SARAH FARIA MONTEIRO MAZZINI

SEMIGRUPOS NUMÉRICOS NÃO ASSOCIADOS A CURVAS ALGÉBRICAS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

VIÇOSA
MINAS GERAIS - BRASIL
2017

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T

M477s 2017

Mazzini, Sarah Faria Monteiro, 1993-
Semigrupos numéricos não associados a curvas algébricas / Sarah Faria Monteiro Mazzini. - Viçosa, MG, 2017.
vii, 89f. : il. ; 29 cm.

Orientador : Lia Feital Fusaro Abrantes.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.89.

1. Teoria dos grupos. 2. Semigrupos. 3. Curvas algébricas. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-graduação em Matemática. II. Título.

CDD 22 ed. 512.22

SARAH FARIA MONTEIRO MAZZINI

SEMIGRUPOS NUMÉRICOS NÃO ASSOCIADOS A CURVAS ALGÉBRICAS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 17 de Fevereiro de 2017

André Luis Contiero

Marinês Guerreiro

Lia Feital Fusaro Abrantes
(Orientadora)

Dedico este trabalho aos meus pais,
Argeu e Suely, e à minha irmã, Luísa.

AGRADECIMENTOS

Agradeço, primeiramente, à Deus, que sempre ouve minhas preces e me mantém firme para seguir em frente.

Aos meus pais, Argeu e Suely, que são meus maiores incentivadores, por todo apoio, carinho, amor e zelo.

À minha irmã Luísa, minha companheira de Viçosa e da vida, por estar sempre presente.

À professora Lia, pela ajuda, paciência e orientação, aos demais professores do DMA, responsáveis por toda minha educação superior, e aos funcionários, principalmente ao João, por ser sempre prestativo e atencioso.

À minha família, meu namorado e meus amigos, pela força, pelas orações e companheirismo.

Finalmente, agradeço à CAPES pelo apoio financeiro indispensável para a realização deste trabalho.

SUMÁRIO

Resumo **vi**

Abstract **vii**

Introdução **1**

1 Corpos de funções algébricas **3**

1.1 Corpos de funções algébricas e lugares 3

1.2 Corpo das funções racionais 16

1.3 Divisores 20

2 O Teorema de Riemann-Roch **28**

3 Curvas algébricas **44**

3.1 Variedades afins 44

3.2 Propriedades locais das curvas planas 52

3.3 Variedades projetivas 54

3.4 O espaço multiprojetivo 60

3.5 Pontos de curvas e anéis de valorização discreta 61

3.6 Séries lineares 64

4 Semigrupos numéricos **66**

4.1 Propriedades de semigrupos numéricos 66

4.2 Semigrupos γ-hiperelípticos 74

5 Semigrupos não-Weierstrass **80**

5.1 Semigrupos não-Weierstrass obtidos por Buchweitz 81

5.2 Semigrupos de Weierstrass em recobrimento duplo de curvas . . . 83

Considerações Finais **88**

Referências Bibliográficas **89**

RESUMO

MAZZINI, Sarah Faria Monteiro, M.Sc. Universidade Federal de Viçosa, Fevereiro de 2017. **Semigrupos numéricos não associados a curvas algébricas**. Orientadora: Lia Feital Fusaro Abrantes.

Neste trabalho estudamos um caso particular de semigrupos numéricos: os semigrupos de Weierstrass. Com o teorema das lacunas de Weierstrass, provado em meados de 1860, foi possível concluir que a todo ponto de uma curva algébrica projetiva, não singular, definida sobre um corpo algebricamente fechado, é associado um semigrupo numérico. Em 1893, o matemático Hurwitz fez a seguinte pergunta: dado um semigrupo numérico H, existe uma curva tal que H está associado a um ponto dessa curva? Se tal semigrupo existir, este será chamado semigrupo de Weierstrass. Em 1980, Buchweitz encontrou o primeiro semigrupo que não era de Weierstrass, respondendo a pergunta de Hurwitz. Em 1993, o matemático Stöhr, utilizando um trabalho de Torres, apresentou o primeiro semigrupo simétrico que não era de Weierstrass. O objetivo deste trabalho é apresentar esses resultados.

ABSTRACT

MAZZINI, Sarah Faria Monteiro, M.Sc. Universidade Federal de Viçosa, February, 2017. **Numerical semigroups not associated with algebraic curves**. Adviser: Lia Feital Fusaro Abrantes.

In this paper we study a particular case of numerical semigroups: the Weierstrass semigroups. With the Weierstrass gap theorem, proved in the mid-1860s, it was possible to conclude that at every point of a non-singular projective algebraic curve, defined on an algebraically closed field, we can associate a numerical semigroup. In 1893 the mathematician Hurwitz asked the following question: given a numerical semigroup H, is there a curve such that H is associated with a point on this curve? If such a semigroup exists, it will be called Weierstrass semigroup. In 1980 Buchweitz found the first non-Weierstrass semigroup, answering Hurwitz's question. In 1993, the mathematician Stöhr, using results of Torres, presented the first symmetric semigroup that was non-Weierstrass.

INTRODUÇÃO

Um semigrupo numérico H é um subconjunto dos números naturais, fechado para a soma, que contém o zero e cujo complemento em $\mathbb{N}$ é finito, ou seja, $\#(\mathbb{N} \setminus H) < \infty$. Os elementos de $\mathbb{N} \setminus H$ são chamados lacunas. A simplicidade dessa estrutura atraiu, no fim do século XIX, vários matemáticos como Frobenius e Silvester. Frobenius propôs o seguinte problema: qual a maior quantia que não podemos obter utilizando apenas moedas previamente determinadas? A solução deste problema é a última lacuna do semigrupo gerado pelos números que representam os valores das moedas, e essa lacuna é chamada número de Frobenius. Na segunda metade do século XX os semigrupos numéricos voltaram a ser estudados em várias áreas da matemática, entre elas a Geometria Algébrica.

Em meados de 1860, o matemático alemão Weierstrass provou o chamado Teorema das Lacunas de Weierstrass, que afirma que dada uma curva algébrica não singular de gênero g definida sobre um corpo algebricamente fechado e dado um ponto nessa curva, a esse ponto está relacionado um semigrupo numérico de gênero g. Esse semigrupo é dito semigrupo de Weierstrass do ponto. Em 1893, o matemático Hurwitz questionou a recíproca deste resultado: *Dado um semigrupo numérico H, existe uma curva e um ponto dessa curva tal que o semigrupo associado a este ponto é H*? Essa pergunta também pode ser formulada da seguinte maneira: *Existe algum semigrupo que não é de Weierstrass*? Depois de muitas respostas equivocadas, o matemático Buchweitz apresentou, em 1980, o primeiro semigrupo que não estava relacionado a uma curva algébrica:

$$H = \{0, 13, 14, 15, 16, 17, 18, 20, 22, 23, 26 \rightarrow\}.$$

O método de Buchweitz consiste em analisar a quantidade de elementos que existe no conjunto das somas de quaisquer n lacunas do semigrupo. Entretanto, devido a um resultado apresentado por Oliveira em [6] e por Oliveira e Stöhr em [8], observou-se que o método de Buchweitz não poderia ser aplicado para semigrupos simétricos e quase-simétricos e assim outra pergunta estava em aberto: *Existe um semigrupo simétrico que não é de Weierstrass*? Essa pergunta só foi respondida em 1993 pelo matemático Stöhr, baseado no trabalho de Torres [11], onde ele apresentou uma família de semigrupos simétricos que não estão relacionados a

uma curva algébrica.

Este trabalho foi organizado da seguinte forma: O Capítulo 1 consiste do estudo de corpos de funções e divisores, cujas definições e resultados servem de preliminares para a dissertação. No Capítulo 2 estudamos um importante resultado da Teoria de Corpos de Funções: o Teorema de Riemann-Roch, que nos permite calcular a dimensão do espaço de Riemann-Roch associado a um divisor utilizando seu gênero e seu grau. No Capítulo 3 apresentamos definições e resultados de curvas algébricas afins e projetivas e mostramos que existe uma bijeção entre os pontos de uma curva algébrica não singular e os lugares do seu corpo de funções, sendo possível transferir todo o estudo feito nos Capítulos 1 e 2 para o Capítulo 3. No capítulo 4 demonstramos importantes resultados da Teoria de Semigrupos Numéricos e estudamos um caso particular de semigrupo: os semigrupos $\gamma-$hiperelípticos, semigrupos estes que são relacionados a curvas $\gamma-$hiperelípticas. No último capítulo exibimos exemplos de semigrupos não-Weierstrass, primeiramente obtidos pelo método de Buchweitz e depois através de recobrimento duplo de curvas.

CAPÍTULO 1

CORPOS DE FUNÇÕES ALGÉBRICAS

Neste capítulo fazemos um estudo sobre corpos de funções algébricas e abordamos conceitos importantes como lugares e divisores de um corpo de funções. Os assuntos tratados neste capítulo são preliminares fundamentais para o entendimento dos demais capítulos. As demonstrações e resultados desse capítulo podem ser encontrados em [9].

1.1 Corpos de funções algébricas e lugares

Seja K um corpo arbitrário.

Definição 1.1. *Um corpo de funções algébricas F/K de uma variável sobre K é uma extensão $F \supseteq K$ tal que F é uma extensão finita e algébrica de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.*

Por simplicidade, nos referimos a F/K como corpo de funções. O conjunto $\widetilde{K} = \{z \in F;$ z é algébrico sobre K$\}$ é um subcorpo de F, pois somas, produtos e inversos de números algébricos são também algébricos. O corpo $\widetilde{K}$ é chamado **corpo de constantes de** F/K. Temos $K \subseteq \widetilde{K} \subsetneq F$. De fato, a primeira inclusão é válida pois todo elemento $\alpha \in K$ é raiz do polinômio $x - \alpha \in K[x]$. A segunda inclusão é clara e $\widetilde{K} \neq F$, pois F é um extensão transcendente de K. Note que K é algebricamente fechado se, e somente se $K = \widetilde{K}$.

Observação 1.2. *Os elementos de F que são transcendentes sobre K são caracterizados da seguinte forma: $z \in F$ é transcendente sobre K se, e somente se a extensão $F \supset K(z)$ tem grau finito.*

Exemplo 1.3. *O exemplo mais simples de corpo de funções é o chamado corpo de funções racionais, que é dado quando $F = K(x)$, onde $x \in F$ é um elemento transcendente sobre K. Neste caso o grau de F sobre $K(x)$ é 1. Cada elemento não nulo $z \in K(x)$ pode ser escrito de maneira única na forma*

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

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

Vamos introduzir agora as noções de anéis de valorização e lugares.

Definição 1.4. *Um **anel de valorização** do corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:*

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

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

Exemplo 1.5. *Seja K um corpo e $K(x)$ seu corpo de funções racionais. Seja $p(x) \in K[x]$ um polinômio mônico e irredutível e considere o conjunto*

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], g(x) \neq 0 \text{ e } p(x) \nmid g(x) \right\}.$$

Então $\mathcal{O}_{p(x)}$ é um anel e $K \subsetneq \mathcal{O}_{p(x)} \subsetneq K(x)$. Vamos mostrar a parte (b) da definição.

Seja $h(x) \in K(x)$. Podemos escrever $h(x) = \frac{f_1(x)}{g_1(x)}$. Se $h(x) \in \mathcal{O}_{p(x)}$ o resultado já está provado. Suponha que $h(x) \notin \mathcal{O}_{p(x)}$. Então $p(x) | g_1(x)$. Como a representação de $h(x)$ é única, assumindo que $mdc(f(x), g(x)) = 1$, temos $p(x) \nmid f_1(x)$ e, portanto, $h^{-1}(x) = \frac{g_1(x)}{f_1(x)} \in \mathcal{O}_{p(x)}$. Logo $\mathcal{O}_{p(x)}$ é um anel de valorização de $K(x)/K$.

Note que se $q(x) \in K[x]$ é um polinômio mônico e irredutível diferente de $p(x)$ então $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

Proposição 1.6. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K. Então as seguintes afirmações são satisfeitas:*

(a) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ possui um único ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^\times$, onde $\mathcal{O}^\times = \{z \in \mathcal{O} / \text{ existe um elemento } w \in \mathcal{O} \text{ com } zw = 1\}$ é o conjunto das unidades de $\mathcal{O}$.

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

(c) Para o corpo $\widetilde{K}$ das constantes de F/K temos $\widetilde{K} \subset \mathcal{O}$ e $\widetilde{K} \cap P = \{0\}$.

Demonstração:

a) Basta mostrarmos que P é um ideal, pois como P não contém apenas as unidades de $\mathcal{O}$, este será maximal.

Sejam $x, y \in P$ e $z \in \mathcal{O}$.

- Temos $xz \notin \mathcal{O}^\times$ pois, caso contrário, x seria uma unidade, o que não acontece. Logo $xz \in P$.
- Como $P \subset F$ temos $x, y \in F$. Daí $\frac{x}{y} \in F$. Suponha, sem perda de generalidade, que $\frac{x}{y} \in \mathcal{O}$. Então

$$\frac{x}{y} \in \mathcal{O} \Rightarrow 1 + \frac{x}{y} \in \mathcal{O} \Rightarrow y\left(1 + \frac{x}{y}\right) \in P \Rightarrow y + x \in P.$$

Logo P é um ideal maximal de $\mathcal{O}$.

(b) Seja $x \in P$. Se $x^{-1} \in \mathcal{O}$, como P é ideal teríamos $xx^{-1} = 1 \in P$, o que é absurdo. Logo $x^{-1} \notin \mathcal{O}$. Reciprocamente, seja $x \in F$ e $x^{-1} \notin \mathcal{O}$. Como $\mathcal{O}$ é anel de valorização, se $x \in \mathcal{O}$ temos $x \in P$, pois o inverso de x não pertence a $\mathcal{O}$.

(c) Seja $x \in \widetilde{K}$ e suponha $x \notin \mathcal{O}$. Como $\mathcal{O}$ é anel de valorização, $x^{-1} \in \mathcal{O}$. Como o corpo $\widetilde{K}$ é formado pelos elementos de F algébricos sobre K e $x \in \widetilde{K}$, então $x^{-1} \in \widetilde{K}$, e daí existe um polinômio com coeficientes em K tal que x^{-1} é raiz, isto é,

$$a_n(x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \cdots + a_1x^{-1} + a_0 = 0.$$

Dividindo os coeficientes por a_0, temos:

$$\begin{aligned} & b_n(x^{-1})^n + \cdots + b_1x^{-1} = -1 \\ \Rightarrow\ & x^{-1}(b_n(x^{-1})^{n-1} + \cdots + b_1) = -1 \\ \Rightarrow\ & x = -(b_n(x^{-1})^{n-1} + \cdots + b_1) \in K[x^{-1}] \subseteq \mathcal{O}, \end{aligned}$$

o que é absurdo pois $x \notin \mathcal{O}$. Portanto, $\widetilde{K} \subseteq \mathcal{O}$. Além disso $\widetilde{K} \cap P = \{0\}$, pois $\widetilde{K}$ é formado pelos elementos algébricos, e esses, com exceção do zero, são inversíveis.

□

Teorema 1.7. *Seja $\mathcal{O}$ o anel de valorização do corpo de funções F/K e seja P seu único ideal maximal. As seguintes afirmações são satisfeitas:*

(a) P é um ideal principal.

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

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

Para demonstrar este teorema vamos mostrar, primeiramente, um lema:

Lema 1.8. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções algébricas F/K, P seu ideal maximal e $0 \neq x \in P$. Sejam $x_1, \cdots, x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$, para $i = 1, \cdots, n-1$. Então*

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

Demonstração: Como F/K é corpo de funções e x é transcendente sobre K, temos, por definição, que a extensão $[F : K(x)]$ é finita. Para mostrar que seu grau é $\geq n$ basta mostrar que $x_1, \cdots, x_n$ são linearmente independentes sobre $K(x)$, pois o grau da extensão é a dimensão de F visto como espaço vetorial sobre $K(x)$.

Suponha que exista uma combinação linear não trivial dos x_i, $\sum_{i=1}^{n} \psi_i(x)x_i = 0$, com $\psi_i(x) \in K(x)$. Podemos assumir que $\psi_i(x)$ sejam polinômios em x e que x não divide pelo menos um deles, pois caso contrário poderíamos dividir todo o polinômio por x. Seja $a_i = \psi_i(0)$ o termo constante de cada $\psi_i(x)$ e $j \in \{1, \cdots, n\}$ tal que $a_j \neq 0$ e $a_i = 0$, para todo $i > j$. Então

$$-\psi_j(x)x_j = \sum_{i \neq j} \psi_i(x)x_i, \tag{1.1}$$

com $\psi_i(x) \in \mathcal{O}$, pois $\psi_i(x)$ são polinômios em $x = x_1 \in P \subset \mathcal{O}$. Além disso $x_i \in x_jP$, para $i < j$, e $\psi_i(x) = xg_i(x)$, para $i > j$, onde g_i é um polinômio em x. Dividindo (1.1) por x_j, temos

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

Todas as parcelas do lado direito pertencem a P, logo $-\psi_j(x) \in P$. Por outro lado, $\psi_j(x) - a_j = xg_j(x)$, com $g_j(x) \in K[x] \subseteq \mathcal{O}$ e $x \in P$, e daí $a_j = \psi_j(x) - xg_j(x) \in P \cap K$. Como $a_j \neq 0$, temos uma contradição com a Proposição 1.6.

□

Demonstração do Teorema 1.7:

(a) Suponha que P não seja um ideal principal e tome $0 \neq x_1 \in P$. Como $P \neq x_1\mathcal{O}$, existe $x_2 \in P \setminus x_1\mathcal{O}$. Então $x_2x_1^{-1} \notin \mathcal{O}$. De fato, se isso ocorresse, teríamos $x_2 = x_2x_1^{-1}x_1 \in x_1\mathcal{O}$, o que é absurdo. Logo $x_2x_1^{-1} \notin \mathcal{O}$ e, pela Proposição 1.6, $(x_2x_1^{-1})^{-1} = x_1x_2^{-1} \in P$. Então $x_1 = x_2x_1x_2^{-1} \in x_2P$. Continuando este processo, obtemos uma sequência infinita $x_1, x_2, \cdots \in P$ tal que $x_i \in x_{i+1}P$, o que contradiz o Lema 1.8. Portanto, P é um ideal principal.

(b) Vamos provar a existência. Seja $z \in F$. Como $\mathcal{O}$ é anel de valorização temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Suponha, sem perda de generalidade, que $z \in \mathcal{O}$, com

$z = t^0 z$. Vamos agora considerar o caso em que $z \in P$. Pelo Lema 1.8 existe $m \geq 0$ maximal para a sequência

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

tal que $z \in t^m\mathcal{O}$. Escreva $z = t^m u$, com $u \in \mathcal{O}$. Então u deve ser uma unidade de $\mathcal{O}$, pois se $u \in P$ temos $u = tw$, com $w \in \mathcal{O}$ e $z = t^{m+1}w \in t^{m+1}\mathcal{O}$, o que contradiz o fato de m ser máximo.

Vejamos agora a unicidade. Suponha $z = t^m u'$, com $u' \in \mathcal{O}^\times$. Assim

$$t^m u' = t^n u \Rightarrow t^{m-n}(uu') = 1,$$

logo t^{m-n} é uma unidade e a representação de z é dada de maneira única.

(c) Seja $\{0\} \neq I \subseteq \mathcal{O}$ um ideal de $\mathcal{O}$. O conjunto $A := \{r \in \mathbb{N}/t^r \in I\}$ é não vazio. De fato, se $0 \neq x \in I$ então $x = t^r u$, com $u \in \mathcal{O}^\times$ e daí $t^r = xu^{-1} \in I$. Seja $n = \min(A)$. Vamos mostrar que $I = t^n\mathcal{O}$. Como I é ideal de $\mathcal{O}$ e $t^n \in I$ temos $t^n\mathcal{O} \subseteq I$. Seja $y \in I$. Então $y = t^s w$, com $w \in \mathcal{O}^\times$ e $s \geq 0$, e daí $t^s \in I$ e $s \geq n$. Logo $y = t^n \cdot t^{s-n}w \in t^n\mathcal{O}$ e assim $I = t^n\mathcal{O}$, donde concuímos que $I = t^n\mathcal{O}$.

□

Definição 1.9. *Um anel que satisfaz as condições do Teorema 1.7 é chamado um* ***anel de valorização discreta.***

Como $\mathcal{O}$ é um anel local, vimos que P é seu único ideal maximal. Então faz sentido a seguinte definição:

Definição 1.10. *(a) Um* ***lugar*** *P de um corpo de funções F/K é o ideal maximal de algum anel de valorização de F/K. Todo elemento $t \in F$ tal que $P = t\mathcal{O}$ é chamado* ***elemento primo*** *de P.*

(b) $\mathbb{P}_F := \{P | P$ *é um lugar de* $F/K\}$.

Sabemos pela Proposição 1.6 que, sendo $\mathcal{O}$ um anel de valorização do corpo de funções F/K e P seu ideal maximal, temos que dado $0 \neq x \in F, x \in P$ se, e somente se $x^{-1} \notin \mathcal{O}$. Então $\mathcal{O}$ é unicamente determinado por P e podemos definir $\mathcal{O}_P = \mathcal{O} = \{z \in F | z^{-1} \notin P\}$. Chamamos $\mathcal{O}_P = \mathcal{O}$ de **anel de valorização do lugar** P.

Definição 1.11. *Uma valorização discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

1. $v(x) = \infty \Leftrightarrow x = 0$.
2. $v(xy) = v(x) + v(y)$, *para todo* $x, y \in F$.
3. $v(x + y) \geq min\{v(x), v(y)\}$, *para todo* $x, y \in F$.

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

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

Lema 1.12 (Desigualdade triangular estrita)**.** *: Seja* v *uma valorização discreta de* F/K *e sejam* $x, y \in F$ *com* $v(x) \neq v(y)$. *Então* $v(x + y) = min\{v(x), v(y)\}$.

