\right]$.

Assim temos $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i - 1} \mathrm{Tr}(\sigma_{ij})$ e $\mathrm{Tr}_{k_i/k}(\pi_i(u)) = \mathrm{Tr}(\gamma_i) = \mathrm{Tr}(\sigma_{ij})$, logo $\mathrm{Tr}(\mu_i) = \sum_{j=0}^{e_i - 1} \mathrm{Tr}_{k_i/k}(\mu_i(u))$. Portanto $\mathrm{Tr}(\mu_i) = e_i \, \mathrm{Tr}_{k_i/k}(\pi_i(u))$.

□

Definição 2.5.4. Seja F'/F extensão algébrica de um corpo de funções e $P \in \mathbb{P}_F$:

1. Uma extensão P' de P é dita ser mansamente (respectivamente selvagemente) ramificada se $e(P'|P) > 1$ e $\mathrm{char}\, K$ não divide $e(P'|P)$ (respectivamente $\mathrm{char}\, K$ divide

$e(P'|P)$);

2. Dizemos que P é ramificado (respectivamente não ramificado) em F'/F se existe pelo menos um $P' \in \mathbb{P}_{F'}$ extensão de P tal que $P'|P$ é ramificada (respectivamente se $P'|P$ é não ramificada para toda $P'|P$). O lugar P é mansamente ramificado em F'/F se é ramificado em F'/F e nenhuma extensão de P em F' é selvagemente ramificada. Se existe pelo menos uma extensão $P'|P$ selvagemente ramificada, dizemos que P é selvagemente ramificado em F'/F;

3. P é totalmente ramificado em F'/F se existe somente uma extensão $P' \in \mathbb{P}_{F'}$ de P em F', e o índice de ramificação é $e(P'|P) = [F' : F]$;

4. F'/F é dita ser ramificada (respectivamente não ramificada) se pelo menos um lugar $P \in \mathbb{P}_F$ é ramificado em F'/F (respectivamente se todo $P \in \mathbb{P}_F$ é não ramificado em F'/F);

5. F'/F é dita ser mansa se nenhum lugar $P \in \mathbb{P}_F$ é selvagemente ramificado em F'/F.

Corolário 2.5.5. *Seja F'/F uma extensão finita separável de um corpo de funções algébricas.*

1. *Se $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ são tais que $P'|P$, então $P'|P$ é ramificada se, e somente se, $P' \leq \mathrm{Diff}(F'/F)$. Se $P'|P$ é ramificada, então:*

$$d(P'|P) = e(P'|P) - 1 \Leftrightarrow P'|P \text{ é mansamente ramificada,}$$
$$d(P'|P) \geq e(P'|P) \Leftrightarrow P'|P \text{ é selvagemente ramificada.}$$

2. *Quase todo os lugares $P \in \mathbb{P}_F$ são não ramificados em F'/F.*

Teorema 2.5.6. *Suponha que $F' = F(y)$ é uma extensão finita separável de um corpo de função F de $[F' : F] = n$. Seja $P \in \mathbb{P}_F$ tal que o polinômio minimal $\varphi(T)$ de y sobre F tem seus coeficientes em O_P, isto é, y é integral sobre O_P, e sejam $P_1, ..., P_r \in \mathbb{P}_{F'}$ todos os lugares que estendem P. Então segue:*

1. $d(P_i|P) \leq v_{P_i}(\varphi'(y)), i = 1, ..., r;$

2. *$\{1, y, ..., y^{n-1}\}$ é uma base integral de F'/F no lugar P se, e somente se, $v_{P_i}(\varphi'(y)) = d(P_i|P), i = 1, ..., r$ (onde $\varphi'(T)$ denota a derivada de $\varphi(T)$ no ane de polinômios $F[T]$).*

Demonstração. Considere a base $\{1, y, ..., y^{n-1}\}$, como $\varphi(y) = 0 \Rightarrow \varphi(T) = (T-y)(c_{n-1}T^{n-1} + ... + c_1T + c_0)$, com $c_{n-1}, ..., c_0 \in F'$ e $c_{n-1} = 1$, (I).

Afirmamos que $\left\{\frac{c_0}{\varphi'(y)}, ...\frac{c_{n-1}}{\varphi'(y)}\right\}$ é base dual de $\{1, y, ..., y^{n-1}\}$, notando que $\varphi'(y) \neq 0$, pois y é separável.

Pela definição de base dual, dizer que $\left\{\frac{c_0}{\varphi'(y)}, ...\frac{c_{n-1}}{\varphi'(y)}\right\}$ é base dual de $\{1, y, ..., y^{n-1}\}$ é equivalente a $\mathrm{Tr}_{F'/F}(\frac{c_i}{\varphi'(y)}) = \delta_{ij}, 0 \leq i, j \leq n-1$.

Considere os n mergulhos distintos $\sigma_1, ..., \sigma_n$ de F'/F em Φ (Φ extensão algebricamente fechado de F).

Definindo $y_j := \sigma_j(y)$, temos $\varphi(T) = \prod_{j=1}^{n}(T - y_j)$.

Derivando esta equação e substituindo $T = y_\nu$, temos $\varphi'(y_\nu) = \prod_{i\neq\nu}(y_\nu - y_i)$ (II).

Agora, para $0 \leq l \leq n-1$, considere o polinômio:

$$\varphi_l(T) := (\sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j}.\frac{y_j^l}{\varphi'(y_j)}) - T^l \in \Phi[T].$$

Seu grau é, no máximo, $n-1$, e para $1 \leq \nu \leq n$, temos:

$$\varphi_l(y_\nu) = (\prod_{i\neq\nu}(y_\nu - y_i)).\frac{y_\nu^l}{\varphi'(y_\nu)} - y_\nu^l = 0,$$

por (II).

Um polinômio de grau menor ou igual a $n-1$ com n raízes distintas é identicamente nulo, então $\varphi_l(T) = 0$, logo:

$$T^l = \sum_{j=1}^{n} \frac{\varphi(T)}{T - y_j}.\frac{y_j^l}{\varphi'(y_j)}, 0 \leq l \leq n-1. \text{ (III)}$$

Os mergulhos $\sigma_i : F' \to \Phi$ podem ser extendidos aos mergulhos $\sigma_i : F'(T) \to \Phi(T)$

definindo $\sigma_i(T) = T$. Assim de (III) obtemos:

$$T^l \underbrace{=}_{(III)} \sum_{j=1}^{n} \frac{\varphi(T)}{T-y_j}.\frac{y_j^l}{\varphi'(y_j)} \underbrace{=}_{(I)} \sum_{j=1}^{n} \sigma_j(\sum_{i=0}^{n-1} c_i T^i.\frac{y^l}{\varphi'(y)}) = \sum_{i=0}^{n-1} \mathrm{Tr}_{F'/F}(c_i\frac{y^l}{\varphi'(y)})T^i,$$

$0 \leq l \leq n-1$.

Comparando os coeficientes, temos $\mathrm{Tr}_{F'/F}(c_i\frac{y^l}{\varphi'(y)}) = \delta_{il}, 0 \leq i,l \leq n-1$.

Mostremos agora que $c_j \in \sum_{i=0}^{n-1} O_P y^i$, para $j = 0, ..., n-1$.

O polinômio minimal $\varphi(T)$ de y sobre F tem a forma $\varphi(T) = T^n + a_{n-1}T^{n-1} + ... + a_1T^1 + a_0$, onde $a_i \in O_P$, pois, por hipótese, y é integral sobre O_P, e, por (I), $\varphi(T) = (T-y)(c_{n-1}T^{n-1} + ... + c_1T + c_0)(T-y)(c_{n-1}T^{n-1} + ... + c_1T + c_0)$. Assim:

$$\text{(IV) } c_{n-1} = 1, c_0y = -a_0 \text{ e } c_iy = c_{i-1} - a_i, \text{ para } 1 \leq i \leq n-1.$$

Suponha que existe $j \in \{1, ..., n-1\}$, onde

$$c_j = \sum_{i=0}^{n-1} s_i y^i, \text{ com } s_i \in O_P.$$

Então $c_{j-1} = a_j + c_iy = a_j + \sum_{i=0}^{n-1} s_i y^{i+1} = a_j + \sum_{i=0}^{n-2} s_i y^{i+1} + s_{n-1}y^n = a_j + \sum_{i=0}^{n-2} s_i y^{i+1} - s_{n-1}\sum_{i=0}^{n-1} a_i y^i \in \sum_{i=0}^{n-1} O_P y^i$. Como $c_{n-1} = 1$, então $c_j \in \sum_{i=0}^{n-1} O_P y^i, j = 0, ..., n-1$, (V).

De forma análoga, podemos mostrar que $y^j \in \sum_{i=0}^{n-1} O_P c_i$, $j = 0, ..., n-1$, (VI).

Com isso podemos demonstrar o teorema:

1. Como antes, seja $\mathcal{C}_P$ o módulo complementar e O'_P o fecho integral de O_P em F'. Mostremos que $d(P_i|P) \leq v_{P_i}(\varphi'(y))$, e isso é equivalente a mostrar que $z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geq -v_{P_i}(\varphi'(y))$.

   Seja $z \in \mathcal{C}_P$, então podemos escrever:

$$z = \sum_{i=0}^{n-1} r_i \frac{c_i}{\varphi'(y)}, \text{ com } r_i \in F.$$

Como y é integral sobre O_P, então y^l também o é, e como $z \in \mathcal{C}_P$, temos:

$$\mathrm{Tr}_{F'/F}(zy^l) \in O_P, l = 0, ..., n-1.$$

Agora observe que $\mathrm{Tr}_{F'/F}(zy^l) = r_l, l = 0, ..., n-1$.

Por (V), temos $z \in \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} O_P y^i \subseteq \frac{1}{\varphi'(y)} O'_P$. Portanto, $v_{P_i}(z) \geq -v_{P_i}(\varphi'(y)), i = 0, ..., r$.

2. Por (V) e (VI), temos que $\sum_{i=0}^{n-1} O_P y^i = \sum_{j=0}^{n-1} O_P c_j$.

   Suponha que $\{1, ..., y^{n-1}\}$ é uma base integral para P, então pela Proposição 2.4.2, temos:

   $$\mathcal{C}_P = \frac{1}{\varphi'(y)} O'_P.$$

   Como $\mathcal{C}_P = tO'_P$, onde $d(P_i|P) = -v_{P_i}(t), \forall P_i|P$, temos $d(P_i|P) = -v_{P_i}(\frac{1}{\varphi'(y)}) = v_{P_i}(\varphi'(y)), i = 0, ..., n-1$.

   Agora suponha que $d(P_i|P) = v_{P_i}(\varphi'(y)), i = 0, ..., n-1$. Temos que provar que $O'_P \subseteq \sum_{i=0}^{n-1} O_P y^i$ (a inclusão contrária segue trivialmente).

   Seja $z \in O'_P \subseteq F'$, então $z = \sum_{i=0}^{n-1} t_i y^i, t_i \in F$, e por (V), $c_j \in \sum_{i=0}^{n-1} O_P y^i \subseteq O'_P$. Além disso, estamos supondo $d(P_i|P) = v_{P_i}(\varphi'(y))$, logo $\mathcal{C}_P = \frac{1}{\varphi'(y)} O'_P$. Assim, $\frac{c_j}{\varphi'(y)} \in \mathcal{C}_P \Rightarrow \mathrm{Tr}_{F'/F}(\frac{c_j}{\varphi'(y)} z) \in O_P$. Daí:

$$O_P \ni \mathrm{Tr}_{F'/F}(\frac{1}{\varphi'(y)} c_j z) = \mathrm{Tr}_{F'/F}(\frac{1}{\varphi'(y)} c_j \sum_{i=0}^{n-1} t_i y^i) =$$

$$= \sum_{i=0}^{n-1} t_j \,\mathrm{Tr}_{F'/F}(y^i \frac{c_j}{\varphi'(y)}) = \sum_{i=0}^{n-1} t_i \delta_{ij} = t_j$$

$$\Rightarrow z \in \sum_{i=0}^{n-1} O_P y^i \Rightarrow O'_P \subseteq \sum_{i=0}^{n-1} O_P y^i.$$

□

Corolário 2.5.7. *Seja $F' = F(y)$ extensão finita separável de corpos de funções de grau*

n, e seja $\varphi(T) \in F[T]$ o polinômio minimal de y sobre F. Suponha $P \in \mathbb{P}_F$ satisfazendo:

$$\varphi(T) \in O_P[T] \text{ e } v_{P'}(\varphi'(y)) = 0,$$

$\forall P' \in \mathbb{P}_{F'}$, tal que $P'|P$. Então P é não ramificado em F'/F, e $\{1, y, ..., y^{n-1}\}$ é uma base integral para F'/F de P.

