Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Classificação de Corpos de Funções Algébricas

Ana Carolina Mardegan

Orientador: Parham Salehyan

Dissertação apresentada ao Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista, Câmpus São José do Rio Preto, como parte dos requisitos para a obtenção do título de Mestre em Matemática

São José do Rio Preto

Setembro - 2009

ANA CAROLINA MARDEGAN

Classificação de Corpos de Funções Algébricas

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

BANCA EXAMINADORA

Prof. Dr. Parham Salehyan
Professor Doutor
UNESP - São José do Rio Preto
Orientador

Prof. Dr. Daniel Levcovitz
Prof. Adjunto (MS5)
USP - ICMC - São Carlos

Prof. Dr. Jéfferson Luiz Rocha Bastos
Professor Doutor
UNESP - São José do Rio Preto

São José do Rio Preto, 03 de setembro de 2009

A minha mãe,

Maria Antonia Bonizzi Mardegan,

dedico.

Agradecimentos

Agradeço a Deus primeiramente por ter me proporcionado a oportunidade de ter chegado até aqui e por ter colocado pessoas maravilhosas em minha vida. Citarei algumas delas as quais gostaria de deixar um sincero agradecimento:

Mãe, sem você nada disso poderia ser possível! Obrigada pelo apoio, incentivo, suporte financeiro e emocional... Amo você!

Pai, André e Léo, obrigada pelo incentivo e a torcida positiva.

Charles, obrigada pelo apoio, carinho, incentivo e por estar sempre ao meu lado.

Aos meus amigos da pós pela ajuda nos estudos e pelo ótimo relacionamento, e um agradecimento em especial às amigas Ana Paula e Marisa as quais seria impossível passar em algumas matérias... Sei que encontrei em vocês verdadeiras amigas!

Aos professores do departamento de matemática que me proporcionaram muito conhecimento, em especial às professoras Ângela e Gorete que me auxiliaram em momentos difíceis, e ao meu orientador Parham, por sua dedicação, paciência e por todo empenho durante sua orientação.

E a muitas outras pessoas que passaram na minha vida, que não são menos importantes, a todas vocês, agradeço por tudo!

"Adoramos a perfeição, porque não a podemos ter; repugna-la-íamos, se a tivéssemos. O perfeito é desumano, porque o humano é imperfeito."

Fernando Pessoa

Resumo

Uma grande parte desse projeto é voltada para o estudo de corpos de funções algébricas e suas propriedades elementares. Inicialmente estudaremos valorizações discretas sobre um corpo qualquer. Seguiremos com o estudo de divisores e provaremos o teorema de Riemann-Roch. Como aplicações deste teorema, calcularemos o gênero de alguns corpos de funções algébricas e classificaremos corpos de funções algébricas de gênero um e dois.

Abstract

The main goal is classification of algebraic function fields of genus one and two. First of all, we will study discreet valuations over any field. Then we will prove the Riemann-Roch Theorem for algebraic function fields. Finally we will use this theorem for computing the genera of some algebraic function fields and classifying algebraic function fields of genus one and two.

Sumário

Introdução

Uma função algébrica y de uma variável x é uma função implícita do tipo $f(x, y) = 0$, onde f é um polinômio em duas variáveis, ou seja, y é uma raiz de uma equação algébrica cujos coeficientes são funções racionais em x. Essa definição é muito semelhante com a definição de um número álgébrico: as funções racionais em x têm o mesmo papel que os números racionais. Por outro lado, a equação $f(x, y) = 0$ representa uma curva no plano e isto estabelece uma relação muito próxima entre a teoria de funções algébricas de uma variável e a teoria de curvas algébricas planas.

Uma grande parte desse projeto é voltada para o estudo de corpos de funções algébricas e suas propriedades elementares. Inicialmente estudaremos valorizações discretas sobre um corpo qualquer, isto tem por motivação a valorização definida naturalmente no corpo das funções meromorfas. Seguiremos com o estudo de divisores e provaremos o teorema de Riemann-Roch. A parte principal do estudo de corpos de funções algébricas está embasado neste teorema. Aplicando este teorema, como exemplo, calcularemos o gênero de alguns corpos de funções algébricas e finalmente classificaremos os corpos de funções algébricas de gênero um e dois.

Capítulo

1

Preliminares

Neste capítulo introduziremos alguns resultados de fundamental importância para o desenvolvimento dos capítulos posteriores.

1.1 Valorizações

Inicialmente definiremos a ordem de uma função meromorfa o que será um dos exemplos principais de valorizações cuja definição virá em seguida. Sejam $\mathbb{C}$ o corpo dos números complexos e $f = f(z) \neq 0$ uma função meromorfa sobre $\mathbb{C} \cup \{\infty\}$. Para cada $c \in \mathbb{C}$ podemos escrevê-la como uma Série de Laurent,

$$f(z) = a_m(z-c)^m + a_{m+1}(z-c)^{m+1} + \cdots,$$

onde $a_i \in \mathbb{C}$, $m \in \mathbb{Z}$ e $a_m \neq 0$. Definimos o valor m como a ordem de f em c e o denotaremos por $v_c(f)$. Observe que f é holomorfa em c se, e somente se $m \geq 0$. Então:

(i) se $m > 0$, então f tem zero de ordem m em c;

(ii) se $m < 0$, então f tem pólo de ordem $-m$ em c.

No ponto "∞" trabalhamos com o parâmetro $\dfrac{1}{z}$, desse modo

$$f(z) = b_r\left(\frac{1}{z}\right)^r + b_{r+1}\left(\frac{1}{z}\right)^{r+1} + \cdots,$$

onde $b_r \neq 0$. Definimos $v_\infty(f) := r$.

Teorema 1.1 *O corpo das funções meromorfas sobre o plano complexo compactificado* $\mathbb{C} \cup \{\infty\}$ *é o corpo* $\mathbb{C}(z)$ *das funções racionais.*

Demonstração: Como f é meromorfa, seus pólos são isolados, então o conjunto dos pólos de f é discreto e como $\mathbb{C} \cup \{\infty\}$ é compacto, f possui somente um número finito de pólos, digamos $c_1, \ldots, c_n \in \mathbb{C}$ e ∞. Para cada $j = 1, \ldots, n$, seja $f(z) = \sum_i a_{ij}(z - c_j)^i$ a Série de Laurent de f em $(z - c_j)$. Consideremos a soma das partes principais:

$$h := \sum_{j=1}^{n} \sum_{i<0} a_{ij}(z - c_j)^i + \sum_{i<0} \frac{b_i}{z^i}.$$

Pela construção de h, $f - h$ não tem pólos em $\mathbb{C} \cup \{\infty\}$ que é compacto, então, $|f - h|$ tem valor máximo em $\mathbb{C} \cup \{\infty\}$. Logo $f - h$ é constante e portanto $f \in \mathbb{C}(z)$. □

Observação 1.1 *Cada ponto* $p \in \mathbb{C} \cup \{\infty\}$ *define uma aplicação* $v_p : \mathbb{C}(z)^* \to \mathbb{Z}$, *tal que* $v_p(f)$ *é a ordem de* f *em* p *e satisfaz:*

(1) $v(fg) = v(f) + v(g)$;

(2) $v(f + g) \geq \min\{v(f), v(g)\}$, *se* $f + g \neq 0$;

(3) $v_p(c) = 0$ *para todo* $c \in \mathbb{C}^*$.

Em geral temos a seguinte definição:

Definição 1.1 *Seja* K *um corpo. Uma valorização de* K *com grupo de valores de* $\mathbb{Z}$ *é uma aplicação sobrejetora* $v : K^* \to \mathbb{Z}$ *tal que:*

(1) $v(fg) = v(f) + v(g)$;

(2) $v(f + g) \geq \min\{v(f), v(g)\}$;

(3) Se $k \leq K$ *é corpo, então a valorização* v *de* K *será chamada de valorização de* $K|k$ *se* $v\big|_{k^*} \equiv 0$.

Observação 1.2 *Segue da definição de valorização:* $v(1) = v(-1) = 0$; $v(f) = v(-f)$ *e* $v\left(\frac{1}{f}\right) = -v(f)$.

Definição 1.2 *Definindo* $v(0) := \infty$ *onde* $\infty > n$ *para todo* $n \in \mathbb{Z}$, *podemos definir as valorizações* $v : K \to \mathbb{Z} \cup \{\infty\}$ *que satisfazem as condições da Definição1.1.*

Lema 1.1 *Sejam* $f_1, \ldots, f_m \in K$, *então:*

(i) $v\left(\sum_{i=1}^{m} f_i\right) \geq \min_{1 \leq i \leq m} \{v(f_i)\}$;

(ii) se existe i *tal que* $v(f_i) < v(f_j)$ *para todo* $i \neq j$ *então* $v\left(\sum_{j=1}^{m} f_j\right) = v(f_i)$;

(iii) se $\sum_{i=1}^{m} f_i = 0$, *então existem* k, l *tais que* $v(f_k) = v(f_i)$.

Demonstração: Definições 1.1 e 1.2. □

A seguir determinaremos todas as valorizações de $k(z)|k$ com o grupo de valores $\mathbb{Z}$, onde k é um corpo algebricamente fechado, isto é, $k = \overline{k}$, e z transcendente sobre k. Seja $v : k(z)^* \to \mathbb{Z}$ uma valorização. Então temos dois casos.

(1) Se $v(z) \geq 0$, então para todo $f \in k[z]^*$, $f(z) = \sum a_i z^i$, temos que

$$v(f(z)) = v\left(\sum a_i z^i\right) = \min_i \left\{iv(z)\right\} \geq 0,$$

ou seja, $v|_{k[z]^*} > 0$. Agora seja $f \in k(z)^*$, então $f = \frac{f_1}{f_2}$, $f_1, f_2 \in k[z]$ e $f_2 \neq 0$, portanto $v(f) = v(f_1) - v(f_2)$, ou seja, para determinar v basta saber $v(f)$ quando $f \in k[z]^*$. Como $v \neq 0$, existe $f \in k[z]^*$ tal que $v(f) > 0$. Como $k = \overline{k}$, existem $c_0, \ldots, c_n \in k$, $c_0 \neq 0$ tais que $f = c_0(z - c_1) \cdots (z - c_n)$. Logo

$$v(f) = \sum_{i=1}^{n} v(z - c_i) > 0.$$

Então existe i tal que $v(z - c_i) > 0$. Seja $c := c_i$, pela sobrejetividade de v, podemos supor $v(z - c) = 1$.

Agora, seja $h = a\prod_{b\in k}(z-b)^{m_b} \in k(z)^*$, $a \in k^*$, logo $v(h) = \sum m_b v(z-b)$. Se $b \neq c$ então,

$$0 = v(b-c) = v((z-c)-(z-b)) \geq \min\{v(z-c), v(z-b)\},$$

mas como $v(f) \geq 0$ para todo $f \in k[z]^*$, teremos $v(z-b) = 0$ para todo $b \neq c$.

Logo $v(h) = m_c v(z-c) = m_c$, portanto $v(h)$ é a ordem de h em c. Neste caso denotaremos v por v_c.

(2) Se $v(z) < 0$, considere $f(z) = \sum_{i=0}^{n} a_i z^i \in k[z]^*$, então

$$v(a_n z^n) = nv(z) < v(a_i z^i),$$

para todo $i = 0, \ldots, n-1$, portanto $v(f) = nv(z)$. Seja $h \in k(z)^*$, então $h = \dfrac{h_1}{h_2}$, com h_1 e $h_2 \in k[x]$ e $h_2 \neq 0$. Logo,

$$v(h) = v(h_1) - v(h_2) = \deg(h_1)v(z) - \deg(h_2)v(z) = (\deg(h_1) - \deg(h_2))v(z).$$

Como v é sobrejetora e $v(z) < 0$, podemos supor $v(z) = -1$. Então

$$v(h) = \deg(h_2) - \deg(h_1).$$

Neste caso denotaremos v por v_∞.

Portanto, verificamos que as valorizações definidas sobre $k(z)|k$ com $k = \overline{k}$, são da forma

$$\begin{aligned} v(f) = v_c(f) \text{ para algum } c \in k \quad &\text{se} \quad v(z) > 0, \\ v(f) = v_\infty(f) \qquad\qquad\quad &\text{se} \quad v(z) < 0. \end{aligned}$$

Definição 1.3 *Seja $K|k$ uma extensão de corpos, definimos como Superfície Abstrata de Riemann o conjunto das valorizações de $K|k$ com o grupo de $\mathbb{Z}$, denotado por $S_{K|k}$.*

Definição 1.4 *Sejam $K = k(z)$, onde k não é necessariamente algebricamente fechado, e z transcendente sobre k. Cada $h \in k(z)^*$ se escreve da forma $h = a\prod \pi^{m_\pi}$ no qual*

$a \in k^*$, $\pi \in k[z]^*$ irredutível e $m_\pi \in \mathbb{Z}$. Definimos como valorização π-ádica sobre $k(z)|k$ a valorização

$$v_\pi(h) = m_\pi \text{ e } v_\infty(h) = -\sum m_\pi \deg \pi.$$

Se $k = \overline{k}$, então $h = a\prod(z-b)^{m_b}, b \in k$, e

$$\sum_v v(h) = 0.$$

Ou seja, o número de zeros contado com suas ordens é igual ao número de pólos contado com suas ordens.

Seguindo o mesmo argumento utilizado para determinar as valorizações de $k(z)|k$ teremos o seguinte teorema:

Teorema 1.2 *Temos que $S_{k(z)|k} = \{v_\pi \mid \pi \in k[z]^* \text{ irredutível}\} \cup \{v_\infty\}$.*

Observação 1.3 *Se k é algebricamente fechado, então teremos a bijeção*

$$\begin{cases} k \cup \{\infty\} & \longrightarrow & S_{k(z)|k} \\ c & \longmapsto & v_{z-c} \\ \infty & \longmapsto & v_\infty \end{cases}$$

Teorema 1.3 *As valorizações do corpo dos números racionais $\mathbb{Q}$ com o grupo de valores de $\mathbb{Z}$ correspondem bijetoramente aos números primos.*

Demonstração: Seja v uma valorização, então $v(m) \geq 0$ para todo $m \in \mathbb{Z}$. Já que $v \neq 0$, existe $n \in \mathbb{Z}$ tal que $v(n) > 0$ e como podemos escrever $n = \pm\prod p^{\alpha(p)}$, p primo, teremos $v(p) > 0$ para algum p. Considere q primo com $q \neq p$, logo existem $r, s \in \mathbb{Z}$ tais que $rp + sq = 1$. Então,

$$0 = v(1) \geq \min\{v(r) + v(p), v(s) + v(q)\},$$

logo $v(q) = 0$ e $v = v_p$. Se $r \in \mathbb{Q}^*$, então $r = \pm \prod_{\alpha(p)\in\mathbb{Z}} p^{\alpha(p)}$, portanto $v_p(r) = \alpha(p)$. □

Definição 1.5 *Uma extensão $K|k$, tal que k é algebricamente fechado, é um corpo de funções algébricas em uma váriavel com corpo de constantes k se, e somente se, existe $z \in K \setminus k$ transcendente sobre k tal que $[K : k(z)] < \infty$.*

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

Cada $x \in K \setminus k$ pode assumir o papel da variável, então procuramos propriedades de corpos de funções algébricas $K|k$ que não dependem da escolha de uma variável.

Definição 1.6 *Seja K um corpo. Uma valorização sobre K é uma aplicação não nula $v : K^* \to (\mathbb{R}, +)$ tal que:*

(i) $v(fg) = v(f) + v(g)$;

(ii) $v(f + g) \geq \min\{v(f), v(g)\}$, *se* $f + g \neq 0$;

(iii) Se $k \leq K$ é corpo, então a valorização v de K será chamada valorização de $K|k$ se $v\big|_{k^*} \equiv 0$.

A valorização v é chamada discreta se existe $r \geq 0$ tal que $v(K^*) \simeq r\mathbb{Z}$, e normalizada se $r = 1$.

Definição 1.7 *Superfície Abstrata de Riemman é o conjunto de todas as valorizações discretas e normalizadas de $K|k$, denotado por $S_{K|k}$.*

Lema 1.2 *Se $L|K$ é algébrica, então $S_{L|K} = \emptyset$, ou seja, para toda valorização v de L, teremos $v|_{K^*} \neq 0$.*

Demonstração: Suponha que exista v, tal que $v(K^*) = 0$, e tome $y \in L$ tal que $v(y) < 0$. Como y é algébrico sobre K, $y^n + c_{n-1}y^{n-1} + \cdots + c_0 = 0$, onde $c_0, \ldots, c_{n-1} \in K$. Observe que $v(y^n) < v(y^i)$ e $v(c_i y^i) = v(y^i)$ para todo $0 \leq i \leq n-1$, então $v(y^n) < v(c_i y^i)$ para todo $0 \leq i \leq n-1$, logo

$$\infty = v(y^n + c_{n-1}y^{n-1} + \cdots + c_0) = v(y^n) < 0.$$

Portanto teremos $v\big|_{K^*} \neq 0$ para todo v. □

Definição 1.8 *Sejam $L|K$ uma extensão algébrica e $v : L^* \to \mathbb{Z}$ uma valorização, logo $v(K^*) \leq (\mathbb{Z}, +)$, e portanto $v(K^*) \simeq e\mathbb{Z}$, para algum $e \in \mathbb{Z}^+$. O valor "e" descrito é chamado de índice de ramificação.*

Observação 1.4 *A valorização $\frac{1}{e} v\Big|_K$ é discreta e normalizada.*

Seja $K|k$ um corpo de funções algébricas, queremos descrever $S_{K|k}$. Seja $z \in K \setminus k$, então $K|k(z)$ é finita. Já conhecemos $S_{k(z)|k}$, agora basta prolongar cada $v \in S_{k(z)|k}$ a K. Se $v \in S_{K|k}$ e "e" é o índice de ramificação sobre $k(z)$, então $\frac{1}{e} v\Big|_{k(z)} \in S_{k(z)|k}$, portanto, teremos a aplicação

$$\begin{cases} S_{K|k} & \longrightarrow & S_{k(z)|k} \\ v & \longmapsto & \frac{1}{e} v\Big|_{k(z)} \end{cases}$$

Se $\overline{k} = k$, teremos a aplicação

$$\begin{cases} S_{K|k} & \longrightarrow & k \cup \{\infty\} \\ v & \longmapsto & z(v) \end{cases},$$

onde $z(v)$ é chamado de ordem de z em v e é definido como:

se $v(z) \geq 0$ então $z(v) = c$ tal que $c \in k$ é único que satisfaz $v(z - c) > 0$;

se $v(z) < 0$ então $z(v) = \infty$;

se $z \in k$, então $z(v) = z$ para todo $v \in S_{K|k}$.

Lema 1.3 *Sejam $v \in S_{K|k}$ uma valorização e $x, y \in k$, tais que $v(x) \geq 0, v(y) \geq 0$. Então, $(x + y)(v) = x(v) + y(v)$ e $(xy)(v) = x(v)y(v)$.*

Demonstração: Sejam $x(v) = a$ e $y(v) = b$, logo $v(x - a) > 0$ e $v(y - b) > 0$. Então,

$$v((x + y) - (a + b)) = v((x - a) + (y - b)) \geq \min\{v(x - a), v(x - b)\} > 0$$

$$v(xy - ab) = v((x - a)y + (y - b)a) \geq \min\{v(x - a) + v(y), v(y - b) + v(a)\} > 0.\square$$

Sejam $K|k$ um corpo de funções algébricas, $k = \overline{k}$ e portanto perfeito, logo existem $x, y \in K$ tais que $K = k(x, y)$. Considere $f \in k[x, y]$ irredutível tal que $f(x, y) = 0$.

Pelo Lema 1.3, para cada $v \in S_{K|k}$ com $v(x) \geq 0, v(y) \geq 0$, teremos $f(x(v), y(v)) = 0$. Portanto temos a seguinte aplicação

$$\begin{cases} \{v \in S_{K|k} \mid v(x) \geq 0,\ v(y) \geq 0\} & \longrightarrow & \{(a,b) \in k^2 \mid f(a,b) = 0\} \\ v & \longmapsto & (x(v), y(v)) \end{cases}$$

Definição 1.9 *Seja $v \in S_{K|k}$. Um elemento $t \in K$ é chamado de uniformizante local em v, ou parâmentro local em v, se $v(t) = 1$. Se v é discreta mas não necessariamente normalizada, definimos t como o menor elemento positivo no grupo de valores $v(K^*)$.*

Exemplo 1.1 Se $K = k(z)$, então $(z - c)$ é um uniformizante local em v_c para cada $c \in k$ e $\dfrac{1}{z}$ é uniformizante local em v_∞.

Proposição 1.1 *Sejam $v \in S_{K|k}$ e t uniformizante local em v. Desse modo, para cada $y \in K^*$, existe um única série formal de Laurent $\sum_{n \geq m} c_n t^n \in k((t))$, onde $m = v(y)$, $c_m \neq 0$ e para todo j,*

$$v\left(y - \sum_{n=m}^{j} c_n t^n\right) > j.$$

Demonstração: Seja $v(y) = m$, logo $v(t^{-m}y) = 0$. Afirmamos que existe $c_m \in k^*$ tal que $v(t^{-m}y - c_m) > 0$, de fato, $\overline{t^{-m}y} \in k_v$ e $\overline{c_m} \in k_v$, logo

$$t^{-m}y - c_m \in \mu_v \Rightarrow v(t^{-m}y - c_m) > 0$$

Então,

$$v(t^m) + v(t^{-m}y - c_m) > v(t^m) \Rightarrow v(y - c_m t^m) > m \Rightarrow v(y - c_m t^m) \geq m + 1.$$

Observamos que $c_m \in k^*$ único, pois se existisse $b \in k^*, b \neq c_m$ tal que $v(y - bt^m) > m$, então

$$0 = v(c_m - b) = v(t^{-m}) + v(t^m(c_m - b)) = -m + v((y - bt^m) + (c_m t^m - y)) \geq$$

$$-m + \min\left\{v(y - bt^m), v(c_m t^m - y)\right\} > -m + m = 0$$

o que também é um absurdo. Seguindo o mesmo raciocínio, existe um único $c_{m+1} \in k^*$ tal que

$$v(y - c_m t^m - c_{m+1} t^{m+1}) \geq m + 2,$$

e assim por diante. □

Pela Proposição anterior, temos uma aplicação injetora do corpo de funções $K \hookrightarrow k((t))$ que é compatível com a adição e a multiplicação, logo $K \subseteq k((t))$. Sejam $y \in K$, t um parâmetro local, $\sum c_n t^n$ a série de Laurent e defina

$$v(y) = \operatorname{ord}_t \left(\sum c_n t^n \right) := \min\{i \mid c_i \neq 0\}.$$

Observamos que esta definição não depende da escolha do parâmetro local. Seja $\pi \in K^*$ outro parâmetro local de v, então

$$\pi = \sum_{i=1}^{\infty} a_i t^i = a_i t + a_2 t^2 + \cdots$$

com $a_1 \neq 0$. Logo $k((t)) = k((\pi))$.

Definição 1.10 *Seja v a valorização definida acima e defina $|y|_v := 2^{-v(y)}$.*

Observamos que $|\cdot|_v$ satifaz as seguintes propriedades que são consequências das propriedades de v como valorização.

(1) $|y|_v \geq 0$ e $|y|_v = 0$ se, e somente se, $y = 0$;

(2) $|yz|_v = |y|_v |z|_v$;

(3) $|y + z|_v \leq \max\{|y|_v, |z|_v\}$.

Em particular vale a desigualdade triangular $|y + z|_v \leq |y|_v + |z|_v$.

De fato $k((t)) = \widehat{K}_v$, ou seja, $k((t))$ é o completamento de K com respeito a $|\cdot|_v$. Como $k(t) \subseteq K \subseteq k((t))$, basta provar que $k((t))$ é um completamento de $k(t)$. Para isso, temos que mostrar que toda sequência de Cauchy em $k(t)$ possui limite em $k((t))$.