Demonstração: Como $v(x) \neq v(y)$ e $v : F \to \mathbb{Z} \cup \{\infty\}$, podemos considerar $v(x) < v(y)$. Suponha $v(x + y) \neq \min\{v(x), v(y)\}$. Daí, pela propriedade (3) da definição, temos $v(x + y) > v(x)$. Note que, para todo $a \in K$, temos $v(ay) = v(y)$. Assim, $v(-y) = v(y)$. Então obtemos

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

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

□

Definição 1.13. *Para um lugar* $P \in \mathbb{P}_F$ *associamos uma função* $v_p : F \to \mathbb{Z} \cup \{\infty\}$ *da seguinte forma: Escolha um elemento primo* t *para* P. *Então todo* $0 \neq z \in F$ *tem uma única representação* $z = t^n u$, *com* $u \in \mathcal{O}_P^\times$ *e* $n \in \mathbb{Z}$. *Defina* $v_P(z) := n$ *e* $v_P(0) = \infty$.

Observação 1.14. *Essa definição depende apenas de* P *e não da escolha de* t. *De fato, seja* t' *um outro elemento primo de* P *tal que* $P = t\mathcal{O} = t'\mathcal{O}$. *Então* $t = t'w$, *para algum* $w \in \mathcal{O}_P^\times$. *Então temos, para* $u \in \mathcal{O}_P^\times$,

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

Teorema 1.15. *Seja* F/K *um corpo de funções.*

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

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

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

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

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

(c) *Suponha que* v *seja uma valorização discreta de* F/K. *Então o conjunto* $P = \{z \in F; v(z) > 0\}$ *é um lugar de* F/K *e* $\mathcal{O}_P = \{z \in F/v(z) \geq 0\}$ *é seu anel de valorização correspondente.*

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

Demonstração:

(a) Vamos provar que a função

$$\begin{array}{rccc} v_P: & F & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ & t^n u & \longmapsto & n \end{array}$$

e $v_P(0)=\infty$ é uma valorização discreta.

1. $v_P(0)=\infty$ por definição e, se $0\neq z=t^n u$, $v_P(z)=v_P(t^n u)=n\neq\infty$. Daí, $v_P(x)=\infty$ se, e somente se $x=0$.
2. Sejam $x,y\in F$. Então $x=t^n u_1$ e $y=t^m u_2$, com $u_1,u_2\in\mathcal{O}_p^\times$. Segue $v_P(xy)=v_P(t^{m+n}u_1u_2)=n+m=v_P(x)+v_P(y)$.
3. Sejam $x,y\in F$. Então $x=t^n u_1$ e $y=t^m u_2$, com $u_1,u_2\in\mathcal{O}_P^\times$, $v_P(x)=n$ e $v_P(y)=m$. Suponha, sem perda de generalidade, $n\leq m<\infty$. Então $x+y=t^n u_1+t^m u_2=t^n(u_1+t^{m-n}u_2)=t^n z$, com $z\in\mathcal{O}_P$. Se $z=0$, temos $v_P(x+y)=\infty>\min\{n,m\}$. Caso contrário $z=t^k u$, com $k\geq 0$, pois $m-n>0$ e $u\in\mathcal{O}_P^\times$. Daí

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

4. Como $t\in P$, temos $t\in F$. Daí $v_P(t)=1$.
5. Seja $0\neq a\in K$. Então $a\in\mathcal{O}^\times$, e daí $a=t^0 a\Rightarrow v_P(a)=0$.

As outras afirmações são óbvias.

(b) ($\Rightarrow$)Seja x um elemento primo de P, ou seja, $P=x\mathcal{O}$. Daí temos $x=x\cdot 1$ e $v_P(x)=1$.
($\Leftarrow$) Seja $x\in P$ tal que $v_P(x)=1$. Então $x=tu$, para $u\in\mathcal{O}_P^\times$ e $P=t\mathcal{O}$. Mas daí $t=xu^{-1}$, ou seja, $P=x\mathcal{O}$. Logo x é um elemento primo de P.

(c) Seja $v: F\to\mathbb{Z}\cup\{\infty\}$ uma valorização discreta de F/K. Então $\mathcal{O}_P=\{z\in F; v(z)\geq 0\}$ é um anel de valorização de F/K e, sabendo que as unidades $k\in\mathcal{O}^\times$ são aquelas em que $v(k)=0$, temos que $P=\{z\in F; v(z)>0\}$ é seu ideal maximal, logo um lugar de F/K.

(d) Seja $\mathcal{O}$ um anel de valorização de F/K, P seu ideal maximal, v_P a valorização discreta associada a P e $z\in F\setminus\mathcal{O}$. Para mostrar que $\mathcal{O}$ é um anel maximal de F precisamos mostrar que $F=\mathcal{O}[z]$. Como $z\notin\mathcal{O}$, temos $v_P(z^k)=k\leq 0$, e daí $v_P(z^{-k})\geq 0$. Assim, para k suficientemente grande e $y\in F$, temos $v_P(yz^{-k})\geq 0$. Daí $w=yz^{-k}\in\mathcal{O}$, ou seja, $y=wz^k\in\mathcal{O}[z]$.

□

Seja P um lugar de F/K e $\mathcal{O}_P$ seu anel de valorização. Como P é um ideal maximal o quociente $\frac{\mathcal{O}_P}{P}$ é um corpo. Para $x\in\mathcal{O}_P$, definimos $x(P)\in\frac{\mathcal{O}_P}{P}$ como a classe residual de x módulo P. Para $x\in F\setminus\mathcal{O}_P$ denotamos $x(P):=\infty$.

Observação 1.16. *Temos $K \subseteq \widetilde{K}$. Daí, pela Proposição 1.6, $K \subseteq \mathcal{O}$ e $K \cap P = \{0\}$. Então a aplicação $\mathcal{O}_P \to \frac{\mathcal{O}_P}{P}$ induz uma inclusão de K em $\frac{\mathcal{O}_P}{P}$. Dessa forma podemos considerar K como um subcorpo de $\frac{\mathcal{O}_P}{P}$ via esta aplicação. Com os mesmos argumentos podemos considerar $\widetilde{K}$ como um subcorpo de $\frac{\mathcal{O}_P}{P}$.*

Definição 1.17. *Seja $P \in \mathbb{P}_F$.*

(a) $F_P = \mathcal{O}_P/P$ é o corpo de classes residuais de P. A aplicação $x \mapsto x(P)$ de F para $F_P \cup \{\infty\}$ é chamada aplicação de classes residuais com respeito a P.

(b) $degP = [F_P : K]$ é chamado grau de P. Um lugar de grau 1 é chamado lugar racional de F/K.

Proposição 1.18. *Se P é um lugar de F/K e $0 \neq x \in P$, então*

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

Demonstração: Como x um elemento transcendende sobre K, pela definição de corpo de funções, temos $[F : K(x)] < \infty$. Portanto, para mostrar que $\deg P \leq [F : K(x)]$ basta tomar $z_1, \cdots, z_n \in \mathcal{O}_P$ cujos resíduos $z_1(P), \cdots, z_n(P)$ sejam linearmente independentes sobre K e mostrar que estes também o são sobre $K(x)$.

Seja

$$\sum \psi_i(x) z_i = 0 \tag{1.2}$$

uma combinação linear não trivial de $z_1, \cdots, z_n$ com $\psi_i(x) \in K(x)$. Podemos supor, sem perda de generalidade, que $\psi_i(x)$ sejam polinômios em x onde existe pelo menos um deles que não é divisível por x, pois, caso contrário, poderíamos dividir os dois lados da igualdade por x. Assim $\psi_i(x) = a_i + xg_i(x)$, com $a_i \in K, g_i(x) \in K[x]$ e pelo menos um dos $a_i's$ não nulo. Como $x \in P$ e $g_i(x) \in \mathcal{O}_P$, temos

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

Passando o quociente por P em (1.2), temos

$$0 = \sum \psi_i(x)(P) z_i(P) = \sum a_i z_i(P),$$

o que contradiz a independência linear de $z_1(P), \cdots, z_n(P)$.

□

Observação 1.19. *Seja P um lugar racional de F/K, isto é, $degP = 1$. Daí $F_P = K$ e a aplicação de classe residual aplica F em $K \cup \{\infty\}$. Se K é um corpo algebricamente fechado, então todos os lugares são racionais. Dessa maneira, dado um elemento $z \in F$ podemos vê-lo como uma função*

$$\begin{array}{rccc} z: & \mathbb{P}_F & \longrightarrow & K \cup \{\infty\} \\ & P & \longmapsto & (P) \end{array}$$

Este é o motivo pelo qual F/K é chamado corpo de funções. Os elementos de K, vistos como funções, são funções constantes, e por essa razão K é chamado corpo constante de F.

Definição 1.20. *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é **zero** de z se $v_P(z) > 0$ e que P é um **polo** de z se $v_P(z) < 0$. Se $v_P(z) = m > 0$, dizemos que P é zero de z de ordem m. Se $v_P(z) = -m < 0$ dizemos que P é polo de z de ordem m.*

Teorema 1.21. *Seja F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Demonstração: Seja o conjunto $\mathcal{F} := \{S | S \text{ é subanel de } F, \text{ com } R \subseteq S \text{ e } IS \neq S\}$, onde IS é um ideal de S formado por todas as somas finitas da forma $\sum a_\alpha S_\alpha$, com $a_\alpha \in I$ e $S_\alpha \in S$.

Como I é ideal próprio de R temos $\mathcal{F} \neq \emptyset$, pois $R \in \mathcal{F}$, e temos também que $\mathcal{F}$ é parcialmente ordenado pela relação de inclusão. Considere $\mathcal{H} \subseteq \mathcal{F}$ um subconjunto totalmente ordenado de $\mathcal{F}$. Então $T := \cup\{S | S \in \mathcal{H}\}$ é um subanel de $\mathcal{F}$ com $R \subseteq T$. Vamos mostrar agora que $IT \neq T$. Suponha $IT = T$. Então

$$1 = \sum_{\alpha=1}^{n} a_\alpha s_\alpha,$$

com $a_\alpha \in I$ e $s_\alpha \in T$. Como $\mathcal{H}$ é totalmente ordenado, existe $S_0 \in \mathcal{H}$ tal que $s_1, \cdots, s_n \in S_0$, e daí teríamos $1 \in IS_0$ o que implica $IS_0 = S_0$, o que é absurdo. Dessa forma temos $\mathcal{F}$ um conjunto não vazio parcialmente ordenado onde todo subconjunto totalmente ordenado possui um elemento maximal, ou seja, existe um anel $\mathcal{O}$, com $\mathcal{O} \subseteq F$ tal que $R \subseteq \mathcal{O} \subseteq F, I\mathcal{O} \neq \mathcal{O}$ e $\mathcal{O}$ é o anel maximal que satisfaz essas propriedades.

Vamos mostrar agora que $\mathcal{O}$ é um anel de valorização. Como $I \neq \{0\}$ e $I\mathcal{O} \neq \mathcal{O}$ temos $\mathcal{O} \subsetneq F$ e $I \subseteq \mathcal{O} \setminus \mathcal{O}^\times$. Assim, para provar que $\mathcal{O}$ é anel de valorização basta provar que, para todo $z \in F$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Suponha que exista $z \in F$ tal que $z \notin \mathcal{O}$ e $z^{-1} \notin \mathcal{O}$. Então $I\mathcal{O}[z] = \mathcal{O}[z]$ e $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Logo podemos encontrar $a_0, \cdots, a_n, b_0, \cdots, b_m \in I\mathcal{O}$ com

$$1 = a_0 + a_1 z + \cdots + a_n z^n \tag{1.3}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \tag{1.4}$$

Como $I\mathcal{O} \neq \mathcal{O}$, temos $1 \notin I\mathcal{O}$, e daí $m, n \geq 1$. Escolha m e n minimais e assuma, sem perda de generalidade, $m \leq n$. Multiplicando (1.3) por $1 - b_0$ e (1.4) por $a_n z^n$, temos

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

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

Somando essas duas equações temos:

$$1 - b_0 = (1 - b_0)a_0 + \cdots + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}$$

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

com $c_i \in I\mathcal{O}$, o que contradiz a minimalidade de n. Assim $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$ e $\mathcal{O}$ é anel de valorização.

□

Corolário 1.22. *Seja F/K um corpo de funções, $z \in F$ transcendente sobre K. Então z tem no mínimo um zero e um polo. Em particular $\mathbb{P}_F \neq \emptyset$.*

Demonstração: Seja o anel $R = K[z]$ e o ideal $I = zK[z]$. Pelo Teorema 1.21, existe um lugar $P \in \mathbb{P}_F$ tal que $zK[z] \subseteq P$, e daí $z \in P$, logo P é um zero de z. Utilizando o mesmo argumento mostramos que z^{-1} possui zero em $Q \in \mathbb{P}_F$, logo z possui um polo em Q. Portanto todo elemento transcendente sobre K possui pelo menos um zero e um polo.

□

Vamos agora provar dois fatos importantes sobre lugares e valorizações: o primeiro deles nos garante que todo corpo de funções possui infinitos lugares, enquanto o segundo afirma que todo elemento $x \in F$ possui um número finito de zeros e polos. Para isso vamos demonstrar primeiro o

Teorema 1.23. *[Teorema da aproximação fraca] Sejam F/K um corpo de funções, $P_1, \cdots, P_n$ lugares de F/K distintos dois a dois, $x_1, \cdots, x_n \in F$ e $r_1, \cdots, r_n \in \mathbb{Z}$. Então existe algum $x \in F$ tal que*

$$v_{P_i}(x - x_i) = r_i \text{ para todo } i = 1, \cdots, n.$$

Demonstração: Por simplicidade vamos denotar v_{P_i} por v_i.

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

Vamos provar essa afirmação por indução. Considere $n = 2$. Então, pelo Teorema 1.15, $\mathcal{O}_{P_1} \nsubseteq \mathcal{O}_{P_2}$ e $\mathcal{O}_{P_2} \nsubseteq \mathcal{O}_{P_1}$, pois os anéis de valorização são subanéis próprios maximais de F. Assim existem $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ e $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Dessa forma temos $v_1(y_1) \geq 0$, $v_2(y_1) < 0, v_1(y_2) < 0$ e $v_2(y_2) \geq 0$. Assim, tomando $u = \dfrac{y_1}{y_2}$ temos

$$v_1(u) = v_1\left(\frac{y_1}{y_2}\right) = v_1(y_1) + v_1\left(\frac{1}{y_2}\right) > 0 \quad \text{e}$$

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

e portanto encontramos o elemento desejado.

Para $n > 2$ temos, pela hipótese de indução, que existe $y \in F$ tal que $v_1(y) > 0$ e $v_2(y), \cdots, v_{n-1}(y) < 0$. Se $v_n(y) < 0$ já temos a afirmação. Suponha $v_n(y) \geq 0$. Podemos então escolher $z \in F$ tal que $v_1(z) > 0$ e $v_n(z) < 0$. Tome

assim $u := y + z^r$, onde $r \geq 1$ é tomado de maneira que $rv_i(z) \neq v_i(y)$, para $i = 1, \cdots, n-1$. Daí

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

para todo $i = 2, \cdots, n$. Note que neste caso a igualdade pode ser tomada, pois $v_i(y) \neq rv_i(z)$ e o resultado segue.

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

Tome u como na afirmação 1 e defina $w := (1+u^s)^{-1}$. Para s suficientemente grande temos

$$v_1(w-1) = v_1\left(\frac{1}{1+u^s} - 1\right) = v_1\left(\frac{-u^s}{1+u^s}\right) = v_1(-u^s) + v_1\left(\frac{1}{1+u^s}\right) = sv_1(u) > r_1,$$

pois para s suficientemente grande temos

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

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

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

Escolha $s \in \mathbb{Z}$ tal que $v_i(y_j) \geq s, \forall i, j \in \{1, \cdots, n\}$. Pela Afirmação 2 existem $w_1, \cdots, w_n$ tais que

$$v_i(w_i - 1) > r_i - s \quad \text{e} \quad v_i(w_j) > r_i - s, \text{ para todo } j \neq i.$$

Assim, tomando $z := \sum_{j=1}^{n} y_j w_j$ temos a afirmação.

Pela Afirmação 3, podemos encontrar $z \in F$ com $v_i(z - x_i) > r_i$, para todo $i = 1, \cdots, n$. Escolhemos z_i, com $v_i(z_i) = r_i$. Ainda pela Afirmação 3, existe z' tal que $v_i(z' - z_i) > r_i$, para todo $i = 1, \cdots, n$. Daí

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

Tomando $x := z + z'$, temos

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

e está provado o teorema.

□

Corolário 1.24. *Todo corpo de funções possui infinitos lugares.*

De fato, suponha que um corpo de funções possua finitos lugares $P_1, \cdots, P_n$. Pelo Teorema da aproximação fraca existe $x \in F$ tal que $v_{P_i}(x) > 0$, para todo

$i = 1, \cdots, n$. Dessa forma x possui n zeros mas nenhum polo, o que contradiz o Corolário 1.22.

Proposição 1.25. *Seja F/K um corpo de funções e sejam $P_1, \cdots, P_r$ zeros de um elemento $x \in F$. Então*

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

Demonstração: Para facilitar a escrita vamos denotar $v_i := v_{P_i}$, $f_i = \deg P_i$ e $e_i = v_i(x)$, ou seja, vamos provar a desigualdade

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

Note que, como $P_1, \cdots, P_r$ são zeros de x, $\sum_{i=1}^{r} e_i f_i > 0$.

Para todo i existe um elemento $t_i \in F$ tal que

$$v_i(t_i) = 1 \text{ e } v_k(t_i) = 0, \quad \text{para} \quad k \neq i.$$

Escolha $s_{i1}, \cdots, s_{if_i} \in \mathcal{O}_{P_i}$ tais que $s_{i1}(P_i), \cdots, s_{if_i}(P_i)$ formam uma base para o corpo de resíduos F_{P_i} sobre K. Pelo Teorema da aproximação fraca podemos encontrar $z_{ij} \in F$ tal que, para todo i, j,

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

Para provar o resultado basta mostrar que os elementos

$$t_i^a \cdot z_{ij}, \text{ com } 1 \leq i \leq r, 1 \leq j \leq f_i, 0 \leq a < e_i$$

são linearmente independentes sobre $K(x)$, pois estes elementos são iguais em número a $\sum_{i=1}^{r} f_i e_i$.

Suponha que exista uma combinação linear não trivial

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i - 1} \phi_{ija}(x) t_i^a z_{ij} = 0, \tag{1.5}$$

onde $\phi_{ija}(x) \in K(x)$. Como este somatório triplo está igualado a zero podemos supor, sem perda de generalidade, $\phi_{ija}(x) \in K[x]$ e que pelo menos um dos $\phi_{ija}(x)$ não é divisível por x. Então existem índices $k \in \{1, \cdots, r\}$ e $c \in \{0, \cdots, e_k - 1\}$ tais que

$$x \mid \phi_{kja}(x), \text{ para todo } a < c \text{ e todo } j \in \{1, \cdots, f_k\}$$

$$x \nmid \phi_{kjc}(x), \text{ para algum } j \in \{1, \cdots, f_k\}. \tag{1.6}$$

Multiplicando (1.5) por t_k^{-c}, temos

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \phi_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0. \tag{1.7}$$

Para $i \neq k$ todos os somandos de (1.7) estão em P_k, pois

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

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

$$v_k(\phi)_{kja}(x) t_k^{a-c} \geq e_k + a - c \geq e_k - c > 0.$$

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

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

Combinando esses resultados com (1.7) temos

$$\sum_{j=1}^{f_k} \phi_{kjc}(x) z_{kj} \in P_k. \tag{1.8}$$

Note que $\phi_{kjc}(x)(P_k) \in K$ e, por (1.6), nem todos $\phi_{kjc}(x)(P_k) = 0$. Portanto (1.8) é uma combinação linear não trivial sobre K

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

o que é uma contradição, pois $z_{k1}(P_k), \cdots, z_{kf_k}(P_k)$ é uma base de F_{P_k} sobre K.

□

Corolário 1.26. *Em um corpo de funções F/K todo elemento $0 \neq x \in F$ possui apenas um número finito de zeros e polos.*

De fato, se x é uma constante $v_P(x) = 0$ para todo lugar P, logo x não possui zeros ou polos. Se x é transcendente sobre K, pela proposição 1.25, o número de zeros deve ser menor ou igual a $[F : K(x)]$. O mesmo argumento mostra que x^{-1} tem apenas um número finito de zeros, logo x também possui um número finito de polos.

1.2 Corpo das funções racionais

Para exemplificar os resultados vistos até aqui vamos analisar os conceitos de valorização e lugar do corpo de funções mais simples que existe: o corpo das funções racionais.

Seja $F = K(x)$, com x transcendente sobre K. Dado um polinômio mônico irredutível $p(x) \in K[x]$, temos o anel de valorização

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, p(x) \nmid g(x) \right\}$$

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

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, p(x) | f(x) \text{ e } p(x) \nmid g(x) \right\} \tag{1.9}$$

No caso particular em que $p(x) = x - \alpha, \alpha \in K$, abreviamos a escrita

$$P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)}.$$

Existe um outro anel de valorização de $K(x)/K$, dado por

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, \ deg f(x) \leq deg\ g(x) \right\}$$

com ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, deg f(x) < deg\ g(x) \right\}. \tag{1.10}$$

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

Proposição 1.27. *Seja $F = K(x)$ o corpo de funções racionais.*

(a) Seja $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ o lugar definido por (1.9), onde $p(x) \in K[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo de P e a valorização v_P pode ser descrita da seguinte forma: Se $z \in K(x) \setminus \{0\}$ é escrito na forma $z = p(x)^n \cdot (f(x)/g(x))$, com $n \in \mathbb{Z}, f(x), g(x) \in K[x], p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo de resíduos $K(x)_P = \mathcal{O}_P/P$ é isomorfo a $K[x]/(p(x))$, com o isomorfismo dado por

$$\phi : \begin{cases} K[x]/(p(x)) & \to & K(x)_P, \\ f(x) mod\ p(x) & \longmapsto & f(x)(P). \end{cases}$$

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

(b) No caso em que $p(x) = x - \alpha$, com $\alpha \in K$, o grau de $P = P_\alpha$ é 1 e a

aplicação de classes residuais é dada por

$$z(P) = z(\alpha), \quad \text{para } z \in K(x),$$

onde $z(\alpha)$ é definido da seguinte maneira: Escreva $z = f(x)/g(x)$, com $f(x)$ e $g(x)$ polinômios relativamente primos em $K[x]$. Então

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

(c) Seja $P = P_\infty$ o lugar infinito de $K(x)/K$ definido por (1.10). Então $degP_\infty = 1$. Um elemento primo de P_∞ é $t = 1/x$. A correspondente valorização discreta v_∞ é dada por

$$v_\infty(f(x)/g(x)) = deg\ g(x) - deg\ f(x),$$

com $f(x), g(x) \in K[x]$. A aplicação de classes residuais correspondente a P_∞ é determinada por $z(P_\infty) = z(\infty)$, onde $z(\infty)$ é definido da seguinte maneira: se

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

então

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

Demonstração:

(a) Seja $P = P_{p(x)}$, com $p(x) \in K[x]$ um polinômio irredutível. Temos $P_{p(x)} \subsetneq \mathcal{O}_{p(x)}$ e $P_{p(x)} = t\mathcal{O}$. Como $P_{p(x)} := \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, p(x) | f(x) \text{ e } p(x) \nmid g(x) \right\}$ temos que $p(x)$ gera $P_{p(x)}$ e, assim, $p(x)$ é um elemento primo de P. Assim, dado $z \in K(x) \setminus \{0\}$ temos $z = p(x)^n \cdot \left(\frac{f(x)}{g(x)} \right)$, com $f(x), g(x) \in K[x], n \in \mathbb{N}, p(x) \nmid f(x)$, $p(x) \nmid g(x)$ e $v_P(z)$ é definido como $v_P(z) = n$. Vamos mostrar agora que $K(x)_P = \dfrac{\mathcal{O}_P}{P}$ é isomorfo a $K[x]/(p(x))$. Considere o homomorfismo de anéis

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

Temos então $Ker\Psi = (p(x))$. Vamos mostrar que Ψ é sobrejetora. Seja $z \in \mathcal{O}_{p(x)}$. Então $z = \frac{u(x)}{v(x)}$, com $u(x), v(x) \in K[x]$ e $p(x) \nmid v(x)$. Como $p(x)$ é irredutível, $v(x) \nmid p(x)$, ou seja, $mdc\{p(x), v(x)\} = 1$. Daí existem $a(x), b(x) \in K[x]$ tais que

$$a(x)p(x) + b(x)v(x) = 1.$$

Então

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

Daí $z(P) = (b(x)u(x))(P)$, logo $z(P)$ é imagem de $b(x)u(x) \in K[x]$ e, portanto, Ψ é sobrejetora. Pelo teorema do isomorfismo temos

$$\frac{K[x]}{(p(x))} \simeq K(x)_P.$$

Dessa forma, temos $degP = [K(x)_P : K] = deg\ p(x)$.