Demonstração. Do Teorema 2.5.6, item 1, temos que $d(P'|P) = v_{P'}(\varphi'(y)) = 0$, assim pelo item 2 do mesmo teorema, temos que a base do enunciado é integral.

Além disso, pelo teorema de Dedekind, temos que $e(P'|P) = 1, \forall P'|P$, logo P é não ramificado em F'/F.

□

Proposição 2.5.8. *Sejam F'/F uma extensão finita separável de corpos de funções, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$. Suponha que $P'|P$ é totalmente ramificada, isto é, $e(P'|P) = n$ (n grau da extensão). Seja $t \in F'/F$ um parâmetro local de P', e considere $\varphi(T) \in F[T]$ o polinômio minimal de t sobre F. Então $d(P'|P) = v_{P'}(\varphi'(t))$ e $\{1, t, ..., t^{n-1}\}$ é uma base integral para F'/F de P.*

Demonstração. Primeiro, afirmamos que $1, t, ..., t^{n-1}$ são linearmente independentes sobre F. De fato, suponha por absurdo que sejam linearmente dependentes. Então existem $r_0, ..., r_{n-1} \in F$, não todos nulos, tais que:

$$\sum_{i=0}^{n-1} r_i t^i = 0.$$

Para $r_i \neq 0$ temos:

$$v_{P'}(r_i t^i) = i + n v_P(r_i) \equiv i \bmod n.$$

Portanto, se $i, j \in \{0, ..., n-1\}$ são tais que $i \neq j$, e $r_i \neq 0$ e $r_j \neq 0$, temos $v_{P'}(r_i t^i) \neq v_{P'}(r_j t^j)$. Logo, pela desigualdade triangular estrita, temos:

$$v_{P'}(\sum_{i=0}^{n-1} r_i t^i) = \min\left\{v_{P'}(r_i t^i); r_i \neq 0\right\} < \infty,$$

gerando uma contradição.

Logo $\{1, t, ..., t^{n-1}\}$ é base de F'/F.

Agora, pela igualdade fundamental (Teorema 2.1.11), temos $\sum e_i f_i = n$, e $P' = P_j$ para algum $j \in \{1, ..., r\}$. Como, por hipótese, $e(P'|P) = n$, segue $e(P'|P)f(P'|P) = \sum e_i f_i$. Portanto P' é o único lugar de F' que estende P, e assim $O'_P = O_{P'}$, o que significa t integral sobre O_P.

Mostremos que $O_{P'} = \sum_{i=0}^{n-1} O_P t^i$.

Seja $z \in F'$ não nulo, então $z = \sum x_i t^i$, para certos $x_i \in F$. Pelo mesmo argumento acima $0 \leq v_{P'}(z) = \min\{nv_P(x_i) + i; 0 \leq i \leq n-1, \text{ com } x_i \neq 0\}$. O que implica $v_{P'}(x_i) \geq 0, i = 0, ..., n-1$. E, portanto $z \in \sum_{i=0}^{n-1} O_P t^i$.

Assim, a base em questão é integral, e pelo Teorema 2.5.6, item 2, temos $d(P'|P) = v_{P'}(\varphi'(t))$.

□

2.6 Extensões por constantes

Aqui, F/K será um corpo de funções algébricas com corpo de constantes K, onde K é um corpo perfeito. Considere $\Phi \supseteq F$ um corpo algebricamente fechado fixado.

Seja $K' \supseteq K$ extensão algébrica de K (com $K' \subseteq \Phi$). O compósito $F' := FK'$ é um corpo de funções algébricas sobre K', e com corpo de constantes uma extensão finita de K'. De fato, se F' é corpo de funções algébricas sobre K', então pelo Corolário 1.1.15, temos que o corpo de constantes de F' é uma extensão finita de K'.

Assim basta mostrar que F' é corpo de funções algébricas sobre K'.

Como F/K é corpo de funções algébricas, então existe $x \in F \backslash K$ tal que $[F : K(x)] < \infty$ (x transcendente), então $[F' : K'(x)] < \infty$. Mais precisamente:

Proposição 2.6.1. *Seja $F' = FK'$ uma extensão algébrica constante de F/K (de grau finito ou infinito). Temos:*

1. *K' é todo o corpo de constantes de F';*

2. *Cada subconjunto de F que é linearmente independente sobre K também é linearmente independente sobre K';*

3. $[F : K(x)] = [F' : K'(x)], \forall x \in F \backslash K$.

Lema 2.6.2. *Suponha $\alpha \in \Phi$ algébrico sobre K. Então $[K(\alpha) : K] = [F(\alpha) : F]$.*

Demonstração. Comparando os polinômios minimais de α nas duas extensões obtemos $[K(\alpha) : K] \geq [F(\alpha) : F]$.

Agora mostremos que vale a igualdade considerando $\varphi(T)$ o polinômio minimal de α sobre K. Suponha que $\varphi(T)$ seja não irredutível sobre F (o que é equivalente a dizer que vale a desigualdade estrita na desigualdade que encontramos acima). Então podemos escrever $\varphi(T) = g(T)h(T)$, onde os coeficientes de $g(T)$ e $h(T)$ estão em F.

Assim, cada raiz de $g(T)$ e $h(T)$ está em Φ e é raiz de $\varphi(T)$. Logo os coefientes de $g(T)$ e $h(T)$ são algébricos sobre K, pois são expressões polinomiais nas raízes de $\varphi(T)$, mas como estes coeficientes estão em F, temos que tais coeficientes estão em K, pois o corpo de constantes de F é K.

Portanto, $\varphi(T)$ é não irredutível sobre K, gerando uma contradição.

□

Demonstração. (da Proposição 2.6.1)

1. Seja $\gamma \in F'$ algébrico sobre K'. Como K'/K é algébrica, então γ é algébrico sobre K.

   Como $\gamma \in F' = K'F$, então existe uma quantidade finita de elementos $\alpha_1, ..., \alpha_r \in K'$ tal que $\gamma \in F(\alpha_1, ..., \alpha_r)$. Consideremos a extenão finita separável $K(\alpha_1, ..., \alpha_r)/K$, então temos $K(\alpha_1, ..., \alpha_r) = K(\alpha)$, para algum $\alpha \in K'$.

   Agora, como γ é algébrico sobre K então existe $\beta \in F'$ tal que $K(\alpha, \gamma) = K(\beta)$. Logo:

   $$F(\beta) = F(\alpha, \gamma) = F(\alpha), \text{ pois } \gamma \in F(\alpha_1, ..., \alpha_r).$$

   Pelo Lema 2.6.2:

   $$[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K], \text{ com } K(\alpha) \subseteq K(\beta).$$

Logo $\gamma \in K(\beta) = K(\alpha) \subseteq K'$.

2. Sejam $y_1, ..., y_r \in F$ linearmente independentes sobre K e consideremos a combinação linear:
$$\sum_{i=1}^{r} \gamma_i y_i = 0, \text{ com } \gamma_i \in K'.$$
Como K é perfeito, então $K(\gamma_1, ..., \gamma_r) = K(\alpha)$, para algum $\alpha \in K'$.

Então podemos escrever:
$$\gamma_i = \sum_{j=0}^{n-1} c_{ij}\alpha^j, \text{ com } c_{ij} \in K \text{ e } n = [K(\alpha) : K].$$

E assim temos:
$$\sum_{j=0}^{n-1} (\sum_{i=1}^{r} c_{ij} y_i)\alpha^j = 0,$$
com $\sum_{i=1}^{r} c_{ij} y_i \in F$. Pelo Lema 2.6.2, $1, \alpha, ..., \alpha^{n-1}$ são linearmente independentes sobre F, o que implica $\sum_{i=1}^{r} c_{ij} y_i = 0, j = 0, ..., n-1$, e pela independência linear dos elementos $y_1, ..., y_r$ sobre K, temos $c_{ij} = 0, i = 1, ..., r$ e $j = 0, ..., n-1$; logo $\gamma_i = \sum_{j=0}^{n-1} c_{ij}\alpha^i = 0, i = 1, ..., r$, e assim temos que $y_1, ..., y_r$ são linearmente independentes sobre K'.

3. Como $[F' : K'(x)] \leq [F : K(x)]$, reta mostrar que quaisquer elementos $z_1, ..., z_s \in F$, que são linearmente independentes sobre $K(x)$, também são linearmente independentes sobre $K'(x)$.

Suponha que não, então:
$$\sum_{i=1}^{s} f_i(x) z_i = 0, \text{ com } f_i \in K'(x) \text{ não todos nulos }.$$

Sem perda de generalidade, já podemos supor que $f_i(x) \in K'[x]$.

Assim, temos que o conjunto $\{x^j z_i; 1 \leq i \leq s \text{ e } j \geq 0\} \subseteq F$ é um conjunto linearmente dependente sobre K'. Logo, pela contra-positiva do item anterior, tal conjunto é linearmente dependente sobre K, e portanto $z_1, ..., z_s$ são linearmente

dependentes sobre $K(x)$, gerando uma contradição.

□

Teorema 2.6.3. *Em uma extensão algébrica constante $F' = FK'$ de F/K temos que F'/F é não ramificada (isto é, $e(P'|P) = 1, \forall P \in \mathbb{P}_F$ e $\forall P' \in \mathbb{P}_{F'}$ com $P'|P$).*

Demonstração. Primeiro será discutido o caso em que a extensão constante é finita, e então provaremos o caso geral.

Então, para começar, vamos assumir que: $K' = K(\alpha)$ é uma extensão finita de K.

Nessa situação, $F' = F(\alpha)$ e o polinômio minimal $\varphi(T)$ de α sobre K permanece irredutível sobre F pelo Lema 2.6.2. Seja $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$, então pelo Teorema 2.5.6, o expoente da diferente $d(P'|P)$ satisfaz $0 \leq d(P'|P) \leq v_{P'}(\varphi(\alpha))$.

Por α ser separável sobre K, então $\varphi'(\alpha) \neq 0$, além disso $\varphi'(\alpha) \in K'$, logo $\varphi'(\alpha) \in O_{P'}^*$, daí $v_{P'}(\varphi'(\alpha)) = 0$, e assim temos $d(P'|P) = v_{P'}(\varphi'(\alpha)) = 0$.

Assim, pelo teorema da diferente de Dedekind (2.5.1), temos $e(P'|P) = 1, \forall P'|P$. Ou seja, $e(P'|P) = 1, \forall P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$.

Logo F'/F é não ramificada.

Consideremos K' uma extensão algébrica qualquer de K.

Seja $P' \in \mathbb{P}_{F'}$ uma extensão de P. Escolha $t \in F'$ parâmetro local de P'. Existe um corpo intermediário $K \subseteq K_1 \subseteq K'$ com $[K_1 : K] < \infty$ e $t \in F_1 = FK_1$. Seja $P_1 = P' \cap F_1$, então $1 = v_{P'}(t) = e(P'|P_1).v_{P_1}(t)$ e portanto $e(P'|P_1) = 1$. Além disso, pelo caso que a extensão é finita temos $e(P_1|P) = 1$. Portanto, $e(P'|P) = 1$.

□

2.7 Extensões de Galois

Nesta sessão estudaremos extensões de Galois de corpos de funções algébricas. Extensões de Galois têm muitas propriedades úteis que não são verdadeiras em uma extensão finita arbitrária.

Uma extensão finita M/L é dita uma extensão de Galois se o grupo de automorfismos:

$$\mathrm{Aut}(M/L) = \{\sigma : M \to M; \sigma \text{ é isomorfismo com } \sigma(a) = a, \forall a \in L\}$$

tem a mesma ordem $[M : L]$. Neste caso, chamamos $\mathrm{Aut}(M/L)$ de grupo de Galois de M/L e escrevemos $\mathrm{Gal}(M/L) := \mathrm{Aut}(M/L)$.

Seja F'/K' uma extensão de um corpo de funções F/K, dizemos que F'/K' é uma extensão de Galois de F/K se F'/F é uma extensão de Galois de grau finito.