Considere $a \in k((t))$, isto é

$$a = \sum_{i \geq -n}^{\infty} c_i t^i = \sum_{i \geq -n}^{-1} c_i t^i + \sum_{i \geq 0} c_i t^i = \frac{c_{-n} + c_{-n+1}t + \cdots + c_{-1}t^{n-1}}{t^n} + \sum_{i \geq 0} c_i t^i = b + \sum_{i \geq 0} c_i t^i,$$

com $b \in k(t)$. Seja $a_m = b + \sum_{i=0}^{m} c_i t^i \in k(t), m > 0$, então, dado $\varepsilon > 0$ temos:

$$|a_m - a|_v = \left| \sum_{i \geq m} c_i t^i \right|_v = 2^{-v\left(\sum_{i \geq m} c_i t_i\right)} = 2^{-m} < \varepsilon$$

quando $m \to \infty$, portanto $a_m \to a$.

Teorema 1.4 *(de Aproximação) Sejam K corpo, $v_1, \ldots, v_m$ valorizações distintas, discretas e normalizadas, $n_1, \ldots, n_m \in \mathbb{Z}$ e $h_1, \ldots, h_m \in K$. Então existe $z \in K$ tal que $v_i(z - h_i) > n_i$ para todo $i = 1, \ldots, m$, e para cada i existe $x \in K$ tal que $v_i(x - h_i) = n_i$.*

Demonstração: Suponha $m \geq 2$ e analisaremos por etapas:

Etapa 1: Existe $x \in K$ tal que $v_1(x) \geq 0$ e $v_2(x) < 0$.

De fato, caso contrário $v_1(x) \geq 0$ e $v_2(x) \geq 0$ ocorre para todo $x \in K$, como v_i são normalizadas, considere $t \in K$ tal que $v_1(t) = 1$ e $y \in K^*$ tal que $v_1(y) = n$. Então:

$$v_1\left(\frac{y}{t^n}\right) = v_1\left(\frac{t^n}{y}\right) = 0 \Rightarrow v_2\left(\frac{y}{t^n}\right) \geq 0 \text{ e } v_2\left(\frac{t^n}{y}\right) \geq 0.$$

Desse modo,

$$nv_2(t) \geq v_2(y) \geq nv_2(t) \Rightarrow v_2(y) = v_1(y)v_2(t) \text{ para todo } y \in K^*,$$

logo v_1 e v_2 são equivalentes, o que é um absurdo.

Etapa 2: Existe $z \in K$ tal que $v_1(z) > 0$ e $v_2(z) < 0$.

De fato, sabemos que existem $x \in K$ tal que $v_1(x) \geq 0$ e $v_2(x) < 0$, e $y \in K$ tal que $v_1(y) < 0$ e $v_2(y) \geq 0$. Considere $z = \dfrac{x}{y}$, logo

$$v_1(z) = v_1(x) - v_1(y) > 0 \text{ e } v_2(z) = v_2(x) - v_2(y) < 0.$$

Etapa 3: Existe $x \in K$ tal que $v_i(x) < 0$ para todo $i > 1$ e $v_1(x) > 0$.

De fato, para $m \geq 3$, existe $y \in K$ tal que $v_1(y) > 0$ e $v_i(y) < 0$ para $1 < i \leq m-1$, e existe $z \in K$ tal que $v_1(z) > 0$ e $v_m(z) < 0$. Considere $x = y + z^r$, no qual $r \in \mathbb{Z}$ e $r \gg 0$ para todo $2 \leq i \leq m$. Então,

$$v_1(x) \geq \min\{v_1(y), rv_1(z)\} > 0 \quad \text{e} \quad v_i(x) = \min\{v_i(y), rv_i(z)\} < 0.$$

Etapa 4: Para todo $n \in \mathbb{Z}^+$, existe $y \in K$ tal que $v_1(y-1) \geq n$ e $v_i(y) \geq n$ para $i > 1$.

De fato, escolha $y = \dfrac{1}{1+x^n}$ onde x é elemento da etapa 3, assim:

$$v_1(y-1) = v_1\left(\frac{1}{1+x^n} - 1\right) = v_1(-x^n) - v_1(1+x^n) \geq nv_1(x) - \min\{0, nv_1(x)\} \geq n;$$

$$v_i(y) = v_i\left(\frac{1}{1+x^n}\right) = -v_i(1+x^n) \geq -\min\{0, nv_i(x)\} \geq n.$$

Etapa 5: Existe $z \in K$ tal que $v_i(z - h_i) > n_i$ para todo i.

De fato, seja $n \in \mathbb{Z}^+, n \gg 0$. Pela etapa 4, para todo i existe y_i tal que $v_i(y_i - 1) \geq n$ e $v_j(y_i) \geq n$ para $j \neq i$. Tomamos $z = \displaystyle\sum_{i=1}^{m} h_i y_i$, logo

$$z - h_i = h_1 y_1 + \cdots + h_i(y_i - 1) + \cdots + h_m y_m.$$

Então,

$$v_i(z - h_i) \geq \min\{v_i(h_1), \ldots, v_i(h_m)\} + n > n_i,$$

pois n é suficientemente grande.

Etapa Final: Seja $f_i \in K$ tal que $v_i(f_i) = n_i$ para $1 \leq i \leq m$.

De fato, pela etapa 5, existem $y, k \in K$ tais que $v_i(y - f_i) > n_i$ e $v_i(z - f_i) > n_i$ para todo i. Considere $x = y + z$ logo,

$$v(x - h_i) = v((y - f_i) + (z - h_i) + f_i) = \min\{v(y - f_i), v(z - h_i), v(f_i)\} = n_i.$$

□

1.2 Anel de Valorização e Corpo Residual

Definição 1.11 *Sejam K um corpo e v uma valorização. Definimos,*

(i) $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ *chamado de anel das valorizações de v;*

(ii) $\mathcal{U}_v := \{x \in K \mid v(x) = 0\}$ *chamado de grupo das unidades de v;*

(iii) $\mu_v := \{x \in K \mid v(x) > 0\}$.

Proposição 1.2 *O anel das valorizações é um anel local e μ_v é seu único ideal maximal.*

Demonstração: Sejam $x, y \in \mu_v$ e $z \in \mathcal{O}_v$, logo

$$v(x+y) \geq \min\{v(x), v(y)\} > 0 \text{ e } v(xz) = v(x) + v(z) > 0,$$

portanto μ_v é ideal sobre $\mathcal{O}_v$. Agora, seja I ideal de $\mathcal{O}_v$ tal que $\mu_v \subset I \subset \mathcal{O}_v$ e $\mu_v \neq I$. Para todo $x \in I$, tal que x não pertença a μ_v, então $v(x) = 0$. Portanto $1 = xx^{-1} \in I$ e $I = \mathcal{O}_v$. □

Sejam v uma valorização normalizada e discreta e $t \in K$ tal que $v(t) = 1$. Cada $x \in \mathcal{O}_v \setminus \{0\}$ com $v(x) = n$ escreve-se unicamente da forma $x = ut^n$ no qual $u \in \mathcal{U}_v$ e $n \in \mathbb{Z}_+$. Assim, $\mathcal{O}_v$ é domínio fatorial que a menos de associados possui um único elemento irredutível, a saber, o uniformizante local t.

Proposição 1.3 *Os ideais de $\mathcal{O}_v$ não nulos são da forma*

$$\mathcal{O}_v t^n = \{xt^n \mid x \in \mathcal{O}_v\} = \{x \in K \mid v(x) \geq n\},$$

para $n \geq 0$.

Demonstração: Sejam I ideal de $\mathcal{O}_v$, $n = \min\{v(x) \mid x \in I\}$, e $y \in I$ tal que $v(y) = n$. Sabemos que $y \in \mathcal{O}_v \setminus \{0\}$ pode ser escrito da forma $y = ut^n$, onde t uniformizante local e $u \in \mathcal{O}_v$. Portanto $I = \langle t^n \rangle$. □

Definição 1.12 *O quociente $k_v := \dfrac{\mathcal{O}_v}{\mu_v}$ é chamado de Corpo Residual de $\mathcal{O}_v$.*

Sejam $L|K$ uma extensão finita, w valorização de L e $v = w|_K$. Temos que $\mathcal{O}_v \subseteq \mathcal{O}_w$ e $\mu_v = \mu_w \cap \mathcal{O}_v$, logo $k_v \hookrightarrow k_w$.

Definição 1.13 *Definimos* $f_{w|v} := [k_w : k_v]$ *como índice de inércia de* $w|v$ *e* $e_{w|v} := [w(L^*) : v(K^*)]$ *como índice de ramicação de* $w|v$.

Lema 1.4 *Seja* $[L : K] < \infty$, *então* $e_{w|v} \leq [L : K]$ *e* $f_{w|v} \leq [L : K]$.

Demonstração: Sejam $y_n \in L^*$, tais que as classes $w(y_n) + v(K^*)$ são distintas. Afirmamos que y_n são linearmente independentes sobre K^*, de fato, sejam $a_n \in K$ não todos nulos. Observamos

$$w\left(\sum a_n y_n\right) = \min\left\{w(a_n) + w(y_n)\right\} < \infty$$

pois as classes são distintas, logo $\sum a_n y_n \neq 0$. Portanto $\{y_n\}$ é linearmente independente sobre K e consequentemente $\sharp\{y_n\} \leq [L : K]$.

Sejam $h_j \in \mathcal{O}_w$, tais que $\overline{h_j} = h_j + \mu_w \in k_w$ e $\overline{h_j}$ são linearmente independentes sobre k_v. Considere $a_j \in K$ tais que $\sum a_j h_j = 0$ e suponha que exista j tal que $a_j \neq 0$, podemos supor $j = 1$. Logo,

$$-\sum_{j>2} a_j h_j = a_1 h_1 \Rightarrow h_1 = -\sum_{j>2} a_j a_1^{-1} h_j.$$

Então,

$$\overline{h_1} = h_1 + \mu_v = -\sum_{j>2} a_j a_1^{-1} h_j + \mu_v = -\sum_{j>2} a_j a_1^{-1}(h_j + \mu_v) = -\sum a_j a_1^{-1}\overline{h_j},$$

o que é absurdo pois $\left\{\overline{h_j}\right\}$ é linearmente independente. Portanto, $a_j = 0$ para todo j, assim $\{h_j\}$ é linearmente independente sobre K e consequentemente $\sharp\{h_j\} \leq [L : K]$. □

Observação 1.5 *Considerando os elementos* $h_j y_n$ *escolhidos na demonstração do lema anterior, vemos que* $e_{w|v} f_{w|v} \leq [L : K]$. *De fato,* $\{h_j y_n\}$ *é linearmente independente sobre* K. *Sejam* $a_{ij} \in K$ *não todos nulos, assim*

$$w\left(\sum_i \sum_j a_{ij} h_j y_i\right) \geq \min\{w(a_{ij} h_j y_i)\} = \min\{v(a_{ij}) + w(y_i)\} < \infty$$

logo ocorre a igualdade pois $v(a_{ij}) + w(y_n)$ são distintos.

Teorema 1.5 *(Desigualdade Fundamental) Sejam $[L : K] < \infty$, v valorização discreta de $K, w_1, \ldots, w_m$ valorizações de L que prolongam $v, e_1, \ldots, e_m$ os índices de ramificação e $f_1, \ldots, f_m$ os índices de inércia. Então $\sum_{i=1}^{m} f_i e_i \leq [L : K]$. Em particular o número de prolongamentos de v a L é finito.*

Demonstração: Podemos supor que v é normalizada, então $v(K^*) \simeq \mathbb{Z}$ e $w_i(L^*) \simeq \frac{1}{e_i}\mathbb{Z}$. Pelo teorema de aproximação, existem $t_i \in L, i = 1, \ldots, m$, tais que $w_i(t_i) = \frac{1}{e_i}$ e $w_q(t_i) = 0$ para $q \neq i$. Para cada i escolhemos elementos $h_{ij} \in \mathcal{O}_{w_i},\ 1 \leq j \leq f_i$, cujas classes residuais em k_{w_i} são linearmente independentes sobre k_v. Escolhendo elementos $g_{ij} \in \mathcal{O}_{w_i},\ 1 \leq j \leq f_i$, cujas classes são linearmente independentes sobre k_v, teremos $w_i(h_{ij} - g_{ij}) > 0$, logo $w_q(h_{ij}) > 0$ para $q \neq i$, e portanto $w_q(h_{ij}) \geq 1$. Afirmamos que se $a_{ijn} \in K,\ 1 \leq j \leq f_i,\ 0 \leq n \leq e_{i-1}$, então

$$\min_q \left\{ w_q \left(\sum_{i,j,n} a_{ijn} h_{ij} t_i^n \right) \right\} = \min_{i,j,n} \left\{ v(a_{ijn}) + \frac{n}{e_i} \right\},$$

o que será demonstrada no Lema 1.5. Então se $a_{ijn} \neq 0$ para algum i, j, n,

$$\min \left\{ v(a_{ijn}) + \frac{n}{e_i} \right\} < \infty \Rightarrow \min_q \left\{ w_q \left(\sum_{i,j,n} a_{ijn} h_{ij} t_i^n \right) \right\} < \infty \Rightarrow \sum a_{ijn} h_{ij} t_i^n \neq 0,$$

ou seja, $h_{ij} t_i^n$ são linearmente independentes sobre K. Então $\sharp\{h_{ij} t_i^n\} \leq [L : K]$. Obsevamos que $\sharp\{h_{ij} t_i^n\} = \sum_i f_i e_i$, portanto $\sum_i f_i e_i \leq [L : K]$. □

Lema 1.5 *Sejam $a_{ijn} \in K,\ 1 \leq i \leq m,\ 1 \leq j \leq f_i, 0 \leq n \leq e_i - 1$, então*

$$\min_q \left\{ w_q \left(\sum a_{ijn} h_{ij} t_i^n \right) \right\} = \min_{i,j,n} \left\{ v(a_{ijn}) + \frac{n}{e_i} \right\}.$$

Demonstração: Temos:

$$w_i(a_{ijn} h_{ij} t_i^n) = w_i(a_{ijn}) + w_i(h_{ij}) + w_i(t_i^n) = v(a_{ijn}) + \frac{n}{e_i},$$

$$w_q(a_{ijn}h_{ij}t_i^n) = w_q(a_{ijn}) + w_q(h_{ij}) + w_q(t_i^n) \geq v(a_{ijn}) + 1 > v(a_{ijn}) + \frac{n}{e_i}.$$

Logo, para todo q

$$w_q\left(\sum_{i,j,n} a_{ijn}h_{ij}t_i^n\right) \geq \min_{i,j,k}\left\{w_q\big(a_{ijn}h_{ij}t_i^n\big)\right\} \geq \min_{i,j,k}\left\{v(a_{ijn}) + \frac{n}{e_i}\right\}.$$

Considere $v(a_{IJN}) + \dfrac{N}{e_I}$ este mínimo, assim basta provar que $w_I\left(\sum a_{ijn}h_{ij}t_i^n\right) = v(a_{IJN}) + \dfrac{N}{e_I}$. Para cada $i \neq I$ temos

$$w_I(a_{ijn}h_{ij}t_i^n) > v(a_{ijn}) + \frac{n}{e_i} \geq v(a_{IJN}) + \frac{N}{e_I},$$

logo basta provar que $w_I\left(\sum_{j,n} a_{Ijn}h_{Ij}t_I^n\right) = v(a_{IJN}) + \dfrac{N}{e_I}$. Para cada $n \neq N$ temos:

$$w_I(a_{Ijn}h_{Ij}t_I^n) = v(a_{Ijn}) + \frac{n}{e_I} \neq v(a_{IjN}) + \frac{N}{e_I},$$

pois

$$v(a_{Ijn}) + \frac{n}{e_I} = v(a_{IjN}) + \frac{N}{e_I} \Rightarrow v(a_{Ijn}) - v(a_{IjN}) = \frac{N-n}{e_I} \in \frac{1}{e_I}\mathbb{Z}$$

e assim,

$$v(a_{Ijn}) - v(a_{IjN}) \equiv N - n\left(\mathrm{mod}\frac{1}{e_I}\mathbb{Z}\right) \Rightarrow v(a_{Ijn}) = v(a_{IjN}) + \frac{N-n}{e_I}.$$

Como $n \neq N$ essa igualdade não ocorre. Desse modo, basta provar que

$$w_I\left(\sum_j a_{IjN}h_{Ij}t_I^N\right) = v(a_{IJN}) + \frac{N}{e_I},$$

ou seja, $w_I\left(\sum_j a_{IjN}h_{Ij}\right) = v(a_{IJN})$, já que $w_I(h_{Ij}) = 0$ e $t_I^N, \dfrac{N}{e_I}$ estão fixos. Ou basta provar que $w_I\left(\sum_j a_j h_{Ij}\right) = 0$ onde $a_j = \dfrac{a_{IjN}}{a_{IJN}}$, o que realmente ocorre, pois

pela minimalidade obtemos $v(a_{IjN}) \geq v(a_{IJN})$, logo $v(a_{IjN}) - v(a_{IJN}) \geq 0$ e portanto $v(a_j) \geq 0$, isto é, $a_j \in \mathcal{O}_v$. Sabemos que $a_J = 1$ e $\overline{h_{Ij}}$ são linearmente independentes sobre K_v logo $\sum_j \overline{a_j h_{Ij}} \neq 0$, portanto, $w_I\left(\sum_j a_j h_{Ij}\right) < \infty$ e como $\overline{a_j h_{Ij}} \in k_{w_I}$ então $w_I(a_j h_{Ij}) = 0$. Como todos os $v(a_j)$ são distintos, teremos $w_I\left(\sum_j a_j h_{Ij}\right) = 0$. □

1.3 Extensões totalmente ramificadas

Definição 1.14 *Sejam $L|K$ uma extensão, $v \in S_{K|k}$, w um prolongamento de v a L. Dizemos que $L|K$ é totalmente ramificada se $[L : K] = e_{w|v}$.*

Proposição 1.4 *Sejam $L|K$ uma extensão totalmente ramificada de grau n, $v \in S_{K|k}$ normalizada, w um prolongamento de v a L e $y \in L$ uniformizante local. Então $L = K(y)$ e o polinômio minimal de y sobre K é da forma $Y^n + a_{n-1}Y^{n-1} + \cdots + a_1 Y + a_0$ no qual $v(a_0) = 1$ e $v(a_i) \geq 1$ para todo $i \geq 1$. (Polinômio de Eisenstein)*

Demonstração: Como $w(y) = \frac{1}{n}$, $e_{w_{|_{K(y)}}|v} \geq n$. Pela desigualdade fundamental $[K(y) : K] \geq n$, logo, $L = K(y)$. Seja $\min_K(y) = Y^n + a_{n-1}Y^{n-1} + \cdots + a_1 Y + a_0$, então

$$w(0) = w(y^n + \cdots + a_1 y + a_0) > \min\left\{1, v(a_{n-1}) + \frac{n-1}{n}, \ldots, v(a_1) + \frac{1}{n}, v(a_0)\right\}.$$

Observe que $v(a_i) + \frac{i}{n} \neq v(a_j) + \frac{j}{n}$, para todo $1 \leq i < j \leq n-1$. Caso contrário

$$v(a_i) + \frac{i}{n} = v(a_j) + \frac{j}{n} \Rightarrow v\left(\frac{a_i}{a_j}\right) = \frac{j-i}{n}$$

o que não ocorre pois $j - i < n$. Portanto, $v(a_0) = w(y^n) = 1$ e $v(a_i) \geq 1$ para todo $i \neq 1$. □

Mostraremos agora que cada polinômio de Eisenstein define uma extensão totalmente ramificada.

Proposição 1.5 *Sejam K um corpo, $v \in S_{K|k}$, $L = K(y)$ e $h = Y^n + a_{n-1}Y^{n-1} + \cdots + a_1 Y + a_0 \in K[Y]$ tal que $h(y) = 0$. Suponhamos $v(a_0) = 1$ e $v(a_i) \geq 1$ para todo $i \geq 1$.*

Afirmamos que h é irredutível, isto é, $[L:K]=n$ e v possui apenas um prolongamento a L, dado por $w\left(\sum_{i=0}^{n-1} z_i y^i\right) = \min_i \left\{ v(z_i) + \frac{1}{n} \right\}$, *$z_i \in K$, além disso, $e_{w|v}=n$, $f_{w|v}=1$ e y é uniformizante local em w.*

Demonstração: Sabemos que existe uma valorização w de L que prolonga v. Como $y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$, concluímos que o mínimo das parcelas é assumido pelo menos duas vezes, logo:

$$w(y^n) = v(a_0) = 1 \Rightarrow nw(y) = 1 \Rightarrow w(y) = \frac{1}{n}.$$

Assim, y é uniformizante local em w e portanto $e_{w|v} \geq n$. Já que $[L:K]=n$ temos pela desigualdade fundamental $n = e$ e $f = 1$. Então,

$$w\left(\sum_{i=0}^{n-1} z_i y^i\right) = \min_{0\leq i\leq n-1} \left\{ v(z_i) + \frac{i}{n} \right\}$$

já que nesse caso o mínimo é assumido apenas uma vez. □

Exemplo 1.2 Seja $k = \overline{k}$ e char$k = 0$. Considerando $K = k(x,y)$ no qual $x \notin k$ e $y^m = (x-c_1)\cdots(x-c_n)$ com $c_i \in k$ distintos e mdc(m, n) = 1. Sabemos que $[K : k(x)] = m$. Considere a aplicação:

$$\begin{cases} S_{K|k} & \longrightarrow & S_{k(x)|k} \\ w & \longmapsto & \frac{1}{e_w} w\Big|_{k(x)} := v \end{cases}.$$

Então:

$$v \in S_{k(x)|k} = \{v_a \mid a \in k^*\} \cup \{v_\infty\}.$$

Portanto teremos três casos:

(1) $v = v_{c_j}$ para algum $1 \leq j \leq m$, então $v(x-c_j) = 1$, $v(x-a) = 0$ para todo $a \neq c_j$ e

$$v(y) = \frac{1}{m} v(y^m) = \frac{1}{m} \sum_{i=1}^{n} v(x-c_i) = \frac{1}{m} v(x-c_j) = \frac{1}{m} \Rightarrow v(y) = \frac{1}{m},$$

logo, y é uniformizante local. Seja $z \in K$, digamos $z := \sum_{i=0}^{m-1} z_i y^i$, $z_i \in k(x)$, logo,

$$v(z) = v\left(\sum_{i=0}^{m-1} z_i y^i\right) = \min_{0\leq i\leq m-1}\left\{v(z_i) + \frac{i}{m}\right\}.$$

Assim, pela Proposição 1.5, v é o único prolongamento de v_{c_j}, $v(K^*) = \frac{1}{m}\mathbb{Z}$ e $e_{w|v} = m$. Portanto, $w(z) = mv(z) = \min_{0\leq i\leq m-1}\{mv(z_i) + i\}$ e y é uniformizante local em w.