(b) Seja $P = P_\alpha, \alpha \in K$. Tome $f(x) \in K[x]$. Então $(x-\alpha)|[f(x) - f(\alpha)]$. De fato, existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x)(x-\alpha) + r(x),$$

onde $r(x) \in K$, pois $\partial r(x) = 0$. Temos também

$$f(\alpha) = q(\alpha)(x-\alpha) + r(\alpha).$$

Subtraindo as duas igualdades e usando o fato de que $r(x) = r(\alpha)$, temos

$$f(x) - f(\alpha) = (q(x) - q(\alpha))(x-\alpha) \Rightarrow (x-\alpha)|f(x) - f(\alpha).$$

Daí, passando o quociente, temos

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

Logo, usando um elemento arbitrário $z = \dfrac{f(x)}{g(x)}$, com $f(x), g(x) \in K[x]$ relativamente primos e $(x-\alpha) \nmid g(x)$, temos $g(x)(P) = g(\alpha) \neq 0$, e daí

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

Definindo $z(\alpha) := \infty$ se $g(\alpha) = 0$, temos

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

Assim, como $p(x)$ é linear, temos $degP = 1$.

(c) Como $P_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], g(x) \neq 0, degf(x) < deg\ g(x) \right\}$, então $\frac{1}{x} \in P_\infty$. Vamos mostrar que $\frac{1}{x}$ é um elemento primo de P_∞. Seja $z \in P_\infty$. Então $z = \dfrac{f(x)}{g(x)}$, com $deg\ f(x) < deg\ g(x)$. Assim podemos escrever

$$z = \frac{1}{x} \cdot \frac{xf(x)}{g(x)}, \text{ com } deg(xf(x)) \leq deg\ g(x).$$

Daí $z \in \frac{1}{x}\mathcal{O}_\infty$, ou seja, $\frac{1}{x}$ gera P_∞ e, portanto, é um elemento primo de P_∞. De maneira natural temos $v_\infty(z) = v\left(\dfrac{f(x)}{g(x)}\right) = deg\ g - deg\ f$. A classe de resíduos é definida de maneira usual.

Teorema 1.28. *Os únicos lugares do corpo de funções racionais $K(x)/K$ são $P_{p(x)}$ e P_∞.*

Demonstração: Seja P um lugar de $K(x)/K$. Vamos dividir essa demonstração em dois casos:

Caso 1: $x \in \mathcal{O}_P$. Neste caso $K[x] \subseteq \mathcal{O}_P$. Seja $I = K[x] \cap P$. Então I é um ideal de $K[x]$. Assim a aplicação de classes de resíduos induz uma inclusão

$$\frac{K[x]}{I} \hookrightarrow K(x)_P.$$

Como $[K(x)_P : K] < \infty$, temos $I \neq \{0\}$. Assim, existe um polinômio mônico e irredutível $p(x) \in K[x]$ tal que $I = K[x] \cap P = p(x) \cdot K[x]$. Daí, dado $g(x) \in K[x]$ com $p(x) \nmid g(x)$, temos $g(x) \notin I \Rightarrow g(x) \notin P$. Logo $\frac{1}{g(x)} \in \mathcal{O}_P$. Então

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

Como todo anel de valorização $\mathcal{O}$ de F/K é um subanel maximal próprio de F, pelo Teorema 1.15 temos $\mathcal{O}_p(x) = \mathcal{O}_P$.

Caso 2: Suponha $x \notin \mathcal{O}_P$. Então, como $\mathcal{O}_P$ é anel de valorização, $x^{-1} \in \mathcal{O}_P$ e daí $K[x^{-1}] \subseteq \mathcal{O}_P$. Logo $x^{-1} \in P \cap K[x^{-1}]$ e $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. Assim, temos

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

Portanto, $\mathcal{O}_P = \mathcal{O}_{p(x)}$ ou $\mathcal{O}_P = \mathcal{O}_\infty$. Como os ideais maximais dos anéis de valorização são únicos, pois estes são locais, segue que os únicos lugares do corpo de funções racionais são $P_p(x)$ e P_∞.

□

Como corolário imediato, temos

Corolário 1.29. *Existe uma bijeção entre os lugares de grau um de $K(x)/K$ e $K \cup \{\infty\}$.*

1.3 Divisores

Nessa seção vamos definir e apresentar resultados de um grupo de extrema importância no Teorema de Riemann-Roch: o grupo dos divisores.

A partir desta seção F/K denotará um corpo de funções e K será um corpo algebricamente fechado.

Definição 1.30. *O* ***grupo divisor*** *de F/K é definido como o grupo abeliano livre aditivo gerado pelos lugares de F/K e é denotado por Div(F). Os elementos de $Div(F)$ são chamados* ***divisores*** *de F/K. Em outras palavras, um divisor é uma soma formal*

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

com $n_P \in \mathbb{Z}$ e com apenas um número finito de n_P não nulos.

Um divisor da forma $D = P$, com $P \in \mathbb{P}_F$, é chamado **divisor primo.**

Dois divisores $D = \sum n_P P$ e $D' = \sum n'_P P$ são somados da seguinte forma:

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

O elemento neutro de $Div(F)$ é o divisor

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

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P \in \mathbb{P}_F} n_P P \in Div(F)$, definimos $v_Q(D) = n_Q$ e daí podemos escrever

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

Definimos uma relação de ordem parcial em $Div(F)$ por

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

Se $D_1 \leq D_2$ e $D_1 \neq D_2$ vamos escrever $D_1 < D_2$. Um divisor D tal que $D \geq 0$, ou seja, $v_P(D) \geq 0$, para todo $P \in \mathbb{P}_F$, é chamado **divisor positivo ou efetivo.**

O grau de um divisor é definido por

$$degD := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot degP,$$

onde a aplicação $deg : Div(F) \to \mathbb{Z}$ é um homomorfismo de grupos. Assim, dados $A, B \in Div(F)$ temos $deg(A + B) = degA + degB$.

Pelo Corolário 1.26, sabemos que todo elemento $0 \neq x \in F$ possui apenas um número finito de zeros e polos. Portanto, a seguinte definição faz sentido.

Definição 1.31. *Seja $0 \neq x \in F$. Denote por Z o conjunto de zeros de x e por N o conjunto de polos. Então definimos*

- $(x)_0 := \sum_{P \in Z} v_P(x)P$ *o* ***divisor zero*** *de x.*
- $(x)_\infty := \sum_{P \in N} (-v_P(x))P$ *o* ***divisor polo*** *de x.*
- $(x) := (x)_0 - (x)_\infty$ *o* ***divisor principal*** *de x.*

Temos $v_P(x) > 0,$ para todo $P \in Z$, e daí os coeficientes de $(x)_0$ são positivos. Além disso, $v_P(x) < 0,$ para todo $P \in N$, e daí $-v_P(x) > 0$ e os coeficientes de $(x)_\infty$ também são positivos. Assim, temos

$$(x) = (x)_0 - (x)_\infty = \sum_{P \in \mathbb{P}_F} v_P(x) \cdot P.$$

Observação 1.32. *Os elementos $0 \neq x \in F$ que são constantes são caracterizados por*

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

De fato, se $x \in K$, então x não possui zeros ou polos, logo $v_P(x) = 0, \forall P \in \mathbb{P}_F$, e daí $(x) = 0$. Reciprocamente, suponha $(x) = 0$. Então $\sum_{P \in Z} v_P(x)P - \sum_{Q \in N} v_Q(x)Q = 0$. Se existisse $P \in \mathbb{P}_F$ tal que $v_P(x) \neq 0$, P deveria ser zero e polo de x, o que é impossível. Portanto $v_P(x) = 0,$ para todo $P \in \mathbb{P}_F$ e $x \in K$.

Definição 1.33. *O conjunto de divisores*

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

é chamado ***grupo de divisores principais de*** *F/K. $Princ(F)$ é um subgrupo de $Div(F)$ pois $(xy) = (x) + (y),$ para todo $0 \neq x, y \in F$.*

O grupo $Cl(F) = Div(F)/Princ(F)$ é chamado ***grupo das classes de*** *F/K.*

Dado $D \in Div(F)$, seu correspondente no grupo das classes é dado por $[D]$, que representa a classe do divisor D. Dois divisores $D, D' \in Div(F)$ são equivalentes e denotados por $D \sim D'$, se $[D] = [D']$, isto é, $D = D' + (x)$, para $x \in F \setminus \{0\}$.

Definição 1.34. *Para um divisor $A \in Div(F)$, definimos o* ***espaço de Riemann-Roch associado a*** *A por*

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

Da definição segue que os elementos $x \in F$ que pertencem a $\mathcal{L}(A)$ são tais que $v_P((x)) \geq v_P(-A)$, para todo $P \in \mathbb{P}_F$. Podemos então fazer a seguinte

interpretação: Se $A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, com $n_i > 0, m_j > 0$, temos $-A = \sum_{j=1}^{s} m_j Q_j - \sum_{i=1}^{r} n_i P_i$, e assim $\mathcal{L}(A)$ consiste dos elementos que:

- têm zeros de ordem maior ou igual a m_j em Q_j para $j = 1, \cdots, s$, e
- têm polos no máximo em $P_1, \cdots, P_r$, com a ordem dos polos limitada por n_i, para $i = 1, \cdots, r$.

Observação 1.35. *Seja $A \in Div(F)$. Então $\mathcal{L}(A) \neq \{0\}$ se, e somente se existe um divisor $A' \sim A$, com $A' \geq 0$.*

De fato, se $\mathcal{L}(A) \neq \{0\}$ então existe $x \in F$ tal que $(x) \geq -A = -A' + (x)$, logo$0 \geq -A'$, e daí $A' \geq 0$. Reciprocamente, se $A \sim A'$, com $A' \geq 0$, temos $A' = A + (x) \geq 0$, o quem implica $(x) \geq -A$.

Lema 1.36. *Seja $A \in Div(F)$. Então:*

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

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

Demonstração: (a) Sejam $x, y \in \mathcal{L}(A)$ e $a \in K$. Então, para todo $P \in \mathbb{P}_F$, temos

- $v_P(x + y) \geq min\{v_P(x) + v_P(y)\} \geq -v_P(A)$.
- $v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A)$.
  Daí $x + y \in \mathcal{L}(A)$ e $ax \in \mathcal{L}(A)$. Portanto $\mathcal{L}(A)$ é um espaço vetorial sobre K.

(b) Como $A \sim A'$, temos $A = A' + (z)$, com $0 \neq z \in F$. A aplicação

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

é linear, pois $\psi(x + y) = (x + y)z = xz + yz = \psi(x) + \psi(y)$, cuja imagem está contida em $\mathcal{L}(A')$, pois $(xz) = (x) + (z) \geq -A + (z)$ e, portanto, $xz \in \mathcal{L}(A')$.

De maneira análoga, temos

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

é uma aplicação linear de $\mathcal{L}(A')$ em $\mathcal{L}(A)$. Como uma é inversa da outra, temos que $\mathcal{L}(A)$ e $\mathcal{L}(A')$ são isomorfos.

□

Lema 1.37. *(a)* $\mathcal{L}(0) = K$.

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

Demonstração: (a) Temos $(x) = 0$ para $0 \neq x \in K$. Então $K \subseteq \mathcal{L}(0)$. Por outro lado, dado $x \in \mathcal{L}(0), x \neq 0$, temos $(x) \geq 0$. Isso significa que x não possui polos, logo x não pode ser transcendente sobre K e daí $x \in K$. Portanto $\mathcal{L}(0) = K$.

(b) Seja $A < 0$ e suponha que exista $0 \neq x \in \mathcal{L}(A)$. Então $(x) \geq -A > 0$, ou seja, x possui pelo menos um zero, mas não possui polos, o que é absurdo. Assim $\mathcal{L}(A) = \{0\}$.

□

Vamos mostrar agora que o espaço de Riemann-Roch $\mathcal{L}(A)$ tem dimensão finita para qualquer divisor $A \in Div(F)$.

Lema 1.38. *Sejam* A *e* B *divisores de* F/K *com* $A \leq B$. *Então* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e*

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

Demonstração: Como $A \leq B$ temos $-A \geq -B$. Seja $x \in \mathcal{L}(A)$. Então $(x) \geq -A \geq -B \Rightarrow x \in \mathcal{L}(B)$. Logo $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.

Suponha $B = A + P$, com $P \in \mathbb{P}_F$. O caso geral segue por indução. Escolha um elemento $t \in F$ tal que $v_P(t) = v_P(B) = v_P(A) + 1$. Dado $x \in \mathcal{L}(B)$,

$$v_P(x) \geq -v_P(B) = -v_P(t).$$

Daí temos $xt \in \mathcal{O}_P$, pois $v_P(x) \geq -v_P(t) \Rightarrow v_P(x) + v_P(t) \geq 0$ e $v_P(xt) = v_P(x) + v_P(t)$. Dessa forma obtemos uma aplicação K-linear

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

Um elemento $x \in Ker\psi$ se, e somente se $v_P(xt) > 0$, pois os elementos de P são os que possuem valorização positiva. Daí, $v_P(x)+v_P(t) > 0 \Rightarrow v_P(x)+v_P(A)+1 > 0 \Rightarrow v_P(x) > -v_P(A) - 1 \Rightarrow v_P(x) \geq -v_P(A)$. Então $Ker\psi = \mathcal{L}(A)$ e, pelo teorema do isomorfismo temos, $\dfrac{\mathcal{L}(B)}{\mathcal{L}(A)} \simeq Im\psi \subseteq F_P$. Portanto

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq dimF_P = degP = degB - degA,$$

pois, como $B = A + P$ e aplicação grau é um homomorfismo, $deg(P) = deg(B) - deg(A)$.

□

Proposição 1.39. *Para cada divisor* $A \in Div(F)$, *o espaço* $\mathcal{L}(A)$ *é um espaço vetorial de dimensão finita sobre* K. *Mais precisamente, se* $A = A_+ - A_-$, *com*

divisores positivos A_+ e A_- então

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

Demonstração: Como $A \leq A_+$, então $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Deste modo é suficiente mostrar a desigualdade

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

Como A_+ é um divisor positivo, temos $A_+ \geq 0$, daí, pelo Lema 1.38,

$$dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq degA_+ - deg0.$$

Como $\mathcal{L}(0) = K$, temos $deg0 = 0$ e, além disso,

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

□

Definição 1.40. *Para $A \in Div(F)$, o inteiro $\ell(A) := dim\mathcal{L}(A)$ é chamado* ***dimensão do divisor A****.*

Um dos problemas mais importantes da teoria de corpo de funções algébricas é o cálculo da dimensão de um divisor. A solução deste problema é o Teorema de Riemann-Roch, que será demonstrado no próximo capítulo.

Teorema 1.41. *Todos os divisores principais tem grau zero. Mais precisamente, sejam $x \in F \setminus K$ e $(x)_0, (x)_\infty$ os divores zero e polo de x, respectivamente. Então*

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

Demonstração: Seja $n = [F : K(x)]$. Tome $B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P_i$, onde $P_1, \cdots, P_r$ são polos de x, ou seja, $v_{P_i}(x) < 0, \forall i = 1, \cdots, r$. Então temos $degB = \sum v_{P_i}(x^{-1}) \cdot degP_i \leq [F : K(x)]$, pela Proposição 1.25. Note que precisamos calcular $v_{P_i}(x^{-1})$, para que os P_i's sejam zeros, e daí poder usar a Proposição 1.25. Disso concluímos que $degB \leq n$.

Vamos mostrar que $n \leq degB$. Seja $u_1, \cdots, u_n$ uma base de $F/K(x)$ e seja $C \geq 0$ um divisor positivo tal que $(u_i) \geq -C$, ou seja, $u_i \in \mathcal{L}(C), \forall i = 1, \cdots, n$. Os elementos da forma $x^i u_j$, com $0 \leq i \leq l$ e $1 \leq j \leq n$ pertencem a $\mathcal{L}(lB + C)$ para todo $l \geq 0$, pois $(x^i u_j) = (x^i) + (u_j) \geq -lB - C$. Note ainda que, como são linearmente independentes sobre $K(x)$, os elementos $x^i u_j$ são linearmentente independentes sobre K. Daí temos

$$\ell(lB + C) \geq n(l + 1).$$

Tomando $c := degC$ temos, pela Proposição 1.39 e usando $lB + C \geq 0$,

$$n(l + 1) \leq \ell(lB + C) \leq deg(lB + C) + 1 = ldegB + c + 1.$$

$$\Rightarrow ldegB - nl \geq n - c - 1 \Rightarrow l(degB - n) \geq n - c - 1, \forall l \in \mathbb{N}.$$

Como o lado direito da desigualdade independe de l, a desigualdade só é possível se $n \leq degB$.

Daí temos $deg(x)_\infty = [F : K(x)]$. Como $(x)_0 = (x^{-1})_\infty$, concluímos que $deg(x)_0 = deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$.

□

Corolário 1.42. *(a) Sejam A, A' divisores com $A \sim A'$. Então $\mathcal{L}(A) = \mathcal{L}(A')$ e $degA = degA'$.*

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

(c) Seja A um divisor de grau 0. As seguintes afirmações são equivalentes:

1. *A é principal;*
2. *$\ell(A) \geq 1$;*
3. *$\ell(A) = 1$.*

Demonstração:

(a) Pelo Lema 1.36, se $A \sim A'$ então $\mathcal{L}(A) \simeq \mathcal{L}(A')$ o que implica $\ell(A) = \ell(A')$. Se $A \sim A'$, então

$$A = A' + (x) \Rightarrow degA = degA' + deg(x) \Rightarrow degA = degA',$$

pois (x) é divisor principal.

(b) Suponha $\ell(A) > 0$. Então $\mathcal{L}(A) \neq \{0\}$. Pela observação 1.35 existe um divisor $A' \sim A$ tal que $A' \geq 0$. Daí $degA' = degA \geq 0$, o que contradiz a hipótese. Logo $\ell(A) = 0$.

(c) (1)⇒(2) Seja $A = (x)$ um divisor principal. Então

$$\mathcal{L}(A) = \{y \in F | (y) \geq -(x)\}$$

e isso implica $x^{-1} \in \mathcal{L}(A)$, e daí $\ell(A) \geq 1$.

(2)⇒(3) Sejam $\ell(A) \geq 1$ e $degA = 0$. Então, pela Observação 1.35 existe um divisor $A' \sim A$ com $A' \geq 0$. Daí temos $A' \geq 0$ e $degA' = 0$ o que implica $A' = 0$. Então $\ell(A) = \ell(A') = \ell(0) = 1$.

(3)⇒(1) Suponha $\ell(A) = 1$ e $degA = 0$. Seja $z \in \mathcal{L}(A)$. Daí $(z) + A \geq 0$. Como $deg((z) + A) = 0$ segue que

$$(z) + A = 0 \Rightarrow A = -(z) \Rightarrow A = (z^{-1}),$$

logo A é principal.

□

Vamos mostrar agora a existência de um limite inferior para $\ell(A)$.

Proposição 1.43. *Existe uma constante $\gamma \in \mathbb{Z}$ tal que, para todos os divisores $A \in Div(F)$, temos*

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

Demonstração: Note que se $A_1 \leq A_2$ então, pelo Lema 1.38, $\mathcal{L}(A_1) \subseteq \mathcal{L}(A_2)$ e

$$dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leq degA_2 - degA_1.$$

Por outro lado temos $dim\mathcal{L}(A_2) - dim\mathcal{L}(A_1) = dim(\mathcal{L}(A_2)/\mathcal{L}(A_1))$. Daí

$$\begin{array}{rl} & \ell(A_2) - \ell(A_1) \leq degA_2 - degA_1 \\ \Rightarrow & degA_1 - \ell(A_1) \leq degA_2 - \ell(A_2) \end{array}$$

Fixe $x \in F/K$ e tome o divisor polo $B := (x)_\infty$. Usando a demonstração do Teorema 1.41 existe um divisor $C \geq 0$ tal que

$$\ell(lB + C) \geq (l+1) \cdot degB, \text{ para todo } l \in \mathbb{N}.$$

Por outro lado temos, pelo Lema 1.38,

$$\ell(lB + C) \leq \ell(lB) + degC,$$

pois $dim(\mathcal{L}(lB + C)/\mathcal{L}(lB)) = \ell(lB + C) - \ell(lB) \leq deg(lB + C) - deg(lB) \Rightarrow \ell(lB + C) \leq \ell(lB) + degC$.