Se P é um lugar de F/K. Então $\mathrm{Gal}(F'/F)$ age no conjunto de todas as extensões $\{P' \in \mathbb{P}_{F'}; P' \text{ é uma extensão de } P\}$ via $\sigma(P') = \{\sigma(x); x \in P'\}$, e pelo Lema 2.5.2, a correspondente valorização discreta $v_{\sigma(P')}$ é dada por:

$$v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y)), \text{ para } y \in F'.$$

Teorema 2.7.1. *Sejam F'/K' uma extensão Galoisiana de F/K e $P_1, P_2 \in \mathbb{P}_{F'}$ extensões de $P \in \mathbb{P}_F$. Então $P_2 = \sigma(P_1)$ para algum $\sigma \in \mathrm{Gal}(F'/F)$.*

Demonstração. Suponha que a afirmação é falsa, isto é, $\sigma(P_1) \neq P_2, \forall \sigma \in G := \mathrm{Gal}(F'/F)$. Pelo teorema da aproximação, existe um elemento $z \in F'$ tal que $v_{P_2}(z) > 0$ e $v_Q(z) = 0, \forall Q \in \mathbb{P}_{F'}$ com $Q|P$ e $Q \neq P_2$. Seja $\mathrm{N}_{F'/F} : F' \to F$ a aplicação norma, então:

$$v_{P_1}(\mathrm{N}_{F'/F}(z)) = v_{P_1}(\prod_{\sigma \in G} \sigma(z)) = \sum_{\sigma \in G} v_{P_1}(\sigma(z)) =$$

$$= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0 \text{ (I)} ,$$

pois P_2 não ocorre entre os lugares $\sigma(P_1), \sigma \in G$.

Por outra lado,

$$v_{P_2}(\mathrm{N}_{F'/F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) = v_{P_2}(z) > 0 \text{ (II)} .$$

Mas, $\mathrm{N}_{F'/F}(z) \in F$, portanto:

$$v_{P_1}(\mathrm{N}_{F'/F}(z)) = 0 \Leftrightarrow v_P(\mathrm{N}_{F'/F}(z)) = 0 \Leftrightarrow v_{P_2}(\mathrm{N}_{F'/F}(z)) = 0,$$

gerando uma contradição para (I) e (II).

□

Corolário 2.7.2. *Nas mesmas condições do Teorema 2.7.1 (em particular F'/F é uma extensão de Galois). Sejam $P_1, ..., P_r$ todos os lugares de F' que são extensões de P. Então:*

1. *$e(P_i|P) = e(P_j|P)$ e $f(P_i|P) = f(P_j|P)$, $\forall i, j$. Portanto, podemos definir $e(P) := e(P_i|P)$ e $f(P) := f(P_i|P)$, e chamamos $e(P)$ (respectivamente $f(P)$) o índice de ramificação (respectivamente o grau relativo) de P em F'/F;*

2. *$e(P)f(P)r = [F' : F]$. Em particular $e(P)$, $f(P)$ e r dividem $[F' : F]$;*

3. *Os expoentes da diferente $d(P_i|P)$ e $d(P_j|P)$ são iguais para todo i e j.*

Demonstração. 1. Segue direto do Teorema 2.7.1 e do Lema 2.5.2.

2. Pelo Teorema 2.1.11 (Igualdade Fundamental) e pelo Teorema 2.7.1, temos:

$$[F' : F] = \sum_{i=1}^{r} e(P_i|P)f(P_i|P) = e(P)f(P)r.$$

3. Considere o fecho integral:

$$O'_P = \bigcap_{i=1}^{r} O_{P_i}$$

de O_P em F', e o módulo complementar:

$$\mathcal{C}_P = \left\{ z \in F'; \mathrm{Tr}_{F'/F}(zO'_P) \subseteq O_P \right\}.$$

Veja que $\forall u \in F'$ temos $\mathrm{Tr}_{F'/F}(u) = \mathrm{Tr}_{F'/F}(\sigma(u)), \forall \sigma \in G$.

Mostremos que $\sigma(O'_P) = O'_P$ e $\sigma(\mathcal{C}_P) = \mathcal{C}_P, \forall \sigma \in G$:

Seja $z \in O'_P$, então $v_{P_i}(z) \geq 0, i = 1, ..., r$. Para $1 \leq j \leq r$, temos $v_{P_j}(\sigma(z)) = v_{\sigma^{-1}(P_j)}(z) = v_{P_i}(z) \geq 0$, para algum i, ou seja, $\sigma(z) \in O'_P$, portanto, $\sigma(O'_P) \subseteq O'_P$.

Isso implica que $O'_P \subseteq \sigma^{-1}(\sigma(O'_P)) \subseteq \sigma^{-1}(O'_P) \subseteq O_{P'}$.

Fazendo o mesmo para σ^{-1} em vez de σ, obtemos a igualdade desejada.

Seja agora $z \in \mathcal{C}_P$, então $\mathrm{Tr}_{F'/F}(zO'_P) \subseteq O_P$, assim $\mathrm{Tr}_{F'/F}(\sigma(z)u) = \mathrm{Tr}_{F'/F}(z\sigma^{-1}(u)) \in O_P, \forall u \in O'_P$, logo $\sigma(\mathcal{C}_P) \subseteq \mathcal{C}_P$, e, como antes, podemos concluir que $\mathcal{C}_P = \sigma(\mathcal{C}_P)$.

Escrevendo $\mathcal{C}_P = tO'_P$, obtemos:

$$\sigma(t)O'_P = \sigma(tO'_P) = \sigma(\mathcal{C}_P) = \mathcal{C}_P = tO_P.$$

Logo, pela Proposição 2.4.2, temos:

$$v_{P_i}(\sigma(t)) = v_{P_i}(t), i = 1, ..., r \Rightarrow -d(P_i|P) = v_{P_i}(\sigma(t)), \forall i \text{ e } \forall \sigma \in G.$$

Seja agora P_i e P_j e $\sigma \in G$ tal que $P_i = \sigma(P_j)$. Então:

$$-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)} = v_{P_j}(t) = -d(P_j|P).$$

Portanto $d(P_i|P) = d(P_j|P)$.

□

Proposição 2.7.3. *(Extensão de Kummer)*

Seja F/K um corpo de funções algébricas onde K contém uma raiz $n-$ésima primitiva da unidade (com $n > 1$ e n relativamente primo com a característica de K). Suponha que $u \in F$ é um elemento satisfazendo:

$$u \neq w^d, \forall w \in F \text{ e } d|n, d > 1. \text{ (I)}$$

Seja $F' = F(y)$, com $y^n = u$. (II)

Tal extensão F'/F é dita ser uma extensão de Kummer. E, nela, temos:

1. *O polinômio $\phi(T) = T^n - u$ é o polinômio minimal de y sobre F (em particular, é irredutível sobre F). A extensão F'/F é de Galois de grau $[F' : F] = n$, seu grupo de Galois é cíclico, e os automorfismos de F'/F são dados por $\sigma(y) = \zeta y$, onde $\zeta \in K$ é uma raiz $n-$ésima da unidade.*

2. *Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ uma extensão de P. Então:*

$$e(P'|P) = \frac{n}{r_P} \text{ e } d(P'|P) = \frac{n}{r_P} - 1,$$

onde $r_P := \mathrm{mdc}(n, v_P(u)) > 0$. *(III)*

3. *Se* K' *denota o corpo constante de* F' *e* g *(respectivamente* g'*) denota o gênero de* F/K *(respectivamente* F'/K'*), então:*

$$g' = 1 + \frac{n}{[K' : K]}(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(1 - \frac{r_P}{n})\deg(P)).$$

Demonstração. 1. Veja no apêndice, Teorema A.6.3.

2. **Caso 1:** $r_P = 1$.

   Por (II), temos:

$$nv_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P'|P)v_P(u)$$

   Como $1 = r_P = \mathrm{mdc}(n, v_P(u))$, então n e $v_P(u)$ são relativamente primos, logo $n|e(P'|P)$ e $v_P(u)|v_{P'}(y)$.

   Mas pelo item 1, $[F' : F] = n$, e pelo Corolário 2.7.2, $e(P'|P)|n$. Portanto, $n = e(P'|P)$.

   Agora, por hipótese, n é relativamente primo com $\mathrm{char}(K)$, assim, pelo teorema da diferente de Dedekind:

$$d(P'|P) = e(P'|P) - 1 = n - 1 = \frac{n}{r_P} - 1.$$

   Caso 2: $r_P = n$.

   Temos $n = r_P = \mathrm{mdc}(n, v_P(u))$, logo $n|v_P(u)$, ou seja, existe l inteiro onde $nl = v_P(u)$.

   Escolha $t \in F$ tal que $v_P(t) = l$ e defina:

$$y_1 := t^{-1}y \text{ e } u_1 := t^{-n}u.$$

   Veja que $y_1^n = u_1$,e $v_{P'}(y_1) = v_P(u_1) = 0$.

O polinômio irredutível de y_1 sobre F é $\psi(T) = T^n - u_1$, pois $\phi(T) = T^n - u$ é o polinômio minimal de y sobre F.

Então y é integral sobre O_P, e pelo Teorema 2.5.6, temos:

$$0 \leq d(P'|P) \leq v_{P'}(\psi'(y_1)).$$

Agora $\psi'(y_1) = ny_1^{n-1}$, então $v_{P'}(\psi'(y_1)) = 0$, logo $d(P'|P) = 0$, e pelo teorema de Dedekind, $e(P'|P) = 1$, obtendo o resultado.

Caso 3: $1 < r_P < n$.

Considere o corpo intermediário $F_0 = F(y_0)$ com $y_0 = y^{\frac{n}{r_P}}$.

Então como $\psi(T) = T^{r_P} - u$ é o polinômio minimal de y_0 sobre F, temos $[F_0 : F] = r_p$ e $[F' : F_0] = \frac{n}{r_P}$.

Seja $P_0 := P' \cap F_0$, então, aplicando o caso 2 em F_0/F, temos $e(P_0|P) = 1$.

Veja ainda que $y_0^{r_P} = u$, então $v_{P_0}(y_0^{r_P}) = v_{P_0}(u) \Rightarrow v_{P_0}(y_0) = \frac{v_P(u)}{r_P}$.

Assim temos $\text{mdc}(\frac{n}{r_P}, v_{P_0}(y_0)) = 1$, e podemos aplicar o caso 1 para a extensão $F_0(y) = F'$, logo $e(P'|P_0) = \frac{n}{r_P}$ e assim $e(P'|P) = e(P'|P_0)e(P_0|P) = \frac{n}{r_P}$.

Por fim, $d(P'|P) = e(P'|P_0)d(P_0|P) + d(P_0|P) = \frac{n}{r_P} - 1$.

3. O grau do divisor da diferente $\text{Diff}(F'/F)$ é:

$$\deg(\text{Diff}(F'/F)) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \deg(P') =$$

$$= \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (\frac{n}{r_P} - 1) \deg(P'), \text{ pelo item 2.}$$

Para $P \in \mathbb{P}_F$ fixado, o índice de ramificação $e(P) = e(P'|P)$ não depende da escolha de P' extensão de P. Assim,

$$\sum_{P'|P} \deg(P') = \frac{1}{e(P)}(\sum_{P'|P} e(P'|P) \deg(P')) = \frac{1}{e(P)} \deg(\sum_{P'|P} e(P'|P)P') =$$

$$= \frac{1}{e(P)} \deg(\mathrm{Con}_{F'/F}(P)) = \frac{r_P}{n} \frac{[F' : F]}{[K' : K]} \deg(P) = \frac{r_P}{[K' : K]} \deg(P').$$

Logo:

$$\deg(\mathrm{Diff}(F'/F)) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (\frac{n}{r_P} - 1) \deg(P') =$$

$$= \sum_{P \in \mathbb{P}_F} ((\frac{n}{r_P} - 1) \sum_{P'|P} \deg(P')) =$$

$$= \sum_{P \in \mathbb{P}_F} (\frac{n}{r_P} - 1) \frac{r_P}{[K' : K]} \deg(P) = \frac{n}{[K' : K]} \sum_{P \in \mathbb{P}_F} (1 - \frac{r_P}{n}) \deg(P).$$

E, substituindo tal resultado na fórmula do gênero de Hurwitz, temos:

$$g' = 1 + \frac{n}{r_P}(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (1 - \frac{r_P}{n}) \deg(P)).$$

□

Corolário 2.7.4. *Sejam F/K um corpo de funções algébricas sobre e $F' = F(y)$ com $y^n = u \in F$, onde não vale que $n \equiv 0 \bmod(\mathrm{char}(K))$ e K contém uma $n-$ésima raiz primitiva da unidade. Assuma que existe um lugar $Q \in \mathbb{P}_F$ tal que $\mathrm{mdc}(v_Q(u), n) = 1$. Então K é o corpo constante de F, a extensão $F' = F(y)$ é cíclica de grau n, e:*

$$g' = 1 + n(g - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \deg(P).$$

Demonstração. Se $\mathrm{mdc}(v_Q(u), n) = 1$, então veja que:

$$u \neq w^d, \forall w \in F \text{ e } d|n, d > 1.$$

De fato, seja $w \in F$ e $d|n, d > 1$, mostremos que $u \neq w^d$. Suponha por absurdo que $u = w^d$, então $v_Q(u) = dv_Q(w) \Rightarrow \mathrm{mdc}(v_Q(u), n) \geq d > 1$, gerando uma contradição.