(2) $v = v_\infty$, então $v(x) = -1$ e

$$v(y) = \frac{1}{m}v(y^m) = \frac{1}{m}\sum_{i=1}^{n} v(x - c_i) = \frac{-n}{m}.$$

Analogamente, consideremos $z := \sum_{i=0}^{m-1} z_i y^i \in K$ com $z_i \in k^*$, logo

$$v(z) = \min_{0\leq i\leq m-1}\left\{v(z_i) - i\frac{n}{m}\right\}$$

pois mdc(n, m) = 1. Logo, pela Proposição 1.3 v é o único prolongamento de v_∞, com:

$$w(z) = mv(z) = \min_{0\leq i\leq m-1}\{mv(z_i) - in\} \text{ e } e_{w|v} = m.$$

(3) $v|_{k(x)} = v_a$, $a \in k \setminus \{c_1, \ldots, c_n\}$, então $v(x - a) = 1, v(x - c) = 0$ para todo $c \neq a$ e

$$v(y) = \frac{1}{m}v(y^m) = 0 \text{ e } x(v) = a.$$

Seja $y(v) = b \in k^*$, então:

$$y^m = \prod_{i=1}^{n}(x - c_i) \Rightarrow b^m = \prod_{i=1}^{n}(a - c_i),$$

que ocorre do Lema 1.3. Logo, $x(v) = a$ determina b a menos de uma raiz m-ésima da unidade. Sejam $\varepsilon \in k$, tal que $\varepsilon^m = 1$ e $\sigma \in Aut_{k(x)}(K)$ $\big($conjunto dos automorfismos de K que fixa os elementos de $k(x)$ definido por:

$$\sum_{i=0}^{m-1} z_i y^i \longmapsto \sum_{i=0}^{m-1} z_i (\varepsilon y)^i.$$

Desse modo, $\widetilde{v} := v \circ \sigma$ é também uma valorização de K que prolonga v_a, logo $y(\widetilde{v}) = \varepsilon b$, pois

$$\widetilde{v}(y - \varepsilon b) = v(\sigma(y - \varepsilon b)) = v(\sigma(y) - \varepsilon b) = v(\varepsilon y - \varepsilon b) = v(\varepsilon) + v(y - b) = 0 + v(y - b) > 0.$$

Assim, temos m prolongamentos distintos entre si que pela Desigualdade Fundamental não são ramificadas. Para w temos $y^m = (x - c_1) \cdots (x - c_n)$ como polinômio em $(x - a)$, digamos $y^m = b^m\big(1 + a_1(x - a) + \cdots + a_n(x - a)^n\big)$, $a_i \in k$, logo

$$\frac{y}{b} = 1 + \sum_{i=1}^{\infty} \binom{\frac{1}{m}}{i} \big(a_1(x - a) + \cdots + a_n(x - a)^n\big)^i.$$

Assim, $K = k(x, y) \subseteq k((x - a))$. A valorização canônica $\mathrm{ord_{x-a}}$ de $k((x - a))$ prolonga a valorização v_a de $k(x)$ e logo sua restrição a K é v, pois $y(w) = b$. Em resumo, temos a bijeção:

$$\left\{ \begin{array}{ccc} S_{K|k} & \longrightarrow & \left\{ (a, b) \in k^2 \;\middle|\; b^m = \prod_{i=1}^{n} (a - c_i) \right\} \cup \left\{ (\infty, \infty) \right\} \\ w & \longmapsto & (x(w), (y(w))) \end{array} \right.$$

1.4 Extensões Totalmente Inerciais

Definição 1.15 *Sejam uma extensão $L|K$, $v \in S_{K|k}$, e w um prolongamento de v a L. Dizemos que $L|K$ é totalmente inercial se $[L : K] = f_{w|v}$.*

Sejam K um corpo, $v \in S_{K|k}$ uma valorização e $L = K(y)$ com $h(y) = 0$ e $h = Y^n + a_{n-1}Y^{n-1} + \cdots + a_0 \in \mathcal{O}_v[Y]$. Suponhamos que o polinômio reduzido $\overline{h} = Y^n +$

$\overline{a_{n-1}}Y^{n-1} + \cdots + \overline{a_0} \in k_v[Y]$ seja irredutível. Então, h é irredutível em $\mathcal{O}_v[Y]$, logo irredutível em $K[Y]$. Afirmamos que a valorização v possui um único prolongamento a L, a saber, a valorização:

$$w\left(\sum_{i=0}^{n-1} z_i y^i\right) = \min_i\{v(z_i)\}$$

para todo $z_i \in K$. De fato, seja w um prolongamento de v a L. Temos $y \in \mathcal{O}_w$, ou seja, $w(y) \geq 0$, pois caso contrário, se $w(y) < 0$ teríamos $w(y^n) < w(a_i y^i)$, logo:

$$w\big(h(y)\big) = w\left(\sum_{i=0}^{n} a_i y^i\right) = \min\{w(a_i y^i)\} = w(y^n) < \infty.$$

Então, $h(y) \neq 0$ o que é um absurdo. Como $\overline{h}$ é irredutível, as classes $\overline{y^0}, \ldots, \overline{y^{n-1}}$ são linearmente independentes sobre k_v. Aplicando o Lema 1.5, temos $w\left(\sum_{i=0}^{n-1} z_i y^i\right) = \min_i\{v(z_i)\}$ para todo $i \in K$, o que prova a afirmação.

Pela afirmação anterior, temos $e_{w|v} = 1$, logo $f_{w|v} \geq 1$ pois $k_v(\overline{y}) \subseteq k_w$ e $[k_v(\overline{y}) : k_v] = n$, então, pela Desigualdade Fundamental $f_{w|v} = n,\ k_w = k_v(\overline{y}.)$ Seja $[L : K] = n$, $v \in S_K$ e w que prolonga v a L. Suponha $f_{w|v} = n$, então $e_{w|v} = 1$ e w e o único prolongamento de v a L.

Suponhamos que $k_w|k_v$ é simples, isto é, existe $\overline{y}$ com $y \in \mathcal{O}_w$ tal que $k_w = k_v(\overline{y})$. Pela desigualdade fundamental,

$$[K(y) : K] \geq [k_v(\overline{y}) : k_v] = [k_w : k_v] = n,$$

logo $[K(y) : K] = n$ e $L = K(y)$. Assim teremos um polinômio irredutível de grau $n,\ h = a_n Y^n + \cdots + a_0 \in K[Y]$, tal que $h(y) = 0$. Multiplicando h por uma potência de uma uniformidade local em v, podemos supor $\overline{h}$ irredutível sobre $k_v[Y]$. De fato, seja $m = \min_{1 \leq i \leq n} v(a_i)$ e $t \in K$ com $v(t) = 1$, assim:

$$v(t^{-m+1}a_i) \geq v(t^{-m+1}) + m = 1 \Rightarrow v(t^{-m+1}a_i) \in \mathcal{O}_v[Y]$$

e portanto teremos $t^{-m+1}\overline{h} \in k_v[Y]$ é irredutível.

Sejam $K|k$ corpo de funções algébricas em uma variável e $v \in S_{K|k}$. A inclusão $k \subseteq \mathcal{O}_v$ implica que $k \hookrightarrow k_v$.

Definição 1.16 *O grau de v é definido como* $\deg v = [k_v : k]$.

Exemplo 1.3 Sejam $K = k(x)$ e bijeção $S_{k(x)|k} \longleftrightarrow \{v_\pi \mid \pi \in k[x]^* \text{ irredutível}\} \cup \{v_\infty\}$. Considere $\varphi : k[x] \longrightarrow k_{v_\pi}$, tal que $\varphi(f(x)) = f(x) + \mu_{v_\pi}$. Teremos $\varphi(f(x)) = 0$ se, e somente se, $\pi | f(x)$, logo

$$\frac{k[x]}{\langle \pi \rangle} \simeq k_{v_\pi}.$$

Então $\deg v_\pi = \deg \pi$ e $\deg v_\infty = 1$.

Lema 1.6 *Seja v uma valorização de $K|k$, então,* $\deg v < \infty$.

Demonstração: Seja $x \in K$ tal que $v(x) = -1$, logo $v|_{k(x)} = v_\infty$. Como $\deg v_\infty = 1$, pela Desigualdade Fundamental, $\deg v = [k_v : k] = [k_v : k_{v_\infty}] \leq [K : k(x)] < \infty$. □

Se $k = \overline{k}$, então, $k_v = k$. Isto é, para cada $y \in \mathcal{O}_v$ existe uma única constante c, tal que $v(y - c) > 0$, logo $y(v) = c$. Também neste caso, $\deg v = 1$ para todo v.

Se $k \neq \overline{k}$, ainda podemos falar do valor $y(v)$ de uma função $y \in K$ em v, se admitirmos valorizações em $k_v \cup \{\infty\}$ tais que $y(v) := \overline{y}$. Claramente, se $\deg v = 1$, então, $k = k_v$ e, portanto, $y(v) \in k \cup \{\infty\}$.

Definição 1.17 *Uma valorização $v \in S_{K|k}$ é chamada de um ponto racional de $S_{K|k}$ se* $\deg v = 1$. *O conjunto de todos os pontos racionais de $S_{K|k}$ é denotado por $S^{rac}_{K|k}$.*

1.5 Prolongamentos de Valorizações

Seja $K|k$ corpo de funções em uma variável x. Como comentamos anteriormente, para determinar valorizações de $K|k$ precisamos apenas prolongar as valorizações de $k(x)|k$. Prolongaremos primeiro a valorização do corpo $k((x))$.

Sejam K corpo, v uma valorização discreta e normalizada de k, $|x|_v := 2^{-v(x)}$,

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x|_v \leq 1\}$$

$$\mu_v = \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x|_v < 1\}.$$

Fixamos um sistema de representante R de k_v, isto é, um subconjunto R de $\mathcal{O}_v$, tal que a aplicação

$$\begin{cases} R & \longrightarrow & k_v \\ r & \longmapsto & r + \mu_v \end{cases}$$

é uma bijeção e, suponha que $0 \in R$. Fixamos também um representante π_i do grau da valorização $v(K^*)$, isto é, $\pi_i \in K^*$, tal que $v(\pi_i) = i$. Seja $x \in K^*$ tal que $v(x) = m$. Existe um único $r_m \in R$ tal que $v(x - r_m\pi_m) \geq m + 1$, de fato,

$$v(x\pi_m^{-1}) = v(x) + v(\pi_m^{-1}) = m - m = 0 \Rightarrow x\pi_m^{-1} \in \mathcal{O}_v \Rightarrow \overline{x\pi_m^{-1}} \in k_v,$$

e considerando a bijeção dada, existe r_m tal que $\overline{r_m} = \overline{x\pi_m^{-1}}$, logo $x\pi_m^{-1} - r_m \in \mu_v$. Desse modo,

$$v(x\pi_m^{-1} - r_m) > 0 \Rightarrow v(x\pi_m^{-1} - r_m) \geq 1 \Rightarrow v(\pi_m) + v(x\pi_m^{-1} - r_m) \geq 1 + v(\pi_m) \Rightarrow$$

$$\Rightarrow v(x\pi_m^{-1}\pi_m - r_m\pi_m) \geq 1 + m \Rightarrow v(x - r_m\pi_m) \geq 1 + m.$$

Seguindo o mesmo argumento, existe $r_{m+1} \in R$ tal que $v(x - r_m\pi_m - r_{m+1}\pi_{m+1}) \geq m + 2$, e assim por diante.

Assim, x define uma série formal $\sum_{i \geq m} r_i\pi_i$ tal que $v\left(x - \sum_{i=m}^{n} r_i\pi_i\right) \geq n + 1$ para todo $n \geq m$, isto é,

$$\left| x - \sum_{i=m}^{n} r_i\pi_i \right|_v < \frac{1}{2^n}.$$

Ou seja, a série converge para x com respeito a $|\cdot|_v$.

Reciprocamente, para cada série formal $\sum_{i \gg -\infty} r_i\pi_i$ no qual $r_i \in R$ e $r_i = 0$ para quase todo $i < 0$, defina uma sequência de Cauchy a respeito de $|\cdot|_v$, e, logo, a sequência converge em $\widehat{K}_v$.

Afirmamos que as aplicações $v : K^* \longrightarrow \mathbb{Z}$ e a aplicação natural $\pi : \mathcal{O}_v \longrightarrow k_v$ são contínuas, onde $\mathbb{Z}$ e k_v são equipados com a topologia discreta. Considere $a \in \mathbb{Z}$.

Mostremos que $v^{-1}(a) = \{x \in K^* \mid v(x) = a\} = \{x \in K^* \mid |x|_v = 2^{-a}\}$ é fechado. Para todo $\varepsilon > 0$, sejam

$$B(a, \varepsilon) = \{x \in K \mid |x - a|_v < \varepsilon\};$$

$$X = \{x \in K \mid |x - a|_v \geq \varepsilon\};$$

$$\overline{B(a, \varepsilon)} = \{x \in K \mid |x - a|_v \leq \varepsilon\}.$$

Observe que X e $\overline{B(a, \varepsilon)}$ são fechados, logo

$$\overline{B(a, \varepsilon)} \cap X = \{x \in K \mid |x - a| = \varepsilon\}$$

é fechado, portanto $v^{-1}(a)$ é fechado.

Analogamente, considere

$$\pi^{-1}(c + \mu_v) = \{x \in \mathcal{O}_v \mid x - c \in \mu_v\} = \{x \mid v(x - c) = 0\} = \{x \mid |x - c|_v = 1\}$$

que também é fechado. Então, v é prolongado a uma valorização $\hat{v}$ de $\widehat{K}_v$ com o mesmo corpo de valores $\mathbb{Z}$ e o mesmo corpo residual k_v. Portanto, temos uma bijeção entre $\widehat{K}_v$ e as séries formais $\sum_i r_i \pi_i,\ r_i \in R$.

Exemplo 1.4 Considere $K = k(t)$ e sua valorização $t-$ádica v, ou de maneira mais geral, seja $K|k$ um corpo de funções algébricas em uma variável, $v \in S^{rac}_{K|k}$ e $v(t) = 1$. Se $R := k, \pi_i = t^i$, então $\widehat{K}_v = k((t))$.

Teorema 1.6 *Sejam $[L : K] = n < \infty$ e v valorização de K tal que (K, v) é completo. Então,*

(i) existe uma única valorização w de L que prolonga v;

(ii) vale a igualdade fundamental $ef = n$;

(iii) (L, w) é completo

Demonstração: (Unicidade) Podemos supor $v(K^*) \simeq \mathbb{Z}$. Seja w um prolongamento de v a L, logo $w(L^*) = \frac{1}{e}\mathbb{Z}$. Considere $t \in K$ tal que $v(t) = 1$, $\pi \in L$ tal que $w(\pi) = \frac{1}{e}$ e $R \subset \mathcal{O}_v$ um sistema de representantes de k_v tal que $0 \in R$. Sejam $h_1, \ldots, h_f \in \mathcal{O}_w$ cujas classes em k_w formam uma base de k_w sobre k_v, então as somas $\sum_{n=1}^{f} r_n h_n,\ r_i \in R$ formam um sistema de representantes de k_w, pois para todo $\overline{\alpha} \in k_w$ existe $\overline{\alpha_i}$, tal que $\overline{\alpha} = \sum_{i=1}^{f} \overline{\alpha_i}\overline{h_i}$ e para todo $\overline{\alpha_i}$ existe $r_i \in R$. Logo, associamos $\overline{\alpha_i}$ a r_i. Os produtos $\pi^i t^j$ onde $0 \leq i \leq e-1$ e $j \in \mathbb{Z}$ formam um sistema de representação de $w(L^*) = \frac{1}{e}\mathbb{Z}$, pois considerando a aplicação:

$$\begin{cases} R' = \{\pi^i t^j \ ;\ 0 \leq i \leq e-1 \text{ e } j \in \mathbb{Z}\} & \longrightarrow & \frac{1}{e}\mathbb{Z} \\ \pi^i t^j & \longmapsto & \frac{i}{e} + j \end{cases}$$

sabemos que ela é sobrejetora e injetora, já que para todo $\alpha \in \frac{1}{e}\mathbb{Z}$ teremos $\alpha = \frac{m}{e} = w(\pi^m t^0)$ e para todo

$$\frac{i}{e} + j = \frac{i'}{e} + j' \Rightarrow \frac{i - i'}{e} = j' - j$$

o que não ocorre, pois $0 \leq i \leq e-1$. Utilizando um argumento parecido como o da demonstração da Proposição 1.1, para todo $l \in L$, existe uma série formal

$$\sum_{i=0}^{e-1} \sum_{j \gg -\infty} \left(\sum_{n=1}^{f} r_{ijn} h_n \right) \pi^i t^j.$$

Reciprocamente, como (K, v) é completo, cada série formal define um elemento de L

$$\sum_i \sum_n \left(\sum_j r_{ijn} t^j \right) h_n \pi^j \in L.$$

Assim, vemos que (L, w) é completo e $L = \bigoplus_{i=0}^{e-1} \bigoplus_{n=1}^{f} K(h_n \pi^i)$. Em particular $[L : K] = ef$. Pela Desigualdade Fundamental concluímos que o prolongamento é único.

(Existência) Suponha que $L|K$ é galoisiana e seja $G_{L|K}$ o seu grupo de Galois. Se existir

w prolongamento de v a L, para cada $\sigma \in G_{L|K}$, a aplicação $w \circ \sigma$ é valorização de L que prolonga v. Pela unicidade do prolongamento temos $w \circ \sigma = w$ para todo σ. Como $[L : K] = n$, temos n isomorfismos em $G_{L|K}$, assim:

$$w(x) = \frac{1}{n} \sum_{\sigma \in G_{L|K}} w\big(\sigma(x)\big) = \frac{1}{n} w \left(\prod_{\sigma \in G_{L|K}} \sigma(x) \right).$$

Temos:

$$N_{L|K}(x) = \prod_{\sigma \in G_{L|K}} \sigma(x) \in K,$$

logo, $w(x) = \frac{1}{n} v\big(N_{L|K}(x)\big)$ e $w|_K = v$.

Agora, suponha que $L|K$ não é galoisiana. Se existir w prolongamento de v a L, considere $x \in L$. Como $[L : K] < \infty$, existe polinômio minimal

$$f = x^m + a_{m-1}x^{m-1} + \cdots + a_0.$$

Seja $\widetilde{L} = K(R_f)$ o corpo das raízes de f, logo $\widetilde{L}|K$ é galoisiana. Portanto, existe um único prolongamento $\widetilde{w}$ de v a $\widetilde{L}$. Podemos escrever

$$f(x) = \prod_{i=1}^{m} (X - x_i),$$

para $x_i \in \widetilde{L}$. Considere o $K-$isomorfismo $\sigma_i : K(x) \longrightarrow K(x_i)$ tal que $\sigma(x) = x_i$ e fixa os elementos de K. Por construção, $\sigma_i \in G_{\widetilde{L}|K}$ e $\widetilde{w} \circ \sigma_i$ é prolongamento de v a $\widetilde{L}$. Pela unicidade, $\widetilde{w} = \widetilde{w} \circ \sigma_i$, então $\widetilde{w}(x_i) = w(x)$ e

$$w(x) = \frac{1}{m} \sum_{i=1}^{m} \widetilde{w}(x_i) = \frac{1}{m} \widetilde{w} \left(\prod x_i \right) = \frac{1}{m} \widetilde{w}(\pm a_0) = \frac{1}{m} v(\pm a_0),$$

portanto, $w(x) = \frac{1}{m} v(\pm a_0),\ w|_K = v.$ □

Teorema 1.7 *Sejam $[L : K] < \infty, v$ valorização de K e $y \in L$ raiz de um polinômio $h(y) = c_o Y^n + \cdots + c_n \in K[Y]$ onde $c_0, c_n \neq 0$. Se w prolonga v, então $w(y)$ é a inclinação*

de um lado do polígono de Newton de $h(y)$, que é definido como o envelope convexo inferior do conjunto $\big\{(i, v(c_i)) \ ; \ 1 \leq i \leq n\big\}$.

Demonstração: Sabendo que

$$\sum_{i=0}^{n} c_i y^{n-i} = 0,$$

temos o mínimo das ordens $w(c_i y^{n-i})$ assumido pelo menos duas vezes, então, existem $1 \leq r \leq s \leq n$, tal que $w(c_r y^{n-r}) = w(c_s y^{n-s})$. Então, para todo $1 \leq i \leq n$,

$$v(c_r) + (n-r)w(y) = v(c_s) + (n-s)w(y) \leq v(c_i) + (n-i)w(y),$$

logo, $w(y) = \dfrac{v(c_s) - v(c_r)}{s-r}$ e $w(y) \leq \dfrac{v(c_i) - v(c_s)}{(i-s)}$. Portanto, $w(y)$ é a inclinação da reta por meio $(r, v(c_r))$ e $(s, v(c_s))$, e os pontos $(i, v(c_i))$ não ficam abaixo desta reta. □

Definição 1.18 *Dado o polinômio como no Teorema 1.7, definimos a inclinação do primeiro lado do polígono de Newton como sendo $\min\limits_{1 \leq i \leq m} w_i(y)$ e denotaremos por $incl_v(y)$.*

Corolário 1.1 *Sejam $[L : K] < \infty$, v valorização de K e $w_1, \ldots, w_m$ as valorizações que prolongam v. Considere $y \in L$ e $Y^n + c_1 Y^{n-1} + \cdots + c_n Y^0$ o polinômio característico da aplicação $\varphi : L \longrightarrow L$ tal que $\varphi(\alpha) = y\alpha$, desse modo $\min\limits_{1 \leq i \leq m} w_i(y) = \min\limits_{1 \leq i \leq n} \dfrac{v(c_i)}{i}$.*

Capítulo

2

Teorema de Riemann-Roch

Neste capítulo veremos o Teorema de Riemann-Roch, que é um resultado importante para o estudo das classficações dos corpos de funções.

2.1 Divisores

Definição 2.1 *Seja $K|k$ um corpo de funções algébricas. Um divisor de $K|k$ é uma soma formal finita*

$$D := \sum_v n_v v$$

com $n_v \in \mathbb{Z}$ $n_v = 0$ para quase todo ponto $v \in S_{K|k}$.

Equivalentemente, D pode ser visto como uma função

$$\begin{cases} S_{K|k} & \longrightarrow & \mathbb{Z} \\ v & \longmapsto & n_v \end{cases}$$

de suporte finito, isto é, $\mathrm{Supp}(D) = \sharp\{v \mid n_v \neq 0\}$ é finito.

Os divisores formam um grupo aditivo ordenado denotado por $\mathcal{D}_K$:

(i) $\sum n_v v + \sum m_v v := \sum (n_v + m_v) v$;

(ii) $\sum n_v v \leq \sum m_v v$ se, e somente se, $n_v \leq m_v$ para todo v.

Definição 2.2 *O grau do divisor D é definido como* $\deg D := \sum n_v \deg v = \sum n_v[k_v : k]$.

Definição 2.3 *Seja* $D = \sum_v n_v v$ *um divisor. Definimos o conjunto* $\mathcal{L}(D)$ *por*

$$\mathcal{L}(D) := \{h \in K^* \mid v(h) \geq -n_v \ \text{ para todo } v \in S_{K|k}\} \cup \{0\}.$$

Proposição 2.1 *Seja D divisor. Então:*

(1) $\mathcal{L}(D)$ é um espaço vetorial sobre k;

(2) se $D \leq E$, então $\mathcal{L}(D) \subseteq \mathcal{L}(E)$.

Demonstração:

(1) Sejam $h_1, h_2 \in \mathcal{L}(D)$. Temos:

$$v(h_1 + h_2) \geq \min\{v(h_1), v(h_2)\} \geq -n_v,$$

ou seja, $h_1 + h_2 \in \mathcal{L}(D)$. Sejam $\alpha \in k$ e $h \in \mathcal{L}(D)$. Quando fazemos a multiplicação αh, como α é constante, não mudamos o número de pólos ou raízes de h, portanto, $v(\alpha h) \geq -n_v$.

(2) Sejam $D = \sum n_v v$ e $E = \sum m_v v$ divisores tais que $D \leq E$, logo $-n_v \geq -m_v$. Se $h \in \mathcal{L}(D)$, então $v(h) \geq -n_v \geq -m_v$, portanto $h \in \mathcal{L}(E)$. □

O nosso objetivo é calcular $\dim \mathcal{L}(D)$, também chamada de dimensão de divisor D, que é um dos problemas mais importantes na teoria de corpos de funções algébricas. A resposta será dada pelo Teorema de Riemann-Roch. Primeiro faremos um exemplo.