Combinando estas desigualdades, temos

$$\begin{array}{rl} \ell(lB) & \geq \ell(lB + C) - degC \geq (l+1)degB - degC \\ & = deg(lB) + degB - degC \\ & = deg(lB) + [F : K(x)] - degC. \end{array}$$

Chamando $[F : K(x)] - degC = -\gamma$, temos

$$\gamma \geq deg(lB) - \ell(lB), \text{ com } \gamma \in \mathbb{Z}.$$

Precisamos mostrar que a desigualdade acima é válida mesmo se substituirmos lB por um divisor qualquer $A \in Div(F)$.

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

Dado um divisor A é possível escolher $A_1 \geq A$ tal que $A_1 \geq 0$. Daí

$$\begin{array}{rl} \ell(lB - A_1) & \geq \ell(lB) - degA_1 \text{ (pelo lema 1.38)} \\ & \geq deg(lB) - \gamma - degA_1 \\ & > 0, \text{ para } \ell \text{ suficientemente grande.} \end{array}$$

Assim, como $\ell(lB - A_1) > 0$, existe $0 \neq z \in \mathcal{L}(lB - A_1)$. Tomando $D := A_1 - (z)$ temos $A_1 \sim D$ e $D \leq A_1 - (A_1 - lB) = lB$ e a afirmação está provada.

Dessa afirmação temos a prova da proposição:

Como $A_1 \geq A$, temos

$$\begin{aligned} degA - \ell(A) &\leq deg(A_1) - \ell(A_1) \text{ (pela observação feita no início da prova)} \\ &= degD - \ell(D), \text{ (pois } D \sim A_1) \\ &\leq deg(lB) - \ell(lB) \\ &\leq \gamma \end{aligned}$$

□

Assim encontramos um limite inferior para $\ell(A) : \ell(A) \geq degA - \gamma$.

Observação 1.44. *Note que γ depende apenas de F/K e não do divisor.*

CAPÍTULO 2

O TEOREMA DE RIEMANN-ROCH

O teorema principal deste capítulo é o Teorema de Riemann-Roch, que torna possível o cálculo da dimensão do espaço de Riemann-Roch associado a um divisor. Na tentativa de calcular essa dimensão temos como primeiro resultado o Teorema de Riemann. Veremos também, como consequência do Teorema de Riemann-Roch, o Teorema das Lacunas de Weierstrass, provado em meados de 1860, que possui muita importância no estudo de curvas algébricas. Neste capítulo F/K será um corpo de funções algébricas e K um corpo algebricamente fechado. As definições e resultados deste capítulo podem ser encontrados em [9]

Definição 2.1. *O* ***gênero*** g *de* F/K *é definido por*

$$g := max\{degA - \ell(A) + 1 | A \in Div(F)\}.$$

O gênero é o invariante mais importante de um corpo de funções.

Observação 2.2. *O gênero de* F/K *é um inteiro não negativo.*

De fato, se $A \geq 0$ então, pela Proposição 1.39, temos $\ell(A) \leq 1 + degA$ e daí $g \geq 0$. Agora, se $\ell(A) \neq 0$, pela Observação 1.35, existe $A' \in Div(F)$, com $A' \sim A$ tal que $A' \geq 0$. Assim, basta analisar o caso em que $A = 0$. Pela definição de gênero, temos

$$deg0 - \ell(0) + 1 = 0 - 1 + 1 = 0.$$

Daí $g \geq 0$.

O primeiro resultado obtido na tentativa de calcular a dimensão de um divisor foi provado por Riemann em 1857 e é conhecido como Desigualdade de Riemann ou Teorema de Riemann.

Teorema 2.3 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então:*

(a) Para todo $A \in Div(F), \ell(A) \geq degA + 1 - g$;

(b) Existe um inteiro c, dependendo apenas de F/K, tal que

$$\ell(A) = degA + 1 - g$$

sempre que $degA \geq c$.

Demonstração:

(a) Pela definição de gênero, temos

$$g \geq degA - \ell(A) + 1 \Rightarrow \ell(A) \geq degA + 1 - g.$$

(b) Escolha A_0 de maneira que $g = degA_0 - \ell(A_0) + 1$ e seja $c = degA_0 + g$. Se $degA \geq c$, temos, por (a),

$$\begin{aligned} \ell(A - A_0) \geq deg(A - A_0) + 1 - g \quad &= degA - degA_0 + 1 - g \\ &\geq c - degA_0 + 1 - g \\ &= degA_0 + g - degA_0 + 1 - g = 1. \end{aligned}$$

Daí temos $\ell(A - A_0) \geq 1$, ou seja, existe $0 \neq z \in \mathcal{L}(A - A_0)$. Considere o divisor $A' = A + (z), A' \sim A$ tal que $A' \geq A_0$. Então

$$\begin{aligned} degA - \ell(A) \quad &= degA' - \ell(A') \\ &\geq degA_0 - \ell(A_0) \\ &= g - 1. \end{aligned}$$

Assim $\ell(A) \leq degA + 1 - g$. Comparando com (a), temos $\ell(A) = degA + 1 - g$ sempre que $degA \geq c$.

□

Exemplo 2.4. *Vamos mostrar que o corpo de funções racionais tem gênero zero. Seja P_∞ o divisor polo de x:*

$$P_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \neq 0 \in K[x] \text{ e deg } f(x) < \text{deg } g(x) \right\}.$$

Seja $r \geq 0$. Então

$$\mathcal{L}(rP_\infty) = \left\{ \frac{rh_1(x)}{h_2(x)} \in K(x); \left(\frac{rh_1(x)}{h_2(x)} \right) \geq \text{deg } f(x) - \text{deg } g(x) \right\}.$$

Assim, $1, x, \cdots, x^r$ são elementos linearmente independentes de $\mathcal{L}(rP_\infty)$, ou seja,

$$r + 1 \leq \ell(rP_\infty) = \text{deg } rP_\infty + 1 - g,$$

para r suficientemente grande. Como deg $P_\infty = 1$ *a desigualdade fica da seguinte forma:*

$$r + 1 \leq r + 1 - g \Rightarrow g \leq 0.$$

Como já provamos que $g \geq 0$*, segue que* $g = 0$*.*

Definição 2.5. *Para* $A \in Div(F)$*, o inteiro*

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

é chamado ***índice de especialidade de A.***

Pelo Teorema de Riemann temos

$$\begin{array}{rl} & \ell(A) \geq degA - g + 1 \\ \Rightarrow & i(A) = \ell(A) - degA + g - 1 \geq 0 \end{array}$$

e, para $degA$ suficientemente grande, temos $i(A) = 0$.

Definição 2.6. *Um* ***adele*** *de* F/K *é uma aplicação*

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

tal que $\alpha_P \in \mathcal{O}_P$ *para quase todo* $P \in \mathbb{P}_F$*, ou seja,* $\#\{P \in \mathbb{P}_F | \alpha_P \notin \mathcal{O}_P\} < \infty$*.*

O conjunto $\mathcal{A}_F := \{\alpha | \alpha \text{ é adele de } F/K\}$, que é um espaço vetorial sobre K com as operações usuais, é chamado **espaço de adeles de** F/K**.** O **adele principal** de um elemento $x \in F$ é o adele em que todas as componentes são iguais a x. As valorizações de F/K se extendem naturalmente a $\mathcal{A}_F$, onde $v_P(\alpha) = v_P(\alpha_P)$, com α_P a $P-$componente do adele α. Como $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$, temos $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

Definição 2.7. *Para* $A \in Div(F)$*, definimos*

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

Afirmação: $\mathcal{A}_F(A)$ é um K-subespaço de $\mathcal{A}_F$.

De fato, sejam $\alpha_1, \alpha_2 \in \mathcal{A}_F(A)$ e $c \in K$. Então

- $v_P(\alpha_1 + \alpha_2) \geq min\{v_P(\alpha_1) + v_P(\alpha_2)\} \geq -v_P(A)$;
- $v_P(c\alpha_1) = v_P(c) + v_P(\alpha_1) = v_P(\alpha_1) \geq -v_P(A)$.

Teorema 2.8. *Para todo divisor A, o índice de especialidade é*

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

Neste teorema *dim* representa dimensão como K-espaço vetorial. Note que, apesar de os espaços $\mathcal{A}_F, \mathcal{A}_F(A)$ e F terem dimensão infinita sobre K, o quociente tem dimensão finita sobre K, a saber o índice de especialidade.

Demonstração: Vamos dividir a demonstração em 3 afirmações:

- **Afirmação 1**: Sejam $A_1, A_2 \in Div(F)$ e $A_1 \leq A_2$. Então $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ e
$$dim(A_F(A_2)/\mathcal{A}_F(A_1)) = degA_2 - degA_1. \tag{2.1}$$

  De fato, seja $\alpha \in \mathcal{A}_F(A_1)$. Então $v_P(\alpha) \geq -v_P(A_1)$, para todo $P \in \mathbb{P}_F$. Mas como $A_1 \leq A_2$, temos

  $$-A_1 \geq -A_2 \Rightarrow -v_P(A_1) \geq v_P(A_2) \Rightarrow v_P(\alpha) \geq -v_P(A_2), \text{ para todo } P \in \mathbb{P}_F,$$

  e daí $\alpha \in \mathcal{A}_F(A_2)$. Portanto $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.

  Para mostrar a igualdade (2.1) vamos supor $A_2 = A_1 + P$, com $P \in \mathbb{P}_F$. O caso geral segue por indução. Escolha $t \in F$ tal que $v_P(t) = v_P(A_1) + 1$ e considere a aplicação

  $$\begin{array}{rccc} \Phi: & \mathcal{A}_F(A_2) & \longrightarrow & F_P \\ & \alpha & \longmapsto & (t\alpha_P)(P) \end{array}$$

  Afirmamos que Φ é uma aplicação sobrejetora e $Ker\Phi = \mathcal{A}_F(A_1)$. De fato, temos

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

  Daí, pelo Teorema do Isomorfismo, temos

  $$\frac{\mathcal{A}_F(A_2)}{\mathcal{A}_F(A_1)} \simeq F_P$$

  Como $A_2 = A_1 + P$, então $degP = degA_2 - degA_1$. Logo

  $$degA_2 - degA_1 = degP = [F_P : K] = dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)).$$

- **Afirmação 2:** Sejam $A_1, A_2 \in Div(F)$ e $A_1 \leq A_2$. Então

  $$dim(\mathcal{A}_F(A_2) + F)/\mathcal{A}_F(A_1) + F) = (degA_2 - \ell(A_2)) - (degA_1 - \ell(A_1)).$$

  Considere a sequência

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

  Vamos mostrar que essa sequência é exata.

  1. $Im\sigma_1 \subseteq Ker\sigma_2$:
  Como $\mathcal{L}(A_2) = \mathcal{A}_F(A_2) \cap F$, dado $x \in \mathcal{L}(A_2)$, temos $x \in F$. Dessa forma

temos

$$\sigma_2(\sigma_1(x+\mathcal{L}(A_1))) = \sigma_2(x+\mathcal{A}_F(A_1)) = 0$$

2. $Ker\sigma_2 \subseteq Im\sigma_1$:
Seja $\alpha \in \mathcal{A}_F(A_2)$ e $\alpha + \mathcal{A}_F(A_1) \in \dfrac{\mathcal{A}_F(A_2)}{\mathcal{A}_F(A_1)}$ tal que $\sigma_2(\alpha+\mathcal{A}_F(A_1)) = 0$. Então $\alpha \in \mathcal{A}_F(A_1) + F$ e daí existe $x \in F$ tal que $\alpha - x \in \mathcal{A}_F(A_1)$. Como $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ pela Afirmação 1, temos $\alpha - x \in \mathcal{A}_F(A_2)$, e daí $x = \alpha - (\alpha - x) \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$. Portanto, temos

$$\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x+\mathcal{L}(A_1)) \Rightarrow \alpha + \mathcal{A}_F(A_1) \in Im\sigma_1.$$

Com isso concluímos que a sequência é exata, e daí

$$dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) + dim((\mathcal{A}_F(A_1)+F)/(\mathcal{A}_F(A_2)+F))$$

$$\begin{aligned} \Rightarrow dim(\mathcal{A}_F(A_2)+F/\mathcal{A}_F(A_1)+F) &= dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1))/dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \\ &= (degA_2 - degA_1) - (\ell(A_2) - \ell(A_1)) \\ &= (degA_2 - \ell(A_2)) - (degA_1 - \ell(A_1)) \end{aligned}$$

onde a segunda igualdade segue da Afirmação 1.

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

  Para iniciar a demonstração observe que, dado $B_1 \in Div(F)$, se $B_1 \geq B$ temos, pelo Lema 1.38,

  $$\begin{aligned} &dim(\mathcal{L}(B_1)/\mathcal{L}(B)) = \ell(B_1) - \ell(B) \leq degB_1 - degB \\ &\Rightarrow \ell(B_1) \leq \ell(B) + degB_1 - degB = degB_1 + 1 - g, \end{aligned} \tag{2.2}$$

  pela hipótese da afirmação.

  Por outro lado, pelo Teorema de Riemann, temos

  $$\ell(B_1) \geq degB_1 + 1 - g. \tag{2.3}$$

  Daí, comparando (2.2) e (2.3), temos $\ell(B_1) = degB_1 + 1 - g$, para todo $B_1 \geq B$.

  Vamos demonstrar agora que $\mathcal{A}_F = \mathcal{A}_F(B)+F$. Já temos $\mathcal{A}_F(B)+F \subseteq \mathcal{A}_F$. Seja $\alpha \in \mathcal{A}_F$. Podemos encontrar um divisor $B_1 \geq B$ tal que $\alpha \in \mathcal{A}_F(B_1)$. Daí temos, pela Afirmação 2,

  $$\begin{aligned} dim((\mathcal{A}_F(B_1)+F)/(\mathcal{A}_F(B)+F)) &= (degB_1 - \ell(B_1)) - (degB - \ell(B)) \\ &= (g-1) - (g-1) = 0 \end{aligned}$$

  Portanto $\mathcal{A}_F(B_1)+F = \mathcal{A}_F(B)+F$. Como $\alpha \in \mathcal{A}_F(B_1), \alpha \in \mathcal{A}_F(B)+F \Rightarrow \mathcal{A}_F(B)+F \supseteq \mathcal{A}_F$.

Seja A um divisor arbitrário. Pelo Teorema de Riemann existe $A_1 \geq A$ tal que $\ell(A_1) = degA_1 + 1 - g$. Pela Afirmação 3, $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$ e, pela Afirmação

2, temos

$$\begin{aligned} dim(\mathcal{A}_F/\mathcal{A}_F(A+F)) &= dim(\mathcal{A}_F(A_1)+F/\mathcal{A}_F(A)+F) \\ &= degA_1 - \ell(A_1) - (degA - \ell(A)) \\ &= (g-1) + \ell(A) - degA = i(A). \end{aligned}$$

□

Observação 2.9. *Como $i(A) := \ell(A) - degA + g - 1$, podemos escrever*

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

que é uma versão preliminar do Teorema do Riemann-Roch.

Corolário 2.10. $g = dim(\mathcal{A}_F/\mathcal{A}_F(0)+F)$

De fato, temos $dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F)) = i(0) = \ell(0) - deg(0) + g - 1 = 1 - 0 + g - 1 = g$.

Definição 2.11. *Uma **diferencial de Weil** de um corpo de funções F/K é uma aplicação K-linear $\omega : \mathcal{A}_F \longrightarrow K$ que se anula em $\mathcal{A}_F(A)+F$, para algum divisor $A \in Div(F)$. Chamamos o conjunto*

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

*de **módulo das diferenciais de Weil de** F/K. Para $A \in Div(F)$, definimos*

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

Consideramos Ω_F como um K-espaço vetorial de modo natural: Sejam $\omega_1, \omega_2 \in \Omega_F$ tais que ω_1 se anula em $\mathcal{A}_F(A_1)+F$ e ω_2 se anula em $\mathcal{A}_F(A_2)+F$. Então $\omega_1+\omega_2$ se anula em $\mathcal{A}_F(A_3)$, com $A_3 \leq A_1$ e $A_3 \leq A_2$, pois $\mathcal{A}_F(A_3)+F \subseteq \mathcal{A}_F(A_1)+F$ e $\mathcal{A}_F(A_3)+F \subseteq \mathcal{A}_F(A_2)+F$.

Lema 2.12. *Para $A \in Div(F)$, temos $dim\Omega_F(A) = i(A)$.*

Demonstração: Temos que $\Omega_F(A)$ é o conjunto das diferenciais de Weil que se anulam em $\mathcal{A}_F(A)+F$, e então $\Omega_F(A)$ é naturalmente isomorfo a $\dfrac{\mathcal{A}_F}{\mathcal{A}_F(A)+F}$. Como $i(A) = dim(\mathcal{A}_F/\mathcal{A}_F(A)+F)$ pelo Teorema 2.8, concluímos que $dim\Omega_F(A) = i(A)$.

□

Definição 2.13. *Para $x \in F$ e $\omega \in \Omega_F$, definimos $x\omega : \mathcal{A}_F \longrightarrow K$ por*

$$(x\omega)(\alpha) = \omega(x\alpha).$$

Observação 2.14. *$x\omega$ também é uma diferencial de Weil de F/K. De fato, se ω se anula em $\mathcal{A}_F(A)+F$ então $x\omega$ se anula em $\mathcal{A}_F(A+(x))+F$.*

Proposição 2.15. *O conjunto Ω_F é um espaço vetorial sobre F de dimensão 1.*

Demonstração: Seja $0 \neq \omega_1 \in \Omega_F$. Para mostrar que Ω_F tem dimensão 1 sobre F precisamos mostrar que, dado $\omega_2 \in \Omega_F$, existe $z \in F$ tal que $\omega_2 = z\omega_1$.

Sejam $A_1, A_2 \in Div(F)$ tais que $\omega_1 \in \Omega_F(A_1)$ e $\omega_2 \in \Omega_F(A_2)$. Seja $B \in Div(F)$ e considere as aplicações K-lineares

$$\begin{array}{rccc} \Psi_i: & \mathcal{L}(A_i+B) & \longrightarrow & \Omega_F(-B) \\ & x & \longmapsto & x\omega_i \end{array}$$

$i = 1, 2$.

Afirmação: Para uma escolha apropriada do divisor B, temos

$$\Psi_1(\mathcal{L}(A_1+B)) \cap \Psi_2(\mathcal{L}(A_2+B)) \neq \{0\}.$$

Se demonstrarmos essa afirmação a Proposição estará demonstrada, pois existem $x_1 \in \mathcal{L}(A_1+B)$ e $x_2 \in \mathcal{L}(A_2+B)$ tais que $x_1\omega_1 = x_2\omega_2 \neq 0 \Rightarrow \omega_2 = (x_2^{-1}x_1)\omega_1$.

Demonstração da afirmação: Vamos utilizar o seguinte fato de Álgebra Linear:

$$dim(U_1 \cap U_2) \geq dimU_1 + dimU_2 - dimV, \tag{2.4}$$

onde U_1, U_2 são subespaços do espaço vetorial V.

Pelo Teorema de Riemann, para $B > 0$ suficientemente grande, temos

$$\ell(A_i + B) = deg(A_i + B) + 1 - g,\ i = 1, 2.$$

Defina $U_i := \Psi_i(A_i + B)$, ou seja, U_i é imagem de Ψ_i e $\Psi_i(A_i + B) \subseteq \Omega_F(-B)$. Daí temos

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

Como $B > 0$, temos $-B < 0$ e $\mathcal{L}(-B) = \{0\}$, ou seja, $dim(-B) = 0$. Além disso temos $v_P(B) > 0$, logo $v_P(-B) < 0$, e daí $-deg(-B) = degB$. Assim

$$dim(-B) - deg(-B) + g - 1 = 0 + degB + g - 1,$$

e, portanto,

$$\begin{aligned} &dimU_1 + dimU_2 - dim\Omega_F(-B) = \\ &= deg(A_1 + B) + 1 - g + deg(A_2 + B) + 1 - g - degB - g + 1 \\ &= degB + [degA_1 + degA_2 + 3(1 - g)]. \end{aligned}$$

Daí, para B suficientemente grande, temos

$$dimU_1 + dimU_2 - dim\Omega_F(-B) > 0,$$

ou seja, por (2.4), $dim(U_1 \cap U_2) > 0$, o que prova a afirmação.

□

Queremos relacionar um divisor a cada diferencial de Weil. Para isso, fixando ω, definimos

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

Lema 2.16. *Seja $0 \neq \omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in M(\omega)$ tal que $A \leq W$, para todo $A \in M(\omega)$.*

Demonstração: Pelo Teorema de Riemann, existe um inteiro c que depende apenas de F/K tal que $i(A) = 0,$ para todo $A \in Div(F)$ com $degA \geq c$.

Pelo Teorema 2.8, temos

$$i(A) = dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) = 0 \Rightarrow \mathcal{A}_F = \mathcal{A}_F(A) + F,$$

ou seja, o adele se anula em todo $\mathcal{A}_F$, logo $\omega = 0$, o que é absurdo. Assim, para $A \in M(\omega)$, temos $degA < c$. Como $c \in \mathbb{Z}$ podemos escolher um divisor $W \in M(\omega)$ de maior grau. Suponha que W não satisfaça a propriedade do Lema, ou seja, existe um divisor $A_0 \in M(\omega)$ com $A_0 > W$, isto é, $v_Q(A_0) > v_Q(W)$ para algum $Q \in \mathbb{P}_F$. Vamos mostrar que $W + Q \in M(\omega)$, o que contradiz a maximalidade de W.

De fato, considere o adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Como $\mathcal{A}_F$ é um espaço vetorial sobre K, podemos escrever $\alpha = \alpha' + \alpha''$, com

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

Daí temos que $\alpha' \in \mathcal{A}_F(W)$ e $\alpha'' \in \mathcal{A}_F(A_0)$, e daí $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. Portanto, ω se anula em $\mathcal{A}_F(W+Q)+F$, o que é absurdo. Disso segue que existe um único $W \in M(\omega)$ tal que $A \leq W,$ para todo $A \in M(\omega)$.