Assim, estamos nas condições da Proposição 2.7.3. Logo, pelos item 3 desta proposição, se $[K' : K] = 1$, temos:

$$g' = 1 + n(g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (1 - \frac{r_P}{n}) \deg(P))$$

$$\Rightarrow g' = 1 + n(g-1) + \frac{1}{2}\sum_{P\in\mathbb{P}_F}(n - r_P)\deg(P),$$

e temos o resultado.

Portanto basta mostrar que $[K' : K] = 1$.

Seja Q' uma extensão de Q em F'. Pelo item 2 da Proposição 2.7.3, $e(Q'|Q) = \frac{n}{r_P} = n = [F' : F]$ $(\star)$.

Suponha que $[K' : K] > 1$, então considere o corpo intermediário $F_1 := FK' \supsetneq F$ e o lugar $Q_1 := Q' \cap F_1$.

Por $(\star)$ temos $e(Q'|Q_1) = [F' : F_1]$, pois:

$$v_{Q_1}(u) = \underbrace{e(Q_1|Q)}_{=1} v_Q(u) = v_Q(u)$$

pelo Teorema 2.6.3. O que implica $1 = e(Q_1|Q) = [F_1 : F] > 1$, gerando um absurdo.

□

Exemplo 2.7.5. Sejam K tal que $\operatorname{char} K \neq 2$ e $F = K(x, y)$, com $y^2 = f(x) = p_1(x)...p_s(x) \in K[x]$, onde $p_1(x), ..., p_s(x)$ são polinômios mônicos irredutíveis e $s \geq 1$. Então K é todo o corpo de constantes de F, e F/K tem gênero g, onde:

$$g = \frac{m-1}{2} \text{ se } m \equiv 1 \bmod 2 \text{ ou}$$

$$g = \frac{m-2}{2} \text{ se } m \equiv 1 \bmod 2,$$

onde $m = \deg(f(x))$.

Demonstração. Temos $F = F_0(y)$, onde $F_0 = K(x)$ é o corpo de funções racionais.

Seja $P_i \in \mathbb{P}_{K(x)}$ o zero de $p_i(x)$ e P_∞ o pólo de x em $K(x)$. Então $v_{P_i}(f(x)) = 1$ e $v_{P_\infty}(f(x)) = -m$. Pelo Corolário 2.7.4, temos F/F_0 é cíclica de grau 2 e que K é todo o corpo constante de F. E quanto aos números r_P, $P \in \mathbb{P}_{K(x)}$, temos:

$$r_P = 2, P \in \mathbb{P}_{K(x)} \setminus \{P_\infty, P_1, ..., P_s\},$$

$$r_{P_i} = 1, 1 \leq i \leq s,$$

$$r_{P_\infty} = 2 \text{ se } m \equiv 0 \bmod 2, \text{ e } r_{P_\infty} = 1 \text{ se } m \equiv 1 \bmod 2.$$

Substituindo na fórmula do corolário, temos:

$$g' = 1 + 2(0-1) + \frac{1}{2}\sum_{i=1}^{s} \deg(P_i) + \frac{1}{2}(2 - r_{P_\infty}) =$$

$$= \frac{m}{2} - 1 + \frac{2 - r_{P_\infty}}{2} = \frac{m - r_{P_\infty}}{2},$$

e assim temos o resultado.

□

Lema 2.7.6. *Seja F/K um corpo de funções algébricas de característica $p > 0$. Dado um elemento $u \in F$ e um lugar $P \in \mathbb{P}_F$, temos:*

1. *ou existe um elemento $z \in F$ tal que $v_P(u - (z^p - z)) \geq 0$,*

2. *ou então, para algum $z \in F$, $v_P(u - (z^p - z)) = -m$, com m e p relativamente primos.*

   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. Provemos inicialmente a afirmação:

Sejam $x_1, x_2 \in F \setminus \{0\}$ onde $v_P(x_1) = v_P(x_2)$, então existe $y \in F$ tal que:

$$v_P(y) = 0 \text{ e } v_P(x_1 - y^p x_2) > v_P(x_1).$$

De fato, $v_P(x_1) = v_P(x_2) \Rightarrow v_P(\frac{x_1}{x_2}) = 0 \Rightarrow \frac{x_1}{x_2} \in O_P \setminus P \Rightarrow (\frac{x_1}{x_2})(P)$ é não nulo. Então como O_P/P é perfeito de característica p, temos que $(\frac{x_1}{x_2})(P) = (y(P))^p$, para algum $y \in O_P \setminus P$. Logo $v_P(y) = 0$ e $v_P(\frac{x_1}{x_2} - y^p) > 0$, assim:

$$v_P(\frac{x_1}{x_2} - y^p) > 0 \Rightarrow v_P(\frac{1}{x_2}(x_1 - y^p x_2)) > 0 \Rightarrow$$

$$\Rightarrow v_P(x_1 - y^p x_2) > v_P(x_2) = v_P(x_1).$$

Agora mostremos que: Se $v_P(u-(z_1^p-z_1))=-lp<0$, então existe $z_2\in F$ onde:

$$v_P(u-(z_2^p-z_2))>-lp.$$

Escolha $t\in F$ tal que $v_P(t)=-l$, então $v_P(u-(z_1^p-z_1))=v_P(t^p)$, e pela afirmação anterior temos que existe $y\in F$ com $v_P(y)=0$ e

$$v_P(u-(z_1^P-z_1)-(yt)^p)>-lp.$$

Como $v_P(y)=0$, então $v_P(yt)=v_P(t)=-l>-lp$, e assim

$$v_P(u-(z_1^p-z_1)-((yt)^p-yt))>-lp.$$

Definindo $z_2:=z_1+yt$, temos:

$$-lp<v_P(u-(z_1^p+(yt)^p-(z+yt)))=v_P(u-((z_1+yt)^p-(z_1+yt)))=$$

$$=v_P(u-(z_2^P-z_2)).$$

Repetindo esse processo um número finito de vezes temos a existência de $z\in F$ tal que um dos itens seja verdadeiro.

Falta então mostrar que se o item 2 é verdadeiro, temos $-m=\max\{v_P(u-(w^p-w));w\in F\}$.

Por hipótese $v_P(u-(z^p-z))=-m<0$, com m não divisível por p; logo $\forall w\in F$ temos $pv_P(w-z)\neq -m$, e temos por consequência 2 casos, $pv_P(w-z)>-m$ e $pv_P(w-z)<-m$:

Caso 1: $pv_P(w-z)>-m\Rightarrow v_P((w-z)^p)>-m$ e $v_P(w-z)>\frac{-m}{p}>-m$, e assim, pela desigualdade triangular $v_P((w-z)^p-(w-z))>-m$. Além disso:

$$v_P(u-(w^p-w))=v_P(u-(z^p-z)-((w^p-w)-(z^p-z)))=$$

$$=v_P(u-(z^p-z)-((w^p-z^p)-(w-z)))=$$

$$= v_P(u - (z^p - z) - ((w - z)^p - (w - z))) = -m$$

(desigualdade triangular estrita).

Caso 2: $pv_P(w - z) < -m$. Procedendo analogamente ao caso anterior obtemos $v_P(u - (w^p - w)) < -m$.

De qualquer forma, $v_P(u - (w^p - w)) \leq -m$.

Pelo o teorema da aproximação existe $w \in F$ tal que $pv_P(w - z) > -m$, e pelo caso 1, temos $v_P(u - (w^p - w)) = -m$.

Portanto, $-m = \max\{v_P(u - (w^p - w)); w \in F\}$.

□

Proposição 2.7.7. *(Extensões de Artin-Schreier)*

Seja F/K um corpo de funções algébricas de característica $p > 0$. Suponha que $u \in F$ é um elemento satisfazendo a seguinte condição:

$$u \neq w^p - w, \forall w \in F.$$

Considere $F' = F(y)$ tal que $y^p - y = u$.
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:

$$m_p = m, \text{ se vale o item 2 de 2.7.6, com respeito ao elemento } u,$$

$$ou$$

$$m_P = -1 \text{ se vale o item 1 de 2.7.6, com respeito ao elemento } u.$$

E então temos:

1. *F'/F é uma extensão de Galois cíclica de grau p. Os automorfismos de F'/F são dados por $\sigma(y) = y + \mu$, com $\mu = 0, ..., p - 1$;*

2. *P é não ramificado em F'/F se, e somente se, $m_P = -1$;*

3. *P é totalmente ramificado em F'/F se, e somente se, $m_P > 0$. Denotando P' como o único lugar que é extensão de P, temos que o expoente da diferente $d(P'|P)$ é dado por:*

$$d(P'|P) = (p-1)(m_P + 1);$$

4. *Se pelo menos um lugar $Q \in \mathbb{P}_F$ satisfaz $m_Q > 0$, então K é algebricamente fechado em F' e:*

$$g' = pg + \frac{p-1}{2}(-2 + \sum_{P \in \mathbb{P}_F} (m_p + 1)\deg(P)),$$

onde g' (respectivamente g) é o gênero de F'/K (respectivamente F/K).

Demonstração. Demonstremos os itens 2 e 3, para o item 1, veja Teorema A.6.2.

Primeiro, consideremos o caso $m_P = -1$, isto é, $v_P(u - (z^p - z)) \geq 0$, 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 $v_P(u_1) = v_P(u - (z^p - z)) \geq 0$, temos $u_1 \in O_P$. Assim, pela Proposição 2.3.1, y_1 é integral sobre o anel de valorização O_p. Além disso, veja que $\varphi_1'(y_1) = py_1^{p-1} - 1 = -1$; assim, se P' é uma extensão de P, temos $v_{P'}(\varphi_1'(y_1)) = 0$, e pelo Teorema 2.5.6, segue:

$$0 \leq d(P'|P) \leq v_{P'}(\varphi_1'(y_1)) = 0 \Rightarrow d(P'|P) = 0.$$

Como, pelo teorema da diferente de Dedekind, $d(P'|P) \geq e(P'|P) - 1$, com $e(P'|P) \geq 1$, temos $e(P'|P) = 1$, ou seja, $P'|P$ é não ramificada. Portanto, P é não ramificado em F'/F.

Agora assuma que $m_P > 0$ e escolha $z \in F$ tal que $v_P(u - (z^p - z)) = -m_P$.

Considere os elementos $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Como antes, temos $F' = F(y_1)$ e $\varphi_1(T) = T^p - T - u_1$ o polinômio minimal de y_1 sobre F. Seja P' uma extensão de P em F'. Como $y_1^p - y_1 = u_1$, então:

$$v_{P'}(u_1) = e(P'|P)v_P(u_1) = -m_P e(P'|P)$$

e

$$v_{P'}(u_1) = v_{P'}(y_1^p - y_1) = pv_{P'}(y_1).$$

E, portanto,

$$-m_p e(P'|P) = pv_{P'}(y_1).$$

Mas, m_p e p são primos entre si, o que implica $p|e(P'|P)$. E assim, como $e(P'|P) \leq [F' : F] = p$, temos $p = e(P'|P)$.

Portanto, $p = e(P'|P)$ e $-m_p = v_{P'}(y_1)$, e consequentemente, P é totalmente ramificado em F'/F.

Agora considere $x \in F$ um parâmetro local do lugar totalmente ramificado P, P' extensão de P e inteiros $i, j \geq 0$ tais que $1 = ip - jm_P$, então o elemento $t = x^i y_1^j$ é um parâmetro local de P', pois:

$$v_{P'}(t) = v_{P'}(x^i y_1^j) = iv_{P'}(x) + jv_{P'}(y_1) = 1.$$

Pela Proposição 2.5.8, o expoente da diferente é $d(P'|P) = v_{P'}(\psi'(t))$, onde $\psi(T)$ é o polinômio minimal de t sobre F.