Exemplo 2.1 Sejam $K = k(x)$ e $D = \sum n_\pi v_\pi + n_\infty v_\infty$, onde $\pi \in k[x]^*$ irredutível, então

$$\mathcal{L}(D) = \{h \in K^* \mid v_\pi(h) \geq -n_\pi \text{ e } v_\infty(h) \geq -n_\infty\} \cup \{0\}.$$

Sejam $d := \deg D = \sum n_\pi \deg \pi + n_\infty$ e $f := \prod \pi^{-n_\pi}$. Então $v_\pi(f) = -n_\pi$ e $v_\infty(f) = \sum n_\pi \deg \pi$. Afirmamos que

$$\mathcal{L}(D) = \{fg \mid g \in k(x), v_\pi(g) \geq 0 \text{ para todo } \pi, v_\infty(g) \geq -d\}.$$

Sejam $h \in \mathcal{L}(D)$ e $g := hf^{-1}$. Então $h = fg$ e

$$v_\pi(g) = v_\pi(h) - v_\pi(f) \geq -n_\pi - (-n_\pi) = 0,$$

$$v_\infty(g) = v_\infty(h) - v_\infty(f) \geq -n_\infty - (d - n_\infty) = -d.$$

Reciprocamente se $g \in k(x)$ tal que $v_\pi(g) \geq 0$ para todo π e $v_\infty(g) \geq -d$, então

$$v_\pi(fg) = v_\pi(f) + v_\pi(g) = -n_\pi + v_\pi(g) \geq -n_\pi,$$

$$v_\infty(fg) = v_\infty(f) + v_\infty(g) = d - n_\infty + v_\infty(g) \geq -n_\infty.$$

Ou seja, $\mathcal{L}(D) = \{fg \mid g \in k[x] \text{ e } \deg g \leq d\}$, portanto

$$\dim_k \mathcal{L}(D) = \begin{cases} d+1 & se \quad d \geq 0, \\ 0 & se \quad d < 0. \end{cases}$$

Lema 2.1 *Sejam $K|k$ um corpo de funções algébricas e $f \in K \setminus k$. Então f possui pelo menos um pólo.*

Demonstração: Seja $f \in K \setminus k$, então $[K : k(f)] < \infty$. Temos que $v \in S_{K|k}$ é pólo de f se, e somente se, $v(f) < 0$, isto é, $\frac{1}{e} v$ é um prolongamento da valorização v_∞ de $k(f)$ a K, onde "e" é o índice de ramificação de v sobre $k(f)$. Pelo Teorema 1.6, temos a existência do prolongamento, logo v possui pelo menos um pólo. □

Corolário 2.1 *Seja $D = 0$, então $\dim_k \mathcal{L}(D) = 1$, ou $\mathcal{L}(D) = k$.*

Lema 2.2 *Sejam $K|k$ um corpo de funções algébricas e $x \in K$. Então x possui um número finito de zeros e pólos.*

Demonstração: Sejam A e B os conjuntos dos pólos e zeros de x respectivamente e B' o conjunto dos pólos de $\frac{1}{x}$. Então

$$\sharp A \leq \sum f_i e_i \leq [K : k(x)] < \infty,$$

e $\sharp B = \sharp B' < \infty$. □

Pelo lema anterior, dada uma função podemos definir um divisor chamado de divisor associado a esta função:

Definição 2.4 *Sejam $K|k$ um corpo de funções algébricas e $x \in K$. Definimos o divisor de x por $\operatorname{div}(x) := \sum_v v(x)v$. O divisor dos zeros de x é $\operatorname{div}_0(x) := \sum_{v(x)>0} v(x)v$ e $\operatorname{div}_\infty(x) := \sum_{v(x)<0} -v(x)v$ é o divisor dos pólos de x. Claramente $\operatorname{div}(x) = \operatorname{div}_0(x) - \operatorname{div}_\infty(x)$.*

Sejam $x \in K \setminus k$, $v_1, \ldots, v_m$ os pólos de x, $e_1, \ldots, e_m$ e $f_1, \ldots, f_m$ suas ordens e seus graus respectivamente, isto é, $e_i = -v_i(x)$ e $f_i = [k_{v_i} : k]$. Então, $\frac{1}{e_i} v_i$, $1 \leq i \leq m$ são os prolongamentos de $v_\infty \in S_{k(x)|k}$ a K e

$$\deg \operatorname{div}_\infty(x) = \sum -v_i(x) \deg v_i = \sum -v_i(x)[k_{v_i} : k] = \sum e_i f_i.$$

Utilizando a definição anterior, podemos descrever $\mathcal{L}(D)$ da seguinte forma. Se $x \in \mathcal{L}(D)$, então $v(x) \geq -n_v$, e

$$\operatorname{div}(x) = \sum v(x)v \geq \sum -n_v v = -\sum n_v v = -D.$$

Portanto

$$\mathcal{L}(D) = \{h \in K^* \mid \operatorname{div}(h) \geq -D\} \cup \{0\}.$$

Lema 2.3 *Sejam D e E divisores tais que $D \leq E$. Então:*

(1) $\dim \dfrac{\mathcal{L}(E)}{\mathcal{L}(D)} \leq \deg(E - D)$;

(2) $\dim \mathcal{L}(D) \leq 1 + \deg D$, *quando* $D \geq 0$;

(3) $\dim \mathcal{L}(D) < \infty$.

Demonstração: *(1)* Seja $D = \sum n_v v$, por indução basta supor $E = D + v$, para algum $v \in S_{K|k}$. A aplicação

$$\begin{cases} \mathcal{L}(D+v) & \longrightarrow & k_v \\ x & \longmapsto & \overline{xt^{n_v+1}} \end{cases}$$

onde $v(t) = 1$, é uma transformação linear e seu núcleo é $\mathcal{L}(D)$, pois se $x \in \mathcal{L}(D)$,

$$v(xt^{n_v+1}) = v(x) + v(t^{n_v+1}) \geq -n_v + n_v + 1 > 0,$$

logo, $xt^{n_v+1} \in \mu_v$. Logo $\dfrac{\mathcal{L}(D+v)}{\mathcal{L}(D)} \cong k_v$ e, $\dim \dfrac{\mathcal{L}(D+v)}{\mathcal{L}(D)} \leq \dim_k k_v = \deg v = \deg(E-D)$.

(2) Se $D \geq 0$ considere $E = 0$, logo teremos $D \geq E$, assim

$$\dim \frac{\mathcal{L}(D)}{\mathcal{L}(0)} \leq \deg(D - 0).$$

Mas $\dim \mathcal{L}(0) = 1$, logo $\dim \mathcal{L}(D) \leq \deg D + 1$.

(3) Seja D um divisor, logo existe $E \geq 0$ tal que $E \geq D$, portanto

$$\dim \mathcal{L}(D) \leq \dim \mathcal{L}(E) \leq 1 + \deg E < \infty.$$

□

Lema 2.4 *Sejam $x \in K \setminus k$, $[K : k(x)] = n < \infty$ e $D_\infty = \operatorname{div}_\infty(x)$. Então existe $g \in \mathbb{Z}$ tal que* $\dim \mathcal{L}(rD_\infty) \geq rn + 1 - g$ *para todo $r \in \mathbb{Z}$.*

Demonstração: Pela hipótese $D_\infty = \sum_{i=1}^{m} e_i v_i$. Seja $\{z_1, \ldots, z_n\}$ uma base para K sobre $k(x)$. Podemos supor que z_i, $i = 1, \ldots, n$ têm pólos apenas em $\{v_1, \ldots, v_m\}$. De fato, se

existe $v(z_i) = -n < 0$ e $v \neq v_j$ para todo $j = 1, \ldots, m$, tome t, tal que $v(t) = 1$, então $v(t^{-n}z_i) = 0$, e podemos substituir z_i por $t^{-n}z_i$. Temos $x \in \mathcal{L}(D_\infty)$, pois

$$\operatorname{div}_\infty(x) = \sum e_i v_i \geq -\sum e_i v_i = -D_\infty.$$

Agora, escolha $j \in \mathbb{Z}$ suficientemente grande tal que $z_i \in \mathcal{L}(jD_\infty)$. Seja $r \geq j,\ r \in \mathbb{Z}$, tal que $x^s z_i \in \mathcal{L}(rD_\infty)$, para todo $s \geq 0$ e $s + j \leq r$. Como $\{z_1, \ldots, z_n\}$ é linearmente independente sobre $k(x)$, o conjunto $\{x^s z_i \mid 0 \leq s \leq r - j, 1 \leq i \leq n\}$ é linearmente independente sobre k, portanto $\dim \mathcal{L}(rD_\infty) \geq (r - j + 1)n$ para todo $r \geq j$ e claramente para todo $r < j$. Tome $g := 1 + (j - 1)n$,

$$\dim \mathcal{L}(rD_\infty) \geq rn - jn + n = rn + 1 - (1 + (j - 1)n) = rn + 1 - g.$$

□

Lema 2.5 *Para todo $x \in K \setminus k$ temos* $\deg \operatorname{div}_\infty(x) = [K : k(x)] = n$.

Demonstração: Pela desigualdade fundamental, $\deg \operatorname{div}_\infty(x) \leq [K : k(x)] = n$. Pelo Lema 2.4, $\dim \mathcal{L}(rD_\infty) \geq rn + 1 - g$ para todo $r \in \mathbb{Z}$. Pelo Lema 2.3 temos que $\dim \mathcal{L}(rD_\infty) \leq 1 + r \deg D_\infty$ para todo $r \geq 0$. Logo,

$$rn + 1 - g \leq 1 + r \deg D_\infty \Rightarrow n - \frac{g}{r} \leq \deg D_\infty \Rightarrow n \leq \deg D_\infty + \frac{g}{r},$$

para todo $r > 0$, então $n \leq \deg \operatorname{div}_\infty(x)$. Portanto, $[K : k(x)] = \deg \operatorname{div}_\infty(x)$. □

Corolário 2.2 *(Fórmula de Produto) Para toda função $x \in K^*$,*

$$\sum_v v(x) \deg v = 0 \quad \textit{ou} \quad \prod_v 2^{-v(x) \deg v} = 1,$$

isto é, $\deg \operatorname{div}_0(x) - \deg \operatorname{div}_\infty(x) = 0$. *Isso nos diz que o número de zeros de x contados com suas ordens é igual ao número de pólos de x contados com suas ordens.*

Demonstração: Basta observar

$$\deg \operatorname{div}_\infty(x) = \big[K : k(x)\big] = \left[K : k\left(\frac{1}{x}\right)\right] = \deg \operatorname{div}_\infty\left(\frac{1}{x}\right) = \deg \operatorname{div}_0(x).$$

□

Lema 2.6 *Seja D um divisor, então $\dim_k \mathcal{L}(D) \leq 1 + \deg D$ se $\deg D \geq 0$ e $\dim_k \mathcal{L}(D) = 0$ caso contrário.*

Demonstração: Suponhamos $\dim \mathcal{L}(D) > 0$. Existe $h \in K^*$, tal que $h \in \mathcal{L}(D)$, ou seja, $\operatorname{div}(h) + D \geq 0$. Seja $E = \operatorname{div}(h) + D$, então, $E \geq 0$ e pelo Lema 2.3, $\dim \mathcal{L}(E) \leq 1 + \deg E$. Pela Fórmula de Produto, $\deg D = \deg E$.

A aplicação $\varphi : \mathcal{L}(E) \longrightarrow \mathcal{L}(D)$, $f \longmapsto fh$ é um isomorfismo entre k-espaços vetoriais, logo $\dim \mathcal{L}(E) = \dim \mathcal{L}(D)$. Portanto $\dim \mathcal{L}(D) \leq 1 + \deg D$. □

Teorema 2.1 *(Teorema de Riemann) Sejam $K|k$ um corpo de funções em uma variável e D um divisor. Então existe $g \in \mathbb{Z}$ tal que $\dim \mathcal{L}(D) \geq \deg D + 1 - g$.*

Demonstração: Sejam $x \in K \setminus k$ e $D_\infty = \operatorname{div}_\infty(x) = \sum_{i=1}^{m} e_i v_i$. Considere $g \in \mathbb{Z}$ como no Lema 2.4, isto é, $\dim \mathcal{L}(rD_\infty) \geq rn + 1 - g$ para todo $r \in \mathbb{Z}$ suficientemente grande. Pelo Lema 2.5, $\deg D_\infty = n = [K : k(x)]$, então

$$\dim \mathcal{L}(rD_\infty) \geq r \deg D_\infty + 1 - g = \deg(rD_\infty) + 1 - g$$

para todo $r \in \mathbb{Z}$. Agora, sejam $D = \sum n_v v$ e $h \in k[x]^*$ com $v(h) \geq n_v$ para todo $v \in S_{K|k} \setminus \{v_i \mid 1 \leq i \leq m\}$, onde v_i são os pólos de x. Considere $r \in \mathbb{Z}$, $r \gg 0$ tal que $E := D - \operatorname{div}(h) \leq rD_\infty$. Temos que $\deg E = \deg D$ e pelo argumento feito na demonstração do Lema 2.6, $\dim \mathcal{L}(E) = \dim \mathcal{L}(D)$. Então, pelo Lema 2.3,

$$\deg D - \dim \mathcal{L}(D) = \deg E - \dim \mathcal{L}(E) \leq \deg(rD_\infty) - \dim \mathcal{L}(rD_\infty) \leq g - 1.$$

Portanto, $\dim \mathcal{L}(D) \geq \deg D + 1 - g$. □

Corolário 2.3 *Para todo $v \in S_{K|k}$, existe uma função x tal que v é o único pólo de x.*

Demonstração: Seja $D = rv$. Então,

$$\dim \mathcal{L}(rv) \geq \deg(rv) + 1 - g = r \deg v + 1 - g,$$

para todo $r \in \mathbb{Z}$. Se $r \gg 0$, então $\dim \mathcal{L}(rv) > 1$, logo, existe $x \in \mathcal{L}(rv) \setminus k$. Como $x \notin k$, pelo Lema 2.1, x possui pelo menos um pólo, e já que $x \in \mathcal{L}(rv)$ então v é o único pólo.□

Teorema 2.2 *(Igualdade Fundamental) Sejam $K|k$ um corpo de funções algébricas em uma variável, $L|K$ uma extensão finita, $v \in S_{K|k}$ e $w_1, \ldots, w_m$ prolongamentos de v a L. Então, $\sum_{i=1}^{m} e_{w_i|v} f_{w_i|v} = [L : K]$.*

Demonstração: O caso em que $K = k(x)$, $v = v_\infty$ e k é algebricamente fechado em L é basicamente o Lema 2.5. Em geral, tome $x \in K$ cujo único pólo é v . Seja l o fecho algébrico de k em L, então:

$$[l : k] = [l(x) : k(x)] \leq [L : k(x)] = [L : K] \cdot [K : k(x)] < \infty,$$

logo, $[l : k]$ é algébrica.

Sendo assim, como w_i é trivial sobre k, teremos w_i trivial sobre l.

Seja v_∞ a valorização infinita de $k(x)|k$ e w_∞ a valorização infinita de $l(x)|k$. Sabemos que w_∞ é o único prolongamento de v_∞ a $l(x)$, então $e_{w_\infty|v_\infty} = 1$ e $f_{w_\infty|v_\infty} = [l : k]$. Portanto,

$$e_{w_\infty|v_\infty}.f_{w_\infty|v_\infty} = [l(x) : k(x)].$$

Desse modo teremos:

$$e_{w_i|v}.e_{v|v_\infty} = [w_i(l) : v(k)].[v(k) : v_\infty(k)] = [w_i(l) : v_\infty(k)] = [w_i(l) : w_\infty(k)] = e_{w_i|w_\infty},$$

logo,

$$e_{w_i|v}.e_{v|v_\infty} = e_{w_i|w_\infty}.e_{w_\infty|v_\infty} \Rightarrow e_{w_i|v} = \frac{e_{w_i|w_\infty}.e_{w_\infty|v_\infty}}{e_{v|v_\infty}}.$$

Seguindo assim,

$$\sum_{i=1}^{m} e_{w_i|v} f_{w_i|v} = \frac{\left(\sum_{i=1}^{m} e_{w_i|w_\infty} f_{w_i|w_\infty}\right) . e_{w_\infty|v_\infty} f_{w_\infty|v_\infty}}{e_{v|v_\infty} f_{v|v_\infty}} =$$

$$= \frac{[L : l(x)].[l(x) : k(x)]}{[K : k(x)]} = \frac{[L : k(x)]}{[K : k(x)]} = [L : k].$$

□

Pelo Teorema de Riemann 2.1, para todo D,

$$g \geq \deg D - \dim \mathcal{L}(D) + 1.$$

Seja $D = 0$. Sabemos que $\deg D = 0$ e $\dim \mathcal{L}(D) = 1$. Então $g \geq 0$. Então pelos Teorema de Riemann e princípio de boa ordem, $g := \max_D\{\deg D - \dim \mathcal{L}(D) + 1\}$ existe.

Definição 2.5 *Chamamos o valor g descrito acima de gênero do corpo de funções.*

Exemplo 2.2 *Se $K = k(x)$, pelo Exemplo 2.1, $g = 0$.*

2.2 Método para calcular o gênero g

Pela demostração do Teorema de Riemann,

$$g = \deg(rD_\infty) - \dim \mathcal{L}(rD_\infty) + 1,$$

onde $r \gg 0$, $r \in \mathbb{Z}$, $D_\infty = \mathrm{div}_\infty(x) = \sum e_i v_i$ e $x \in K$ um elemento qualquer. Temos $\deg(rD_\infty) = r[K : k(x)]$, logo, basta calcularmos $\dim \mathcal{L}(rD_\infty)$.

Sejam v_∞ a valorização infinita de $k(x)|k$, $w_1, \ldots, w_m$ os prolongamentos de v_∞ a K, e e_i, f_i, $0 \leq i \leq m$, os índices de ramificação e inércia respectivamente. Como $v_i = e_i w_i \in S_{K|k}$ e $D_\infty = \mathrm{div}_\infty(x) = \sum_{i=1}^{m} e_i v_i$,

$$\mathcal{L}(rD_\infty) = \Big\{ z \in K \mid v_i(z) \geq -re_i \text{ e } v(z) \geq 0, \ \forall\ v \in S_{K|k} \setminus \{v_i\} \Big\}.$$

Sabendo que, $v_i(z) \geq -re_i$ para cada i, então $\text{incl}_{v_\infty}(z) = \min w_i(z) \geq -r$, logo,

$$\mathcal{L}(rD_\infty) = \{z \in K \mid \text{incl}_{v_\infty}(z) \geq -r \text{ e } \text{incl}_v(z) \geq 0,\ \forall\ v \neq v_\infty\}.$$

Exemplo 2.3 Sejam $K = k(x, y)$ com char$k \neq 2$ e $y^2 = h(x) = \sum_{i=0}^{n} c_i x^{n-i}$ onde $c_i \in k$ e $c_0 \neq 0$. A seguir calcularemos o gênero deste corpo de funções.

Pela relação dada entre x e y, $[K : k(x)] = 2$ e $\mathcal{B} = \{1, y\}$ é uma base de K sobre $k(x)$. Seja $z = a + by \in K$ onde $a, b \in k(x)$ e considere a aplicação

$$\begin{cases} K & \longrightarrow & K \\ \varphi & \longmapsto & z\varphi \end{cases}.$$

Esta aplicação é uma transormação linear e sua matriz na base $\mathcal{B}$ é dada por

$$\begin{bmatrix} a & b \\ bh & a \end{bmatrix}$$

Seja $c(z)$ o polinômio característico dessa trasnformação, logo:

$$c(z) = \begin{vmatrix} z-a & -b \\ -bh & z-a \end{vmatrix} = z^2 - 2za + (a^2 - b^2h).$$

Pelo Corolário 1.1 temos

$$\text{incl}_v(z) = \min\left\{v(-2a), \frac{v(a^2 - b^2h)}{2}\right\} = \min\left\{v(a), \frac{1}{2}v(a^2 - b^2h)\right\}.$$

Seja $z \in \mathcal{L}(rD_\infty)$, então $\text{incl}_{v_\infty}(z) \geq -r$ e para $v \neq v_\infty$, $\text{incl}_v(z) \geq 0$. Então

$$\begin{array}{lll} v_\infty(a) \geq -r, & \frac{1}{2}\, v_\infty(a^2 - b^2h) \geq -r & \Leftrightarrow \\ v_\infty(a) \geq -r, & \frac{1}{2}\, v_\infty(b^2h) \geq -r & \Leftrightarrow \\ v_\infty(a) \geq -r, & v_\infty(b) + \frac{1}{2}\, v_\infty(h) \geq -r & \Leftrightarrow \\ v_\infty(a) \geq -r, & v_\infty(b) - \dfrac{n}{2} \geq -r & \Leftrightarrow \\ v_\infty(a) \geq -r, & v_\infty(b) \geq -r + \dfrac{n}{2}. & \end{array}$$

E $v(a) \geq 0, v(b) + \frac{1}{2}v(h) \geq 0$. Observe que $v(h) = 0$ ou $v(h) = 1$, portanto $v(a) \geq 0$ e $v(b) \geq 0$. Então,

$$\mathcal{L}(rD_\infty) = \left\{ z = a + by \mid v_\infty(a) \geq -r,\ v_\infty(b) \geq -r + \frac{n}{2} \text{ e } v(a) \geq 0,\ v(b) \geq 0,\ \forall\ v \neq v_\infty \right\},$$

ou ,

$$\mathcal{L}(rD_\infty) = \left\{ z = a + by \mid a, b \in k[x], \deg a \leq r, \deg b \leq r - \frac{n}{2} \right\}.$$

Agora calcularemos $\dim \mathcal{L}(rD_\infty)$. Seja $n = 2l + 2$, se n for par e $n = 2l + 1$, se for ímpar.

(1) Se $r < 0$, então $\dim \mathcal{L}(rD_\infty) = 0$.

(2) Se $0 \leq r \leq l$,

$$\deg b \leq r - \frac{2l+1}{2} = r - l - \frac{1}{2} < 0,$$

$$\deg b \leq r - \frac{2l+2}{2} = r - l - 1 < 0,$$

logo $\dim \mathcal{L}(rD_\infty) = \deg a + 1$, ou seja, $\dim \mathcal{L}(rD_\infty) = r + 1$.

(3) Se $r \geq l$,

$$\deg b \leq r - l - \frac{1}{2} < r - l - 1.$$

Então $\dim \mathcal{L}(rD_\infty) = \deg a + 1 + \deg b + 1 = r + 1 + r - l - 1 + 1 = 2r - l + 1$.

Então

$$\dim \mathcal{L}(rD_\infty) = \begin{cases} 2r - l + 1 & \text{se} \quad r \geq l; \\ r + 1 & \text{se} \quad 0 \leq r \leq l; \\ 0 & \text{se} \quad r < 0. \end{cases}$$

Por outro lado, $\deg(rD_\infty) = r[K : k(x)] = 2r$, portanto no caso (2) acima, $g \leq l$; e no caso 3, $g = l$. Então

$$g = \left[\frac{n-1}{2} \right].$$

Exemplo 2.4 Sejam $K = k(x, y)$ com char$k \neq 3$ e $y^3 = h(x) \in k[x] \setminus k$ de grau n. Considere $v_\infty \in S_{k(x)|k}$ com único prolongamento $w_\infty \in S_{K|k}$, isto é, $rD_\infty = rw_\infty$.