□

Definição 2.17. *(a) O divisor (ω) de uma diferencial de Weil $\omega \neq 0$ é o divisor unicamente determinado de F/K que satisfaz:*

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

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

*(c)Um lugar é dito zero (resp. polo) de ω, se $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). A diferencial de Weil ω é regular em P se $v_P(\omega) \geq 0$ e ω é dita **regular (ou holomórfica)** se é regular em todos os lugares $P \in \mathbb{P}_F$.*

*(d) Um divisor W é dito **divisor canônico** de F/K se $W = (\omega)$, para algum $\omega \in \Omega_F$.*

Observação 2.18. *Temos* $\Omega_F(A) = \{\omega \in \Omega_F | \omega$ *se anula em* $A_F(A) + F\}$. *Então, pela definição anterior, podemos escrever*

$$\Omega_F(A) = \{\omega \in \Omega_F / \omega = 0 \text{ ou } (\omega) \geq A\}.$$

Observe que $\omega = 0$ *se anula em* $\mathcal{A}_F(A) + F$, *por isso adicionamos essa condição na nova definição de* $\Omega_F(A)$.

Temos $\mathcal{A}_F(0) = \{\alpha \in \mathcal{A}_F | v_P(\alpha) \geq 0, \forall P \in \mathbb{P}_F\}$. *Daí podemos escrever*

$$\begin{aligned}\Omega_F(0) &= \{\omega \in \Omega_F | \omega \text{ se anula em } \mathcal{A}_F(0) + F\} \\ &= \{\omega \in \Omega_F | (w) \geq 0\} \\ &= \{\omega \in \Omega_F | v_P(\omega) \geq 0, \text{ para todo } P \in \mathbb{P}_F\} \\ &= \{\omega \in \Omega_F | \omega \text{ é regular}\}.\end{aligned}$$

Proposição 2.19. *(a) Para* $0 \neq x \in F$ *e* $0 \neq \omega \in \Omega_F$, *temos* $(x\omega) = (x) + (\omega)$.

(b) Quaisquer dois divisores canônicos de F/K *são equivalentes.*

Demonstração: (a) Sejam $x \in F$ e $\omega \in \Omega_F$. Se ω se anula em $\mathcal{A}_F(A) + F$, então $x\omega$ se anula em $\mathcal{A}_F(A + (x)) + F$. Assim, pela definição anterior, temos $(x\omega) \geq A + (x)$. Por outro lado $(\omega) \geq A$. Subtraindo essas duas equações, temos $(x\omega) - (\omega) \geq (x) \Rightarrow (x\omega) \geq (x) + (\omega)$. Usando isso temos $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega) \Rightarrow (x\omega) \leq (\omega) - (x^{-1})$. Combinando essas duas desigualdades temos

$$\begin{aligned}(x) + (\omega) \leq (x\omega) \leq (\omega) - (x^{-1}) = (\omega) + (x) \\ \Rightarrow (x) + (\omega) = (x\omega).\end{aligned}$$

(b) Sejam W e W' dois divisores canônicos. Precisamos mostrar que existe um divisor principal (z) tal que $W' = W + (z)$. Como Ω_F é espaço vetorial de dimensão 1 sobre F existe $z \in F$ tal que $W' = zW$. Pela parte (a) temos $(zW) = (z) + W \Rightarrow W' = W + (z)$ e, portanto, $W \sim W'$.

□

Teorema 2.20 (Teorema da dualidade)**.** *Seja* A *um divisor arbitrário e* $W = (\omega)$ *um divisor canônico de* F/K. *Então a aplicação*

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

é um isomorfismo de K-espaços vetoriais. Em particular,

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

Demonstração: Seja $x \in \mathcal{L}(W - A)$. Então

$$(x\omega) = (x) + (\omega) \geq -(W - A) + W = A \Rightarrow x\omega \in \Omega_F(A),$$

onde a primeira igualdade segue da Proposição 2.19 e a implicação segue da Observação 2.18. Daí temos que μ aplica $\mathcal{L}(W - A)$ em $\Omega_F(A)$.

μ **é linear:** Sejam $x, y \in \mathcal{L}(W - A)$ e $c \in K$. Então,

- $\mu(x + y) = (x + y)\omega = x\omega + y\omega = \mu(x) + \mu(y)$.
- $\mu(cx) = (cx)\omega = c(x\omega) = c\mu(x)$.

μ **é injetora:** Suponha $\mu(x) = x\omega = 0$. Como $\omega \neq 0$, temos $x = 0$ e daí $Ker\mu = \{0\}$ e μ é injetora.

μ **é sobrejetora:** Seja $\omega_1 \in \Omega_F(A)$. Como $\Omega_F(A)$ tem dimensão 1 sobre F, podemos escrever $\omega_1 = x\omega$ para $x \in F$. Daí

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A, (\text{ pois } \omega_1 \in \Omega_F(A))$$

e assim temos

$$(x) \geq A - W = -(W - A) \Rightarrow x \in \mathcal{L}(W - A) \text{ e } \omega_1 = \mu(x).$$

Dessa forma, como μ é bijeção, temos $\ell(W - A) = dim\Omega_F(A) = i(A)$.

□

A partir do Teorema de Riemann, o matemático Gustav Roch demonstrou, em 1865, uma versão do Teorema de Riemann-Roch para superfícies de Riemann. O resultado foi generalizados posteriormente para vários outros assuntos, como, por exemplo, curvas algébricas.

Teorema 2.21 (Teorema de Riemann-Roch)**.** *Seja W um divisor canônico de F/K. Então, para cada divisor $A \in Div(F)$,*

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

Demonstração: Definimos o índice de especialidade como

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

Pelo Teorema da dualidade temos $i(A) = \ell(W - A)$, e daí

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

□

Corolário 2.22. *Para um divisor canônico W, temos $degW = 2g-2$ e $\ell(W) = g$.*

Demonstração: Para $A = 0$, temos

$$\ell(0) = deg0 + 1 - g + \ell(W - 0) \Rightarrow \ell(W) = g.$$

Tomando $A = W$, temos

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

Corolário 2.23. $dim\Omega_F(0) = g$.

De fato, pelo Teorema da Dualidade, temos $\Omega_F(0) \simeq \mathcal{L}(W)$. Daí, pelo Teorema de Riemann-Roch, temos $dim\Omega_F(0) = \ell(W) = g$.

Isso significa que podemos ver o gênero do corpo de funções F/K como a dimensão do espaço $\Omega_F(0)$. Além disso, como $\Omega_F(0)$ é espaço vetorial sobre K existem exatamente g diferenciais de Weil regulares linearmente independentes sobre K.

Teorema 2.24. *Se A é um divisor de F/K de grau $degA \geq 2g-1$, então*

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

Demonstração: Pelo teorema de Riemann-Roch, dado um divisor canônico W, temos

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

Como $degA \geq 2g-1$, por hipótese e $degW = 2g-2$, temos

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

pelo Corolário 1.42. Daí

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

□

Vejamos agora algumas consequências do Teorema de Riemann-Roch. O primeiro resultado garante que este teorema caracteriza o gênero e a classe canônica de F/K. Outro resultado importante, que será usado posteriormente no trabalho, é o Teorema das Lacunas de Weierstrass, provado por Weierstrass em meados de 1860, que será particularizado para curvas. Além destes resultados provaremos também o Teorema de Clifford, que fornece uma relação entre a dimensão e o grau de um divisor A, com $0 \leq deg\ A \leq 2g-2$.

Proposição 2.25. *Suponha que $g_0 \in \mathbb{Z}$ e $W_0 \in Div(F)$ satisfaçam*

$$\ell(A) = degA + 1 - g_0 + \ell(W_0 - A)$$

para todo $A \in Div(F)$. Então $g_0 = g$ e W_0 é um divisor canônico.

Demonstração: Seja $A = 0$. Então temos $\ell(0) = deg(0) + 1 - g_0 + \ell(W_0)$ logo $\ell(W_0) = g_0$.

Seja agora $A = W_0$. Daí

$$g_0 = \ell(W_0) = degW_0 + 1 - g_0 + \ell(0)$$

$$\Rightarrow degW_0 = 2g_0 - 2.$$

Seja W um divisor canônico de F/K. Escolha um divisor A tal que $degA > max\{2g-2, 2g_0-2\}$. Então, pelo Teorema 2.24, temos

$$\ell(A) = degA + 1 - g. \tag{2.5}$$

Por outro lado, temos $degA > degW_0$ e daí $deg(W_0 - A) < 0 \Rightarrow \ell(W_0 - A) = 0$. Assim,

$$\ell(A) = degA + 1 - g_0. \tag{2.6}$$

Comparando (2.5) e (2.6), temos $g = g_0$. Agora, substituindo $A = W$ na equação inicial, temos

$$\begin{aligned} & \ell(W) = degW + 1 - g + \ell(W_0 - W) \\ \Rightarrow \quad & g = 2g - 2 + 1 - g + \ell(W_0 - W) \\ \Rightarrow \quad & \ell(W_0 - W) = 1 \end{aligned}$$

Além disso, $deg(W_0 - W) = degW_0 - degW = 2g - 2 - (2g - 2) = 0$. Daí, pela parte (c) do Corolário 1.42, $W_0 - W$ é um divisor principal e, como $W_0 = W + (W_0 - W)$, temos $W \sim W_0$.

□

Proposição 2.26. *Um divisor B é canônico se, e somente se $degB = 2g - 2$ e $\ell(B) \geq g$.*

($\Rightarrow$) Já sabemos que dado um divisor canônico $B, degB = 2g - 2$ e $\ell(B) = g$ pelo Corolário 2.22.

($\Leftarrow$) Suponha $degB = 2g - 2$, $\ell(B) \geq g$ e seja W um divisor canônico. Vamos mostrar que $W \sim B$. Temos

$$\begin{aligned} g \leq \ell(B) \quad & = degB + 1 - g + \ell(W - B) \quad (\text{ pelo Teorema de Riemann-Roch }) \\ & = 2g - 2 + 1 - g + \ell(W - B) \\ & = g - 1 + \ell(W - B) \\ & \Rightarrow g \geq g - 1 + \ell(W - B) \Rightarrow \ell(W - B) \geq 1 \end{aligned}$$

Note ainda que $deg(W - B) = 0$, pois $degW = degB = 2g - 2$. Daí, novamente pelo Corolário 1.42, $W - B$ é um divisor principal, o que implica $W \sim B$. Logo B é canônico.

□

Vamos agora definir uma estrutura que será utilizada em todo o trabalho: um sumigrupo numérico.

Definição 2.27. *Um **semigrupo numérico** é um subconjunto H de $\mathbb{N}$ fechado para a adição, que contém o 0 e que possui complemento finito em relação aos naturais, isto é, $\#(\mathbb{N} \setminus H) < \infty$.*

Proposição 2.28. *Seja $P \in \mathbb{P}_F$. Então, para cada $n \geq 2g$, existe um elemento $x \in F$ com divisor polo $(x)_\infty = nP$.*

Demonstração: Temos $\mathcal{L}((n-1)P) = \{x \in F / v_P(x) \geq -n + 1 > -n\} \Rightarrow \mathcal{L}((n-1)P) \subseteq \mathcal{L}(nP)$.

Por outro lado, pelo Teorema 2.24, como $n \geq 2g$, temos

$$\ell((n-1)P) = (n-1)degP + 1 - g \quad \text{e} \quad \ell(nP) = ndegP + 1 - g,$$

ou seja, $\ell(nP) > \ell((n-1)P)$. Logo $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Dessa forma, tome $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$. Então $-n+1 > v_P(x) \geq -n \Rightarrow v_P(x) = -n$. Portanto, x tem divisor polo $(x)_\infty = nP$.

□

Definição 2.29. *Seja $P \in \mathbb{P}_F$. Um inteiro $n \geq 0$ é chamado **número polo de P** se existe um elemento $x \in F$ tal que $(x)_\infty = nP$. Caso contrário, n é chamado **lacuna** de P.*

Observação 2.30. *n é um número polo de P se, e somente se $\ell(nP) > \ell((n-1)P)$.*

Demonstração: ($\Rightarrow$) Suponha que n seja um número polo de P. Então existe $x \in F$, com $(x)_\infty = nP$. Como $\mathcal{L}((n-1)P) \subseteq \mathcal{L}(nP)$, para que n seja número polo de P devemos ter $\ell(nP) > \ell((n-1)P)$ para obtermos $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$.

($\Leftarrow$) Se $\ell(nP) > \ell((n-1)P)$ segue que $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$ e daí existe $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$, o que implica $v_P(x) = -n \Rightarrow (x)_\infty = nP$ e, portanto, n é número polo de P.

Observação 2.31. *O conjunto dos números polos de P é um subconjunto de $\mathbb{N}$ fechado para a soma.*

Sejam $(x_1)_\infty = n_1P$ e $(x_2)_\infty = n_2P$, com $x_1, x_2 \in F$. Então $x_1x_2 \in F$ e $(x_1x_2)_\infty = (n_1+n_1)P$. De fato, temos $v_P(x_1) = -n_1$, ou seja, $x_1 = t^{-n_1}u$, onde $u \in \mathcal{O}^\times$ e t é um elemento primo de P. De maneira análoga, $x_2 = t^{-n_2}v$, com $v \in \mathcal{O}^\times$. Assim, $(x_1x_2)_\infty = (n_1+n_2)P$ e daí n_1+n_2 pertence ao conjunto de polos de P.

Para concluir que o conjunto de polos de P é um semigrupo numérico basta mostrar que seu complemento em $\mathbb{N}$ é finito, pois já mostramos que ele é fechado para a soma.

Teorema 2.32 (Teorema das Lacunas de Weierstrass)**.** *Suponha que F/K tenha gênero $g > 0$ e seja P um lugar de grau 1. Então existem exatamente g lacunas $i_1, \cdots, i_g$ de P, com $i_1 = 1$ e $i_g \leq 2g-1$.*

Demonstração: Pela Proposição 2.28, cada lacuna é menor ou igual a $2g-1$ pois, para $n \geq 2g$ existe um elemento $x \in F$ com divisor polo $(x)_\infty = nP$. Temos também que 0 é um número polo, pois $0 = (k)_\infty$, com $k \in K$.

Temos a seguinte caracterização para lacunas:

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

Essa caracterização se dá pelo fato de que n é um número polo de P se, e somente se $\ell(nP) > \ell((n-1)P)$.

Considere então a sequência de espaços vetoriais

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P). \tag{2.7}$$

Temos $dim\mathcal{L}(0) = 1$. Pelo Teorema 2.24, se $degA \geq 2g-1$, então $\ell(A) = degA + 1 - g$, daí

$$dim\mathcal{L}((2g-1)P) = deg((2g-1)P) + 1 - g = 2g - 1 + 1 - g = g.$$

Além disso, temos, pelo Lema 1.38,

$$dim\left(\frac{\mathcal{L}(iP)}{\mathcal{L}((i-1)P)}\right) \leq deg(iP) - deg(i-1)P = i - i + 1 = 1.$$

Assim

$$dim\mathcal{L}(iP) - dim\mathcal{L}((i-1)P) \leq 1 \Rightarrow dim\mathcal{L}(iP) \leq 1 + dim\mathcal{L}((i-1)P),$$

para todo i. Como $dim\mathcal{L}((2g-1)P) = g$, temos

$$g \leq dim\mathcal{L}((2g-2)P) + 1 \Rightarrow dim\mathcal{L}((2g-2)P) \geq g - 1,$$

e assim sucessivamente. Portanto existem exatamente $g-1$ números i entre 1 e $2g-1$ com $\mathcal{L}((i-1)P) \subsetneq \mathcal{L}(iP)$. Dessa forma, existem $2g-1-(g-1) = g$ lacunas de P. Para finalizar basta mostrar que 1 é a primeira lacuna. Suponha que 1 seja polo. Como o conjunto dos números polos é fechado para a soma, todo $n \in \mathbb{N}$ seria polo, o que é absurdo pois $g > 0$. Assim $i_1 = 1$ e $i_g \leq 2g-1$.

□

Com esse teorema provamos que o número de lacunas de um lugar P é finito e, portanto, o conjunto de números polos de um lugar P é um semigrupo numérico.

Sabemos que o espaço de Riemann-Roch associado a um divisor de grau negativo contém apenas o zero. Além disso, pelo Teorema 2.24, se o grau do divisor é maior que $2g-2$ o Teorema de Riemann-Roch se resume a $\ell(A) = degA + 1 - g$, ou seja, a dimensão de A depende apenas do grau de A e do gênero do corpo de funções. Vamos agora analisar o caso em que $0 \leq degA \leq 2g-2$.

Definição 2.33. *Um divisor $A \in Div(F)$ é chamado **não especial** se $i(A) = 0$. Caso contrário A é chamado especial.*

Proposição 2.34. *(a) Um divisor A é não especial se, e somente se $\ell(A) = degA + 1 - g$.*

(b) Se $degA > 2g-2$, então A é não-especial.

(c) A propriedade de um divisor ser especial ou não depende apenas da classe $[A]$ de A.

(d) Divisores canônicos são especiais.

(e) Todo divisor A com $\ell(A) > 0$ e $degA < g$ é especial.

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

Demonstração: (a) Como $i(A) = \ell(A) - degA + g - 1$, temos $i(A) = 0 \Leftrightarrow \ell(A) = degA + 1 - g$.

(b) Pelo Teorema 2.24, se $degA \geq 2g-1$, então $\ell(A) = degA+1-g \Rightarrow i(A) = 0$.

(c) Como dois divisores equivalentes possuem mesmo grau e dimensão, a propriedade de ser especial ou não depende apenas da classe.

(d) Seja W um divisor canônico. Então, pelo Teorema da dualidade, temos $i(W) = \ell(W - W) = \ell(0) = 1$. Logo W é especial.

(e) $1 \leq \ell(A) = degA+1-g+i(A) \Rightarrow i(A) \geq g-degA > 0$. Logo A é especial.

(f) Pelo Teorema 2.8 temos $i(A) = dim(\mathcal{A}_F/\mathcal{A}_F(A) + F)$. Assim, se A é não especial, segue que $\mathcal{A}_F = \mathcal{A}_F(A) + F$. Se $B \geq A$ então $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B) \Rightarrow dim(\mathcal{A}_F/\mathcal{A}_F(B) + F) = 0 \Rightarrow i(B) = 0$ e B é não especial.

□

Teorema 2.35 (Teorema de Clifford)**.** *Para todos os divisores A, com $0 \leq degA \leq 2g-2$, temos*

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

Para demonstrar o teorema vamos, primeiramente, provar o seguinte lema:

Lema 2.36. *Suponha que A e B sejam divisores tais que $\ell(A) > 0$ e $\ell(B) > 0$. Então $\ell(A) + \ell(B) \leq 1 + \ell(A + B)$.*

Demonstração: Como $\ell(A) > 0$ e $\ell(B) > 0$ podemos encontrar, pela Observação 1.35, $A_0, B_0 > 0$ tais que $A \sim A_0$ e $B \sim B_0$. O conjunto

$$X = \{D \in Div(F) | D \leq A_0 \text{ e } \mathcal{L}(D) = \mathcal{L}(A_0)\}$$

é não vazio, pois $A_0 \in X$. Por definição, temos $degD = \sum_{p \in \mathbb{P}_F} v_P(x) \cdot degP$, onde $degP > 0$, pois $degP = [F_P : K]$. Como $\mathcal{L}(D) = \mathcal{L}(A_0)$ segue $\mathcal{L}(A_0) \subseteq \mathcal{L}(D)$, e daí, dado $x \in \mathcal{L}(A_0)$, temos $v_P(x) \geq -v_P(A_0) \geq -v_P(D) \Rightarrow v_P(D) \geq v_P(A_0) \geq 0$. Portanto $degD \geq 0$ para todo $D \in X$. Disso temos que existe um divisor $D_0 \in X$ de grau minimal. Para todo $P \in \mathbb{P}_F$ temos

$$\ell(D_0 - P) < \ell(D_0).$$

Afirmação: $\ell(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0)$

Seja $suppB_0 = \{P_1, \cdots, P_r\}$ o conjunto dos lugares em que $v_{P_i} \neq 0$. Então $\mathcal{L}(D_0 - P_i)$ é um subespaço próprio de $\mathcal{L}(D_0)$, para $i = 1, \cdots, r$. Assumindo que K é infinito e usando o fato de que um espaço vetorial sobre um corpo infinito não é a união de um número finito de subespaços próprios, é possível encontrar $z \in \mathcal{L}(D_0)$ tal que

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

Considere a aplicação

$$\begin{array}{rccc} \Phi: & \mathcal{L}(B_0) & \longrightarrow & \mathcal{L}(D_0+B_0)/\mathcal{L}(A_0) \\ & x & \longmapsto & xz\ mod\mathcal{L}(A_0) \end{array}$$

Temos $Ker\Phi = \{x \in \mathcal{L}(B_0) | xz \in \mathcal{L}(A)\} = K$, e daí concluímos que

$$dim\mathcal{L}(B_0) - 1 \leq dim\mathcal{L}(B_0 + D_0) - dim\mathcal{L}(A_0).$$

Como $dim\mathcal{L}(A_0) = dim\mathcal{L}(D_0)$, temos

$$\mathcal{L}(D_0) + \ell(B_0) \leq 1 + \ell(D_0 + B_0),$$

e a afirmação está provada.

Usando essa afirmação, temos

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

□

Demonstração do Teorema: Se $\ell(A) = 0$, como $degA \geq 0$ temos $\ell(A) \leq 1 + \frac{1}{2}degA$.

Se $\ell(W - A) = 0$, pelo Teorema de Riemann-Roch temos

$$\ell(A) = degA + 1 - g = 1 + \frac{1}{2}degA + \frac{1}{2}(degA - 2g).$$

Como $degA \leq 2g - 2$, temos $degA - 2g \leq -2 \Rightarrow \frac{1}{2}(degA - 2g) \leq -1$. Daí $\ell(A) < 1 + \frac{1}{2}degA$.

Vamos considerar então o caso em que $\ell(A) > 0$ e $\ell(W - A) > 0$. Pelo lema anterior, temos

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

Por outro lado, pelo Teorema de Riemann-Roch, temos

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

Somando essa duas equações, temos

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

CAPÍTULO 3

CURVAS ALGÉBRICAS

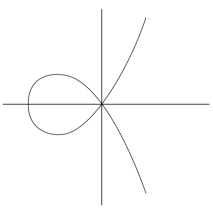
Neste capítulo vamos expor as definições e os principais resultados sobre curvas algébricas afins e projetivas. Mostraremos também que existe uma bijeção entre pontos de uma curva não singular e lugares de seu corpo de funções, e com isso conseguiremos transferir todo o estudo feito para corpos de funções algébricas para o estudo da curvas. As definições e resultados deste capítulo são encontrados em [2].