Seja $G := \mathrm{Gal}(F'/F)$ o grupo de Galois de F'/F e considere o polinômio:

$$\prod_{\sigma \in G} (T - \sigma(t)).$$

Veja que como $\psi(T)$ é o polinômio minimal de t sobre F, e F'/F é de Galois, então:

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t)h(T), \text{ onde } h(T) = \prod_{\sigma \neq id} (T - \sigma(t)) \in F'[T].$$

Então $\psi'(t) = h(t)$, e portanto:

$$d(P'|P) = v_{P'}(\prod_{\sigma \neq id} (t - \sigma(t))) = \sum_{\sigma \neq id} v_{P'}(t - \sigma(t)).$$

Como cada $\sigma \in G \setminus \{0\}$ tem a forma: $\sigma(y_1) = \sigma(y - z) = y + \mu - z = (y - z) + \mu = y_1 + \mu$,

com $\mu \in \{1, ..., p-1\}$, temos:

$$t - \sigma(t) = x^i y_1^j - x^i (y_1 + \mu)^j = -x^i((y_1 + \mu)^j - y_1^j) =$$

$$= -x^i (\sum_{l=0}^{j} \binom{j}{l} y_1^{j-l} \mu^l - y_1^l) = -x^i (\sum_{l=0}^{j} \binom{j}{l} y_1^{j-l} \mu^l).$$

Como $v_{P'}(y_1^{j-1}) < v_{P'}(y_1^{j-2})$ para $l \geq 2$, então, pela desigualdade triangular estrita:

$$v_{P'}(t - \sigma(t)) = v_{P'}(-x^i (\sum_{l=0}^{j} \binom{j}{l} y_1^{j-l} \mu^l)) =$$

$$= v_{P'}(-x^i) + v_{P'}(\sum_{l=0}^{j} \binom{j}{l} y_1^{j-l} \mu^l) = ip + v_{P'}(\binom{j}{1} \mu y_1^{j-1}) = ip + v_{P'}(j\mu y_1^{j-1}) =$$

$$= ip + (j-1)(-m_P) = ip - jm_P + m_P = 1 + m_P.$$

Portanto, $d(P'|P) = (p-1)(1 + m_P)$.

Para provar o item 4, assuma que $m_Q > 0$, para pelo menos um lugar $Q \in \mathbb{P}_F$. Pelo item 3, Q é totalmente ramificado em F'/F, então, como feito no Corolário 2.7.4, temos que K é todo o corpo de constantes de F'. Agora, pela fórmula do gênero de Hurwitz:

$$2g' - 2 = p(2g-2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \deg(P') =$$

$$= p(2g-2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (m_P + 1)(p-1) \deg(P') =$$

$$= p(2g-2) + (p-1) \sum_{P \in \mathbb{P}_F} \frac{(m_P+1)}{e(P)} \deg(\sum_{P'|P} e(P'|P) P') =$$

$$= p(2g-2) + (p-1) \sum_{P \in \mathbb{P}_F} \frac{(m_P+1)}{e(P)} \deg(\mathrm{Con}_{F'/F}(P)) =$$

$$= 2pg - 2p + (p-1) \sum_{P \in \mathbb{P}_F} (m_P + 1) \deg(P)$$

$$\Rightarrow g' = pg + \frac{(p-1)}{2}(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \deg(P)).$$

□

Observação 2.7.8. Com as notações da proposição anterior, suponha que existe um lugar $Q \in \mathbb{P}_F$ tal que $v_Q(u) < 0$ e p não divide $v_Q(u)$. Então para todo $k \in K$, temos $v_Q(k^p - k) = 0$ ou $v_Q(k^p - k) = \infty$, logo não existe $k \in K$ tal que $k^p - k = u$. Isso vale também para todo $k \in O_Q$.

Seja agora $w \in F \backslash O_Q$, veja que se $w^p - w = u$ então $v_Q(w^p - w) < 0$,e assim $v_Q(w^P) < v_Q(w) < 0$. Portanto, pela desigualdade triangular estrita, $v_Q(u) = pv_Q(w)$, que é divisível por p.

Logo, não existe $w \in F$ tal que $u = w^p - w$. Ou seja, u satisfaz as condições da Proposição 2.7.7, e portanto, a proposição se aplica a este caso.

A maioria dos argumentos na prova da Proposição 2.7.7 se aplicam em uma situação mais geral:

Chamemos um polinômio da forma específica:

$$a(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + ... + a_1 T^p + a_0 T \in K[T],$$

onde $p = \text{char}(K) > 0$, de polinômio aditivo sobre K. Observe que $a(T)$ é separável se, e somente se, $a(T)$ e $a'(T)$ não tem fator comum de grau maior que 0. E, como $a'(T) = a_0$, então $a(T)$ é separável se, e somente se, $a_0 \neq 0$.

Tal polinômio tem a seguinte propriedade:

$$a(u + v) = a(u) + a(v),$$

para qualquer u e v em alguma extensão de K. Em particular, se $a(T)$ é um polinômio aditivo e separável sobre K, com todas as suas raízes em K, então suas raízes formam um subgrupo do grupo aditivo de K de ordem $p^n = \deg(a(T))$.

Proposição 2.7.9. *Sejam F/K um corpo de funções algébricas com corpo de constantes K de característica $p > 0$, $a(T) \in K[T]$ um polinômio aditivo separável de grau p^n com todas as suas raízes em K, e $u \in F$. Suponha que para cada $P \in \mathbb{P}_F$ existe um elemento $z \in F$ (dependendo de P) tal que:*

1. $v_P(u - a(z)) \geq 0$ *ou*

2. $v_P(u - a(z)) = -m$ *com* $m > 0$ *e não múltiplo de* p.

(Estamos supondo que $a(w) \neq u, \forall w \in F$*.)*

Defina $m_P := -1$ *se vale 1, e* $m_p := m$ *se vale 2. Pelo Lema 2.7.6, o inteiro* m_P *está bem definido.*

Considere a extensão $F' = F(y)$ *de* F *onde* y *satisfaz a equação* $a(y) = u$*. Se existir pelo menos um lugar* $Q \in \mathbb{P}_F$ *com* $m_Q > 0$*, então:*

1. F'/F *é extensão de Galois ,* $[F' : F] = p^n$ *e o grupo de Galois de* F'/F *é isomorfo ao grupo abeliano* $\{\alpha \in K; a(\alpha) = 0\}$*, portanto isomorfo a* $(\mathbb{Z}/p\mathbb{Z})^n$ *(tal grupo é dito ser grupo abeliano elementar de expoente* p*, então* F'/F *é chamado um extensão abeliana elementar de expoente* p *e grau* p^n*);*

2. K *é algebricamente fechado em* F'*;*

3. *Cada* $P \in \mathbb{P}_F$ *com* $m_P = -1$ *é não ramificado em* F'/F*;*

4. *Cada* $P \in \mathbb{P}_F$ *com* $m_p > 0$ *é totalmente ramificado em* F'/F*, e o expoente da diferente* $d(P'|P)$ *da extensão* P' *de* P *é* $d(P'|P) = (p^n - 1)(m_p + 1)$*;*

5. *Seja* g' *(respectivamente* g*) o gênero de* F' *(respectivamente* F*). Então:*

$$g' = p^n g + \frac{p^n - 1}{2}(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \deg(P)).$$

Capítulo

3

Corpos de funções algébricas com um número prescrito de lugares racionais

Retornemos agora às questões inicialmente propostas para este trabalho: para determinados inteiros não negativos g e N, e q uma potência de um primo, existe um corpo de funções F sobre $\mathbb{F}_q$ tal que $g(F) = g$ e $\mathrm{N}(F) = N$? Quais são as condições necessárias para se garantir tal existência?

Neste capítulo apresentamos o resultado mais importante a constituir este trabalho, que diz respeito justamente a estas questões e às relações existentes entre gênero e número de lugares racionais de um corpo de funções com corpo constante $\mathbb{F}_q$.

Mais precisamente, o que fazemos é fixar um N número inteiro não negativo e q uma potência de um primo para, assim, estudar o gênero de um corpo de funções sobre $\mathbb{F}_q$ com exatamente N lugares racionais, concluindo que, para todo g suficientemente grande, sempre existirá um corpo de funções $F/\mathbb{F}_q$ com $\mathrm{N}(F) = N$ e $g(F) = g$.

3.1 Corpos de funções com um número prescrito de lugares racionais

Lema 3.1.1. *Dado um corpo de funções algébricas $F/\mathbb{F}_q$ de gênero g, existe uma constante $C \geq 0$ tal que para todo inteiro $k \geq C$, existe um lugar $P \in \mathbb{P}_F$ com* $\deg(P) = k$.

Demonstração. Inicialmente podemos supor que $g > 0$, pois no caso do corpo de funções racionais $K(x)$ (veja a observação 1.6.4), existem lugares de todos os graus, dado que existem polinômios irredutíveis em $K[x]$ de todos os graus.

Sejam B_r e N_s como definidos abaixo:

$$B_r := B_r(F) = |\{P \in \mathbb{P}_F; \deg(P) = r\}|,$$

$$N_s := \left|\left\{P \in \mathbb{P}_{F\mathbb{F}_{q^s}}; \deg(P) = 1\right\}\right|,$$

onde $F\mathbb{F}_{q^s}$ é extensão por constantes de $F/\mathbb{F}_q$.

Existe uma forte relação entre B_r e N_s dada em [8] (pág. 206):

$$N_s = \sum_{d|s} dB_d.$$

Pela fórmula da inversão de Möbius (ver [6], pág. 92), temos:

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) N_d,$$

onde $\mu : \mathbb{N} \to \{-1, 0, 1\}$ é a função de Möbius definida por:

$$\mu(n) := \begin{cases} 1 & \text{se } n = 1; \\ 0 & \text{se existe } k > 1 \text{ tal que } k^2|n; \\ (-1)^l & \text{se } n \text{ é produto de } l \text{ primos distintos.} \end{cases}$$

Pelo Teorema de Hasse-Weil ([8], pág. 197) temos $N_d = q^d + 1 + S_d$, onde $|S_d| \leq 2gq^{\frac{d}{2}}$,

e por [6], pág. 92:

$$\sum_{d|r} \mu\left(\frac{r}{d}\right) = 0, \text{ para } r > 1.$$

Então para $r \geq 2$:

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) N_d = \sum_{d|r} \mu\left(\frac{r}{d}\right) (q^d + S_d)$$

$$\Rightarrow B_r - \frac{q^r}{r} = \frac{1}{r} \sum_{d|r \text{ e } d<r} \mu\left(\frac{r}{d}\right) q^d + \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right) S_d.$$

E a partir de alguns cálculos, que vamos omitir, se pode concluir que:

$$\left| B_r - \frac{q^r}{r} \right| \leq \left(\frac{q}{q-1} + 2g \frac{\sqrt{q}}{\sqrt{q}-1} \right) \frac{\sqrt{q^r}-1}{r}, \text{ para } r > 1.$$

Logo, para todo $r > 1$, temos:

$$B_r - \frac{q^r}{r} \geq - \left(\frac{q}{q-1} + 2g \frac{\sqrt{q}}{\sqrt{q}-1} \right) \frac{\sqrt{q^r}-1}{r}$$

$$\Rightarrow B_r \geq \frac{q^r}{r} - \left(\frac{q}{q-1} + 2g \frac{\sqrt{q}}{\sqrt{q}-1} \right) \frac{\sqrt{q^r}-1}{r}.$$

Veja agora que:

$$\frac{q^r}{r} > \left(\frac{q}{q-1} + 2g \frac{\sqrt{q}}{\sqrt{q}-1} \right) \frac{\sqrt{q^r}-1}{r} \Leftrightarrow \frac{q^r}{(\sqrt{q^r}-1)} > \frac{q}{q-1} + 2g \frac{\sqrt{q}}{\sqrt{q}-1}$$

$$\Leftrightarrow \frac{q^r(\sqrt{q}-1)}{(\sqrt{q^r}-1)} > \frac{q}{\sqrt{q}+1} + 2g\sqrt{q}$$

$$\Leftrightarrow \frac{q^r(\sqrt{q}-1)}{\sqrt{q}(\sqrt{q^r}-1)} > \frac{\sqrt{q}}{\sqrt{q}+1} + 2g = \frac{1}{1+q^{-\frac{1}{2}}} + 2g.$$

Veja ainda:

$$2g + \frac{1}{1+q^{-\frac{1}{2}}} < 2g + 1,$$

pois $q^{-\frac{1}{2}} > 0$. Além disso:

$$q^{\frac{(r-1)}{2}}(q^{\frac{1}{2}}-1) < \frac{q^r(q^{\frac{1}{2}}-1)}{q^{\frac{1}{2}}(q^{\frac{r}{2}}-1)}.$$

De fato,

$$q^{\frac{(r-1)}{2}}(q^{\frac{1}{2}}-1) < \frac{q^r(q^{\frac{1}{2}}-1)}{q^{\frac{1}{2}}(q^{\frac{r}{2}}-1)} \Leftrightarrow q^{\frac{r}{2}} - q^{\frac{(r-1)}{2}} < \frac{q^{\frac{(2r+1)}{2}} - q^r}{q^{\frac{(r+1)}{2}} - q^{\frac{1}{2}}}$$

$$\Leftrightarrow q^{\frac{(2r+1)}{2}} - q^{\frac{(r+1)}{2}} - q^r + q^{\frac{r}{2}} < q^{\frac{(2r+1)}{2}} - q^r \Leftrightarrow q^{\frac{(r+1)}{2}} > q^{\frac{r}{2}}.$$

Seja então r de tal sorte que:

$$2g+1 \leq q^{\frac{(r-1)}{2}}(q^{\frac{1}{2}}-1),$$

temos:

$$2g + \frac{1}{1+q^{-\frac{1}{2}}} < 2g+1 \leq q^{\frac{(r-1)}{2}}(q^{\frac{1}{2}}-1) < \frac{q^r(q^{\frac{1}{2}}-1)}{q^{\frac{1}{2}}(q^{\frac{r}{2}}-1)}.$$

Se $r \geq 4g+3$, então:

$$2g+1 < 2^{2g+1}(2^{\frac{1}{2}}-1) = 2^{\frac{((4g+3)-1)}{2}}(2^{\frac{1}{2}}-1)$$

$$\leq 2^{\frac{(r-1)}{2}}(2^{\frac{1}{2}}-1) \leq q^{\frac{(r-1)}{2}}(q^{\frac{1}{2}}-1).$$

Fazendo $C \geq 4g+3$, temos o resultado.