Temos $[K : k(x)] = 3$ e $\mathcal{B} = \{1, y, y^2\}$ é uma base de K sobre $k(x)$. Seja $z = a+by+cy^2 \in K$ onde $a, b, c \in k(x)$ e considere a aplicação

$$\begin{cases} K & \longrightarrow & K \\ \varphi & \longmapsto & z\varphi \end{cases}.$$

Esta aplicação é uma transormação linear e sua matriz na base $\mathcal{B}$ é dada por

$$\begin{bmatrix} a & b & c \\ ch & a & b \\ bh & ch & a \end{bmatrix}$$

e seu polinômio característico é $c(z) = z^3-3az^2+(3a^2-3bch)z+(3bcah-a^3-b^3h-c^3h^2)$. Pelo Corolário 1.1 temos:

$$\text{incl}_{v_\infty}(z) = \min\left\{v_\infty(-3a), \frac{v_\infty(3a^2-3bch)}{2}, \frac{v_\infty(3bcah-a^3-b^3h-c^3h^2)}{3}\right\} =$$

$$= \min\left\{3v_\infty(a), \frac{3}{2}\big(v_\infty(b)+v_\infty(c)-n\big), v_\infty(b)+v_\infty(c)+v_\infty(a)-n, 3v_\infty(b)-n, 3v_\infty(c)-2n\right\}.$$

Temos

$$\text{incl}_{v_\infty}(z) \geq -r \Leftrightarrow v(a) \geq \frac{-r}{3},\ v(b) \geq \frac{-r+n}{3},\ v(c) \geq \frac{-r+2n}{3}.$$

Portanto,

$$\dim \mathcal{L}(rw_\infty) = \left\{a+by+cy^2 \mid a, b, c \in k(x) \text{ e } \deg a \leq \frac{r}{3},\ \deg b \leq \frac{r-n}{3},\ \deg c \leq \frac{r-2n}{3}\right\}.$$

Por outro lado $\deg(rw_\infty) = r \deg w_\infty = r$. Se $3 \mid n$,

$$\dim \mathcal{L}(rw_\infty) = \frac{r}{3}+1+\frac{r-3t}{3}+1+\frac{r-6t}{3}+1 = r-3t+3 = r-n+3.$$

Então

$$g = \deg(rw_\infty) - \dim \mathcal{L}(rw_\infty) + 1 = r - r + n - 3 + 1 = n - 2.$$

Nos demais casos: $n = 3t + 1$ ou $n = 3t + 2$, $t \in \mathbb{Z}$, obteremos $g = n - 1$.

Teorema 2.3 *Seja $K|k$ um corpo de funções algébricas. Então $K|k$ é isomorfo a $k(x)|k$ se, e somente se, $g = 0$ e $S^{rac}_{K|k} \neq \emptyset$. Em particular, se $k = \overline{k}$, K é isomorfo a $k(x)$ se, e somente se, $g = 0$.*

Demonstração: Se K é isomorfo a $k(x)$, $g = 0$ e $\deg v_\infty = 1$, ou seja, $S^{rac}_{K|k} \neq \emptyset$. Reciprocamente, sejam $v \in S^{rac}_{K|k}$, $g = 0$ e considere o divisor $D := v$. Pelos Lema 2.6 e Teorema de Riemann, $\dim_k \mathcal{L}(v) = 1 + \deg v = 2 > 1$. Tome $x \in \mathcal{L}(v) \setminus k$, então v é o único pólo de x, isto é, $\mathrm{div}_\infty(x) = v$. Pela Igualdade Fundamental, $[K : k(x)] = \deg \mathrm{div}_\infty(x) = 1$, portanto K é isomorfo a $k(x)$. □

Teorema 2.4 *Seja $k = \mathbb{R}$. Então a menos de isomorfismo, existem exatamente dois corpos de funções algébricas de gênero zero: $\mathbb{R}(x)|\mathbb{R}$ e $\mathbb{R}(x, y)|\mathbb{R}$ onde $y^2 + x^2 + 1 = 0$.*

Demonstração: Se $S^{rac}_{K|k} \neq \emptyset$, então, $K \simeq \mathbb{R}(x)$ pelo Teorema 2.3. Se $S^{rac}_{K|k} = \emptyset$, seja $v \in S_{K|k}$. Então,

$$1 < \deg v = [\mathbb{R}_v : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2,$$

logo, $\deg v = 2$ e $\dim \mathcal{L}(v) = 1 + \deg v = 3 > 1$. Então existe $x \in \mathcal{L}(v) \setminus k$ tal que $\mathrm{div}_\infty(x) = v$. Pela Igualdade Fundamental, $[K : \mathbb{R}(x)] = \deg \mathrm{div}_\infty(x) = \deg v = 2$. Então existe $y \in K$ tal que $K = \mathbb{R}(x, y), y^2 = h(x)$. Como $g = 0$, pelo Exemplo 2.3 temos:

$$\left[\frac{n-1}{2}\right] = 0 \Rightarrow \deg h \leq 2.$$

Se $\deg h = 2$, então:

$$h = ax^2 + bx + c.$$

Como $S^{rac}_{K|k} = \emptyset$, $a < 0$ como x não possui zeros racionais $c < 0$. Fazendo a mudança $x \longrightarrow x - \dfrac{b}{2a}$ podemos supor $b = 0$, e substituindo x e y por multiplos constantes, podemos supor $a = c = -1$. Portanto, $y^2 + x^2 + 1 = 0$. □

Definição 2.6 *Um divisor D é chamado de divisor especial se* $\dim \mathcal{L}(D) > \deg D + 1 - g$.

Pela minimalidade de g, existe um divisor D, tal que $\dim \mathcal{L}(D) = \deg D + 1 - g$, ou seja, D não é especial.

Lema 2.7 *Se D não for especial, então todo divisor $E \geq D$ também não é especial.*

Demonstração: Seja E um divisor tal que $E \geq D$. Pelos Teorema de Riemann e Lema 2.3:

$$g = \deg D - \dim \mathcal{L}(D) + 1 \leq \deg E - \dim \mathcal{L}(E) + 1 \leq g.$$

□

2.3 Álgebra e Subalgebra dos Adeles

Seja $K|k$ um corpo de funções algébricas e lembre-se as definições e notações da Seção 1.1. O conjunto

$$\widehat{\mathcal{A}}_{K|k} = \left\{ (x_v) \in \prod_{v \in S_{K|k}} \widehat{K}_v \;\middle|\; x_v \in \mathcal{O}_v \text{ para quase todo } v \right\}$$

munido de operações

(1) $(x_v) + (y_v) = (x_v + y_v)$;

(2) $(x_v) \cdot (y_v) = (x_v \cdot y_v)$;

(3) $c(x_v) = (cx_v)$, para todo $c \in k$.

é uma k-álgebra.

Definição 2.7 *A Álgebra dos Adeles de $K|k$ é a k-álgebra $\widehat{\mathcal{A}}_{K|k}$.*

Normalmente trabalhamos com a subalgebra da Álgebra dos Adeles definida por

$$\mathcal{A}_{K|k} = \left\{ (x_v) \in \prod_{v \in S_{K|k}} K \;\middle|\; x_v \in \mathcal{O}_v \text{ para quase todo } \; v \right\}.$$

Para cada divisor $D = \sum n_v v$, associamos um $k-$espaço vetorial definido por

$$\mathcal{A}(D) = \big\{(x_v) \in \mathcal{A}_{K|k} \mid v(x_v) \geq -n_v, \text{ para todo } v\big\}.$$

Observe que K é uma subalgebra de $\mathcal{A}_{K|k}$ através da aplicação $f : K \longrightarrow \mathcal{A}_{K|k}$ tal que $f(x) = (x_v)$ onde $x_v := x$ para todo v; e que

$$\mathcal{A}(D) \cap K = \big\{x \in K \mid v(x) \geq -n_v, \text{ para todo } v\big\} = \mathcal{L}(D).$$

Lema 2.8 *Sejam D e E dois divisores tais que $D \leq E$. Então $\mathcal{A}(D) \subseteq \mathcal{A}(E)$ e* $\dim_k \dfrac{\mathcal{A}(E)}{\mathcal{A}(D)} = \deg(E - D)$.

Demonstração: Pela definição, claramante $\mathcal{A}(D) \subseteq \mathcal{A}(E)$. Por indução, podemos supor $E = D + v$ com $v \in S_{K|k}$. Seja $t \in K$, tal que $v(t) = 1$, então:

$$\frac{\mathcal{A}(E)}{\mathcal{A}(D)} = \frac{\mathcal{A}(D+v)}{\mathcal{A}(D)} \cong \frac{\{x \in K \mid v(x) \geq -n_v - 1\}}{\{x \in K \mid v(x) \geq -n_v\}} = \frac{\mathcal{O}_v t^{-n_v-1}}{\mathcal{O}_v t^{-n_v}} \cong \frac{\mathcal{O}_v}{t\mathcal{O}_v} = k_v.$$

Então

$$\dim_k \frac{\mathcal{A}(E)}{\mathcal{A}(D)} = \dim_k k_v = [k_v : k] = \deg v = \deg(E - D).$$

□

2.4 Teorema de Riemann-Roch

Iniciaremos essa seção com um Teorema que é o resultado principal a ser utilizado na demonstração do Teorema de Riemann-Roch. Daqui em diante usaremos a notação $l(D)$ para $\dim \mathcal{L}(D)$.

Teorema 2.5 *Sejam $K|k$ um corpo de funções algébricas de gênero g e D um divisor. Então*

(i) $\delta(D) := \dim_k \dfrac{\mathcal{A}_{K|k}}{\mathcal{A}(D) + K} < \infty$;

(ii) $l(D) = \deg D + 1 - g + \delta(D)$.

Demonstração: Sejam $D \leq E$ divisores. O homomorfismo natural

$$\varphi : \frac{\mathcal{A}(E)}{\mathcal{A}(D)} \longrightarrow \frac{\mathcal{A}(E)+K}{\mathcal{A}(D)+K}$$

é sobrejetor, logo

$$\dim_k \frac{\mathcal{A}(E)}{\mathcal{A}(D)} \geq \dim_k \frac{\mathcal{A}(E)+K}{\mathcal{A}(D)+K}.$$

Pelo Lema 2.8,

$$\dim_k \frac{\mathcal{A}(E)}{\mathcal{A}(D)} = \deg(E-D),$$

portanto $\dim_k \dfrac{\mathcal{A}(E)+K}{\mathcal{A}(D)+K} < \infty$. Agora basta mostrar que existe um divisor E tal que $E \geq D$ e $\mathcal{A}(E)+K = \mathcal{A}_{K|k}$. Sabemos que existe $E \geq D$ não especial tal que $l(E) = \deg E + 1 - g$. Pelo Lema 2.7, para todo $F \geq E$, $l(F) = \deg F + 1 - g$, portanto,

$$\dim \frac{\mathcal{L}(F)}{\mathcal{L}(E)} = \deg(F-E).$$

Usando esta igualdade e o fato que o núcleo de φ quando definido para F e E é $\dfrac{\mathcal{L}(F)}{\mathcal{L}(E)}$, concluímos que $\mathcal{A}(E)+K = \mathcal{A}(F)+K$. Então $\mathcal{A}_{K|k} \subseteq \mathcal{A}(E)+K$, ou, $\mathcal{A}(E)+K = \mathcal{A}_{K|k}$.

Finalmente pelos argumentos acima,

$$\deg(E-D) = l(E) - l(D) + \delta(D).$$

Como $l(E) = \deg E + 1 - g$, temos:

$$l(D) = \deg D + 1 - g + \delta(D).$$

□

Definição 2.8 *O termo de correção $\delta(D)$ descrito no Teorema 2.5 é chamado de Índice de Especialidade de D.*

Definição 2.9 *Uma Diferencial do corpo de funções algébricas $K|k$ é uma função linear $\lambda : \mathcal{A}_{K|k} \longrightarrow k$ tal que $\lambda|_K = 0$ e para algum divisor D, $\lambda|_{\mathcal{A}(D)} = 0$.*

Definição 2.10 *Para cada divisor D, definimos $\Omega(D)$ como o espaço das diferenciais que se anulam sobre $\mathcal{A}(D)$, ou seja, o espaço das funções lineares $\lambda : \mathcal{A}_{K|k} \longrightarrow k$ que se anulam sobre $\mathcal{A}(D) + K$.*

Observação 2.1 *Pela definição e pelo argumento usado na demonstração do Teorema 2.5,*

$$\dim \Omega(D) = \dim \frac{\mathcal{A}_{K|k}}{A(D) + K} = \delta(D).$$

Então podemos reescrever o Teorema 2.5 da seguinte forma:

Teorema 2.6 *(de Riemann-Roch) Sejam $K|k$ um corpo de funções algébricas de gênero g e D um divisor. Então*

$$l(D) = \deg D + 1 - g + \dim \Omega(D).$$

Corolário 2.4 $\dim \Omega(0) = g$.

Demonstração: Segue do fato que $\dim_k \mathcal{L}(0) = 1$. □

Definição 2.11 *O espaço $\Omega(0)$ é chamado de Espaço das Diferenciais Regulares. Definimos $\Omega = \Omega_{K|k}$ como o espaço de todas as diferenciais de $K|k$, isto é, $\Omega = \bigcup_D \Omega(D)$.*

Definição 2.12 *Sejam $z \in K$ e $\lambda \in \Omega$. Definimos a diferencial $z\lambda$ por $(z\lambda)(a) := \lambda(za)$, $a \in \mathcal{A}_{K|k}$. Desta forma Ω possui estrutura de K-espaço vetorial.*

Observação 2.2 *Se $z \in K^*$, $\lambda \in \Omega(D)$, então $z\lambda \in \Omega(D + \operatorname{div}(z))$.*

Proposição 2.2 $\dim_K \Omega = 1$.

Demonstração: Por definição, $\Omega \neq 0$. Então $\dim_K \Omega \geq 1$. Suponha, por absurdo, que existam duas diferenciais linearmente independentes $\lambda \in \Omega(D_1)$ e $\mu \in \Omega(D_2)$, onde D_1 e D_2 divisores. Seja D um divisor tal que $D \leq D_1$ e $D \leq D_2$, então $\lambda, \mu \in \Omega(D)$. Sejam

E um divisor e $\{z_1, \ldots, z_m\}$ uma base de $\mathcal{L}(E)$, então $z_i\lambda, z_i\mu \in \Omega(D-E)$, para todo $1 \leq i \leq m$; de fato,

$$z_i \in \mathcal{L}(E) \Rightarrow \operatorname{div}(z_i) \geq -E \Rightarrow D + \operatorname{div}(z_i) \geq D - E,$$

e pela Observação 2.2, $z_i\lambda$ e $z_i\mu \in \Omega(D + \operatorname{div}(z_i))$. Logo, $z_i\lambda$ e $z_i\mu \in \Omega(D-E)$.

Como λ, μ são linearmente independentes sobre K e $z_1, \ldots, z_m$ são linearmente independentes sobre k, $\{z_i\lambda, z_i\mu \mid 1 \leq i \leq m\}$ é linearmente independente sobre k. Então,

$$2m \leq \dim \Omega(D-E) \Rightarrow 2l(E) \leq \delta(D-E).$$

Pelo Teorema de Riemann-Roch,

$$2(\deg E + 1 - g + \delta(E)) \leq l(D-E) - \deg(D-E) - 1 + g,$$

isto é, para todo E,

$$\deg E \leq l(D-E) - \deg D - 3 + 3g - 2\delta(E).$$

Escolhemos E tal que $\deg E \gg 0$, então $\deg(D-E) < 0$ e pelo Lema 2.6, $l(D-E) = 0$, portanto

$$\deg E \leq -\deg D - 3 + 3g - 2\delta(E),$$

o que é absurdo, pois, $\deg E \gg 0$. Então $\dim_K \Omega = 1$. □

Lema 2.9 *Se* $\deg D > 2g-2$, *então* $\Omega(D) = 0$, *ou seja, D não é especial.*

Demonstração: Suponha por absurdo que $\Omega(D) \neq 0$, logo existe $\lambda \in \Omega(D) \setminus \{0\}$. Sejam E um divisor e $\{z_1, \ldots, z_m\}$ uma base de $\mathcal{L}(E)$, pelo argumento utilizado na demonstração do teorema anterior, $z_i\lambda \in \Omega(D-E)$ e $\{z_i\lambda \mid i = 1, \ldots, m\}$ é linearmente independente sobre k. Então $l(E) \leq \delta(D-E)$. Pelo Teorema de Riemann-Roch,

$$\deg E + 1 - g + \delta(E) \leq l(D-E) - \deg(D-E) - 1 + g,$$

isto é, para todo E

$$\deg D \leq l(D-E) - 2 + 2g - \delta(E).$$

Escolhemos E de tal maneira que $\deg E > \deg D$, então $\deg(D-E) < 0$. Logo, pelo Lema 2.6, $l(D-E) = 0$, e

$$\deg D \leq -2 + 2g - \delta(E) \leq 2g - 2$$

o que é um absurdo. Portanto $\Omega(D) = 0$. □

Teorema 2.7 *(da Aproximação Forte) Sejam $K|k$ corpo de funções algébricas e $v_0, \ldots, v_m \in S_{K|k}$ valorizações distintas entre si. Considere $x_1, \ldots, x_m \in K$ e $n_1, \ldots, n_m \in \mathbb{Z}$, então existe $x \in K$ tal que $v_i(x - x_i) = n_i$ para todo $1 \leq i \leq m$ e $v(x) \geq 0$ para todo $v \in S_{K|k} \setminus \{v_0, \ldots, v_m\}$.*

Demonstração: Seja $D := -n_1 v_1 - \cdots - n_m v_m + n v_0$, onde $n \gg 0$ tal que $\deg D > 2g-2$. Então pelo Lema 2.9, $\Omega(D) = 0$, e como $\dim \Omega(D) = \dim \dfrac{\mathcal{A}_{K|k}}{\mathcal{A}(D) + k}$, teremos:

$$\mathcal{A}(D) + K = \mathcal{A}_{K|k}.$$

Ou seja, para todo adele $(x_v) \in \mathcal{A}_{K|k}$, existe $x \in K$ tal que $(x - x_v) \in \mathcal{A}(D)$, isto é,

$$v_i(x - x_i) \geq n_i,\ v_0(x - x_{v_0}) \geq -n \text{ e } v(x - x_v) \geq 0$$

para todo $v \in S_{K|k} \setminus \{v_0, \ldots, v_m\}$. Tomamos

$$x_v := \begin{cases} x_i & \text{se } v = v_i, \text{ com } i \geq 1 \\ 0 & \text{caso contrário} \end{cases}$$

Agora, para mostrar que $v_i(x - x_i) = n_i$, basta usar o mesmo argumento do Teorema da Aproximação 1.4. □

Proposição 2.3 *Seja $\lambda \neq 0$ uma diferencial de $K|k$. Então existe um divisor C tal que para todo divisor D, se $\lambda \in \Omega(D)$, então $D \leq C$.*

Demonstração: Por definição, existe C divisor, tal que $\lambda \in \Omega(C)$. Pelo Lema 2.9, $\deg C \leq 2g-2$. Escolhemos C tal que $\deg C = 2g-2$. Seja D outro divisor tal que $\lambda \in \Omega(D)$. Seja E o menor divisor tal que $E \geq C$ e $E \geq D$, de fato

$$C = \sum m_v v,\ D = \sum n_v v \Longrightarrow E = \sum \max\{n_v, m_v\} v.$$

Então $\mathcal{A}(E) = \mathcal{A}(C) + \mathcal{A}(D)$ e, portanto $\lambda \in \Omega(E) = \Omega(D) \cap \Omega(C)$. Pela maximalidade de $\deg C$, $\deg E \leq \deg C$, mas, como $E \geq C$, então, $E = C$. Portanto, $D \leq C$. □

Definição 2.13 *O divisor C descrito na Proposição 2.3 é chamado de divisor de λ e denotado por* $\mathrm{div}(\lambda) := C$.

Seja μ um diferencial não nulo. Como $\dim_k \Omega = 1$, $\mu = z\lambda$, para algum $z \in K \setminus \{0\}$, logo

$$\mathrm{div}(\mu) = \mathrm{div}(z\lambda) = \mathrm{div}(z) + \mathrm{div}(\lambda) = \mathrm{div}(z) + C.$$

Seja D um divisor, então

$$\mu \in \Omega(D) \Leftrightarrow D \leq \mathrm{div}(\mu) \Leftrightarrow D \leq \mathrm{div}(z) + C \Leftrightarrow \mathrm{div(z)} \geq D - C \Leftrightarrow z \in \mathcal{L}(C - D),$$

ou seja, $\Omega(D) = \lambda\mathcal{L}(C-D)$, em particular, $\dim \Omega(D) = \dim \mathcal{L}(C-D)$. Então o Teorema de Riemann-Roch pode ser enunciado da seguinte forma:

Teorema 2.8 *(de Riemann-Roch) Seja $K|k$ um corpo de funções algébricas. Então existem um $g \in \mathbb{Z}$ e um divisor C, tais que* $\dim \mathcal{L}(D) = \deg D + 1 - g + \dim \mathcal{L}(C - D)$.

Observação 2.3 *O divisor C não é unicamente determinado. De fato, seja C' um divisor linearmente equivalente a C, ou seja, $C' = C + \mathrm{div}(z), z \in K^*$, então:*

$$h \in \mathcal{L}(C-D) \Leftrightarrow \mathrm{div(h)} \geq D - C \Leftrightarrow \mathrm{div}(hz^{-1}) \geq D - C' \Leftrightarrow hz^{-1} \in \mathcal{L}(C' - D),$$

portanto, $\mathcal{L}(C-D) = z^{-1}\mathcal{L}(C'-D)$, ou $l(C-D) = l(C'-D)$.

Corolário 2.5 $l(C) = g$ *e* $\deg C = 2g - 2$.

Demonstração: Basta tomarmos $D = 0$ e $D = C$ no Teorema de Riemann-Roch. □

Corolário 2.6 *Se* $\deg D > 2g - 2$*, então,* $l(D) = \deg D + 1 - g$.

Demonstração: Se $\deg D > 2g-2$, então, $\deg(C-D) < 0$. Pelo Lema 2.6, $l(C-D) = 0$. Logo do Teorema de Riemann-Roch, $l(D) = \deg D + 1 - g$. □

Observação 2.4 *Então quando* $\deg D > 2g - 2$ *e* $\deg D < 0$ *conseguimos calcular* $l(D)$*. Ou seja, resolvemos o problema de Riemann-Roch nestes casos. Faltam apenas os casos em que* $0 \leq \deg D \leq 2g - 2$.

Lema 2.10 *Seja* D *um divisor. Se* $\deg D = 0$*, então,* $l(D) = 1$ *quando* $D = \mathrm{div}(z)$*,* $z \in K^*$ *e* $l(D) = 0$ *caso contrário.*

Demonstração: Se $D = \mathrm{div}(z)$, então,

$$h \in \mathcal{L}(D) \Rightarrow \mathrm{div}(h) \geq -D \Rightarrow \mathrm{div}(hz) \geq 0 \Rightarrow hz \in \mathcal{L}(0) = k,$$

logo, $\mathcal{L}(D) = zk$ e $l(D) = 1$.

Suponha $l(D) > 0$, então, existe $z \in K^*$, tal que $\mathrm{div}(z) \geq -D$. Pela Fórmula de Produto, $\deg \mathrm{div}(z) = 0 = \deg D$, logo $\mathrm{div}(z) = D$ e $l(D) = 1$. □

Corolário 2.7 *Seja* D *divisor. Se* $\deg D = 2g - 2$*, então,* $l(D) = g$ *quando* D *é linearmente equivalente a* C *e* $l(D) = g - 1$ *caso contrário.*

Demonstração: Pelo Corolário 2.5, $\deg(C - D) = 0$, logo, pelo Lema 2.10

$$l(C - D) = \begin{cases} 1 & \text{se } C \text{ é linearmente equivalente a } D \\ 0 & \text{caso contrário} \end{cases}$$

Pelo Teorema de Riemann-Roch 2.8, se D é equivalente a C teremos $l(D) = g$, e caso contrário, $l(D) = g - 1$. □

Definição 2.14 *A classe de equivalência linear do divisor C é chamada de Classe Canônica. Os divisores da classe canônica serão chamados apenas de canônicos.*

Corolário 2.8 *O divisor D é canônico se, e somente se,* $\deg D = 2g - 2$ *e* $l(D) = g$.

Demonstração: Corolários 2.5 e 2.7. □

Observação 2.5 *Pelos Lema 2.10 e Corolário 2.8,*

(i) quando $g = 0$, *D é canônico se, e somente se,* $\deg D = -2$;

(ii) quando $g = 1$, *D é canônico se, e somente se,* $D = \mathrm{div}(z)$, $z \in K^*$.

Corolário 2.9 *O divisor D é canônico se, e somente se,* $\deg D = 2g - 2$ *e* $l(D) \geq g$.

Demonstração: Corolários 2.7 e 2.8. □

Exemplo 2.5 Neste exemplo determinaremos os divisores canônicos do corpo de funções $K|k$ onde k é corpo com char$k \neq 3$, $K = k(x, y)$, $y^3 = f(x) \in k[x]$ com $\deg f = 4$.