3.1 Variedades afins

Seja k um corpo. Denotamos por $\mathbb{A}^n(k)$, ou simplesmente $\mathbb{A}^n$ (quando o corpo k já estiver subentendido) o produto cartesiano de k n-vezes. Dessa forma $\mathbb{A}^n$ é o conjunto de todas as n-uplas de elementos de k. Chamaremos os elementos de $\mathbb{A}^n$ de **pontos**.

Se $F \in k[X_1, \cdots, X_n]$, um ponto $P = (a_1, \cdots, a_n) \in \mathbb{A}^n$ é chamado **zero** de F se $F(a_1, \cdots, a_n) = 0$. O conjunto de todos os zeros de F é chamado **hipersuperfície** definida por F e é denotado por $V(F)$.

Exemplo 3.1. *Seja* $k = \mathbb{R}$. *Dado* $F = Y^2 - X^2(X+1)$ *temos* $V(F) = V(Y^2 - X^2(X+1)) = \{(x, y) \in \mathbb{A}^2 | y = \pm\sqrt{x^2(x+1)}\} \subset \mathbb{A}^2$.



A curva plana afim representa o conjunto $V(Y^2-X^2(X+1))$, que é o conjunto de zeros de $F = Y^2 - X^2(X+1)$.

Se $S \subset k[X_1, \cdots, X_n]$ é um conjunto de polinômios, denotamos

$$V(S) = \{P \in \mathbb{A}^n | F(P) = 0, \text{ para todo } F \in S\}.$$

Note que podemos escrever $V(S) = \bigcap_{F \in S} V(F)$, pois $P \in V(S)$ deve anular todos os polinômios de S.

Definição 3.2. *Um conjunto $X \subset \mathbb{A}^n$ é um **conjunto algébrico** se $X = V(S)$ para algum conjunto de polinômios $S \subset k[X_1, \cdots, X_n]$.*

Vejamos algumas propriedades dos conjuntos algébricos:

(1) *Todo conjunto algébrico $V(S)$ é igual a $V(I)$, para algum ideal I de $k[X_1, \cdots, X_n]$.*

De fato, seja I o ideal gerado por S. Então $V(I) = \bigcap_{F \in I} V(F) = V(S)$.

(2) *Se $\{I_\alpha\}$ é uma coleção de ideais, então $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$,* ou seja, a interseção de qualquer coleção de conjuntos algébricos é um conjunto algébrico.

(3) *Se $I \subset J$ então $V(I) \supset V(J)$.*

De fato, seja $I \subset J$. Então $V(I) = \bigcap_{F \in I} V(F) \supset \bigcap_{F \in J} V(F) = V(J)$.

(4) *$V(FG) = V(F) \cup V(G)$, para quaisquer polinômios F e G.*

Isso é claro, pois todo ponto de $\mathbb{A}^n$ que anula F anula FG e todo ponto de $\mathbb{A}^n$ que anula G também anula FG. Temos $V(I) \cup V(J) = V(\{FG | F \in I \text{ e } G \in J\})$ e, de maneira geral, podemos concluir que a união finita de conjuntos algébricos é um conjunto algébrico.

(5) $V(0) = \mathbb{A}^n(k)$, pois qualquer ponto de $\mathbb{A}^n$ é raiz do polinômio nulo. $V(1) = \varnothing$, pois nenhum ponto de $\mathbb{A}^n$ anula um polinômio constante e $V(X_1 - a_1, \cdots, X_n - a_n) = \{(a_1, \cdots, a_n)\}$. Com essa última propriedade concluímos que qualquer conjunto finito de $\mathbb{A}^n$ é um conjunto algébrico, pois basta tomar o produto dos polinômios que são anulados pelos pontos do conjunto.

Dado um conjunto $X \in \mathbb{A}^n(k)$, vamos analisar o conjunto dos polinômios que se anulam em X. Estes polinômios formam um ideal de $k[X_1, \cdots, X_n]$ chamado **ideal de** X e denotado por $I(X)$, onde

$$I(X) = \{F \in k[X_1, \cdots, X_n] | F(a_1, \cdots, a_n) = 0, \forall (a_1, \cdots, a_n) \in X\}.$$

As propriedades abaixo nos dão relações entre ideais e conjuntos algébricos:

Sejam X, Y conjuntos algébricos.

(6) *Se* $X \subset Y$ *então* $I(X) \supset I(Y)$.

De fato, seja $F \in I(Y)$. Então $F(a_1, \cdots, a_n) = 0,$ para todo $(a_1, \cdots, a_n) \in Y$. Como $X \subset Y$ temos $F(b_1, \cdots, b_n) = 0,$ para todo $(b_1, \cdots, b_n) \in X \Rightarrow F \in I(X)$. Portanto, $I(Y) \subset I(X)$.

(7) $I(\varnothing) = k[X_1, \cdots, X_n]$. $I(\mathbb{A}^n(k)) = (0)$, pois o polinômio nulo é o único anulado por todos os pontos de $\mathbb{A}^n$. $I((a_1, \cdots, a_n)) = (X_1 - a_1, \cdots, X_n - a_n)$, para $a_1, \cdots, a_n \in k$.

(8) $I(V(S)) \supset S$, *para qualquer conjunto* S *de polinômios e* $V(I(X)) \supset X$, *para qualquer conjunto* X *de pontos.*

Seja $F \in S$. Então temos

$$V(S) = \{(a_1, \cdots, a_n) \in \mathbb{A}^n | F(a_1, \cdots, a_n) = 0, \forall F \in S\}.$$

Daí $I(V(S)) = \{G \in k[X_1, \cdots, X_n] | G(a_1, \cdots, a_n) = 0, \forall (a_1, \cdots, a_n) \in V(S)\}$. Logo $F \in I(V(S))$. A demonstração é análoga quando consideramos um conjunto X de pontos.

(9) $V(I(V(S))) = V(S)$, para qualquer conjunto S de polinômios e $I(V(I(X))) = I(X)$, para qualquer conjunto X de pontos.

Um ideal de um conjunto algébrico de pontos possui uma propriedade particular: Se $I = I(X)$ e $F^n \in I$, para algum inteiro $n > 0$, então $F \in I$. Se I é um ideal em um anel R definimos o **radical de I** como

$$Rad\ I = \{a \in R | a^n \in I, \text{ para algum } n > 0\}.$$

Afirmação: $Rad\ I$ é um ideal de R.

- $0 \in Rad\ I$, pois $0^n \in I$ para todo $n > 0, n \in \mathbb{Z}$.
- Sejam $a, b \in Rad\ I$. Então $a^n, b^m \in I$ para $m, n > 0, m, n \in \mathbb{Z}$. Daí temos

$$(a+b)^{m+n} = \underbrace{a^{n+m}}_{\in I} + \underbrace{a^{n+m-1}b}_{\in I} + \cdots + \underbrace{a^n b^m}_{\in I} + \cdots \underbrace{b^{m+n}}_{\in I} \in I.$$

  Dessa forma, $a + b \in Rad\ I$.

- Seja $a \in Rad\ I$ e $r \in R$. Então $a^n \in I$ para algum $n > 0, n \in \mathbb{Z}$. Daí temos $(ar)^n = a^n r^n \in I$, pois I é ideal. Portanto, $ar \in Rad\ I$. Logo $Rad\ I$ é ideal de R.

Note que $I \subset Rad\ I$. Com essa definição temos a seguinte propriedade:

(10) *$I(X)$ é um ideal radical, para qualquer $X \subseteq \mathbb{A}^n(k)$.*

De fato, já temos $I(X) \subseteq Rad\ I$. Seja agora $F \in Rad\ I$. Então $F^n \in I(X)$, para algum $n > 0$. Isso significa que $F^n(a_1 \cdots, a_n) = 0$, para todo $(a_1 \cdots, a_n) \in X$. Mas daí $F(a_1, \cdots, a_n) = 0 \Rightarrow F \in I(X)$. Portanto, $Rad\ I \subseteq I(X)$ e $I(X)$ é radical.

Apesar de termos definido um conjunto algébrico como $X = V(S)$ para um conjunto S qualquer de polinômios, veremos agora que S é finitamente gerado.

Definição 3.3. *Um anel é dito* ***noetheriano*** *se todo ideal deste anel é finitamente gerado.*

Exemplo 3.4. *Como exemplos de anéis noetherianos temos corpos e domínios de ideais principais.*

Teorema 3.5 (Teorema da base de Hilbert)**.** *Se R é um anel noetheriano, então $R[X_1, \cdots, X_n]$ é um anel noetheriano.*

Demonstração: Como $R[X_1, \cdots, X_n]$ é isomorfo a $R[X_1, \cdots, X_{n-1}][X_n]$, se provarmos que $R[X]$ é noetheriano utilizando que R é noetheriano, o resultado segue por indução.

Seja I um ideal de $R[X]$. Precisamos mostrar que I é finitamente gerado. Seja $F = a_0 + a_1X + \cdots + a_dX^d \in R[X]$ e J o conjunto de todos os coeficientes líderes de todos os polinômios em I.

Afirmação: J é um ideal de R.

- $0 \in J$, pois 0 é coeficiente líder do polinômio nulo.
- Sejam $a_n, b_m \in J$. Então existem $p(x) = a_0 + a_1X + \cdots + a_nX^n, g(x) = b_0 + b_1X + \cdots + b_mX^m \in I$. Assim, se $p(x)$ e $g(x)$ possuem o mesmo grau, $a_m + b_m$ é coeficiente líder do polinômio $p(x) + g(x) \in I$.
- Seja $a \in J$ e $r \in R$. Então ar é coeficiente líder do polinômio $r(a_0 + a_1X + \cdots + aX^n) \in I$.

Como J é ideal de R e R é noetheriano, existem polinômios $F_1, \cdots, F_r \in I$ cujos coeficientes líderes geram J. Tome N um inteiro maior que o grau de cada F_i. Para cada $m \leq N$, seja J_m o ideal de R consistindo de todos os coeficientes líderes de todos os polinômios $F \in I$ tais que $deg(F) \leq m$. Novamente, como R é noetheriano, temos um conjunto finito $\{F_{m_j}\}$ de polinômios em I de grau menor ou igual a m cujos coeficientes líderem geram J_m. Seja I' o conjunto gerado pela união dos $F_i's$ e dos $F'_{m_j}s$, que é finito. Basta mostrarmos agora que $I = I'$. Já temos $I' \subseteq I$. Suponha $I' \subsetneq I$. Seja $G \in I$ o elemento de menor grau que não está em I'. Se $degG > N$ podemos encontrar polinômios Q_i tais que $\sum Q_iF_i$ e G possuem o mesmo coeficiente líder e o mesmo grau. Mas daí

$$deg(G - \sum Q - iF_i) < degG \Rightarrow G - \sum Q_iF_i \in I' \Rightarrow G \in I'.$$

Se $degG = m \leq N$, podemos encontrar polinômios Q_j de maneira que G e $\sum Q_j F_{m_j}$ possuam o mesmo coeficiente líder e o mesmo grau e, repetindo o processo feito acima teremos $G \in I'$. Portanto $I = I'$.

□

Corolário 3.6. *O anel $k[X_1, \cdots, X_n]$ é noetheriano, para qualquer corpo k.*

Teorema 3.7. *Todo conjunto algébrico é a interseção de um número finito de hipersuperfícies.*

Demonstração: Seja um conjunto algébrico $V(I)$, para algum ideal $I \subseteq k[X_1 \cdots, X_n]$. Como $k[X_1, \cdots, X_n]$ é noetheriano, I é finitamente gerado. Assim

$$V(I) = V(F_1, \cdots, F_r) = V(F_1) \cap V(F_2) \cap \cdots \cap V(F_r),$$

onde $F_1, \cdots, F_r$ são os geradores de I.

Definição 3.8. *Um conjunto algébrico $V \subseteq \mathbb{A}^n$ é **redutível** se $V = V_1 \cup V_2$, onde V_1, V_2 são conjuntos algébricos em $\mathbb{A}^n$ e $V_1, V_2 \neq V$. Caso contrário V é dito **irredutível.***

Proposição 3.9. *Um conjunto algébrico V é irredutível se, e somente se $I(V)$ é primo.*

Demonstração: ($\Rightarrow$) Suponha que $I(V)$ não seja primo. Então dado $F_1F_2 \in I(V)$ temos que nem F_1 nem F_2 pertencem a $I(V)$. Dessa forma temos $V(F_1) \cap V(F_2) = \varnothing$, mas $V(F_1) \cup V(F_2) = V$. Portanto temos $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$, logo V é redutível.

($\Leftarrow$) Suponha que V seja redutível, isto é, $V = V_1 \cup V_2$, onde $V_i \subsetneq V$. Daí $I(V_i) \supsetneq I(V), i = 1, 2$. Seja $F_i \in I(V_i)$ e $F_i \notin I(V)$. Então F_1F_2 é anulado por todos os elementos de V, ou seja, $F_1F_2 \in I(V)$. Portanto, $I(V)$ não é primo.

□

Vamos provar agora que um conjunto algébrico é a união finita de conjuntos algébricos irredutíveis.

Lema 3.10. *Seja $\mathcal{L}$ uma coleção não nula de ideais em um anel noetheriano R. Então $\mathcal{L}$ tem um elemento maximal, isto é, existe um ideal I de $\mathcal{L}$ que não está contido em nenhum outro ideal de $\mathcal{L}$.*

Demonstração: Escolha um ideal em cada subconjunto de $\mathcal{L}$. Seja I_0 o ideal escolhido no próprio conjunto $\mathcal{L}$. Seja $\mathcal{L}_1 = \{I \in \mathcal{L} | I \supsetneq I_0\}$ e tome $I_1 \in \mathcal{L}_1$. Seja $\mathcal{L}_2 = \{I \in \mathcal{L} | I \supsetneq I_1\}$, e assim sucessivamente. Precisamos mostrar que algum $\mathcal{L}_n$ é vazio, com $n \in \mathbb{N}$. Suponha que $\mathcal{L}_n$ não seja vazio para nenhum n. Tome então $I = \bigcup_{n=0}^{\infty} I_n$, que é um ideal de R. Como R é noetheriano, existem elementos $F_1, \cdots, F_r$ que geram I. Para n suficientemente grande, cada $F_i \in I_n$, para

$i \in \{1, \cdots, r\}$. Mas daí temos $I = I_n$ e $I_{n+1} = I_n$, o que é absurdo. Portanto, toda coleção não nula de ideais em um anel noetheriano tem um elemento maximal.

□

Observação 3.11. *Sejam I, J ideais em um anel noetheriano. Sabemos que se $I \subset J$ então $V(J) \subset V(I)$. Dessa forma, como toda coleção de ideais em um anel noetheriano tem elemento maximal, então toda coleção de conjuntos algébricos em $\mathbb{A}^n(k)$ tem elemento minimal.*

Teorema 3.12. *Seja V um conjunto algébrico em $\mathbb{A}^n(k)$. Então existem únicos conjuntos algébricos irredutíveis $V_1, \cdots, V_m$ tais que $V = V_1 \cup \cdots \cup V_m$ e $V_i \nsubseteq V_j$, para todo $i \neq j$.*

Demonstração: Considere o conjunto

$$\mathcal{X} = \left\{ \begin{array}{l} \text{Conjuntos algébricos } V \subseteq \mathbb{A}^n / \quad V \text{ não pode ser escrito como} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{união finita de conjuntos algébricos.} \end{array} \right\}$$

Vamos mostrar que esse conjunto é vazio. Como vimos na observação anterior, toda coleção de conjuntos algébricos tem um elemento minimal. Seja então V o elemento minimal de $\mathcal{X}$. Temos que V não é irredutível, pois se o fosse seria escrito como um único elemento irredutível e não pertenceria a $\mathcal{X}$. Assim $V = V_1 \cup V_2, V_i \subsetneq V, i = 1, 2$. Pela minimalidade de V, temos $V_i \notin \mathcal{X}$, e daí $V_i = V_{i_1} \cup \cdots \cup V_{i_{m_i}}$, onde cada V_{ij} é irredutível. Temos o mesmo para V_j. Daí $V = \bigcup_{i,j} V_{ij}$, o que contradiz o fato de $V \in \mathcal{X}$. Assim $\mathcal{X} = \varnothing$ e todo conjunto algébrico é a união finita de conjuntos algébricos irredutíveis. Para que $V_i \nsubseteq V_j$, para todo $i \neq j$, basta desconsiderar os conjuntos algébricos em que $V_i \subset V_j$, para $i \neq j$. Para demonstrar a unicidade dos $V_i's$ suponha que $V = W_1 \cup \cdots \cup W_n$ seja outra decomposição de V. Temos $V_i = \bigcup_j (W_j \cap V_i)$, daí $V_i \subset W_{j(i)}$ para algum $j(i)$. Do mesmo modo temos $W_{j(i)} \subset V_k$, para algum k. Mas daí $V_i \subset V_k \Rightarrow i = k$, e assim $V_i = W_{j(i)}$. De maneira análoga concluímos que cada W_j é igual a um $V_{i(j)}$ e, portanto, a decomposição é única.

□

Exemplo 3.13. *Vamos mostrar que o conjunto algébrico $V(Y - X^2) \subset \mathbb{A}^n(\mathbb{C})$ é irredutível. Pela Proposição 3.9 temos que V é irredutível se, e somente se $I(V)$ é primo. Pela Propriedade (9) temos $I(V(I(X))) = I(X)$. Assim*

$$I(V(Y - X^2)) = (Y - X^2).$$

Como o polinômio $F = Y - X^2$ é irredutível sobre $\mathbb{C}[X, Y]$ temos que $(Y - X^2)$ é primo e, portanto, $V(Y - X^2)$ é irredutível.

Exemplo 3.14. *Vamos decompor $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ em componentes irredutíveis. Temos $Y^4 - X^2 = (Y^2 + X)(Y^2 - X)$ e $Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 + X)(Y - X)(Y + X)$. Utilizando as propriedades*

de que $V(f,g) = V(f) \cap V(g)$ *e* $V(fg) = V(f) \cup V(g)$*, temos*

$$V(Y^4-X^2, Y^4-X^2Y^2+XY^2-X^3) = V((Y^2+X)(Y^2-X), (Y^2+X)(Y-X)(Y+X))$$

$$= (V(Y^2+X) \cup V(Y^2-X)) \cap (V(Y^2+X) \cup V(Y-X) \cup V(Y+X)).$$

$V(Y^2+X)$ *pertence a essa interseção. Além disso* $V(Y^2+X)$ *é irredutível pois* $I = (Y^2+X)$ *é primo já que* Y^2+X *é irredutível em* $\mathbb{C}[X,Y]$*.*

Agora precisamos verificar se existe mais alguma interseção entre $V(Y^2-X)$ *e* $V(Y-X) \cup V(Y+X)$*. Temos*

$$Y^2 - X = 0 \Rightarrow Y = \pm\sqrt{X},$$

e assim os pontos $(0,0), (1,1)$ *e* $(1,-1)$ *também pertencem a essa interseção. Como* $(0,0)$ *já pertence a* $V(Y^2+X)$*, a decomposição em fatores irredutíveis é dada por*

$$V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) = V(Y^2+X) \cup \{(1,1)\} \cup \{(1,-1)\}.$$

Vamos considerar, daqui para frente, k como um corpo algebricamente fechado.

Definição 3.15. *Um conjunto algébrico irredutível será chamado* ***variedade afim.*** *Quando já estiver subentendido que este conjunto é afim o chamaremos apenas de variedade.*

Seja $V \subset \mathbb{A}^n$ uma variedade não vazia. Usando a Proposição 3.9 temos que $I(V)$ é um ideal primo de $k[X_1, \cdots, X_n]$. Desta forma, o quociente $\frac{k[X_1,\cdots,X_n]}{I(V)}$ é um domínio.

Definição 3.16. *O domínio* $\Gamma(V) = \dfrac{k[X_1, \cdots, X_n]}{I(V)}$ *é chamado* ***anel de coordenadas de V****.*

Seja V uma variedade não vazia em $\mathbb{A}^n$ e $\Gamma(V)$ seu anel de coordenadas. Como $\Gamma(V)$ é um domínio, vamos considerar seu corpo quociente:

Definição 3.17. *O corpo quociente* $k(V)$ *de* $\Gamma(V)$ *é chamado* ***corpo de funções racionais*** *em* V*. Um elemento de* $k(V)$ *é chamado* ***função racional*** *em* V*.*

Se f é uma função racional em V e $P \in V$, diremos que f está definida em P se existem $a, b \in \Gamma(V)$ tais que $f = \dfrac{a}{b}$ e $b(P) \neq 0$. Diremos então que f está definida em P se for possível encontrar um denominador para f que não se anule em P. Existem diversas maneiras de escrever uma função f como quociente de dois elementos de $\Gamma(V)$. Entretanto, se $\Gamma(V)$ for um domínio de fatoração única podemos escrever $f = \dfrac{a}{b}$ de maneira única, onde a, b não possuem fatores em comum.

Exemplo 3.18. *Seja* $V = V(XW - YZ) \subset \mathbb{A}^4(k)$. *Então* $\Gamma(V) = \dfrac{k[X,Y,Z,W]}{(XW-YZ)}$. *Sejam* $\overline{X}, \overline{Y}, \overline{Z}, \overline{W}$ *os resíduos de* X, Y, Z, W *em* $\Gamma(V)$. *Então* $\overline{XW} - \overline{YZ} = 0$, *o que implica* $\dfrac{\overline{X}}{\overline{Y}} = \dfrac{\overline{Z}}{\overline{W}}$. *Assim,* $f = \dfrac{\overline{X}}{\overline{Y}} = \dfrac{\overline{Z}}{\overline{W}} \in k(V)$ *está definida em* $P = (x, y, z, w) \in V$ *se* $y \neq 0$ *ou* $w \neq 0$.

Seja V uma variedade e $P \in V$. Definimos $\mathcal{O}_P(V)$ como sendo o conjunto das funções racionais definidas em P. Então temos, de maneira imediada, a inclusão:

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V).$$

Definição 3.19. *O anel* $\mathcal{O}_P(V)$ *é chamado* ***anel local*** *de* V *em* P.

Definição 3.20. *O conjunto de pontos* $P \in V$ *onde a função* f *não está definida é chamado* ***conjunto de polos de*** f.