□

Lema 3.1.2. *Seja $F/\mathbb{F}_q$ um corpo de funções algébricas e $z \in F\backslash\mathbb{F}_q$ um elemento não constante com divisor de pólos $(z)_\infty = r_1Q_1 + ... + r_sQ_s$. Assuma que $r_1, ..., r_s$ são relativamente primos com q. Seja $E := F(y)$, onde y satisfaz a equação:*

$$y^q - y = z.$$

Então segue:

1. *A extensão E/F é uma extensão de Galois de grau $[E:F] = q$;*

2. *Os lugares $Q_1, ..., Q_s$ são totalmente ramificados em E/F, e todos os outros lugares de F são não ramificados em E/F;*

3. *O expoente da diferente de Q_j no divisor da diferente de E/F é:*

$$d(Q_j) = (r_j + 1)(q - 1),$$

para $j = 1, ..., s$. Então o grau do divisor da diferente de E/F é:

$$\deg(\mathrm{Diff}(E/F)) = \sum_{j=1}^{s} (r_j + 1)(q - 1)\deg(Q_j);$$

4. *Se $Q \in \mathbb{P}_F$ é um lugar racional de $F/\mathbb{F}_q$, que é zero de z, então Q se decompõe completamente em E/F, ou seja, existem q lugares racionais de E que estendem Q;*

5. *Se $Q \in \mathbb{P}_F$ é um lugar racional de $F/\mathbb{F}_q$, que é zero de $z-\alpha$, para algum $\alpha \in \mathbb{F}_q \setminus \{0\}$, então Q é inerte em E/F, isto é, Q não tem nenhuma extensão racional em E.*

Demonstração. Os itens 1,2 e 3 seguem da Proposição 2.7.9. Já os itens 4 e 5 seguem do Teorema de Kummer (2.3.7), pois $y^q - y = 0$ tem q raízes distintas em $\mathbb{F}_q$ e $y^q - y = a$ não tem raiz em $\mathbb{F}_q$ para $a \neq 0$.

□

Lema 3.1.3. *Para quaisquer inteiros não negativos j e N, existe um corpo de funções $E/\mathbb{F}_q$ com $g(E) \equiv j \bmod (q-1)$ e $\mathrm{N}(E) \geq N$.*

Demonstração. A prova será feita por indução sobre N, então comecemos com $N \leq 2$, ou seja, mostremos que para $0 \leq j$ inteiro, existe um corpo de funções $E_j/\mathbb{F}_q$ tal que $g(E_j) \equiv j \bmod (q-1)$.

Para $j = 0$, basta considerar o corpo de funções racionais $E_0 = \mathbb{F}_q(x)$ sobre $\mathbb{F}_q$. Suponhamos, então, $j \geq 1$ e vamos considerar dois casos: $\mathrm{char}(\mathbb{F}_q) = 2$ e $\mathrm{char}(\mathbb{F}_q) \neq 2$.

1. Para $\mathrm{char}(\mathbb{F}_q) = 2$, seja $E_j = E_0(y)$, onde y satisfaz a equação:

$$y^2 - y = x^{(2j+1)}.$$

Então, pelo Teorema de Kummer (2.3.7) e pela Proposição 2.7.7, temos:

(a) P_∞ pólo de x é totalmente ramificado e P_0 zero de x se decompõe completamente. Logo $\mathrm{N}(E_j) \geq 2$;

(b) Pela fórmula do gênero de Hurwitz:

$$g(E_j) = \frac{1}{2}(-2 + 2j + 2) = j.$$

2. Para $\mathrm{char}(\mathbb{F}_q) \neq 2$, veja o exemplo 2.7.5.

Agora suponhamos $N > 2$, pela hipótese de indução, existe um corpo de funções $H/\mathbb{F}_q$ tal que:

$$g(H) \equiv j \bmod (q-1) \text{ e } \mathrm{N}(H) \geq N - 1.$$

Sejam $P_1, ..., P_{N-1}$ lugares racionais de H, considere o lugar $P \in \mathbb{P}_H$ tal que $\deg(P) \geq g(H) + (N-1)$ (possível pelo Lema 3.1.1). Então $\deg(P - (P_1 + ... + P_{N-1})) \geq g(H)$, e pelo Teorema de Riemann-Roch (1.5.15), temos $\ell(P - (P_1 + ... + P_{N-1})) > 0$.

Seja $z \in \mathcal{L}(P - (P_1 + ... + P_{N-1}))$ um elemento não nulo, então z tem somente um pólo, P, e ele é de ordem 1. Temos ainda que os lugares $P_1, ..., P_{N-1}$ são zeros de z.

Considere a extensão $E := H(y)$ de H onde $y^q - y = z$.

Pelo Lema 3.1.2, E/H é uma extensão de Galois de grau $[E : H] = q$, o corpo de constantes de E é $\mathbb{F}_q$, o lugar P é o único lugar de H que é ramificado (totalmente) em E/H, e o grau do divisor da diferente de E/H é:

$$\deg(\mathrm{Diff}(E/H)) = 2(q-1)\deg(P).$$

Então, pela fórmula do gênero de Hurwitz segue:

$$2g(E) - 2 = q(2g(H) - 2) + 2(q-1)\deg(P)$$

$$\Rightarrow g(E) = qg(H) + (q-1)(\deg(P) - 1) \equiv j \bmod (q-1).$$

Os lugares $P_1, ..., P_{N-1}$, por serem zeros de z, se decompõem completamente em E/H

(Lema 3.1.2). Logo $N(E) \geq q(N-1) > N$.

□

Teorema 3.1.4. *Para qualquer corpo finito $\mathbb{F}_q$ e qualquer inteiro $N \geq 0$, existe $g_0 \geq 0$ tal que para todo $g \geq g_0$, existe um corpo de funções F com corpo de constantes $\mathbb{F}_q$, gênero $g(F) = g$ e tendo exatamente N lugares racionais.*

Demonstração. Sejam q e N dados, mostremos que para todo $j = 0, ..., (q-2)$, existe uma constante $g_0^{(j)}$ tal que para todo $g \geq g_0^{(j)}$ com $g \equiv j \bmod(q-1)$, existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) = g$ e $\mathrm{N}(F) = N$.

Primeiramente, pelo Lema 3.1.3, podemos considerar um corpo de funções $E/\mathbb{F}_q$ onde:

$$g(E) \equiv j \bmod(q-1) \text{ e } \mathrm{N}(E) \geq N.$$

Pelo Lema 3.1.1, existe um inteiro $C \geq 0$ tal que:

$(*)$ $C > 2g(E) + (\mathrm{N}(E) - N)$;

$(**)$ para todo $t \geq C$, existe $P \in \mathbb{P}_E$ com $\deg(P) = t$.

Defina:

$$g_0^{(j)} := g(E) + (q-1)(g(E) - 1 + C + N).$$

Veja que $g_0^{(j)} \equiv g(E) \equiv j \bmod(q-1)$.

Seja $g \geq g_0^{(j)}$ um inteiro tal que $g \equiv j \bmod(q-1)$, então $g = g_0^{(j)} + r(q-1)$. Denote por:

$$P_1, ..., P_N, Q_1, ..., Q_s$$

todos os lugares racionais de E (finito pela cota de Hasse-Weil), então $s = \mathrm{N}(E) - N$. Seja $P \in \mathbb{P}_E$ com $\deg(P) = C + r$ (existe por $(**)$).

Segue de $(*)$ que:

$$\deg(P - (Q_1 + ... + Q_s)) = C + r - s = C + r - (\mathrm{N}(E) - N) > 2g(E) > 2g(E) - 2.$$

Pelo Teorema de Riemann-Roch, $\ell(P-(Q_1+...+Q_s)) > 1$ e $\ell(P+P_i-(Q_1+...+Q_s)) = \ell(P-(Q_1+...+Q_s))+1 > 2$, $i = 1, ..., N$. Então existem elementos não nulos $u, x_1, ..., x_N$

tais que:

$$u \in \mathcal{L}(P - (Q_1 + ... + Q_s))$$

e

$$x_i \in \mathcal{L}(P + P_i - (Q_1 + ... + Q_s))\backslash\mathcal{L}(P - (Q_1 + ... + Q_s)), i = 1, ..., N.$$

Assim u tem pólo somente em P e, ou x_i tem pólo somente em P_i (de ordem 1), ou tem pólos em P e P_i, $i = 1, ..., N$.

Então podemos definir o seguinte elemento:

$$x := x_1 + ... + x_N, \text{ se } P \text{ é pólo de } x_1 + ... + x_N$$

e

$$x := x_1 + ... + x_N + u, \text{ se } P \text{ não é pólo de } x_1 + ... + x_N.$$

Os pólos de x só podem ser pólos de alguma parcela da soma que constitui x, assim temos que o divisor de pólos de x é dado por:

$$(x)_\infty = P + P_1 + ... + P_N.$$

De fato:

1. Se P é pólo de $x_1 + ... + x_N$, então:

$$0 > v_P(x) = v_P(x_1 + ... + x_N) \geq \min\{v_P(x_j), j = 1, ..., N\} \geq -1$$

$$\Rightarrow v_P(x) = -1.$$

E, pela forma em que os elementos x_i foram escolhidos, temos:

$$v_{P_i}(x_j) \geq 0, \text{ sempre que } i \neq j$$

$$\Rightarrow v_{P_i}(x) = v_{P_i}(x_i) = -1.$$

2. Se P não é pólo de $x_1 + ... + x_N$, então:

$$v_P(x_1 + ... + x_N) \geq 0 \text{ e } v_P(u) = -1$$

$$\Rightarrow v_P(x) = v_P(x_1 + ... + x_N + u) = -1.$$

Como u tem pólo somente em P, então segue que $v_{P_i}(u) \geq 0$, e de forma análoga ao caso anterior, concluímos que $v_{P_i}(x) = -1, i = 1, ..., N$.

Além disso, $Q_1, ..., Q_s$ são zeros de x.

Defina agora o corpo $F := E(y)$, onde:

$$y^q - y = x + 1.$$

Observe que $(x+1)_\infty = (x)_\infty$.

Segue do Lema 3.1.2 que F/E é uma extensão de Galois de grau $[F : E] = q$, os lugares $P, P_1, ..., P_N$ são totalmente ramificados em F/E, com o expoente da diferente $d = 2(q-1)$, os outros lugares de E são não ramificados em F e os lugares $Q_1, ..., Q_s$ não têm extensões racionais em F/E.

Seja então $P' \in \mathbb{P}_F$ um lugar racional, temos que a restrição de P' em E é um lugar racional de E, logo: $P' \cap E \in \{P_1, ..., P_N\} \Rightarrow \mathrm{N}(F) = N$, pois os demais lugares racionais não têm extensões racionais.

Assim, pela fórmula do gênero de Hurwitz:

$$2g(F) - 2 = q(2g(E) - 2) + 2(q-1)(C + r + N).$$

Então:

$$g(F) = q(g(E)-1)+(q-1)(C+r+N)+1 = g(E)+(q-1)g(E)-(q-1)+(q-1)(C+r+N)$$

$$= g(E) + (q-1)(g(E) - 1 + C + N) + r(q-1) = g_0^{(j)} + r(q-1) = g.$$

Defina $g_0 := \max\left\{g_0^{(j)}, j = 0, ..., q-2\right\}$. Temos que para todo $g \geq g_0$, existe $j \in$

$\{0, ..., q-2\}$ tal que $g \equiv j \bmod(q-1)$ e $g \geq g_0^{(j)}$, e temos que existe $F/\mathbb{F}_q$ corpo de funções com $g(F) = g$ e $\mathrm{N}(F) = N$.