Já sabemos que x possui um único pólo, digamos w_∞, $\deg w_\infty = 1$, $\mathrm{div}_\infty(x) = 3w_\infty, \mathrm{div}_\infty(y) = 4w_\infty$ e $g = 3$. Seja $D := 4w_\infty$, logo $\deg D = 4 \deg w_\infty = 4$ e $l(D) \geq 3$ pois $1, x, y \in \mathcal{L}(D)$. Pelos Corolários 2.9 e 2.5, D é canônico e $l(D) = 3$, então, $\{1, x, y\}$ é uma base para $\mathcal{L}(D)$. Os divisores canônicos positivos são da forma $D + \mathrm{div}(z)$ com $z \in \mathcal{L}(D) \setminus \{0\}$, logo, $z = a + bx + cy$ onde $a, b, c \in k$ não nulos simultâneamente. Então

$$D + \mathrm{div}(z) = \begin{cases} \mathrm{div}_0(a + bx + cy) & \text{se} \quad c \neq 0 \\ \mathrm{div}_0(a + bx) + w_\infty & \text{se} \quad c = 0, b \neq 0 \\ 4w_\infty & \text{se} \quad b = c = 0, a \neq 0 \end{cases}$$

Corolário 2.10 *Um divisor D é especial se, e somente se, $D \leq C'$ para algum divisor canônico C'.*

Demonstração: Por definição, D é especial se $l(D) > \deg D + 1 - g$. Pelo Teorema de Riemann-Roch sabemos que D é especial se, e somente se, $l(C - D) > 0$, isto é, existe $z \in K^*$, tal que $z \in \mathcal{L}(C - D)$, logo, $\mathrm{div}(z) \geq D - C$. Tomamos $C' := C + \mathrm{div}(z)$. □

Pelo Teorema 2.3, se $g = 0$ e $S^{rac}_{K|k} \neq \emptyset$, então, $K|k$ é isomorfa a $k(x)|k$ e, ou seja, $K|k$ é racional. Analisaremos agora, o que acontece quando $g = 0$ e $S^{rac}_{K|k} = \emptyset$.

Teorema 2.9 *Seja $K|k$ um corpo de funções algébricas de gênero g,* char$k \neq 2$ *e $S^{rac}_{K|k} = \emptyset$. Então, $g = 0$ se, e somente se, existem x e $y \in K$ tais que $K = k(x, y)$ e $y^2 = ax^2 + b,\ a, b \in k$.*

Demonstração: Seja C o divisor canônico, então $\deg C = -2$. Tomamos $D := -C$. Temos que $\deg D = 2 > 2g - 2$. Pelo Corolário 2.6, $l(D) = 3 > 0$, logo existe divisor positivo linearmente equialente a D.

Como $S^{rac}_{K|k} = \emptyset$, existe $v \in S_{K|k}$ de grau 2 e $l(v) = 3 > 1$. Seja $x \in \mathcal{L}(v) \setminus k$. Então $\mathrm{div}_\infty(x) = v$, logo, $[K : k(x)] = \deg v = 2$. Portanto, $K = k(x, y)$ onde $y^2 = h(x) \in k[x]$. De $g = 0$ e pelo Exemplo 2.3, $\deg h = 2$. Fazendo a mudança $x \longmapsto x + c$ para algum $c \in k$, podemos normalizar $h(x) = ax^2 + b,\ a, b \in k$. □

Capítulo

3

Corpo de Funções Algébricas de Gênero 1 e 2

Neste capítulo, aplicaremos o Teorema de Riemann-Roch para classificar os Corpos de Funções Algébricas de gênero 1 e 2.

3.1 Corpo de Funções Algébricas de Gênero $g = 1$

Teorema 3.1 *Seja $K|k$ corpo de funções algébricas de gênero g e* char$k \neq 2, 3$. *Então $g = 1$ e $S^{rac}_{K|k} \neq \emptyset$ se, e somente se, existem $x, y \in K$, tais que $K = k(x, y)$ e $y^2 = 4x^3 - g_2x - g_3$ onde $g_i \in k$, $g_2^3 - 27g_3^2 \neq 0$.*

Demonstração: Suponha $g = 1$ e $S^{rac}_{K|k} \neq \emptyset$. Seja $v \in S^{rac}_{K|k}$, como $g = 1$, $l(dv) = d$ para todo $d \in \mathbb{N}$. Então existem $x \in \mathcal{L}(2v) \setminus \mathcal{L}(v)$ e $y \in \mathcal{L}(3v) \setminus \mathcal{L}(2v)$, logo $\text{div}_\infty(x) = 2v, \text{div}_\infty(y) = 3v$ e $[K : k(x)] = 2, [K : k(y)] = 3$. Então $[K : k(x, y)]|2$ e $[K : k(x, y)]|3$. Portanto $[K : k(x, y)] = 1$, ou seja, $K = k(x, y)$.

As 7 funções $y^2, xy, y, x^3, x^2, x, 1$ possuem um único pólo em v de ordem $6, 5, 3, 6, 4, 2, 0$. Logo pertencem ao espaço $\mathcal{L}(6v)$ e como $l(6v) = 6$, são linearmente dependentes. Então existe uma relação não trivial

$$a_1y^2 + a_2xy + a_3y + a_4x^3 + a_5x^2 + a_6x + a_7 = 0,\ a_i \in k.$$

Temos $a_1 \neq 0$ e $a_4 \neq 0$. Fazendo a mudança $y = ay'$, $x = ax', a \in k^*$ e depois dividindo a equação por a_1a^2, podemos supor $a_1 = 1$ e $a_4 = -4$. Então:

$$(y')^2 + a_2'x'y' + a_3'y' - 4(x')^3 + a_5'(x')^2 + a_6'x' + a_7' = 0,$$

onde $a = \dfrac{-4a_1}{a_4}, a_2' = \dfrac{a_2}{a_1}, a_3' = \dfrac{a_3}{a_1a}, a_5' = \dfrac{a_5}{a_1}, a_6' = \dfrac{a_6}{a_1a}$ e $a_7' = \dfrac{a_7}{a_1a}$. Podemos supor também $a_2' = a_3' = 0$. Isto pode ser feito via mudança $y' := \tilde{y} - \dfrac{1}{2}(a_2'x' + a_3')$. Então

$$\tilde{y}^2 + b_1(x')^2 + b_2x' - 4(x')^3 + b_3 = 0,$$

no qual $b_1 = \left(\dfrac{-(a_2')^2}{4} + a_5'\right), b_2 = \left(\dfrac{-a_2'a_3'}{2} + a_6'\right)$ e $b_3 = \left(\dfrac{-(a_3')^2}{2} + a_7'\right)$. Finalmente podemos supor $b_1 = 0$, por meio da mudança $x' = \tilde{x} + \dfrac{b_1}{12}$. Desta maneira obtemos

$$\tilde{y}^2 = 4\tilde{x}^3 + g_2\tilde{x} + g_3,$$

onde $-g_2 = \left(\dfrac{b_1}{12} + b_2\right)$ e $-g_3 = \left(\dfrac{b_1b_2}{12} + \dfrac{b_1^3}{216} + b_3\right)$.

Observamos que a equação $4\tilde{x}^3 + g_2\tilde{x} + g_3 = 0$ possui raízes distintas. Caso contrário, existem $c, d \in k$ tais que $4\tilde{x}^3 - g_2\tilde{x} - g_3 = 4(\tilde{x} - c)^2(\tilde{x} - d)$. Portanto

$$\tilde{y}^2 = 4(\tilde{x} - c)^2(\tilde{x} - d) \Rightarrow \left(\frac{\tilde{y}}{\tilde{x} - c}\right)^2 = 4(\tilde{x} - d) \Rightarrow K = k\left(\frac{y}{x - c}\right) \Rightarrow g = 0,$$

o que é um absurdo. Então o discriminante será não nulo, ou seja,

$$\Delta = g_2^3 - 27g_3^2 \neq 0.$$

Reciprocamente, se $g_2^3 - 27g_3^2 \neq 0$, o polinômio $4x^3 - g_2x - g_3$ é livre de quadrado, então, temos

$$g = \left[\frac{3-1}{2}\right] = 1.$$

O único pólo de x é racional. □

Definição 3.1 *Os corpos de funções de gênero um são chmados de corpos de funções elípticas. A forma obtida no Teorema 3.1 para representá-los é chamada de Forma Normal de Weierstrass.*

Lembramos que $\deg \operatorname{div}(z) = 0$ para todo $z \in K$. Então seria natural propor o seguinte problema, que é conhecido como Problema de Abel:

Quando um divisor de grau zero é divisor de uma função não nula?

Lembrando a estrutura de grupo do conjunto de divisores e suas propriedades, podemos considerar o seguinte grupo quociente:

Definição 3.2 *O Grupo das Classes é:*

$$C^0_{K|k} := \frac{\{D \in \mathcal{D}_K \mid \deg D = 0\}}{\{\operatorname{div}(z) \mid z \in K^*\}}.$$

A próxima proposição é o primeiro resultado para identificar este grupo.

Proposição 3.1 *Sejam $K|k$ um corpo de funções elípticas e $v_0 \in S^{rac}_{K|k}$. Então temos a seguinte bijeção:*

$$\begin{array}{rccc} \varphi: & S^{rac}_{K|k} & \longrightarrow & C^0_{K|k} \\ & v & \longmapsto & \overline{v - v_0} \end{array}$$

Demonstração: Seja $\overline{v_1 - v_0} = \overline{v_2 - v_0}$; $v_1, v_2 \in S^{rac}_{K|k}$. Logo $v_1 - v_2 = \operatorname{div}(z), z \in K^*$. Se $v_1 \neq v_2$, então, $div_\infty(z) = v_2$, logo $[K : k(z)] = 1$, ou, $g = 0$, o que é um absurdo. Portanto $v_1 = v_2$ e φ é injetora.

Para a sobrejetividade, seja $D \in \mathcal{D}_K$ tal que $\deg D = 0$, logo $\deg(D + v_0) = 1$. Pelo Corolário 2.6, $l(D + v_0) = 1$, então, existe um divisor positivo linearmente equivalente a $D + v_0$ de grau 1, ou seja, existe $v \in S^{rac}_{K|k}$, tal que $v \sim D + v_0$. Portanto, $\overline{D} = \overline{v - v_0}$ e φ é sobrejetora. □

Em particular, $S^{rac}_{K|k}$ terá estrutura de um grupo abeliano induzida por φ cujo elemento neutro é v_0. Denotaremos sua operação por $\oplus$ e a subtração por $\ominus$.

Seja $D \in \mathcal{D}_K$ da forma

$$D = \sum_{i=1}^{n} v_i - \sum_{i=1}^{m} w_i, \quad v_i, w_i \in S^{rac}_{K|k}.$$

Se $k = \overline{k}$, todo divisor é dessa forma, pois não supomos os $v_i's$ e $w_i's$ diferentes entre si. Nesse caso, D é divisor de uma função não nula se $n = m$ e

$$\bigoplus_{i=1}^{n} v_i = \bigoplus_{i=1}^{m} w_i.$$

A seguir descreveremos explicitamente a adição $\oplus$ em $S_{K|k}^{rac}$ para um corpo de funções elípticas quando char$k \neq 2, 3$ e $k = \overline{k}$. A aplicação

$$\begin{cases} S_{K|k}^{rac} & \longrightarrow & \{(a,b) \in k^2 \mid b^2 = 4a^3 - g_2a - g_3\} \cup \{(\infty, \infty)\} \\ v & \longmapsto & (x(v), y(v)) \end{cases}$$

está bem definida, pois, $x(v) = \infty$ se, e somente se, $y(v) = \infty$. De fato,

$$v(y) = \frac{1}{2}v(y^2) = \frac{1}{2}v(4x^3 - g_2x - g_3) \begin{cases} \geq 0 & \text{se} \quad v(x) \geq 0 \\ < 0 & \text{se} \quad v(x) < 0 \end{cases}$$

e é uma bijeção. O único pólo de x é o elemento neutro de $S_{K|k}^{rac}$.

Em particular, $C_{K|k}^{0}$ possui estrutura de uma curva cúbica plana projetiva quando $k = \overline{k}$.

Teorema 3.2 *Sejam (x_i, y_i), $i = 1, 2, 3$, pontos da cúbica $y^2 = 4x^3 - g_2x - g_3$. Então, $\bigoplus_{i=1}^{3}(x_i, y_i) = (\infty, \infty)$ se, e somente se, esses pontos são colineares.*

Demonstração: Sejam $v_1, v_2 \in S_{K|k}^{rac}$, $(x_i, y_i) = (x(v_i), y(v_i))$, $i = 1, 2$ e $(x_1, y_1) \neq (x_2, y_2)$. Considere a reta secante dada por $f := y - \beta x - \gamma$, $\beta = \dfrac{y_2 - y_1}{x_2 - x_1}$ e $\gamma = y_1 - \beta x_1$, que passa por esses pontos. Então f possui zeros em v_1, v_2, ou seja, $\text{div}_0(f) \geq v_1 + v_2$ e

$$\text{div}_\infty(f) = \text{div}_\infty(y - \beta x - \gamma) = 3v_\infty.$$

Pela Fórmula de Produto, existe $v_3 \in S_{K|k}^{rac}$ tal que $\text{div}(f) = v_1 + v_2 + v_3 - 3v_\infty$, assim $v_1 \oplus v_2 \oplus v_3 = v_\infty$. Pela construção $(x_3, y_3) = (x(v_3), y(v_3))$ é o terceiro ponto da reta secante.

O caso em que $x_1 = x_2 \neq \infty,\ y_1 = y_2$ é parecido com o caso anterior. Lembramos que a reta dada por f neste caso, será a reta tangente à cúbica no ponto $(x_1, y_1) = (x_2, y_2)$.

Se $x_1 = x_2 \neq \infty$ e $y_1 = -y_2$, considere a reta secante dada por $f = x - x_1$ que passa por (x_1, y_1) e $(x_2, y_2) = (x_1, -y_1)$. Então $(x_1, y_1) \oplus (x_2, y_2) = (\infty, \infty)$e pela hipótese, $(x_3, y_3) = (\infty, \infty)$. Pela definição da estrutura do grupo da cúbica, os pontos são colineares. □

Observação 3.1 *O ponto (x_3, y_3) no Teorema 3.2, quando $x_1 \neq x_2$, é dado por*

$$x_3 = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ e } y_3 = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1)$$

Proposição 3.2 *(Homogeneidade em $g = 1$) Sejam $K|k$ um corpo de funções elípticas e $v_1, v_2 \in S^{rac}_{K|k}$. Então existe um automorfismo α de $K|k$ tal que $v_2 = v_1 \circ \alpha$.*

Demonstração: Defina $v_0 := v_2 \ominus v_1,\ (x_0, y_0) := \big(x(v_0), y(v_0)\big)$. Podemos supor $v_1 \neq v_2$, pois caso contrário, bastaria escolher α como a aplicação identidade. Então $v_0 \neq v_\infty$, logo, x_0, y_0 não são infinitos e, portanto, $x_0, y_0 \in k$. Definimos:

$$\alpha(x) = \frac{1}{4}\left(\frac{y - y_0}{x - x_0}\right)^2 - x_0 - x,\ \alpha(y) = -y_0 - \left(\frac{y - y_0}{x - x_0}\right)\big(\alpha(x) - x_0\big).$$

Temos $y^2 = 4x^3 - g_2x - g_3$, e pela Observação 3.1, $\big(\alpha(x), \alpha(y)\big)$ também é ponto da cúbica, isto é, $\alpha(y)^2 = 4\alpha(x)^3 - g_2\alpha(x) - g_3$. Assim, temos um automorfismo α de $K = k(x, y)|k$. Para cada $v \in S^{rac}_{K|k}$ temos:

$$\big(x(v \circ \alpha), y(v \circ \alpha)\big) = \Big(\big(\alpha(x)\big)(v), \big(\alpha(y)\big)(v)\Big) = \big(x(v), y(v)\big) \oplus \big(x(v_0), y(v_0)\big),$$

logo, $v \circ \alpha = v \oplus v_0$ para todo $v \in S^{rac}_{K|k}$, em particular, $v_1 \circ \alpha = v_1 \oplus v_0 = v_2$. □

Teorema 3.3 *Sejam $K|k$ e $\widetilde{K}|k$ corpos de funções algébricas,* char$k \neq 2, 3$ *de gênero 1. Então $K|k \cong \widetilde{K}|k$ se, e somente se, existe $\mu \in k^*$, tal que $g_2 = \mu^4\tilde{g}_2$ e $g_3 = \mu^6\tilde{g}_3$, onde $g_2, g_3, \tilde{g}_2$ e $\tilde{g}_3$ são os coeficientes das formas de Weierstrass de $K|k$ e $\widetilde{K}|k$.*

Demonstração: Suponhamos que exista um k-isomorfismo $\alpha : K \longrightarrow \widetilde{K}$ e sejam v_∞, $\tilde{v}_\infty$ os únicos pólos de x, $\tilde{x}$ respectivamente. Consideremos $v = \tilde{v}_\infty \circ \alpha \in S^{rac}_{K|k}$. Pela

Proposição 3.2, existe um automorfismo β de $K|k$ tal que $v_\infty = v \circ \beta$. Seja $\gamma = \alpha \circ \beta$, logo $\gamma : K \longrightarrow \widetilde{K}$ é um $k-$isomorfismo e $v_\infty = \tilde{v}_\infty \circ \gamma$. Como $\mathrm{div}_\infty(x) = 2v_\infty$ e $\mathrm{div}_\infty(y) = 3v_\infty$, claramente:

$$\begin{aligned} &\mathrm{div}_\infty(\gamma(x)) = 2\tilde{v}_\infty, \quad l(2\tilde{v}_\infty) = 2, \quad \mathcal{L}(2\tilde{v}_\infty) = k \oplus k\tilde{x}, \\ &\mathrm{div}_\infty(\gamma(y)) = 3\tilde{v}_\infty, \quad l(3\tilde{v}_\infty) = 3, \quad L(3\tilde{v}_\infty) = k \oplus k\tilde{x} \oplus k\tilde{y}. \end{aligned}$$

Logo, $\gamma(x) = a + b\tilde{x},\ a, b \in k,\ b \neq 0$ e $\gamma(y) = e + d\tilde{x} + c\tilde{y},\ c, d, e \in k,\ c \neq 0$. Como $y^2 = 4x^3 - g_2x - g_3$, temos:

$$\gamma(y)^2 = 4\gamma(x)^3 - g_2\gamma(x) - g_3 \Rightarrow (e + d\tilde{x} + c\tilde{y})^2 = 4(a + b\tilde{x})^3 - g_2(a + b\tilde{x}) - g_3. \quad (3.1)$$

Dividindo a equação (3.1) por c^2 e comparando com a equação $\tilde{y}^2 = 4\tilde{x}^3 - \tilde{g}_2\tilde{x} - \tilde{g}_3$ chegamos em:

$$d = e = a = 0,\ \frac{b^3}{c^2} = 1,\ \tilde{g}_2 = g_2\frac{b}{c^2} \text{ e } \tilde{g}_3 = \frac{g_3}{c^2}.$$

Seja $\mu = \dfrac{c}{b}$, logo $g_2 = \mu^4\tilde{g}_2$ e $g_3 = \mu^6\tilde{g}_2$.

Reciprocamente, escolhendo $\gamma(x) = \mu^2\tilde{x},\ \gamma(y) = \mu^3\tilde{y}$ obtemos um $k-$isomorfismo $\gamma : K \longrightarrow K$. □

Se $K \simeq \widetilde{K}$, então:

$$\frac{g_2^3}{g_3^2} = \frac{\mu^{12}(\tilde{g}_2)^3}{\mu^{12}(\tilde{g}_3)^2} = \frac{(\tilde{g}_2)^3}{(\tilde{g}_3)^2},$$

isto é, $\dfrac{g_2^3}{g_3^2}$ é um invariante de $K|k$. Para evitar o anulamento do denominador, consideramos o quociente $\dfrac{g_2^3}{g_2^3 - 27g_3^2} \in k$.

Definição 3.3 *O quociente* $J = \dfrac{g_2^3}{g_2^3 - 27g_3^2}$ *é um invariante de* $K|k$ *chamado de Invariante Modular.*

Observe que $\{\alpha \in \mathrm{Aut}(K|k) \mid v \circ \alpha = v\}$ é um subgrupo de $\mathrm{Aut}(K|k)$. A seguir identificaremos este subgrupo.

Corolário 3.1 *Sejam $K|k$ um corpo de funções algébricas,* $\mathrm{char}k \neq 2, 3$*, $g = 1$ e $v \in S^{rac}_{K|k}$. Então $\{\alpha \in \mathrm{Aut}(K|k) \mid v \circ \alpha = v\}$ é isomorfo a*

- $\{\mu \in k \mid \mu^6 = 1\}$ *se* $J = 0$*;*
- $\{\mu \in k \mid \mu^4 = 1\}$ *se* $J = 1$*;*
- $\{-1, 1\}$ *se* $J \neq 0, 1$.

Demonstração: Pela Proposição 3.2 podemos supor $v = v_\infty$, e da prova do Teorema 3.3, os automorfismos α de $K|k$ tais que $v_\infty \circ \alpha = v_\infty$ são dados por $x \longmapsto \mu^2 x$ e $y \longmapsto \mu^3 y$ onde $\mu \in k$ satisfaz $g_2 = \mu^4 g_2,\ g_3 = \mu^6 g_3$.

Se $J = 0$ então $g_2 = 0$ e $g_3 \neq 0$, logo, $\mu^6 = 1$.

Se $J = 1$ então $g_2 \neq 0$ e $g_3 = 0$, logo, $\mu^4 = 1$.

Se $J \neq 0, 1$ então $g_2, g_3 \neq 0$, logo, $\mu^4 = 1$ e $\mu^6 = 1$, ou seja, $\mu = \pm 1$. □

A seguir, escrevemos todas as classes de isomorfismos dos corpos de funções elípticas sobre k com o invariante J.

Se $J = 0$, então, $g_2 = 0$,

$$\begin{cases} \{\text{classes de isomorfismo com } J = 0\} & \longrightarrow & \dfrac{k^*}{(k^*)^6} \\ k(x, \sqrt{4x^3 - g_3}) & \longmapsto & \left(g_3 \bmod (k^*)^6\right) \end{cases}$$

Se $J = 1$, então, $g_3 = 0$,

$$\begin{cases} \{\text{classes de isomorfismo com } J = 1\} & \longrightarrow & \dfrac{k^*}{(k^*)^4} \\ k(x, \sqrt{4x^3 - g_2 x}) & \longmapsto & \left(g_3 \bmod (k^*)^4\right) \end{cases}$$

Se $J \neq 0, 1$, então, $g_2 \neq 0, g_3 \neq 0$. Consideremos $I := \dfrac{g_2^3}{g_3^2} = 27\dfrac{J}{J-1}$,

$$\begin{cases} \{\text{classes de isomorfismo com } J \neq 0, 1\} & \longrightarrow & \dfrac{k^*}{(k^*)^2} \\ k(x, \sqrt{4x^3 - g_2 x - g_3}) & \longmapsto & \left(\dfrac{g_3}{g_2} \bmod (k^*)^2\right) \end{cases}$$

A inversa desta aplicação é dada por $(c \bmod (k^*)^2) \longmapsto k(x, \sqrt{4x^3 - c^2Ix - c^3I})$.

Então obtemos os seguintes colorários:

Corolário 3.2 *Seja $k = \overline{k}$ e $chark \neq 2, 3$, então,*

$$\begin{cases} \{\textit{classes de isomorfismo de corpos de funções de } \ g = 1\} & \longrightarrow \quad k \\ K|k & \longmapsto \quad J, \end{cases}$$

é uma bijeção.