Proposição 3.21. *O conjunto polo de uma função racional é um conjunto algébrico.*

Demonstração: Seja $V \subset \mathbb{A}^n$ um conjunto algébrico. Para $G \in k[X_1, \cdots, X_n]$ denote o resíduo de G em $\Gamma(V)$ por $\overline{G}$. Seja $f \in k(V)$ uma função racional. Vamos definir o conjunto

$$J_f = \{G \in k[X_1, \cdots, X_n] | \overline{G}f \in \Gamma(V)\}.$$

Como $\overline{G}f \in \Gamma(V), \overline{G}$ cancela o denominador de f.
Afirmação: J_f *é um ideal de* $k[X_1, \cdots, X_n]$ *contendo* $I(V)$.

- $0 \in J_f$, pois $0f = 0 \in \Gamma(V)$;
- Sejam $G_1, G_2 \in J$. Então $\overline{(G_1 + G_2)}f = (\overline{G_1} + \overline{G_2})f = \overline{G_1}f + \overline{G_2}f \in \Gamma(V)$. Portanto, $G_1 + G_2 \in J_f$.
- Seja $F \in k[X_1, \cdots, X_n]$ e $G \in J_f$. Então $FG \in J_f$, pois $\overline{FG}f = \overline{F}(\overline{G}f) \in \Gamma(V)$.

Além disso J_f contém $I(V)$, pois qualquer elemento $G \in I(V)$ anula o produto $\overline{G}f$ em $\Gamma(V)$ e, portanto, $I(V) \subset J_f$.

Observe agora que $V(J_f)$ são os pontos onde G se anula. Porém, como $\overline{G}$ anula o denominador de $f, V(J_f)$ são os pontos onde f não está definida. Logo o conjunto polo de uma função racional é algébrico.

□

Suponha $f \in \mathcal{O}_P(V)$. Definimos o valor de f em P da seguinte maneira: Seja $f = \dfrac{a}{b}, a, b \in \Gamma(V), b(P) \neq 0$. O valor de f em P é $f(P) = \dfrac{a(P)}{b(P)}$. Note que este

valor independe da escolha de a e b, pois se a e b possuem fatores em comum estes serão cancelados.

Considere o homomorfismo

$$\begin{array}{rccc} \phi: & \mathcal{O}_P(V) & \longrightarrow & k \\ & f & \longmapsto & f(P) \end{array}$$

Temos $Ker\phi = \{f \in \mathcal{O}_P(V) | f(P) = 0\}$. Chame $Ker\phi = \mathfrak{m}_P(V)$. Assim temos

$$\frac{\mathcal{O}_P(V)}{\mathfrak{m}_P(V)} \simeq k,$$

e daí $\mathfrak{m}_P(V)$ é um ideal maximal de $\mathcal{O}_P(V)$ chamado **ideal maximal de V em P.**

Observação 3.22. *Um elemento $f \in \mathcal{O}_P(V)$ é uma unidade em $\mathcal{O}_P(V)$ se, e somente se $f(P) \neq 0$.*

De fato, $f \in \mathcal{O}_P(V)$ é uma unidade em $\mathcal{O}_P(V) \Leftrightarrow \frac{1}{f} \in \mathcal{O}_P(V) \Leftrightarrow f(P) \neq 0$. Dessa forma, temos $\mathfrak{m}_P(V) = \{$ não unidades de $\mathcal{O}_P(V)\}$.

Com os resultados provados no Capítulo 1, $\mathcal{O}_P(V)$ é um anel local e $\mathfrak{m}_P$ é seu ideal maximal. Além disso, $\mathcal{O}_P(V)$ é um anel de valorização discreta e podemos definir a **ordem** de um elemento $z \in k(V)$ da mesma maneira que foi definida a valorização no Capítulo 1: Se t é um parâmetro, então todo $z \in k(V)$ pode ser escrito na forma $z = ut^n$, com u uma unidade, e definimos $ord(z) = n$ e $ord(0) = \infty$.

3.2 Propriedades locais das curvas planas

Vamos reduzir nosso estudo ao plano afim $\mathbb{A}^2$ para apresentar algumas propriedades das curvas planas. Primeiramente vamos encontrar todos os conjuntos algébricos de $\mathbb{A}^2$.

Proposição 3.23. *Sejam F, G polinômios em $k[X, Y]$ sem fatores em comum. Então $V(F, G) = V(F) \cap V(G)$ é um conjunto finito de pontos.*

Demonstração: Pelo Lema de Gauss, como F e G não tem fatores em comum em $k[X][Y]$ então F e G também não possuem fatorem em comum em $k(X)[Y]$. Como $k(X)[Y]$ é um domínio de ideais principais temos $mdc(F, G) = 1$, e daí existem $R, S \in k(X)[Y]$ tais que

$$RF + SG = 1.$$

Seja $D \in k[X], D \neq 0$, tal que $DR = A \in k[X, Y]$ e $DS = B \in k[X, Y]$. Então temos

$$AF + BG = D.$$

Dado $(a, b) \in V(F, G)$, temos

$$D(a) = A(a, b)F(a, b) + B(a, b)G(a, b) = 0,$$

pois $F(a, b) = G(a, b) = 0$. Mas D possui apenas um número finito de raízes, a saber, o grau de D. Dessa forma existe apenas um número finito de coordenadas x nos pontos de $V(F, G)$. De maneira análoga mostramos que também existe apenas um número finito de coordenadas y nos pontos de $V(F, G)$, e daí concluímos que $V(F, G)$ é finito.

□

Corolário 3.24. *Se F é um polinômio irredutível em $k[X, Y]$ tal que $V(F)$ é infinito, então $I(V(F)) = (F)$ e $V(F)$é irredutível.*

Demonstração: Seja $G \in I(V(F))$. Então G é um polinômio que é anulado por todos os elementos de $V(F)$. Como $V(F)$ é infinito, $V(F, G)$ é infinito. Pela Proposição 3.23 temos que F e G tem fatores em comum e, como F é irredutível, temos $F|G$. Logo $G \in (F)$ e daí $I(V(F)) \subset (F)$. Já temos a inclusão contrária pela Propriedade (8). Como $k[X, Y]$ é um domínio de fatoração única temos (F) primo pois F é irredutível. Daí, pela Proposição 3.9, $V(F)$ é irredutível.

Corolário 3.25. *Suponha k infinito. Então os conjuntos algébricos irredutíveis de $\mathbb{A}^2$ são: $\mathbb{A}^2, \varnothing$, pontos e curvas planas irredutíveis $V(F)$, onde F é um polinômio irredutível e $V(F)$ é infinito.*

Demonstração: Se $I(V) = 0$ então $V = \mathbb{A}^2$ e se V é finito, V é formado por pontos. Se V é infinito, $I(V)$ contém um polinômio não constante F. Como $I(V)$ é primo, pela Proposição 3.9, algum fator irredutível de F pertence a $I(V)$ e,assim, podemos assumir F irredutível. Portanto $I(V) = (F)$.

As curvas planas afins correspondem a polinômios não-constantes $F \in k[X, Y]$ sem fatores múltiplos.

Definição 3.26. *Dizemos que $F, G \in k[X, Y]$ são **equivalentes** se $F = \lambda G$, para algum $\lambda \in k$. Definimos como uma curva plana afim a classe de equivalência dos polinômios que satisfazem essa relação. O **grau** de uma curva é o grau do polinômio que a define. Por exemplo, se o grau é 1, a curva é uma reta. Se $F = \prod F_i^{e_i}$ onde os F_i são os fatores irredutíveis de F, dizemos que F_i são as componentes e e_i é a multiplicidade de F_i. F_i é uma **componente simples** se $e_i = 1$. Caso contrário é dito **múltiplo.***

Se $F = F_1^{e_1} \cdots F_n^{e_n}$ é a decomposição de F em fatores irredutíveis então $V(F) = V(F_1) \cup \cdots \cup V(F_n)$. Assim é possível descobrir F_i a partir de $V(F)$. Entretanto a multiplicidade de cada componente não pode ser descoberta.

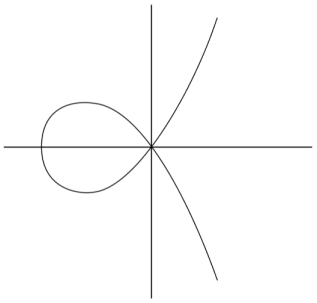
Se F é irredutível, pelo Corolário 3.24, $V(F)$ é irredutível, logo $V(F)$ é uma variedade em $\mathbb{A}^2$.

Definição 3.27. *Seja F uma curva e $P = (a, b) \in F$, ou seja, $F(P) = 0$. O ponto P é chamado* ***simples*** *se $\dfrac{\partial F}{\partial x}(P) \neq 0$ ou $\dfrac{\partial F}{\partial y}(P) \neq 0$. Neste caso,*

$$F_x(P)(x - a) + F_y(P)(y - b) = 0$$

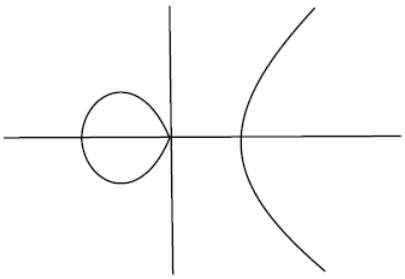
é chamada ***reta tangente*** *a F em P. Se um ponto não é simples ele é chamado* ***singular.*** *Uma curva que só contém pontos simples é dita* ***curva não-singular ou regular.***

Exemplo 3.28. *Considere a curva do início do capítulo definida pelo polinômio $F = Y^2 - X^3 - X^2$:*



Neste caso, temos $F_X = -3X^2 - 2X$ e $F_Y = 2Y$. Logo $(0, 0)$ é um ponto singular. Note que o ponto $\left(-\frac{2}{3}, 0\right)$ também zera F_X e F_Y simultaneamente, entretanto este ponto não pertence à curva. Logo $(0, 0)$ é o único ponto singular.

Exemplo 3.29. *Considere a curva definida pelo polinômio $G = Y^2 - X^3 + X$.*



Neste caso temos $G_X = -3X^2 + 1$ e $F_Y = 2Y$. Os pontos $\left(\pm\frac{\sqrt{3}}{3}, 0\right)$ zeram G_X e G_Y simultaneamente, entretanto esses pontos não pertencem à curva. Assim G é uma curva não-singular e a reta tangente à curva em um ponto (a, b) é dada por

$$r : (-3a^2 + 1)(x - a) + 2b(y - b) = 0.$$

Em $(0, 0)$ a reta tangente é $x = 0$.

3.3 Variedades projetivas

Definição 3.30. *Seja $\mathbb{A}^{n+1}(k)$. O conjunto de todas as retas de $\mathbb{A}^{n+1}$ que passam pela origem é chamado* ***espaço projetivo n-dimensional*** *e denotado por $\mathbb{P}^n(k)$.*

Os elementos de $\mathbb{P}^n$ *são chamados* ***pontos.*** *Podemos identificar*

$$\mathbb{P}^n = (\mathbb{A}^{n+1} \setminus \{0\})/k^*,$$

onde $(x_1, \cdots, x_{n+1}) \sim (\lambda x_1, \cdots, \lambda x_n)$, *para todo* $\lambda \in k^*$, *ou seja, dois pontos em* $\mathbb{A}^{n+1} \setminus \{0\}$ *são equivalentes se estão sobre a mesma reta que passa pela origem. Assim* $\mathbb{P}^n$ *pode ser identificado com o conjunto das classes de equivalência dos pontos em* $\mathbb{A}^{n+1} \setminus \{0\}$.

Dado $P \in \mathbb{P}^n$, a $(n+1)-$upla $(a_1, \cdots, a_{n+1})$ pertencente à classe de equivalência de P será chamada **coordenada homogênea de P.** As classes de equivalência são denotadas por $[a_1 : \cdots : a_{n+1}]$. Note que $[a_1 : \cdots : a_{n+1}] = [\lambda a_1 : \cdots : \lambda a_{n+1}]$, para todo $\lambda \in k$.

Seja $U_i = \{[x_1 : \cdots : x_{n+1}] | x_i \neq 0\}$. Como $x_i \neq 0$, a razão $\dfrac{x_j}{x_i}$ está bem definida para todo j. Portanto, cada $P \in U_i$ pode ser escrito de maneira única como

$$P = [x_1 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots : x_{n+1}].$$

Exemplo 3.31. *Sejam* $[x : y : z]$ *as coordenadas de P. Então*

$$U_1 = \left\{ \left[x, \frac{y}{x}, \frac{z}{x} \right] \in \mathbb{P}^2; x \neq 0 \right\} \simeq \{[1, u, v] | u, v \in k\} \simeq \{(u, v) | u, v \in k\} = \mathbb{A}^2.$$

Defina a função $\psi_i : \mathbb{A}^n \longrightarrow U_i$ por

$$\psi_i(a_1, \cdots, a_n) = [a_1 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_{n+1}].$$

Essa função é claramente bijetora. Logo existe uma correspondência um a um entre os pontos de $\mathbb{A}^n$ e os pontos de U_i. Note também que $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$, ou seja, $\mathbb{P}^n$ é coberto por $n+1$ conjuntos que se comportam como $\mathbb{A}^n$.

Definição 3.32. *O conjunto*

$$H_\infty = \mathbb{P}^n \setminus U_{n+1} = \{[x_1 : x_2 : \cdots : x_{n+1}]; x_{n+1} = 0\}$$

será chamado ***hiperplano no infinito.***

A correspondência $[x_1 : \cdots : x_{n+1}] \longleftrightarrow [x_1 : \cdots : x_n : 0]$ faz com que H_∞ seja identificado com $\mathbb{P}^{n-1}$. Além disso temos

$$\mathbb{P}^n = H_\infty \cup U_{n+1},$$

ou seja, o espaço projetivo nada mais é do que a união entre um $n-$espaço afim (representado por U_{n+1}) e todas as suas direções (representadas por H_∞).

Exemplo 3.33. • $\mathbb{P}^0(k)$ *é um ponto.*

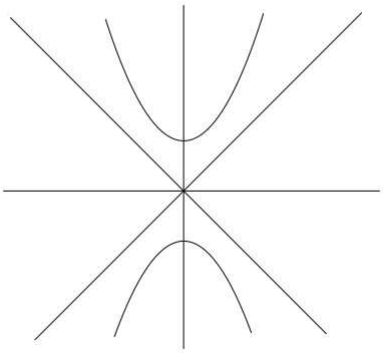
- $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0 = \{[x:1] | x \in k\} \cup \{[1:0]\}$. *Portanto* $\mathbb{P}^1$ *é a reta afim mais um ponto no infinito. Chamaremos* $\mathbb{P}^1$ *de* ***reta projetiva.***

Exemplo 3.34. *Vamos mostrar que retas paralelas se encontram no infinito: Considere a reta* $Y = mX + b$ *em* $\mathbb{A}^2$*. Podemos identificar* $\mathbb{A}^2$ *com* $U_3 \subset \mathbb{P}^2$*. Com essa identificação os pontos da reta correspondem aos pontos* $[x:y:z] \in \mathbb{P}^2$ *tais que* $y = mx + bz$ *(Precisamos tomar essa equação homogêna para que as soluções se tornem invariantes por equivalência). Os pontos da reta que estão no infinito são dados por*

$$\mathbb{P}^2 \cap H_\infty = \{[x:y:z] \in \mathbb{P}^2 | y = mx + bz\} \cap \{[x:y:0] | x, y \in k\} = \{[1:m:0]\}.$$

Assim, todas as retas com o mesmo coeficiente angular m*, isto é, todas as retas paralelas, se encontram no mesmo ponto no infinito.*

Exemplo 3.35. *Seja a curva* $Y^2 = X^2 + 1$*.*



Podemos identificar os pontos de $\mathbb{A}^2$ *com os de* U_3 *da seguinte maneira:*

$$Y^2 = X^2 + Z^2, Z \neq 0.$$

Assim, a interseção entre $\{[x:y:z] \in \mathbb{P}^2; y^2 = x^2 + z^2\}$ *e* H_∞ *é dada por*

$$\begin{aligned} \{[x:y:z] \in \mathbb{P}^2; y^2 = x^2 + z^2\} \cap \{[x:y:0]; x, y \in k\} &= \{[x:y:0]; x^2 = y^2\} \\ &= \{[1:-1:0]\}, \{[1:1:0]\}. \end{aligned}$$

Os pontos $[-1:1:0]$ *e* $[-1:-1:0]$ *também estão na interseção, mas estão na mesma classe de equivalência dos pontos* $[1:-1:0]$ *e* $[1:1:0]$*.*

Definição 3.36. *Se* $F \in k[X_1, \cdots, X_{n+1}]$ *então* $P = [a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$ *é zero de* F *se* $F(\lambda a_1, \cdots, \lambda a_{n+1}) = 0, \forall \lambda \in k$*, e denotaremos por* $F(P) = 0$*. Seja* $S \subset k[X_1, \cdots, X_{n+1}]$ *um conjunto de polinômios. Então*

$$V_p(S) = \{P \in \mathbb{P}^n; F(P) = 0, \forall F \in S\}$$

é o ***conjunto de zeros de S em*** $\mathbb{P}^n$***.*** *Se* $Y = V_p(S) \subset \mathbb{P}^n$ *para algum conjunto* S *então* Y *é chamado* ***conjunto algébrico projetivo.***

Definição 3.37. *Dado* $Y \subset \mathbb{P}^n$ *definimos*

$$I_p(Y) = \{F \in k[X_1, \cdots, X_{n+1}]; F(P) = 0, \text{ para todo } P \in Y\}$$

o ***ideal*** *de Y.*

Lema 3.38. *Seja $F \in k[X_1, \cdots, X_{n+1}]$ tal que $F = F_0 + F_1 + \cdots + F_m$, onde cada F_i é uma forma de grau i. Então, para todo $P \in \mathbb{P}^n$, temos $F(P) = 0$ se, e somente se $F_i(P) = 0$, para todo $i = 1, \cdots, m$.*

Demonstração: Suponha $F(P) = 0, P = [a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$. Então definimos $G(\lambda) = F(\lambda P) = F(\lambda a_1 \cdots, \lambda a_{n+1}) = \sum_{i=1} \lambda^i F_i(P) = 0$, pois $F(P) = F(\lambda P) = 0$. Assim temos G um polinômio em λ com coeficientes $b_i = F_i(a_1, \cdots, a_{n+1})$. Como $G(\lambda)$ se anula para todo $\lambda \in k$ e k é infinito, temos $b_i = F_i(a_1, \cdots, a_{n+1}) = 0$. Portanto todas as formas são nulas. A recíproca é óbvia.

□

Proposição 3.39. *Todo conjunto algébrico projetivo é zero de um número finito de formas.*

Demonstração: De fato, se Y é um conjunto algébrico então $Y = V_p(S)$ para algum $S \subset k[X_1, \cdots, X_{n+1}]$ e, além disso, $V_p(S) = V_p(I)$, onde I é o ideal gerado por S. Como $k[X_1, \cdots, X_{n+1}]$ é noetheriano temos que I é finitamente gerado por polinômios em $k[X_1, \cdots, X_{n+1}]$. Como cada polinômio possui finitas formas I será gerado por finitas formas e, portanto, Y é zero de finitas formas.

□

Definição 3.40. *Um ideal $I \subset k[X_1, \cdots, X_{n+1}]$ é dito* ***homogêneo*** *se, sempre que $F \in I$, cada componente homogênea de F pertença a I.*

Proposição 3.41. *Um ideal $I \subset k[X_1, \cdots, X_{n+1}]$ é homogêneo se, e somente se é formado por um número finito de formas.*

Demonstração: ($\Rightarrow$) Se $I = (F_1, \cdots, F_m)$ é homogêneo (Note que I é finitamente gerado pois $k[X_1, \cdots, X_{n+1}]$ é noetheriano) então cada forma $F_j \in I$, e como cada polinômio é composto por um número finito de formas, I é formado por um número finito de formas.
($\Leftarrow$) Seja $S = \{F^{(\alpha)}\}$ o conjunto finito de formas que geram I. Para mostrar que I é homogêneo devemos mostrar que dado $F = F_1 + \cdots + F_m \in I$, onde cada F_i tem grau i, temos $F_i \in I$. Considere $deg(F^{(\alpha)}) = d_\alpha$. Seja $F = F_m + \cdots + F_n \in I$. Note que basta mostrar que $F_m \in I$, pois daí $F - F_m \in I$ e, prosseguindo indutivamente, teremos $F_i \in I, \forall i$. Como $F \in I$ temos $F = \sum A^{(\alpha)} F^{(\alpha)}$, onde $A^{(\alpha)} \in k[X_1, \cdots, X_{n+1}]$. Então temos $F_m = \sum A^{(\alpha)}_{m-d_\alpha} F^{(\alpha)}$, ou seja, $F_m \in I$.

□

Exemplo 3.42.

- *$(x), (x^2, y)$ são ideais homogêneos pois são formados por um número finito de formas.*
- *(x^2+x) não é gerado por uma forma e nem podemos gerá-lo com um número finito de formas, logo este ideal não é homogêneo.*

Definição 3.43. *Um conjunto algébrico projetivo é dito* ***irredutível*** *se não pode ser escrito como a união de dois conjuntos algébricos projetivos menores. Um conjunto algébrico irredutível em $\mathbb{P}^n$ é chamado* ***variedade projetiva.***

Observação 3.44. *Assim como no caso afim, um conjunto algébrico projetivo pode ser escrito de maneira única como a união de variedades projetivas. Além disso, a interseção arbitrária e a união finita de conjuntos algébricos projetivos ainda é um conjunto algébrico projetivo.*

Proposição 3.45. *Seja $Y \subset \mathbb{P}^n$ um conjunto algébrico projetivo. Então Y é irredutível se, e somente se $I_p(Y)$ é primo.*

Demonstração: ($\Rightarrow$) Pela Proposição 3.39, todo conjunto algébrico $Y \subset \mathbb{P}^n$ é zero de um número finito de formas. Daí podemos considerar que $I_p(Y)$ é gerado por formas. Sejam $F, G \in k[X_1, \cdots, X_{n+1}]$ formas tais que $FG \in I_p(Y)$ mas $F \notin I_p(Y)$ e $G \notin I_p(Y)$. Dessa forma temos $V_p(F) \subsetneq Y$, $V_p(G) \subsetneq Y$ e $V_p(F) \cup V_p(G) = Y$, pois FG é anulado por todo conjunto Y. Assim

$$Y = (Y \cap V_p(F)) \cup (Y \cap V_p(G)),$$

e daí Y é redutível.
($\Leftarrow$) Suponha $Y = V_1 \cup V_2$, onde $V_i \subsetneq Y, i = 1, 2$. Então $I_p(V_i) \supsetneq I_p(Y)$. Sejam $F_i \in I_p(V_i)$ tais que $F_i \notin I_p(Y), i = 1, 2$. Então $F_1 F_2 \in I_p(Y)$, pois $Y = V_1 \cup V_2$. Logo $I_p(Y)$ não é um ideal primo.