□

3.2 Algumas consequências

Definição 3.2.1. Sejam q, N e g inteiros não negativos. Definimos os seguintes conjuntos:

$$\mathcal{G}(q, N) := \{g;\ \text{existe um corpo de funções } F/\mathbb{F}_q \text{ onde } g(F) = g \text{ e } \mathrm{N}(F) = N\},$$

$$\mathcal{N}(q, g) := \{N;\ \text{existe um corpo de funções } F/\mathbb{F}_q \text{ onde } g(F) = g \text{ e } \mathrm{N}(F) = N\}.$$

Proposição 3.2.2. *Sejam q e $N_1, ..., N_m$ inteiros não negativos dados. Então existe $g_0 \geq 0$ tal que para todo $g \geq g_0$, $\{N_1, ..., N_m\} \subseteq \mathcal{N}(q, g)$.*

Demonstração. Fixado q, pelo Teorema 3.1.4, para cada $i = 1, ..., m$, existe uma constante g_i tal que:

$$\mathcal{G}(q, N_i) \supseteq [g_i, +\infty).$$

Defina $g_0 := \max\{g_i, i = 1, ..., m\}$, então:

$$[g_0, +\infty) \subseteq \bigcap_{i=1}^{m} \mathcal{G}(q, N_i),$$

onde $\bigcap_{i=1}^{m} \mathcal{G}(q, N_i)$ é o conjundo dos inteiros não negativos g tal que para cada $i = 1, ..., m$, existe um corpo de funções $F_i/\mathbb{F}_q$ onde $g(F_i) = g$ e $\mathrm{N}(F_i) = N_i$.

Em outras palavras, para todo $g \in [g_0, +\infty)$, temos a existência de corpos de funções $F_i/\mathbb{F}_q, i = 1, ..., m$, tais que $g(F_i) = g$ e $\mathrm{N}(F_i) = N_i$, ou seja:

$$\{N_1, ..., N_m\} \subseteq \mathcal{N}(q, g).$$

□

Corolário 3.2.3. *Dados q e N inteiros não negativos, existe uma constante $g_1 = g_1(q, N)$*

tal que para todo inteiro $g \geq g_1$ e para todo $S \in \{0, ..., N\}$, existe um corpo de funções $F/\mathbb{F}_q$ onde $g(F) = g$ e $\mathrm{N}(F) = S$.

Demonstração. Na Proposição 3.2.2, considere $i = 1, ..., (N+1)$ e $N_i = i - 1$. Logo existe $g_1 \geq 0$ tal que $\{0, ..., N\} \subseteq \mathcal{N}(q, g)$, para todo $g \in [g_1, +\infty)$, ou seja, para todo $g \geq g_1$ e para todo $S \in \{0, ..., N\}$, existe um corpo de funções $F/\mathbb{F}_q$ onde $g(F) = g$ e $\mathrm{N}(F) = S$.

□

3.3 Um caso particular: $N = 2$

Aqui exibiremos um subconjunto de $\mathcal{G}(q, 2)$.

Proposição 3.3.1. *Seja q uma potência de número primo, então:*

$$\mathcal{G}(q,2) \supseteq \left[6q^2 - 12q + 5 + (q-2)(q-1)\left\lfloor 2\sqrt{q} \right\rfloor, +\infty\right).$$

Demonstração. Na demonstração do Teorema 3.1.4, definimos $g_0 = \max\left\{g_0^{(j)}, j = 0, ..., q-2\right\}$, onde $g_0^{(j)} = g(E) + (q-1)(g(E) - 1 + C + N)$ e é satisfeito:

1. $g(E) \equiv j \bmod (q-1)$ e $\mathrm{N}(E) \geq N$;
2. $C \geq 4g(E) + 3$ (Lema 3.1.1);
3. $C > 2g(E) + (\mathrm{N}(E) - N)$.

Seja então $C = 4g(E) + (\mathrm{N}(E) - N) + 3$, satisfazendo os itens 2 e 3. Temos:

$$g_0^{(j)} = g(E) + (q-1)(g(E) - 1 + C + N)$$

$$= g(E) + (q-1)(g(E) - 1 + (4g(E) + (\mathrm{N}(E) - N) + 3) + N)$$

$$= g(E) + (q-1)(5g(E) + \mathrm{N}(E) + 2).$$

Quando $N = 2$, pelo Lema 3.1.3, podemos considerar $g(E) = j$, e assim temos:

$$(*)\ g_0^{(j)} = j + (q-1)(5j + \mathrm{N}(E) + 2), \text{onde } \mathrm{N}(E) \geq 2.$$

Observemos que pela cota de Serre temos:

$$\mathrm{N}(E) \leq q + 1 + j \left\lfloor 2\sqrt{q} \right\rfloor .$$

Portanto:

$$(**)\ 2 \leq \mathrm{N}(E) \leq q + 1 + j \left\lfloor 2\sqrt{q} \right\rfloor .$$

Assim, por $(*)$ e $(**)$, temos por um lado:

$$g_0^{(j)} = j + (q-1)(5j + \mathrm{N}(E) + 2)$$

$$\leq j + (q-1)(5j + q + 1 + j \left\lfloor 2\sqrt{q} \right\rfloor + 2)$$

$$= (q^2 - 1) + 2(q-1) + j(5q - 4 + (q-1) \left\lfloor 2\sqrt{q} \right\rfloor).$$

E por outro lado:

$$g_0^{(j)} = j + (q-1)(5j + \mathrm{N}(E) + 2)$$

$$\geq j + (q-1)(5j + 2 + 2) = j + (q-1)(5j+4) = j(5q-4) + 4(q-1).$$

Portanto:

$$j(5q-4) + 4(q-1) \leq g_0^{(j)} \leq (q^2-1) + 2(q-1) + j(5q - 4 + (q-1) \left\lfloor 2\sqrt{q} \right\rfloor)$$

$$\Rightarrow \max_{j=0,\ldots,(q-2)} \{j(5q-4) + 4(q-1)\} \leq g_0$$

$$\leq \max_{j=0,\ldots,(q-2)} \left\{(q^2-1) + 2(q-1) + j(5q - 4 + (q-1) \left\lfloor 2\sqrt{q} \right\rfloor)\right\} .$$

E assim:

$$(q-2)(5q-4) + 4(q-1) \leq g_0$$

$$\leq (q^2-1) + 2(q-1) + (q-2)(5q - 4 + (q-1) \left\lfloor 2\sqrt{q} \right\rfloor)$$

$$\Rightarrow 5q^2 - 10q + 4 \leq g_0 \leq 6q^2 - 12q + 5 + (q-2)(q-1) \left\lfloor 2\sqrt{q} \right\rfloor .$$

Logo, podemos garantir que:

$$\mathcal{G}(q,2) \supseteq \left[6q^2 - 12q + 5 + (q-2)(q-1)\left\lfloor 2\sqrt{q}\right\rfloor, +\infty\right).$$

□

Observe que esta não é uma estimativa muito boa, pois, por exemplo, tomando $q = 2$, temos $4 \leq g_0 \leq 5$ e só pedíamos garantir $\mathcal{G}(2,2) \supseteq [5, +\infty)$, sendo que $\mathcal{G}(2,2) = [1, +\infty)$, como será visto a seguir.

3.4 Exemplos

Proposição 3.4.1. *1.* $\mathcal{G}(2,0) = \mathcal{G}(2,6) = [2, +\infty)$*;*

2. $\mathcal{G}(2,1) = \mathcal{G}(2,2) = \mathcal{G}(2,4) = \mathcal{G}(2,5) = [1, +\infty)$*;*

3. $\mathcal{G}(2,3) = [0, +\infty)$*;*

4. $\mathcal{G}(2,7) \subseteq [3, +\infty)$.

Demonstração. Mostremos o item 1: $\mathcal{G}(2,0) = \mathcal{G}(2,6) = [2, +\infty)$.

Aqui $q = 2$ e $N \in \{0, 6\}$, então pela cota de Serre:

$$|N - (q+1)| \leq g\left\lfloor 2\sqrt{q}\right\rfloor$$

$$\Rightarrow |N - 3| \leq g\left\lfloor 2\sqrt{2}\right\rfloor$$

$$\frac{|N-3|}{2} \leq g \Rightarrow g \geq 2, \text{ para } N \in \{0,6\}.$$

Logo, para $g \in \mathcal{G}(2,0)$ (respectivamente $g \in \mathcal{G}(2,6)$), devemos ter $g \geq 2$. Então mostremos que para todo $g \geq 2$, existe um corpo de funções $F/\mathbb{F}_2$ sem nenhum lugar racional (respectivamente com exatamente seis lugares racionais).

Sejam $g \geq 2$ e $f(x) \in \mathbb{F}_2[x]$ um polinômio irredutível de grau $\deg(f(x)) = g+1$, então

considere o corpo de funções $F = \mathbb{F}_2(x, y)$, onde:

$$y^2 + y = \frac{x^2 + x}{f(x)} + 1.$$

Como $(\frac{x^2+x}{f(x)})_\infty = P_{f(x)}$, então $(\frac{x^2+x}{f(x)} + 1)_\infty = P_{f(x)}$.

Pela fómula do gênero de Hurwitz, $g(F) = g$. Veja ainda que se P é um lugar racional de $\mathbb{F}_2(x)$, então $v_P(\frac{x^2+x}{f(x)}+1) = 0$, logo $\frac{x^2+x}{f(x)}+1$ não tem zeros ou pólos em lugares racionais.

Além disso $(\frac{x^2+x}{f(x)})_0 = P_0 + P_1 + P_\infty$.

Logo, pelo itens 4 e 5 do Lema 3.1.2, temos $\mathrm{N}(F) = 0$. Portanto $\mathcal{G}(2, 0) = [2, +\infty)$.

E, considerando:

$$y^2 + y = \frac{x^2 + x}{f(x)},$$

de forma análoga, temos $g(F) = g$ e $\mathrm{N}(F) = 6$.

Os itens 2 e 3 são obtidos por construções sinilares.

Já para a última afirmação, novamente pela cota de Serre, $g \in \mathcal{G}(2, 7) \Rightarrow g \geq 2$. Como todo corpo de funções $F/\mathbb{F}_2$ de gênero 2 tem um subcorpo de funções racionais de grau $[F : \mathbb{F}_2(x)] = 2$, seu número de lugares racionais é no máximo 6. Portanto $2 \notin \mathcal{G}(2, 7)$.

□

Apêndice

$\mathcal{A}$

Teoria de corpos

A.1 Extensões algébricas de corpos

Proposição A.1.1. *Sejam K e L corpos, α algébrico sobre K e $q_\alpha(T) = a_0 + a_1T + ... + a_nT^n$ o polinômio minimal de α sobre K. Se $\psi : K(\alpha) \to L$ é um homomorfismo e φ é a restrição de ψ em K, então $\psi(\alpha)$ é raiz de ${}^{\varphi}q_\alpha(T) = \varphi(a_0) + \varphi(a_1)T + ... + \varphi(a_n)T^n$ sobre L. Reciprocamente, para todo $\varphi : K \to L$ homomorfismo e para toda raiz β de ${}^{\varphi}q_\alpha(T)$, existe um único homomorfismo de corpos $\psi : K(\alpha) \to L$ que estende φ e leva α em β.*

Proposição A.1.2. *Sejam $K \subseteq E \subseteq F$ corpos. Se F/K é uma extensão algébrica, então E/K e F/E são extensões algébricas.*

Proposição A.1.3. *Sejam $K \subseteq E \subseteq F$ corpos. Se E/K e F/E são extensões algébricas, então F/K é uma extensão algébrica.*

Teorema A.1.4. *Todo homomorfismo de um corpo K em um corpo algébricamente fechado pode ser extendido a qualquer extensão algébrica de K.*

Teorema A.1.5. *Todo corpo K tem uma extensão algébrica que contém todas as raízes de todo polinômio com coeficientes em K.*

Teorema A.1.6. *Todo corpo K tem uma extensão algébrica $\overline{K}$ que é algébricamente fechada. Além disso, $\overline{K}$ é único a menos de $K-$isomorfismos.*

Definição A.1.7. Um fecho algébrico de um corpo K é uma extensão algébrica $\overline{K}$ de K que é algébricamente fechada.

A.2 Extensões separáveis

Definição A.2.1. O grau de separabilidade $[E:K]_s$ de uma extensão algébrica E/K é o número de $K-$homomorfismos de E no fecho algébrico $\overline{K}$ de K.