Corolário 3.3 *Se $k = \mathbb{R}$, então, os corpos de funções elípticas sobre os $\mathbb{R}$ são dados por:*

$$\begin{array}{lll} \mathbb{R}(x, \sqrt{4x^3 \pm 1}) & se & J = 0 \\ \mathbb{R}(x, \sqrt{4x^3 \pm x}) & se & J = 1 \\ \mathbb{R}(x, \sqrt{4x^3 - Ix \pm I}) & se & J \neq 0, 1 \ onde \ I = 27\dfrac{J}{J-1}. \end{array}$$

Seja $K|\mathbb{R}$ corpo de funções elípticas, ou seja, $K = \mathbb{R}(x, y)$, $y^2 = 4x^3 - g_2x - g_3$ e $g_2 - 27g_3^2 \neq 0$. Seja

$$4x^3 - g_2x - g_3 = 4(x - e_1)(x - e_2)(x - e_3), e_i \in \mathbb{C},$$

então:

$$g_2^3 - 27g_3^2 = 16 \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2 \neq 0.$$

Observamos que $g_2^3 - 27g_3^2$ é invariante de $K|\mathbb{R}$ e

(i) se $g_2^3 - 27g_3^2 > 0$, então, $e_i \in \mathbb{R}$ e $S_{K|k}^{rac}$ consiste em dois caminhos fechados;

(ii) se $g_2^3 - 27g_3^2 < 0$ apenas uma raiz é real, então, $S_{K|k}^{rac}$ consiste apenas de um caminho fechado.

Agora sejam $K = k(x, y)$ um corpo de funções algébricas, $k = \overline{k}$ e $chark \neq 2, 3$, $y^2 = \prod_{i=1}^{4}(x - e_i), e_i \in k$ distintos e $g = 1$. Queremos definir o invariante modular neste caso.

Primeiramente, faremos a substituição $\tilde{x} := \dfrac{1}{x - e_4}$, isto é, $x = \dfrac{1}{\tilde{x}} + e_4$. Então,

$$y^2 = \prod_{i=1}^{4}(x - e_i) = \prod_{i=1}^{4}\left(\frac{1}{\tilde{x}} + e_4 - e_i\right) = \frac{1}{\tilde{x}^4}\prod_{i=1}^{3}\big(1 + (e_4 - e_i)\tilde{x}\big),$$

logo,

$$(y\tilde{x}^2)^2 = \prod_{i=1}^{3}(e_4 - e_i)\left(\tilde{x} - \frac{1}{e_i - e_4}\right).$$

Sejam $a^{-2} := \prod_{i=1}^{3}(e_4 - e_i)$, $\tilde{y} := ay\tilde{x}^2$, logo $K = k(\tilde{x}, \tilde{y})$ tal que

$$\tilde{y}^2 = \prod_{i=1}^{3}\left(\tilde{x} - \frac{1}{e_i - e_4}\right).$$

Agora, fazendo a mudança $x' := \left(\tilde{x} - \dfrac{1}{e_3 - e_4}\right) b^2$, onde $b^2 = \dfrac{(e_2 - e_4)(e_3 - e_4)}{(e_2 - e_3)}$, teremos a equação

$$(\tilde{y}b^3)^2 = x'(x' - 1)(x' - \lambda),$$

onde $\lambda = \dfrac{e_1 - e_3}{e_1 - e_4} : \dfrac{e_2 - e_3}{e_2 - e_4}$. Seja $y' := \tilde{y}b^3$, logo, teremos $K = k(x', y')$ tal que

$$y'^2 = x'(x' - 1)(x' - \lambda).$$

Definindo $x' := \dfrac{(\lambda - 1)}{3} + \bar{x}$ e $y' = \dfrac{\bar{y}}{2}$ teremos:

$$\bar{y}^2 = 4\bar{x}^3 - \frac{4}{3}(\lambda^2 - \lambda + 1)\bar{x} + \frac{4}{27}(-2\lambda^3 + 3\lambda^2 + 3\lambda - 2),$$

e, assim, obtemos a forma normal de Weierstrass com $J = \dfrac{4}{27}\dfrac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1 - \lambda)^2}$.

Observação 3.2 *O valor λ descrito acima, não é invariante do corpo de funções, pois para qualquer elemento do conjunto* $\left\{\lambda,\ 1 - \lambda,\ \dfrac{1}{\lambda},\ \dfrac{1}{1 - \lambda},\ \dfrac{\lambda - 1}{\lambda}, \dfrac{\lambda}{\lambda - 1}\right\}$ *encontraremos o mesmo valor para J.*

Teorema 3.4 *Seja $K|\mathbb{R}$ de gênero $g = 1$. Então $S^{rac}_{K|\mathbb{R}} = \emptyset$, se e somente se, existem $x, y \in K$, tal que $K = \mathbb{R}(x, y)$, onde $y^2 = -(x^2 + 1)(x^2 + \mu)$ e $0 < \mu < 1$.*

Demonstração: Seja $v \in S_{K|\mathbb{R}}$ e considere o divisor $D := v$. Então $\deg D = 2$, $l(D) = 2$ e existe $x \in \mathcal{L}(v) \setminus \mathbb{R}$, tal que $\mathrm{div}_\infty(x) = v$. Pela Igualdade Fundamental, $[K : \mathbb{R}(x)] = \deg \mathrm{div}_\infty(x) = 2$, logo, $K = \mathbb{R}(x, y)$, onde $y^2 = h(x) \in \mathbb{R}[x]$ é livre de quadrado. Como $g = 1$, $\deg h(x) = 3$ ou 4, e existe bijeção

$$\{v \in S^{rac}_{K|\mathbb{R}} \mid v(x) \geq 0\} \longleftrightarrow \{(a, b) \in \mathbb{R}^2 \mid b^2 = h(a)\}.$$

Mas $S^{rac}_{K|\mathbb{R}} = \emptyset$, então, $h(x) = 0$ não possui raízes reais e, portanto, $\deg h(x) = 4$. Logo,

$$h(x) = c(x - \alpha)(x - \bar{\alpha})(x - \beta)(x - \bar{\beta}),\ \alpha, \beta \in \mathbb{C} \setminus \mathbb{R}.$$

Podemos supor, $\mathrm{Im}\alpha > 0$ e $\mathrm{Im}\beta > 0$. Seja $\alpha = a + bi$ e pela mudança $\tilde{x} := \dfrac{x - a}{b}$, obtemos:

$$(x - \alpha)(x - \bar{\alpha}) = (\tilde{x}b - bi)(\tilde{x}b + bi) = b^2(\tilde{x} - i)(\tilde{x} + i) = b^2(\tilde{x}^2 + 1).$$

Então podemos supor $\alpha = i$, ou seja, $h(x) = c(x^2 + 1)(x - \beta)(x - \bar{\beta})$. Substituindo $\tilde{x} = \dfrac{ax + b}{bx + a}$ e $\tilde{y} = (b\tilde{x} + a)^2 y$ e escolhendo $a, b \in \mathbb{R}$, podemos supor $\mathrm{Re}\beta = 0$ e $\mu := \mathrm{Im}\beta < 1$. Como $h(x)$ é livre de quadrado, então $c < 0$ e, transformando $y^2 \to dy^2$, onde $-c = d$ podemos supor $c = -1$. □

Da demosntração acima, obtemos o invariante modular de $\mathbb{C}(x, y)|\mathbb{C}$ que será dado por:

$$J = 1 + \frac{4}{27}\left(\frac{(\lambda + 1)(\lambda - 2)(\lambda - \frac{1}{2})}{\lambda(\lambda - 1)}\right)^2 \geq 1.$$

3.2 Corpos de Funções de Gênero $g \geq 2$

Definição 3.4 *Sejam $K|k$ um corpo de funções algébricas de gênero $g \geq 2$ e C seu divisor canônico. Definimos como Corpo Canônico, denotado por K_0, o subcorpo de K gerado pelas funções $\dfrac{x}{y}$; $x, y \in \mathcal{L}(C) \setminus \{0\}$.*

Observamos que K_0 não depende do divisor canônico C. De fato, se C' é outro divisor canônico, então, $C' = C + \mathrm{div}(z),\ z \in K^*$, logo $\mathcal{L}(C') = \frac{1}{z}\mathcal{L}(C)$.

Alternativamente, K_0 é gerado por funções $\frac{\lambda}{\mu}$, onde λ, μ percorrem as diferenciais regulares não nulas.

Suponhamos $C \geq 0$, sendo assim $1 \in \mathcal{L}(C)$ e, logo, K_0 é gerado por $\mathcal{L}(C)$. Se $1, x_1, \ldots, x_{g-1}$ formam uma base para $\mathcal{L}(C)$, então, $K_0 = k(x_1, \ldots, x_{g-1})$. Como $g \geq 2$, então, $k \subset K_0$. Então $K_0|k$ é corpo de funções em uma variável e $[K : K_0] < \infty$.

Teorema 3.5 *Seja $K|k$ corpo de gênero g e* $\mathrm{char} k \neq 2$. *Temos $g = 2$ se, e somente se, existem $x, y \in K$ tais que $K = k(x, y),\ y^2 = h(x) \in k[x]$ livre de quadrados e* $\deg h = 5$ *ou* 6.

Demonstração: Seja C um divisor canônico, então pelo Corolário 2.5, $\deg C = 2$ e $l(C) = 2$. Como $l(C) > 0$, existe um divisor positivo linearmente equivalente a C, assim, podemos supor $C \geq 0$. Sendo $l(C) > 1$, existe $x \in \mathcal{L}(C) \setminus k$, tal que $\mathrm{div}_\infty(x) \leq C$. Já que $[K : k(x)] = \deg \mathrm{div}_\infty(x) \leq \deg C = 2$ e $K \neq k(x)$, pelo Teorema 2.3, $[K : k(x)] = 2$. Logo, existe $y \in K$, tal que $K = k(x, y),\ y^2 = h(x)$ com $h(x) \in k[x]$ livre de quadrados. Pelo Exemplo 2.3, temos:

$$g = \left[\frac{\deg h - 1}{2}\right] = 2,$$

então $\deg h(x) = 5$ ou 6. □

Definição 3.5 *Diremos que $K|k$ é hiperelíptico se, e somente se, $K|k$ possui um subcorpo quadrático racional, ou seja, existe $x \in K$, tal que $[K : k(x)] = 2$.*

Observação 3.3 *Se $K|k$ é hiperelíptico e* $\mathrm{char} k \neq 2$, *então, existe $y \in K$, tal que $K = k(x, y),\ y^2 = h(x)$ com $h(x) \in k[x]$ livre de quadrado e* $\deg h(x) = 2g + 1$ *ou* $2g + 2$.

Teorema 3.6 *Seja $K|k$ hiperelíptico, então,*

(a) os divisores canônicos positivos são da forma

$$(g-1)\mathrm{div}_\infty(x) + \mathrm{div}(c_0 + c_1 x + \cdots + c_{g-1}x^{g-1}),\ x \in K, c_i \in k \text{ não todos nulos};$$

(b) $K_0 = k(x)$, para algum $x \in K$.

Demonstração: *(a)* Seja $C := (g-1)\mathrm{div}_\infty(x),\ x \in K$. Já que $\deg \mathrm{div}_\infty(x) = [K : k(x)] = 2$, teremos $\deg C = (g-1)\deg \mathrm{div}_\infty(x) = 2g-2$. Afirmamos que $x^0, x, \ldots, x^{g-1} \in \mathcal{L}(C)$, de fato,

(i) $x^0 = 1$ e como $C \geq 0$ temos $1 \in \mathcal{L}(C)$;

(ii) se $x \notin \mathcal{L}(C)$, então,

$$\mathrm{div}(x) = \mathrm{div}_0(x) - \mathrm{div}_\infty(x) < -(g-1)\mathrm{div}_\infty(x) \Rightarrow \mathrm{div}_0(x) < -(g-2)\mathrm{div}_\infty(x),$$

o que é um absurdo pois $\mathrm{div}_0(x) \geq 0$ e $-(g-2)\mathrm{div}_\infty(x) < 0$.

(iii) Se $x^2 \notin \mathcal{L}(C)$, então,

$$2\mathrm{div}_0(x) < -(g-3)\mathrm{div}_\infty(x),$$

o que é um absurdo.

Analogamente, verifica-se que $x^3, \ldots, x^{g-1} \in \mathcal{L}(C)$. Então $l(C) \geq g$ e pelos Corolários 2.9 e 2.5, C é canônico e $l(C) = g$. Portanto, $\mathcal{L}(C) = \bigoplus_{i=0}^{g-1} kx^i$. Como os divisores canônicos positivos são da forma $C + \mathrm{div}(z)$ com $z \in \mathcal{L}(C)$, e $z = c_0x^0 + c_1x + \cdots + c_{g-1}x^{g-1}, c_i \in k$ não todos nulos, chegamos ao resultado esperado.

(b) Como $g \geq 2$ e $C \geq 0$, então, $k(x) = k(x^1, \ldots, x^{g-1}) = K_0$. □

Observação 3.4 *Se $K|k$ corpo de gênero $g \geq 2$ e K_0 o subcorpo canônico de $K|k$, então, K_0 é o corpo gerado por $\mathcal{L}(C)$ onde C é um divisor canônico positivo.*

Teorema 3.7 *Se K' for um subcorpo quadrático racional de $K|k$, então $K_0 = K'$.*

Demonstração: Como K' é um subcorpo quadrático racional, então, existe $x \in K$, tal que $K' = k(x)$ e $[K : k(x)] = 2$. Pelo Teorema 3.6, $K' = K_0$. □

Exemplo 3.1 Considere $K = k(x, y)$ com char$k \neq 3$ e $y^3 = h(x) \in k[x]$ de grau 4 livre de quadrados.

Se $g = 3$, pelo Exemplo 2.5, $C := \mathrm{div}_\infty(y)$ é divisor canônico e $\{1, x, y\}$ forma uma base para $\mathcal{L}(C)$. Portanto, $\mathcal{L}(C) = k \oplus kx \oplus ky$ e $K_0 = k(x, y) = K$. Com isso, vemos que não existe corpo quadrático racional, isto é, $K|k$ não é hiperelíptico.

Lema 3.1 *Sejam $K|k$ corpo de gênero g e C divisor canônico, desse modo,*

se $g \geq 1$, então, $l(C - v) = l(C) - 1$, para todo $v \in S^{rac}_{K|k}$;

se $g \geq 2$ e K não é hiperelíptico, então, $l(C - v - w) = l(C) - 2$, para todo $v, w \in S^{rac}_{K|k}$.

Demonstração: Aplicando o teorema de Riemann-Roch para $C, C - v$ e $C - v - w$ obtemos

$$l(C) = g \text{ e } \deg C = 2g - 2; \tag{3.2}$$

$$l(C - v) = g - 2 + l(v); \tag{3.3}$$

$$l(C - v - w) = g - 3 + l(v + w). \tag{3.4}$$

Subtraindo (3.2) de (3.3) e (3.2) de (3.4) obtemos:

$$l(C - v) = l(C) - 2 + l(v) \text{ e } l(C - v - w) = l(C) - 3 + l(v + w).$$

Agora, basta provar que $\mathcal{L}(v) = k, \mathcal{L}(v + w) = k$. Se existe $x \in \mathcal{L}(v) \setminus k$, então, $[K : k(x)] = \deg \mathrm{div}_\infty(x) = \deg v = 1$. Logo $K = k(x)$ e pelo Teorema 2.3 $g = 0$, o que é um absurdo, portanto, $\mathcal{L}(v) = k$. Se existe $x \in \mathcal{L}(v+w)\setminus k$, então, $[K : k(x)] = \deg \mathrm{div}_\infty(x) \leq \deg v + \deg w = 2$. Logo, $K = k(x)$ ou $[K : k(x)] = 2$ e pelo Teoremas 2.3 e a Definição 3.5, $g = 0$ ou K é hiperelíptico, o que é um absurdo, portanto, $\mathcal{L}(v + w) = k$. □

Teorema 3.8 *Seja $K|k$ com $k = \overline{k}$ e $g \geq 2$. Se $K|k$ não admite um subcorpo quadrártico racional, então, $K_0 = K$.*

Demonstração: Sejam C um divisor canônico positivo e $w \in S^{rac}_{K|k}$ tal que $w \leq C$, isto é, $w \in \mathrm{Supp}(C)$. Considere $v \in S_{K_0|k}$, tal que w é um prolongamento de v normalizado. Sejam $w_1 = w, w_2, \ldots, w_m$ pontos de $S_{K|k}$ acima de v, isto é, as normalizações dos prolongamentos de v a K, $e_1, \ldots, e_m$ os índices de ramificação e $f_1, \ldots, f_m$ os índices de inércia. Defina $E := \sum_{i=1}^{m} e_i w_i$, logo,

$$\deg E = \sum e_i \deg w_i = \sum e_i [k_{w_i} : k_v][k_v : k] = \sum e_i f_i \deg v = [K : K_0] \deg v = [K : K_0],$$

já que $k = \overline{k}$ então, $\deg v = 1$. Como $w \leq E$, então:

$$C - w \geq C - E \Rightarrow \mathcal{L}(C - E) \subseteq \mathcal{L}(C - w).$$

Sejam $x \in \mathcal{L}(C - w)$ e $z \in \mathcal{L}(C) \setminus \mathcal{L}(C - w)$ que existe pelo Lema 3.1. Considere $t = \dfrac{x}{z} \in K_0$, logo, por construção, $w(t) > 0$ e, assim, $v(t) \geq 1$. Desse modo, para todo i

$$e_i v(t) \geq e_i \Rightarrow w_i(t) \geq e_i \Rightarrow w_i(x) \geq e_i + w_i(z),$$

pela definição da função t. Logo, $x \in \mathcal{L}(C - E)$. Portanto, teremos:

$$\mathcal{L}(C - w) = \mathcal{L}(C - E).$$

Suponhamos, por absurdo, $K \neq K_0$, ou seja, $\deg E \geq 2$, logo, existe $w' \in \{w_1, \ldots, w_m\}$, tal que $w + w' \leq E$. Como $\mathcal{L}(C - w) = \mathcal{L}(C - E)$ e, claramente, $C - E \leq C - w - w' \leq C - w$ teremos $\mathcal{L}(C - w - w') = \mathcal{L}(C - w)$, e pelo Lema 3.1, K será hiperelíptico, o que é um absurdo. Portanto, $K = K_0$. □

Capítulo

4

Apêndice

Nesse Apêndice faremos uma revisão de alguns conceitos e resultados utilizados nos capítulos anteriores.

4.1 Pontos no Infinito

As retas $aX + bY + c$ e $aX + bY + c'$ com $c \neq c'$ não se cruzam a distância finita, assim como a hipérbole $XY = 1$ e os eixos coordenados. Esses são exemplos de que há interseções "faltando", logo, para considerar esses pontos iremos introduzir o conceito de pontos no infinito.

4.1.1 O Plano Projetivo

Consideremos o plano afim no espaço tridimensional, por exemplo, o plano π de equação $z = 1$. Cada ponto do plano π determina uma reta passando pela origem e pelo ponto dado, logo, cada reta de π determina um plano passando pela origem.

Definição 4.1 *O Plano Projetivo $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional passando pela origem.*

Analisando o exemplo visto acima, temos o plano π que se identifica naturalmente com um subconjunto de $\mathbb{P}^2$, o qual ainda denotaremos por π. Os pontos de $\mathbb{P}^2 \setminus \pi$ são chamados *pontos no infinito.*

Denotaremos por $(x : y : z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem O a um ponto $(x, y, z) \neq O$. Chamaremos x, y, z de *coordenadas homogêneas* do ponto $(x : y : z)$ relativas à base canônica $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

Por definição, temos $(x : y : z) = (x', y', z')$ se, e somente se, existe uma constante $t \neq 0$, tal que $(x, y, z) = t(x', y', z')$.

Em geral, fixada uma base qualquer no espaço tridimensional, as coordenadas de um ponto não nulo relativas a essa base são chamadas de *coordenadas homogêneas* do ponto correspondente de $\mathbb{P}^2$. Coordenadas homogêneas de um ponto de $\mathbb{P}^2$ só estão bem definidas a menos de um fator escalar não nulo.

Para introduzir a topologia quociente em $\mathbb{P}^2$, considere a aplicação:

$$\begin{array}{rccc} q: & \mathbb{R}^3 - \{0\} & \longrightarrow & \mathbb{P}^2 \\ & (x, y, z) & \longmapsto & (x : y : z) \end{array}$$

Dizemos que um subconjunto $U \subset \mathbb{P}^2$ é *aberto* se $q^{-1}(U)$ é aberto em $\mathbb{R}^3 - \{0\}$ com sua topologia usual.

Estabelecemos assim, em $\mathbb{P}^2$ uma noção de vizinhança, segundo qual dois pontos de $\mathbb{P}^2$ estão próximos se as retas associadas em $\mathbb{R}^3$ formam um ângulo pequeno.

O subconjunto

$$\mathbb{A}^2 = \{(x : y : z) \in \mathbb{P}^2 \mid z \neq 0\},$$

é aberto e denso em $\mathbb{P}^2$, pois $q^{-1}(\mathbb{A}^2)$ é o complementar do plano $z = 0$ em $\mathbb{R}^3$, logo, é aberto e denso em $\mathbb{R}^3 - \{0\}$.

Agora, considerando a aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{R}^2 & \longrightarrow & \mathbb{A}^2 \subset \mathbb{P}^2 \\ & (x, y) & \longmapsto & (x : y : 1) \end{array}$$

é uma bijeção contínua com inversa contínua, desse modo, podemos considerar o plano afim $\mathbb{R}^2$ como contido em $\mathbb{P}^2$ e o identificaremos com $\mathbb{A}^2$.

4.1.2 O Plano Projetivo

Definição 4.2 *O espaço projetivo* $\mathbb{P}(V)$ *associado a um espaço vetorial* V *é o conjunto dos subespaçoes de* V *de dimensão* 1.

Se $V = K^{n+1}$, escrevemos $\mathbb{P}^n_K = \mathbb{P}(V)$ ou apenas $\mathbb{P}^n$. As *coordenadas homogêneas* de um ponto $P \in \mathbb{P}(V)$, relativas a uma base $\{v_0, \ldots, v_n\}$ de V, são as coordenadas $(x_0, \ldots, x_n)$ de um vetor não nulo do subespaço unidimensional representado por P.

Fixada a base, escrevemos $P = (x_0 : \cdots : x_n)$ para indicar um ponto com essas coordenadas homogêneas.

Para cada $i = 0, \ldots, n$, seja o subconjunto de $\mathbb{P}^n$

$$U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$$

que pode ser identificado com K^n através da bijeção

$$(x_0 : \cdots : x_n) \longleftrightarrow \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

omitindo o termo $\frac{x_i}{x_i}$. Convencionaremos $\mathbb{A}^n = U^n$, e salvo mensão do contrário, indentificamos K^n com $\mathbb{A}^n \subset \mathbb{P}^n$.

O complementar de $\mathbb{A}^n$ em $\mathbb{P}^n$ consiste em pontos da forma $(x_0 : \cdots : x_{n-1} : 0)$, assim podemos identificar $\mathbb{P}^n \setminus \mathbb{A}^n$ com $\mathbb{P}^{n-1}$, o qual chamaremos *hiperplano no infinito.*

Em particular, $\mathbb{P}^0$ consiste de um só ponto. Já $\mathbb{P}^1$, a *reta projetiva,* é a reta usual $\mathbb{A}^1$ com um ponto extra no infinito, a qual podemos visualizar através da projeção estereográfica, identificando-a com a circunferência.

4.1.3 Curvas Projetivas

Para o resultado seguinte suporemos $K = \mathbb{R}$.

Proposição 4.1 *Sejam* $l : aX + bY + c = 0$ *com* a *ou* b *diferentes de zero e* $\bar{l}$ *o fecho de* l *em* $\mathbb{P}^2$. *Então,* $\bar{l} = l \cup \{(b : -a : 0)\} = \{(x : y : z) \mid ax + by + cz = 0\}$.