Proposição A.2.2. *Seja α é algébrico sobre K e $p_\alpha(T) \in K[T]$ o polinômio minimal de α sobre K. Então $[K(\alpha):K]_s$ é o número de raízes distintas de $p_\alpha(T)$ em $\overline{K}$. Portanto, $[K(\alpha):K]_s \leq [K(\alpha):K]$ e, além disso, $[K(\alpha):K]_s = [K(\alpha):K]$ se, e somente se, $p_\alpha(T)$ é separável.*

Proposição A.2.3. *Se F é algébrico sobre K e $K \subseteq E \subseteq F$, então $[F:K]_s = [F:E]_s [E:K]_s$.*

Proposição A.2.4. *Para uma extensão finita E/K, são equivalente:*

1. *E é separável sobre K;*
2. *E é gerado por uma quantidade finita de elementos separáveis sobre K;*
3. *$[E:K]_s = [E:K]$.*

A.3 Extensões puramente inseparáveis

Lema A.3.1. *Se K é um corpo de característica $p > 0$ e α é algébrico sobre K, então $\alpha^{p^n} \in K$ para algum $n \geq 0$ se e somente se o polinômio minimal de α sobre K tem a forma $\varphi(T) = T^{p^m} - a$, para algum $a \in K$ e $m \geq 0$.*

Definição A.3.2. Se K é um corpo de característica $p > 0$ e α é algébrico sobre K, então α é dito puramente inseparável quando existe $n \geq 0$ tal que $\alpha^{p^n} \in K$.

Proposição A.3.3. *Seja K um corpo de característica $p > 0$ e E uma extensão algébrica de K, então são equivalentes:*

1. *E é puramente inseparável sobre K;*

2. Todo elemento de E é puramente inseparável sobre K;

3. $[E : K]_s = 1$.

Proposição A.3.4. *Se todo $\alpha \in S$ é puramente inseparável sobre K, então $K(S)$ é puramente inseparável sobre K.*

Proposição A.3.5. *Sejam $K \subseteq E \subseteq F$ extensões algébricas. Se F é puramente inseparável sobre K, então E é puramente inseparável sobre K e F é puramente inseparável sobre E.*

Proposição A.3.6. *Sejam $K \subseteq E \subseteq F$ extensões algébricas. Se E é puramente inseparável sobre K e F é puramente inseparável sobre E, então F é puramente inseparável sobre K.*

Proposição A.3.7. *Se E é puramente inseparável sobre K e o compósito EF existe, então EF é puramente inseparável sobre KF.*

Proposição A.3.8. *Todo compósito de extensões algébricas puramente inseparáveis sobre K é um extensão puramente inseparável sobre K.*

Definição A.3.9. Seja F uma extensão algébrica de K e S o maior subcorpo de F contendo K tal que S/K é uma extensão separável. O grau $[S : K]$ é chamado de grau de separabilidade de F sobre K e o grau $[F : S]$ é chamdo de grau de inseparabilidade de F sobre K, e são denotados, respectivamente por $[F : K]_s$ e $[F : K]_i$.

A.4 Norma e traço de extensões de corpos

Definição A.4.1. Sejam F uma extensão finita de K, $\overline{K}$ o fecho algébrico de K contendo F e $\sigma_1, ..., \sigma_r$ todos os $K-$homomorfismos distinto $F \to \overline{K}$. Se $u \in F$, a norma de u, denotada por $\mathrm{N}_{F/K}(u)$, é o elemento:

$$\mathrm{N}_{F/K}(u) = (\sigma_1(u)...\sigma_r(u))^{[F:K]_i}.$$

O traço de u, denotado por $\mathrm{Tr}_{F/K}(u)$, é o elemento:

$$\mathrm{Tr}_{F/K}(u) = [F:K]_i\,(\sigma_1(u) + ... + \sigma_r(u)).$$

Teorema A.4.2. *Seja F/K uma extensão de Galois e $\mathrm{Gal}(F/K) = \{\sigma_1, ..., \sigma_n\}$, então para todo $u \in F$ temos:*

$$\mathrm{N}_{F/K}(u) = \sigma_1(u)...\sigma_n(u) \text{ e}$$

$$\mathrm{Tr}_{F/K}(u) = \sigma_1(u) + ... + \sigma_n(u).$$

Teorema A.4.3. *Seja F uma extensão finita de K. Então para todos $u, v \in F$:*

1. $\mathrm{N}_{F/K}(u)\,\mathrm{N}_{F/K}(v) = \mathrm{N}_{F/K}(uv)$ *e* $\mathrm{Tr}_{F/K}(u) + \mathrm{Tr}_{F/K}(v) = \mathrm{Tr}_{F/K}(u+v)$;
2. *se $u \in K$, então* $\mathrm{N}_{F/K}(u) = u^{[F:K]}$ *e* $\mathrm{Tr}_{F/K}(u) = [F:K]\,u$;
3. $\mathrm{N}_{F/K}(u)$ *e* $\mathrm{Tr}_{F/K}(u)$ *são elementos de K, mais precisamente,* $\mathrm{N}_{F/K}(u) = ((-1)^n a_0)^{[F:K(u)]}$ *e* $\mathrm{Tr}_{F/K}(u) = -\,[F:K(u)]\,a_{n-1}$, *onde $f(T) = T^n + a_{n-1}T^{n-1} + ... + a_0 \in K\,[T]$ é o polinômio minimal de u sobre K;*
4. *se E é um corpo intermediário, então* $\mathrm{N}_{E/K}(\mathrm{N}_{F/E}(u)) = \mathrm{N}_{F/K}(u)$ *e* $\mathrm{Tr}_{E/K}(\mathrm{Tr}_{F/E}(u)) = \mathrm{Tr}_{F/K}(u)$.

Proposição A.4.4. *Seja F/K uma extensão finita, então F/K é separável se e somente se $\mathrm{Tr}_{F/K}$ não é a aplicação identicamente nula, ou seja, $\mathrm{Tr}_{F/K}$ é sobrejetora.*

A.5 Corpos perfeitos

Definição A.5.1. Um corpo K é dito perfeito quando toda extensão algébrica finita F/K é uma extensão separável.

Corolário A.5.2. *Um corpo K é perfeito se e somente se todo extensão algébrica F/K é separável.*

Teorema A.5.3. *Seja K um corpo, então são equivalentes:*

1. *K é um corpo perfeito;*

2. *todo polinômio irredutível de* $K[T]$ *é separável;*

3. *todo fecho algébrico* $\overline{K}$ *de* K *é Galois sobre* K*;*

4. *toda extensão algébrica de* K *é separável sobre* K*;*

5. *ou* $\mathrm{char}(K) = 0$ *ou* $\mathrm{char}(K) = p > 0$ *e* $K = K^p$*.*

Corolário A.5.4. *Sejam* K *um corpo tal que* $\mathrm{char}(K) = p > 0$*,* $n \geq 1$ *e a aplicação de Frobenius* $\varphi_n : K \to K$*, onde* $\varphi_n(u) = u^{p^n}$*. Então* K *é perfeito se e somente se* φ *é um isomorfismo.*

Corolário A.5.5. *Todo corpo finito é perfeito.*

A.6 Extensões cíclicas

Teorema A.6.1. *(Teorema de Hilbert)*

Sejam E/F *uma extensão cíclica de grau* n *com grupo de Galois* G*,* σ *um gerador de* G *e* $\beta \in E$*. A norma* $\mathrm{N}_{E/F}(\beta)$ *é igual a* 1 *se e somente se, existe um elemento* $\alpha \neq 0$ *em* E *tal que* $\beta = (\sigma(\alpha))^{-1}\alpha$*.*

Teorema A.6.2. *(Artin-Schreier)*

Seja F *um corpo de característica* $p > 0$*. Então:*

1. *Seja* E *uma extensão cíclica de* F *com grau* p*. Então existe* $y \in E$ *tal que* $E = F(y)$ *e* y *satisfaz a equação* $T^p - T - z = 0$*, para algum* $z \in F$*;*

2. *Reciprocamente, dado* $z \in F$*, o polinômio* $\varphi(T) = T^p - T - z$ *ou tem uma raiz em* F*, e nesse caso todas elas estão em* F*, ou é irredutível. No segundo caso, se* y *é uma raiz de* $\varphi(T)$*, então* $F(y)/F$ *é uma extensão cíclica de grau* p*.*

Demonstração. 1. Seja E/F cíclica de grau p. Então $\mathrm{Tr}_{E/F}(-1) = 0$ (isso é a soma de -1 consigo mesmo p vezes). Seja σ um gerador do grupo de Galois. Pela forma aditiva do Teorema de Hilbert (A.6.1), existe $y \in E$ tal que $\sigma(y) - y = 1$, em outras palavras, $\sigma(y) = y + 1$. Então $\sigma^i(y) = y + i$, para todo inteiro $i = 0, ..., p - 1$, e y tem p conjulgados distintos. Portanto, $[F(y) : F] \geq p$, seguindo que $F(y) = E$.

Note ainda que:

$$\sigma(y^p - y) = \sigma(y)^p - \sigma(y) = (y+1)^p - (y+1) = y^p - y.$$

Portanto, $y^p - y$ é fixado por σ, e assim, fixado por qualquer potência de σ. Logo, fixado por todo o grupo de Galois.

Assim, $y^p - y \in F$. Fazendo $z := y^p - y \in F$, temos o resultado.

2. Seja $z \in F$. Se y é uma raiz de $\varphi(T) = T^p - T - z$, então $y + i$ é também raiz para $i = 0, ..., p-1$. Então $\varphi(T)$ tem p raízes distintas. Se uma delas está em F, então todas estarão em F. Assuma qua não existem raízes em F. Devemos mostrar que $\varphi(T)$ é irredutível.

   Suponha que $\varphi(T) = g(T)h(T)$, com $g(T), h(T) \in F[T]$ e $1 \leq \deg(g(T)) < p$. Como:

$$\varphi(T) = \prod_{i=0}^{p-1} T - y - i,$$

   temos que $g(T)$ é um produto sobre certos inteiros i. Seja $d = \deg(g(T))$. O coeficiente de T^{d-1} em $g(T)$, é a soma dos termos $-(y+i)$ destes precisamente d inteiros i. Assim, esse coeficiente é igual a $-dy + j$, para algum j inteiro. Mas $d \neq 0$ em F, e então y está em F, pois os coeficientes de $g(T)$ estão em F, gerando um contradição.

   Portanto, $\varphi(T)$ é irredutível. Todas as raízes estão em $F(y)$, logo $F(y)/F$ é normal. Como $\varphi(T)$ não tem raízes multiplas, segue que $F(y)/F$ é uma extensão de Galois. Existe um automorfismo σ de $F(y)/F$ tal que $\sigma(y) = y + 1$, pois $y + 1$ é também raiz de $\varphi(T)$. Logo as potências σ^i de σ são $\sigma(y) = y + i$, para $i = 0, ..., p-1$, e são diferentes. E concluimos que o grupo de Galois consiste destas potência e é cíclico, provando o teorema.

□

Teorema A.6.3. *(Extensão de Kummer)*

Sejam F um corpo, n um inteiro > 0 relativamente primo com a característica de F, e assuma que existe $n-$ésima raiz primitiva da unidade em F.

1. *Seja E uma extensão cíclica de grau n. Então existe $\alpha \in E$ tal que $E = F(\alpha)$, e α satisfaz a equação $T^n - a = 0$, para algum $a \in F$;*

2. *Recíprocamente, sejam $a \in F$ e α uma raiz de $T^n - a$. Então $F(\alpha)$ é uma extensão cíclica sobre F, de grau d, $d|n$, e α^d é um elemento de F.*

Referências Bibliográficas

[1] Garcia, A. Stichtenoth, H. Elementary abelian p-extensions of algebraic functions fields. *Manuscripta Mathematica 72* (1991), 67–79.

[2] Garcia, A. Stichtenoth, H. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Inventiones Math. 121* (1995), 211–222.

[3] Goppa, V. D. Codes on algebraic curves. *Soviet Math. Dokl 24*, 1 (1981), 170–172.

[4] Kani, E. Relations between the genera and between the hasse-witt invariants of galois coverings of curves. *Canad. Math. Bull. 28*, 3 (1985), 321–327.

[5] Lang, S. *Algebra*, 3ª ed. Adison-Wesley, 1995.

[6] Lidl, R. Niederreiter, H. *Finite fields*, 2ª ed. Cambridge Univ. Press, Cambridge, 1997.

[7] Stöhr, K. O. Viana, P. A study of hasse-witt matrices by local methods. *Math. Z. 200* (1989), 397–407.

[8] Stichtenoth, H. *Algebraic Function Fields and Codes*, 2ª ed. Springer-Verlag, Berlin-Heidelberg, 2009.

[9] Stichtenoth, H. Curves with a prescribed number of rational points. *Finite Fields and Their Applications 17*, 6 (2011), 552–559.

[10] Voss, C. Hoholdt, T. An explicit construction of a sequence of codes attaining the tsfasman-vladut-zink bound. *IEEE Transactions on Information Theory 43*, 1 (1997), 128–135.