Demonstração: Suponha $b \neq 0$ e considere $l^* = \{(x : y : z) \mid ax + by + cz = 0\}$. Utilizando a aplicação já vista

$$\begin{array}{rccc} \varphi: & \mathbb{R}^2 & \longrightarrow & \mathbb{A}^2 \subset \mathbb{P}^2 \\ & (x, y) & \longmapsto & (x : y : 1) \end{array}$$

temos, se $z = 0$ então, $ax+by = 0$, logo, $y = \dfrac{-a}{b}\, x$ e $\left(1 : \dfrac{-a}{b} : 0\right) = (b : -a : 0)$. Portanto $l^* = l \cup \{(b : -a : 0)\}$.

Por definição da topologia de $\mathbb{P}^2$, resulta l^* fechado em $\mathbb{P}^2$. Como $l \subset l^*$ e l^* é fechado temos $\bar{l} \subset l^*$. Resta mostrar que o ponto no infinito $P = (b : -a : 0)$ pertence a $\bar{l}$. Sendo assim, basta encontrarmos uma sequência de pontos $P_n \in l$ com $\lim\limits_{n\to 0} P_n = P$. Seja $P_n = (bn : -an - c : b)$, logo,

$$P_n = \left(n : \frac{-an - c}{b} : 1\right) = \left(b : -a - \frac{c}{n} : \frac{b}{n}\right).$$

A primeira igualdade mostra que $P_n \in l$, e a segunda mostra que $P_n \to P$, pois

$$\lim_{n\to\infty} \left(b : -a - \frac{c}{n} : \frac{b}{n}\right) = (b, -a, 0)$$

em $\mathbb{R}^3 \setminus \{0\}$ e $q : \mathbb{R}^3 \setminus \{0\} \longrightarrow \mathbb{P}^2$ é contínua. □

Definição 4.3 *Seja* $f = \sum_{i=0}^{d} f_i$, *onde cada* $f_i \in K[X, Y]$ *é homogêneo de grau* i, $f_d \neq 0$. *A homogeneização de* f *é o polinômio homogêneo de grau* $d = \deg f$,

$$f^*(X, Y, Z) = \sum Z^{d-i} f_i(X, Y).$$

A Proposição 4.1 se generaliza para uma curva arbitrária f, isto é, o subconjunto de $\mathbb{P}^2$, $\{(x : y : z)\ ;\ f^*(x, y, z) = 0\}$ é igual ao fecho de f em $\mathbb{P}^2$. De fato, como $f^*(X, Y, Z) = \sum Z^{d-i} f_i(X, Y)$, logo, os pontos no infinito são da forma

$$\{(x : y : 0)\} = \{(x, y) \mid f_d(x, y) = 0\},$$

e como $f_d = \prod_{i=1}^{d}(a_iX + b_iY)$ que são retas, coincide com a Proposição 4.1.

Definição 4.4 *Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes, $F \in K[X, Y, Z]$, módulo a relação que identifica dois tais polinômios, F, G, se um for múltiplo constante do outro.*

Qualquer um dos polinômios dessa classe é denominado *equação* de uma curva. O *grau* de uma curva F é o grau de sua equação e quando possuem grau $1, 2$ e 3 são chamadas *retas, cônicas* e *cúbicas* respectivamente. O *traço* de uma curva é o conjunto das soluções da equação.

Uma curva é *irredutível* se admite uma equação que é um polinômio irredutível e as componentes irredutíveis de uma curva F são as curvas definidas pelos fatores irredutíveis de F.

Observemos que se F é um polinômio homogêneo de grau d, a relação

$$F(tx, ty, tz) = t^dF(x, y, z)$$

mostra que a condição para que um ponto $(x : y : z)$ pertença ao traço de uma curva projetiva é independente das coordenadas homogêneas.

A reta $Z = 0$ é usualmente chamada de *reta no infinito* e seu complementar $Z \neq 0$ é o plano $\mathbb{A}^2$, onde os pontos são ditos estarem a *distância finita.* A escolha dessa reta não é obrigatória, pois mudando a base de K^3, podemos escolher qualquer reta de $\mathbb{P}^2$ para ser reta no infinito.

O *fecho projetivo* de uma curva afim f é a curva projetiva definida pela homogeneização f^*. Os pontos a distância finita sobre uma curva F são dados pela equação $F(X, Y, 1) = 0$, e esse polinômio dado nessa equação é a *desomogeneização de F com respeito a Z,* denotado por F_*.

Note que F_* é não constante, a menos que F seja igual a uma potênica de Z.

Daqui em diante, as curvas algébricas planas afins $f(X, Y) = 0$ serão consideradas como a parte que se acha a distância finita sobre a curva projetiva $f^*(X, Y, Z) = 0$. O termo *curva* será utilizado para *curva plana projetiva,* salvo menção em caso contrário.

Definição 4.5 *Uma curva irredutível F é racional se existir um par de funões racionais $x(T),\ y(T)$, não ambas constantes, tal que $F(x(T), y(T)) = 0$ em $K(T)$. O par $x(T),\ y(T)$ é chamado uma parametrização racional.*

Dizemos que a parametrização $x(T),\ y(T)$ de uma curva C é boa se a inclusão

$$\begin{array}{rccc} \varphi: & K(C) & \hookrightarrow & K(T) \\ & (X,Y) & \mapsto & \varphi(x(T), y(T)) \end{array}$$

é sobrejetora.

4.1.4 Mudança de Coordenadas Projetivas

Definição 4.6 *Seja $T : K^3 \longrightarrow K^3$ uma aplicação composta de uma translação com um isomorfismo linear, tal que preserva retas de K^3 passando pela origem. Sendo assim, temos definida uma bijeção natural, ainda designada por $T : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$, chamada projetividade ou mudança de coordenadas projetivas em $\mathbb{P}^2$.*

Temos também um $K-$isomorfismo, $T_\bullet : K[X, Y, Z] \longrightarrow K[X, Y, Z]$, tal que para todo $(x, y, z) \in K^3$ e todo polinômio f,

$$(T_\bullet f)(x, y, z) = f(T^{-1}(x, y, z)).$$

Explicitamente, escrevendo $X = X_1,\ Y = X_2,\ Z = X_3$ e designando por (a_{ij}) a matriz de T^{-1} relativa à base canônica de K^3, temos

$$(T_\bullet f)(X_1, X_2, X_3) = f\left(\sum a_{1j}X_j, \sum a_{2j}X_j, \sum a_{3j}X_j\right)$$

A *imagem de uma curva projetiva F* por uma projetividade T é a curva definida por $T_\bullet F$. As curvas F e $T_\bullet F$ são ditas *congruentes*.

4.1.5 Índice de Interseção

Definiremos primeiramente a Resultande de duas curvas, que será utilizada posteriormente na definição do índice de interseção.

Definição 4.7 *Sejam os polinômios com coeficientes em* $K[X,Y]$:

$$F = A_dY^d + \cdots + A_0,\ d \geq 1,$$
$$G = B_eY^e + \cdots + B_0,\ e \geq 1.$$

onde $A_i,\ B_j$ *são homogêneos de grau* i, j.

Definimos a resultante de F *e* G *por:*

$$R = R_{F,G} = \begin{vmatrix} A_d & A_{d-1} & \dots & A_0 & & & \\ & A_d & \dots & A_1 & A_0 & & \\ & \dots & & & & & \\ & & & & & A_d & \dots & A_0 \\ B_e & B_{e-1} & \dots & B_0 & & & \\ & \dots & & & & & \\ & & & & & B_e & \dots & B_0 \end{vmatrix},$$

ou seja, o determinante da matriz $(d+e)\times(d+e)$, *com* e *linhas de a's e* d *linhas de b's. Os espaços em branco, são preenchidos com zeros.*

Definição 4.8 *Sejam* $P_i = (x_i : y_i : z_i),\ i = 1, \dots, r$ *os distintos pontos de* $F \cap G$. *Dizemos que* $F,\ G$ *estão bem posicionada se* $P_0 = (0:1:0) \notin F \cap G$. *Dizemos que* $F,\ G$ *estão muito bem posicionadas se* $P_0 \notin F \cap G$ *e se, para cada par* $P_i, P_j \in F \cap G$, *temos* $P_0,\ P_i,\ P_j$ *não colineares.*

Suporemos daqui pra frente que $F,\ G$ não tem componente em comum. Considere os polinômios com coeficientes em $K[X,Z]$,

$$F = A_dY^d + \cdots + A_0,\ d \geq 1,$$
$$G = B_eY^e + \cdots + B_0,\ e \geq 1,$$

onde $A_i,\ B_j$ são homogêneos de grau i, j.

Temos $(0:1:0) \in F$ se, e somente se, $A_0 = 0$. Logo estando $F,\ G$ bem posicionadas, temos A_0 ou $B_0 \neq 0$, e a resultante $R = R(X,Z)$ de $F,\ G$ com respeito a Y é homogênea de grau $d.e$ ([5], pg 27).

Por outro lado, levando em conta que A_0 ou $B_0 \neq 0$, para cada $(x : z) \in \mathbb{P}^1$ temos que $R(x, z) = 0$ se, e somente se, existe $(x : y : z) \in F \cap G$. Supondo F, G muito bem posicionadas, concluímos que R escreve-se na forma

$$R(X, Z) = c \prod_{i=1}^{r} (z_i X - x_i Z)^{m_i},$$

onde c é uma constante não nula, $P_i = (x_i, y_i, z_i), i = 1, \ldots, r$ são os distintos pontos de $F \cap G$, e os expoentes $m_i \in \mathbb{Z}_+^*$ e $\sum m_i = d.e.$

Sendo assim, definimos:

Definição 4.9 *A multiplicidade ou índice de interseção de F, G no ponto P é dada por*

$$(F, G)_P = \begin{cases} 0 & se \quad P \notin F \cap G \\ m_i & se \quad P = P_i. \end{cases}$$

Proposição 4.2 *O índice de interseção $(F, G)_P$ satisfaz as seguintes propriedades:*

(1) $(F, G)_P = (G, F)_P$ *é* ∞ *ou um número inteiro maior ou igual a zero;*

(2) $(F, G)_P = 0$ *se, e somente se,* $P \notin F \cap G$;

(3) $(F, G)_P = \infty$ *se, e somente se,* $P \in H$;

(4) $(F, G)_P = (T_\bullet F, T_\bullet G)_{T_\bullet P}$, *para toda projetividade* $T : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$;

(5) $(X, Y)_P = 1$, *onde* $P = (0 : 0 : 1)$;

(6) $(F, G + AF)_P = (F, G)_P$ *para todo A homogêneo com* $\deg A = \deg G - \deg F$.

(7) $(F, G_1 G_2)_P = (F, G_1)_P + (F, G_2)_P$.

Demonstração: [5], Capítulo 6. □

4.2 Cúbicas Não Singulares

Primeiramente introduziremos o Teorema que apresenta as Fórmulas de Plücker, as quais serão utilizadas posteriormente.

Teorema 4.1 *Seja F uma curva irredutível de grau $d \geq 2$ cujas únicas singularidades são δ (nós) e χ (cúspides). Então temos:*

$$\begin{aligned} d(d-1) &= \tilde{d} + 2\delta + 3\chi, \\ 3d(d-2) &= i + 6\delta + 8\chi, \end{aligned}$$

onde $\tilde{d}$ e i denotam o número de retas tangentes e o número de retas inflexionais, ou seja, tem contato triplo, passando por um ponto $P \notin F$, respectivamente.

Demonstração: [5], Capítulo 7. □

Proposição 4.3 *Toda cúbica não singular é congruente por uma projetividade a uma cúbica do tipo*

$$ZY^2 = X(X - Z)(X - \lambda Z)$$

para alguma constante $\lambda \in K$, $\lambda \neq 0, 1$.

Demonstração: Pelas Fórmulas de Püker, temos que uma cúbica não singular F admite nove pontos de inflexão. Considere $(0 : 1 : 0)$ um deles com tangente $Z = 0$, e podemos supor $(0 : 0 : 1) \in F$, com tangente $X = 0$. Temos então F na forma

$$F = X^3 + Z(aX^2 + bXY + cY^2) + dZ^2X,$$

com $d \neq 0 \neq c$, pois caso contrário F seria divisível por X.

Fazendo a mudança $Y = \dfrac{Y}{\sqrt{c}}$, podemos normalizar $c = 1$. Substituindo $Y = Y - \dfrac{bX}{2}$, encontramos $b = 0$. Desse modo, reduzimos F à forma

$$F = X^3 + Z(Y^2 + a'X^2) + b'XZ^2$$

com $b' \neq 0$, pois caso contrário, $(0 : 0 : 1)$ seria um ponto singular. Seja α uma raiz de $X^2 + a'X + b'$. Substituindo $X = \alpha X$ encontramos

$$F = ZY^2 + \alpha^3 X(X - Z)(X - Z\lambda),$$

com $\lambda = \dfrac{b}{\alpha^2}$.

Finalmente, com a mudança $Y = (\alpha)^{\frac{3}{2}}Y$, obtemos a forma normal do enunciado. □

4.3 Ciclos de Equivalência Racional

Definição 4.10 *Um ciclo na curva F é uma expressão do tipo*

$$n_1P_1 + \cdots + n_rP_r,$$

onde os n_i são inteiros e os P_i são pontos de F.

Definimos o grau de um ciclo por $\deg\left(\sum n_iP_i\right) = \sum n_i$.

Evidentemente, se D, D' são ciclos, temos

$$\deg(D + D') = \deg D + \deg D'.$$

Definição 4.11 *Seja G uma curva distinta de F. Definimos o ciclo de interseção de G com F por*

$$(G) = (G)_F = \sum (F, G)_P P.$$

Seja $\varphi \in K(F)$ uma função racional não nula. Suponhamos

$$\varphi = \frac{\overline{G}_0}{\overline{H}_0} = \frac{\overline{G}_1}{\overline{H}_1},$$

com G_i, H_i homogêneos, $\deg G_i = \deg H_i$ e $\overline{H}_0\overline{H}_1 \neq 0$. Temos então $G_0H_1 = H_0G_1 + AF$, para algum $A \in K[X, Y, Z]$, logo,

$$(G_0H_1)_F = (H_0G_1)_F$$

e portanto,

$$(G_0)_F - (H_0)_F = (G_1)_F - (H_1)_F$$

por propriedade do índice de interseção.

Definição 4.12 *Definimos o ciclo associado à função racional $\varphi \neq 0$ por*

$$(\varphi) = (\varphi)_F = (G)_F - (H)_F,$$

onde, $\varphi = \dfrac{\overline{G}}{\overline{\overline{H}}}$ é uma representação de φ como quociente de classes de polinômios homogêneos do mesmo grau.

Definição 4.13 *Sejam D, D' ciclos de uma curva F irredutível. Dizemos que D é racionalmente equivalente a D' se existir uma função racional $\varphi \in K(F)$ tal que*

$$D - D' = (\varphi).$$

Escrevemos $D \equiv D'$ para denotar equivalência racional.

Lema 4.1 *Equivalência racional é uma relação de equivalência, compatível com a adição de ciclos. Ou seja, para todo ciclo D, D', D'', temos:*

(1) $D \equiv D$;

(2) $D \equiv D'$ *se e somente se,* $D' \equiv D$;

(3) $D \equiv D', D' \equiv D''$ *então* $D \equiv D''$.

Demonstração: Sejam φ e ψ duas funções racionais não nulas, sendo assim,

(1) temos $D - D = 0$, que é o ciclo da função constante 1;

(2) se $D - D' = (\varphi)$, então $D' - D = (\varphi^{-1})$;

(3) Se $D - D' = (\varphi)$ e $D' - D'' = (\psi)$, temos evidentemente

$$(\varphi\psi) = (\varphi) + (\psi) = D - D' + D' - D'' = D - D''.$$

□

Proposição 4.4 *Seja F uma curva irredutível nao singular. Se existirem $P \neq Q$ em F racionalmente equivalentes, então F é racional.*

Demonstração: [5], Capítulo 9. □

4.4 A Estrutura de Grupos

Necessitaremos mais adiante do seguinte resultado preliminar:

Proposição 4.5 *Se F é uma cúbica não singular, então F não é racional.*

Demonstração: Podemos supor F_* na forma normal

$$Y^2 = X(X-1)(X-\lambda)$$

com $\lambda \neq 0, 1$.

Suponha F racional, logo, existem $a, b, c, d \in K[T]$, tais que $x = \dfrac{a}{c}$, $y = \dfrac{b}{d}$ constituem uma boa parametrização e podemos supor que $MDC(a, c) = MDC(b, d) = 1$. Substituindo na equação acima obtemos em $K[T]$:

$$c^3 b^2 = d^2 a(a-c)(a-\lambda c).$$

Note que c e $a - \lambda c$ também são primos relativos, pois caso contrário, a e c não seriam primos entre si, e pela unicidade da fatoração, segue-se que c^3 e d^2 são associados. Simplificando e absorvendo a constante $\dfrac{c^3}{d^2}$ em b, temos:

$$b^2 = a(a-c)(a-\lambda c). \tag{4.1}$$

Suponhamos que $\deg b = 3, \deg a = 2 \geq \deg c$ e $b = b_1 b_2 b_3$ com $\deg b_i = 1$. Notando que $a, a-c, a-\lambda c$ são dois a dois primos relativos, deduzimos que o mesmo ocorre com os b_i's e que $b_1^2 = a,\ b_2^2 = a - c,\ b_3^2 = a - \lambda c$ a menos de reordenação ou fator constante. Assim,

$$c = (b_1 - b_2)(b_1 + b_2) \quad \text{e} \quad (1-\lambda)c = (b_3 - b_2)(b_3 + b_2).$$

Segue-se que $b_1 \pm b_2$ é associado a $b_3 \pm b_2$. Sem perda de generalidade, podemos escrever relações:

$$b_1 - b_2 = \alpha(b_3 - b_2)$$

$$b_1 + b_2 = \beta(b_3 + b_2),$$

com $\beta - \alpha \neq 0$, e assim, concluimos que b_2 e b_3 são associados, o que é um absurdo.

Resta mostrar que $\deg b = 3$ e $\deg a = 2 \geq \deg c$. De fato, quase toda reta horizontal $Y = y_0$ corta F em três pontos distintos. Como a parametrização é por hipótese boa, esses pontos dão da forma $(x(t), y_0)$ para justamente três valores do parâmetro. Estes valores são dados pela condição $y(t) = \dfrac{b(t)}{d(t)} = y_0$.

Assim o polinômio $b(T) - y_0 d(T)$ admite exatamente três raízes distintas para quase todo y_0. Logo, $\deg b \leq 3$, então $\deg d = 3$ e daí $\deg c = 2$ pois $\dfrac{c^3}{d^2}$ é constante. Observando a equação (4.1), deduz-se $\deg b = 2$ e $\deg a = 0$ ou 2. Escreve-se $b = b_1 b_2$ e procede-se como antes, chegando a uma contradição. Se $\deg b = 3$, então $\deg d \leq 3$, acarretando $\deg c \leq 2$. Lembrando a equação (4.1) mais uma vez, vê-se que $\deg a = 2$. □

Corolário 4.1 *Se F é uma cúbica não singular e $P, Q \in F$ então P é racionalmente equivalente a Q se e somente se, $P = Q$.*

Demonstração: Proposições 4.4 e 4.5. □

Vejamos agora como é definida a estrutura de grupo.

Fixemos um ponto $O \in F$. Para cada par de pontos $P,\ Q \in F$, consideremos a interseção de F com a reta L que os contém. Se $P = Q$, tomamos L igual a reta tangente. Podemos escrever

$$(L) = P + Q + R$$

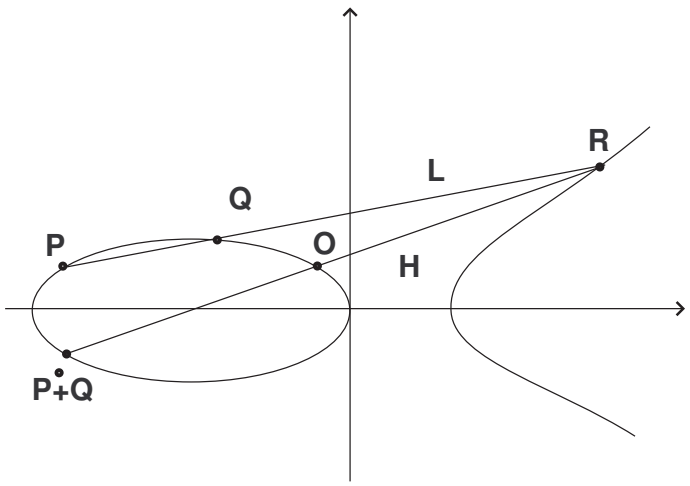
para algum R em F, bem determinado pelo par $P,\ Q$.

Seja H a reta definida pelo par R, O, e seja finalmente $P \dot{+} Q$ o terceiro ponto de interseção de H com F, de modo que

$$(H) = R + O + (P \dot{+} Q).$$

Notemos que, pondo $\varphi = \dfrac{L}{H} \in K(F)$, temos

$$(\varphi) = (P + Q + R) - (R + O + (P \dot{+} Q)),$$



e portanto

$$P\dot{+}Q \equiv P + Q - O. \tag{4.2}$$

Desse modo, pelo Corolário 4.1, determinamos $P\dot{+}Q$ como o único ponto de F racionalmente equivalente ao ciclo $P + Q - O$.

Proposição 4.6 *Seja F uma cúbica não singular e seja $O \in F$ um ponto de inflexão. A lei de composição $(P, Q) \longmapsto P\dot{+}Q$ acima descrita estabelece uma estrutura de grupo abeliano em F. O elemento neutro é o ponto O e o inverso aditivo de um ponto $P \in F$ é o terceiro ponto de interseção da reta OP com F, denotado por $\dot{-}P$.*

Demonstração: Pela construção de $P\dot{+}Q$ temos

$$P\dot{+}Q = Q\dot{+}P.$$

Levando em conta (4.2) temos que O funciona como elemento neutro e $\dot{-}P$ como inverso de P. Basta agora verificarmos a associatividade. Dados $P,\ Q,\ R \in F$, temos

$$(P\dot{+}Q)\dot{+}R \equiv (P\dot{+}Q) + R - O \equiv (P + Q - O) + R - O \equiv$$

$$P + (Q + R - O) - O \equiv P + (Q\dot{+}R) - O \equiv P\dot{+}(Q\dot{+}R)$$

□

Proposição 4.7 *(i)* $P\dot{+}Q\dot{+}R = O$ *se, e somente se, existe uma reta* H*, tal que* $(H)_F = P + Q + R$*.*

(ii) A reta que une dois pontos de inflexão cruza F *num terceiro ponto de inflexão.*

Demonstração:

(i) Seja L tangente de F em O, assim, temos $(L)_F = 3O$. Por outro lado,

$$P\dot{+}Q\dot{+}R \equiv P + Q + R - 2O.$$

Portanto, o primeiro membro é igual a O se, e somente se, $P + Q + R \equiv 3O$. Supondo que isso é válido, seja H a reta determinada pelo par P, Q. Considerando $(H) = P+Q+R'$, o quociente $\dfrac{L}{H}$ fornece uma função racional cujo ciclo é $3O-(H)$. Logo, $R \equiv R'$ e portanto pelo Corolário 4.1 $R = R'$.

(ii) Se $P + Q + R$ é ciclo de interseção de F com uma reta, e se P, Q são pontos de inflexão, deduzimos que $P\dot{+}Q\dot{+}R = O$, donde $3R = O$ e R é um ponto de inflexão. □

Referências Bibliográficas

[1] Chevalley, C. **Introduction to the Theory of Algebraic Functions of One Variable**, Mathematical Surveys and Monographs, Volume 6, AMS, 1951.

[2] Fulton, W. **Algebraic Curves**, Benjamin Cummings, 1969.

[3] Lang, S. **Introduction to Algebraic and Abelian Functions**, 2nd ed., New York, Springer-Verlag, 1982.

[4] Stichetnoth, H. **Algebraic Function Fields and Codes**, Springer-Verlag, 1993.

[5] Vainsencher, I. **Introdução às Curvas Algébricas Planas**, IMPA, Rio de Janeiro, 2005.