□

Definição 3.46. *Seja $\theta : \mathbb{A}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}^n$ a projeção canônica*

$$\theta(x_1, \cdots, x_{n+1}) = [x_1 : \cdots : x_{n+1}].$$

Se $Y \subset \mathbb{P}^n$, o ***cone afim*** *sobre Y é*

$$C(Y) = \theta^{-1}(Y) \cup \{(0, \cdots, 0)\} \subseteq \mathbb{A}^{n+1}.$$

Propriedades do cone:

1) Se $P \in \mathbb{P}^n$, então $C(\{P\})$ é a reta em $\mathbb{A}^{n+1}$ que passa por P e pela origem.

2) $C(\varnothing) = \{(0, 0, \cdots, 0)\}$.

3) $C(Y_1 \cup Y_2) = C(Y_1) \cup C(Y_2)$.

4) Se $Y \subset \mathbb{P}^n$, então $I_p(Y) = I_a(C(Y))$, onde I_a denota o ideal afim.
De fato, seja $F \in I_p(Y)$. Então $F(P) = 0$, para todo $P \in Y$. Mas se $P = [a_1 : \cdots : a_{n+1}] \in Y$, então $(a_1, \cdots, a_{n+1}) \in C(Y)$ e daí $F(a_1, \cdots, a_{n+1}) = 0 \Rightarrow F \in I_a(C(Y))$. A outra inclusão é análoga.

5) Se $I \subset k[X_1, \cdots, X_{n+1}]$ é um ideal homogêneo tal que $V_p(I) \neq \varnothing$, então $C(V_p(I)) = V_a(I)$.

A idéia de usar o cone é reduzir os problemas de $\mathbb{P}^n$ para problemas em $\mathbb{A}^{n+1}$.

Exemplos de conjuntos algébricos projetivos:

1) $V_p(1) = \varnothing$ e, pela Propriedade 5) do cone, $V_p(I) = \varnothing$, para qualquer ideal I tal que $V_a(I) = \{(0, \cdots, 0)\}$.

2) $\mathbb{P}^n = V_p(0)$.

3) Seja $P = [a : b] \in \mathbb{P}^1$. Então $\{P\} = V_p(bX - aY)$, e $C(\{P\})$ é a reta que passa por P e pela origem de $\mathbb{A}^2$, que é exatamente $V_a(bX - aY)$.

4) Seja $Y = V_p(X - Y, X^2 - YZ) \subset \mathbb{P}^2$. Então

$$C(Y) = V_a(X - Y, X^2 - YZ).$$

Temos então

$$\begin{cases} X - Y = 0 & \Rightarrow X = Y \\ X^2 - YZ = 0 & \Rightarrow Y^2 - YZ = 0 \Rightarrow Y(Y - Z) = 0 \Rightarrow Y = 0 \text{ ou } Y = Z. \end{cases}$$

Logo

$$\begin{aligned} C(Y) &= V_a(X, Y) \cup V_a(X - Y, Y - Z) \\ &= \{(0, 0, s) | s \in k\} \cup \{(t, t, t) | t \in k\}. \end{aligned}$$

Daí $Y = V_p(X, Y) \cup V_p(X - Y, Y - Z) = [0 : 0 : 1] \cup [1 : 1 : 1]$.

Definição 3.47. *Seja V uma variedade projetiva em $\mathbb{P}^n$. Então $I(V)$ é um ideal primo e o anel de resíduos $\Gamma_h(V) = \dfrac{k[X_1, \cdots, X_{n+1}]}{I(V)}$ é um domínio chamado* ***anel de coordenadas homogêneas de*** *V.*
Se I é um ideal homogêneo de $k[X_1, \cdots, X_{n+1}]$, seja $\Gamma = \dfrac{k[X_1, \cdots, X_{n+1}]}{I}$. Um elemento $f \in \Gamma$ será chamado ***forma de grau d*** *se existe uma forma F de grau d em $k[X_1, \cdots, X_{n+1}]$ cujo resíduo é f.*

Proposição 3.48. *Todo elemento $f \in \Gamma$ pode ser escrito unicamente como $f = f_0 + f_1 + \cdots + f_m$, com f_i uma forma de grau i.*

Demonstração: Como $f \in \Gamma$ é resíduo de um polinômio $F \in k[X_1, \cdots, X_{n+1}]$, F pode ser escrito como $F = \sum F_i$ e daí $f = \sum f_i$, onde cada f_i é resíduo de F_i. Vamos mostrar agora a unicidade. Suponha $f = \sum g_i$, onde g_i é resíduo de $G_i \in k[X_1, \cdots, X_{n+1}]$. Então

$$\sum f_i - \sum g_i = 0 \Rightarrow \sum (f_i - g_i) = 0 \Rightarrow \sum (F_i - G_i) \in I.$$

Como I é homogêneo, temos $F_i - G_i \in I, \forall i = 1, \cdots, n + 1 \Rightarrow f_i = g_i, \forall i = 1, \cdots, n + 1$. Portanto, f é escrito de maneira única.

□

Note que, diferente do caso de anéis de coordenadas afins, os elementos de $\Gamma_h(V)$ não podem ser considerados funções, a menos que estes sejam constantes.

De fato, $f \in \Gamma_h(V)$ define uma função em V se, e somente se $f(\lambda x_1, \cdots, \lambda x_{n+1}) = f(x_1, \cdots, x_{n+1})$, para todo $\lambda \in k^*$. Se $f = f_0 + \cdots + f_d$ é a decomposição de f em formas, isso acontece se, e somente se

$$\begin{aligned} f(x_1, \cdots, x_{n+1}) &= f(\lambda x_1, \cdots, \lambda x_{n+1}) \\ &= f_0(x_1, \cdots, x_{n+1}) + \lambda f_1(x_1, \cdots, x_{n+1}) + \cdots + \lambda^d f_d(x_1, \cdots, x_{n+1}), \end{aligned}$$

para todo $\lambda \in k^*$, o que acontece apenas quando f é constante.

Definição 3.49. *Chamaremos o corpo quociente de $\Gamma_h(V)$ de **corpo de funções homogêneas de V** e o denotaremos por $k_h(V)$.*

Definição 3.50. *O **corpo de funções de V**, denotado por $k(V)$, é definido como o conjunto*

$$\{z \in k_h(V) | \text{ para formas } f, g \in \Gamma_h(V) \text{ de mesmo grau temos } z = f/g\}.$$

Com essa definição, temos

$$k \subset k(V) \subset k_h(V) \quad \text{e} \quad \Gamma_h(V) \nsubseteq k(V).$$

Os elementos de $k(V)$ são chamados de **funções racionais** em V.

Sejam $P \in V, z \in k(V)$. Dizemos que z está **definido em P** se z pode ser escrito como $z = f/g$, onde f, g são formas de mesmo grau e $g(P) \neq 0$.

Definição 3.51. *Seja*

$$\mathcal{O}_P(V) = \{z \in k(V) | z \text{ é definido em } P\}.$$

*$\mathcal{O}_P(V)$ é um subanel de $k(V)$ chamado **anel local de V em P** e $\mathcal{O}_P(V)$ é um anel local com ideal maximal*

$$\mathfrak{m}_P(V) = \{z; z = f/g, g(P) \neq 0, f(P) = 0\}.$$

Dessa forma, o valor $z(P) = \frac{f(P)}{g(P)}$ de uma função $z \in \mathcal{O}_P(V)$ está bem definido.

3.4 O espaço multiprojetivo

O objetivo dessa seção é caracterizar o produto de duas variedades como uma variedade. Se tomarmos duas variedades afins $V_1 \subset \mathbb{A}^n$ e $V_2 \subset \mathbb{A}^m$, teremos $V_1 \times V_2 \subset \mathbb{A}^n \times \mathbb{A}^m \simeq \mathbb{A}^{n+m}$, que é um espaço conhecido. Portanto não existe dificuldade em trabalhar com o produto cartesiano de variedades afins. Já o produto $\mathbb{P}^n \times \mathbb{P}^m$ requer um pouco mais de atenção.

Vamos denotar $k[X_1, \cdots, X_{n+1}, Y_1 \cdots, Y_{m+1}]$ por $k[X, Y]$. Um polinômio $F \in k[X, Y]$ é chamado uma biforma de bigrau (p, q) se F é uma forma de grau p quando considerado como um polinômio de $X_1, \cdots, X_{n+1}$ em $k[Y_1, \cdots, Y_{m+1}]$ e se F é uma forma de grau q quando considerado como um polinômio de $Y_1, \cdots, Y_{m+1}$

em $k[X_1, \cdots, X_{n+1}]$. Dessa forma temos que todo polinômio $F \in k[X, Y]$ pode ser escrito unicamente como $F = \sum_{p,q} F_{p,q}$, onde $F_{p,q}$ é uma biforma de bigrau (p, q).

Se S é um conjunto qualquer de biformas em $k[X, Y]$, definimos

$$V_b(S) = \{(x, y) \in \mathbb{P}^n \times \mathbb{P}^m | F(x, y) = 0, \text{ para todo } F \in S\}.$$

Um subconjutno V de $\mathbb{P}^n \times \mathbb{P}^m$ é dito **algébrico** se $V = V_b(S)$ para algum $S \subset k[X, Y]$.

Dado um conjunto algébrico $V \subset \mathbb{P}^n \times \mathbb{P}^m$, definimos

$$I_b(V) = \{F \in k[X, Y] | F(x, y) = 0, \text{ para todo } (x, y) \in V\}.$$

Definimos também o anel de coordenadas bihomogêneas $\Gamma_b(V) = \dfrac{k[X, Y]}{I_b(V)}$, onde $k_b(V)$ é seu corpo quociente, e o corpo de funções de V é dado por

$$k(V) = \{z \in k_b(V) | z = f/g, \text{ onde } f, g \text{ são formas de mesmo grau em } \Gamma_b(V)\}.$$

Dessa forma podemos generalizar essas definições para variedades multiprojetivas $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_r}$ e para os chamados multiespaços $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$, que são compostos de variedades afins e projetivas. No caso dos multiespaços, um polinômio deve ser homogêneo em cada conjunto de variáveis que correspondem ao espaço projetivo $\mathbb{P}^{n_i}$, mas não possui nenhuma restrição nos conjuntos que correspondem a $\mathbb{A}^m$.

3.5 Pontos de curvas e anéis de valorização discreta

Nesta seção vamos definir uma bijeção entre pontos de uma curva e anéis de valorização discreta e, dessa forma, seremos capazes de transferir as definições e os resultados provados no Capítulo 1 para o estudo de curvas.

Seja $X = \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. A **Topologia de Zariski em X** é definida da seguinte forma: Um conjunto $U \subset X$ é aberto se $X \setminus U$ é um conjunto algébrico de X. Dessa maneira os conjuntos fechados na topologia de Zariski são os conjuntos algébricos. Como sabemos que a interseção arbitrária de conjuntos algébricos é um conjunto algébrico e que a união finita de conjuntos algébricos também o é, segue que a topologia de Zariski é realmente uma topologia. Note ainda que, dados dois subconjuntos não vazios abertos U_1, U_2 em uma variedade V, temos $U_1 \cap U_2 \neq \varnothing$. De fato, se tivéssemos $U_1 \cap U_2 = \varnothing$ poderíamos escrever $V = (V \setminus U_1) \cup (V \setminus U_2)$, que é a união disjunta de dois fechados, contrariando o fato de V ser uma variedade.

Seja V um conjunto algébrico irredutível em $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$. Qualquer

subconjunto aberto X de V será chamado de **variedade.** Definimos $k(X) = k(V)$ o corpo das funções racionais em X e se $P \in X$ definimos $\mathcal{O}_P(X)$ como $\mathcal{O}_P(V)$ o anel local de X em P. Se U é um conjunto aberto de X então U também é aberto em V, logo U também é uma variedade. Diremos que U é uma **subvariedade aberta** de X.

Se Y é um subconjunto fechado de X, diremos que Y é irredutível se Y não é a união de dois subconjuntos fechados próprios. Então Y também é uma variedade, pois se $\bar{Y}$ é o fecho de Y em V, então $\bar{Y}$ é irredutível em V e $Y = \bar{Y} \cap X$, logo Y é fechada em $\bar{Y}$. Essa variedade é chamada **subvariedade fechada** de X.

Seja X uma variedade e U um subconjunto aberto não vazio de X. Definimos $\Gamma(U, \mathcal{O}_X)$, ou simplesmente $\Gamma(U)$, como o conjunto das funções racionais em X que são definidas em cada $P \in U$. Se $z \in \Gamma(U)$, z determina uma função em U que assume valores em k. Vamos denotar por $\mathcal{F}(U, k)$ o anel de todas as funções em U com valores em k.

Se $\psi : X \to Y$ é uma aplicação qualquer entre os conjuntos X e Y, temos o homomorfismo de anéis $\widetilde{\psi} : \mathcal{F}(Y, k) \to \mathcal{F}(X, k)$, onde $\widetilde{\psi}(f) = f \circ \psi$.

Definição 3.52. *Sejam X e Y variedades. Um **morfismo** de X em Y é uma aplicação $\psi : X \to Y$ tal que*

1. *ψ é contínua.*
2. *Para todo conjunto aberto U de Y, se $f \in \Gamma(U, \mathcal{O}_Y)$, então $\widetilde{\psi}(f) = f \circ \psi$ está em $\Gamma(\psi^{-1}(U), \mathcal{O}_X)$.*

*Um **isomorfismo** $\psi : X \to Y$ é um morfismo injetor tal que ψ^{-1} também é um morfismo.*

Observação 3.53. *Seja $f : X \to Y$ um morfismo não constante entre curvas não singulares. Este morfismo induz um homomorfismo $\widetilde{f} : k(X) \to k(Y)$ e o inteiro $n = [k(X) : k(Y)]$ é chamado **grau** de f.*

Um ponto P em uma curva arbitrária X é dito um **ponto simples** se $\mathcal{O}_P(X)$ é um anel de valorização discreta. Uma curva X é dita **singular** se todo ponto de X é simples. Denotamos por ord_P a **função ordem** em $k(X)$ definida por $\mathcal{O}_P(X)$.

Seja K um corpo contendo k. Dizemos que um anel local A é um **anel local** de K se A é um subanel de K, K é o corpo quociente de A e A contém k. Por exemplo, se V é uma variedade e $P \in V$, então $\mathcal{O}_P(V)$ é um anel local de $k(V)$. De maneira análoga definimos um anel de valorização discreta de K como um anel de valorização discreta que é um anel local de K.

Definição 3.54. *Se A e B são anéis locais e A é um subanel de B, dizemos que B domina A se o ideal maximal de B contém o ideal maximal de A.*

Teorema 3.55. *Seja X uma curva projetiva e $K = k(X)$. Seja L um corpo contendo K e R um anel de valorização discreta de L. Assuma que $R \not\supseteq K$. Então existe um único ponto $P \in X$ tal que R domina $\mathcal{O}_P(X)$.*

Demonstração: **Existência:** Sabemos que existe uma bijeção entre $\mathbb{P}^{n-1}$ e $H_\infty \subset \mathbb{P}^n$. Dessa forma se V é uma variedade em $\mathbb{P}^n$ contida em H_∞, então V é isomorfa a uma variedade em $\mathbb{P}^{n-1}$ e, de modo particular, qualquer variedade projetiva é isomorfa a uma subvariedade fechada $V \subset \mathbb{P}^n$ tal que V não está contida em nenhum hiperplano de $\mathbb{P}^n$, ou seja, se denotarmos $U_i = \mathbb{P}^n \setminus H_i$ teremos $V \cap U_i \neq \varnothing$, para todo $i \in \{1, \cdots, n+1\}$.

Dessa maneira podemos considerar X como uma subvariedade fechada de $\mathbb{P}^n$ tal que $X \cap U_i \neq \varnothing$, para todo $i \in \{1, \cdots, n+1\}$. Então $\Gamma(X) = \dfrac{k[X_1, \cdots, X_n]}{I(X)} = k[x_1, \cdots, x_n]$ com cada $x_i \neq 0$. Seja $N = max_{i,j} ord(x_i/x_j)$. Vamos assumir $N = ord(x_j/x_{n+1})$, para algum j (Se isso não ocorrer basta fazer uma mudança de coordenadas). Então temos, para todo i,

$$ord(x_i/x_{n+1}) = ord\left(\frac{x_j}{x_{n+1}} \cdot \frac{x_i}{x_j}\right) = ord\left(\frac{x_j}{x_{n+1}} / \frac{x_j}{x_i}\right) = N - ord(x_j/x_i) \geq 0.$$

Se denotarmos por X_* a curva afim correspondente a $X \cap U_{n+1}$, podemos identificar $\Gamma(X_*)$ com $k\left[\frac{x_1}{x_{n+1}}, \cdots, \frac{x_n}{x_{n+1}}\right]$, e daí $R \supset \Gamma(X_*)$. Seja m o ideal maximal de R e tome $J = m \cap \Gamma(X_*)$. Então J é um ideal primo e corresponde a uma subvariedade W de X_*. Se $W = X_*$ então $J = 0$, e daí todo elemento de $\Gamma(X_*)$ é uma unidade de R, e teríamos $K \subset R$, o que é absurdo. Então $W = \{P\}$ é um ponto, e daí R domina $\mathcal{O}_P(X_*) = \mathcal{O}_P(X)$.

Unicidade: Se R domina $\mathcal{O}_P(X)$ e $\mathcal{O}_Q(X)$, escolha $f \in \mathfrak{m}_P(X)$ tal que $\frac{1}{f} \in \mathcal{O}_Q(X)$. Então $ord(f) > 0$ e $ord(\frac{1}{f}) \geq 0$, o que é absurdo.

□

Corolário 3.56. *Seja X uma curva projetiva não singular e $K = k(X)$. Então existe uma bijeção entre os pontos de X e anéis de valorização discreta de K. Se $P \in X, \mathcal{O}_P(X)$ é seu correspondente anel de valorização.*

Demonstração: Já temos que $\mathcal{O}_P(X)$ são anéis de valorização de K. Vamos mostrar agora que qualquer outro anel de valorização de K é igual a $\mathcal{O}_P(X)$ para algum ponto $P \in X$. Seja R um anel de valorização discreta de K. Pelo teorema anterior, R domina um único $\mathcal{O}_P(X)$, ou seja, $\mathcal{O}_P(X) \subset R$ e o ideal maximal de R contém o ideal maximal de $\mathcal{O}_P(X)$. Seja $M = (q)$ o ideal maximal de R e $N = (p)$ o ideal maximal de $\mathcal{O}_P(X)$. Suponha que exista $r \in R \setminus \mathcal{O}_P(X)$. Então $r = uq^n$, com $n < 0$ e u uma unidade de R. Daí $r^{-1} = u'q^{-n} \in N \subset M$. Como $r \in R$ e M é ideal de R, $rM \subset M$. Mas $r^{-1} \in M$, e daí teríamos $M = (1)$, o que contradiz o fato de M ser ideal próprio. Portanto $R = \mathcal{O}_P(X)$.

□

Como sabemos que a cada anel de valorização corresponde um único ideal maximal, dada uma curva projetiva não singular X, existe uma bijeção entre os pontos de X e os lugares associados aos anéis de valorização. Essa correspondência permite que as definições e resultados dados no Capítulo 1 para corpos de funções possam ser utilizadas também para curvas. Dessa maneira

temos, também para curvas, as definições de divisores, divisores canônicos, gênero, diferenciais e todos os resultados que envolvem essas definições.

Um resultado importante que será utilizado no Capítulo 5, cuja demonstração está na página 52 de [5], é a *fórmula de Riemann-Hurwitz:* Seja $f : X \to Y$ um morfismo sobrejetor de grau n entre curvas projetivas não-singulares X e Y de gênero g_X e g_Y, respectivamente. Se $P \in X, f(P) = Q$, seja $t \in \mathcal{O}_Q(Y)$ um parâmetro. O inteiro $e(P) = ord_P(t)$ é chamado **índice de ramificação de** f **em** P. Os pontos $P \in X$ tais que $e(P) > 1$ são chamados **pontos totalmente ramificados.** A fórmula de Riemann-Hurwitz nos dá uma relação entre o gênero das curvas X e Y e o grau do morfismo f:

$$2g_X - 2 = (2g_Y - 2)n + \sum_{P \in X} (e(P) - 1).$$

3.6 Séries lineares

Definição 3.57. *Seja X uma curva algébrica e $K = k(X)$ seu corpo de funções. Para todo $f \in K$ definimos o* ***divisor de*** *f como $div(f) = \sum_{P \in X} ord_P(f)P$.*

Definição 3.58. *Seja X uma curva algébrica e D um divisor em X. Seja V um subespaço vetorial de $\mathcal{L}(D) = \{f \in k(X); ord_P(f) \geq -n_P, \forall P \in X\}$, onde $D = \sum_{P \in X} n_P P$. O conjunto dos divisores efetivos*

$$\{div(f) + D; f \in V\}$$

é chamado ***série linear****.*

Denotamos uma série linear por g^r_d, onde $d = degD$ e $r = dim_k V - 1$, em que r é chamada **dimensão projetiva da série linear.** Uma série linear é dita **completa** quando $V = \mathcal{L}(D)$ e, neste caso, vamos representá-la por $|D|$, com

$$|D| = \{E; E \geq 0 \text{ e } E \equiv D\}.$$

Note que se $f_1, \cdots, f_{r+1}$ é base de V, então a aplicação

$$div\left(\sum \lambda_i f_i\right) + D \mapsto (\lambda_1, \cdots, \lambda_{r+1})$$

nos dá uma correspondência um a um entre séries lineares e $\mathbb{P}^r$. Se a série linear $|D|$ é completa podemos associar $|D|$ ao espaço projetivo associado ao espaço $\mathcal{L}(D)$. Dessa maneira temos que uma série linear g^r_d induz um morfismo

$$\phi : X \to \mathbb{P}^r.$$

ϕ é chamado **birracional** se o grau de $\phi = 1$. Uma série linear completa é dita **simples** se a aplicação induzida é birracional.

Definição 3.59. *Dada uma série linear $|D|$, um ponto $P \in X$ é um* ***ponto de base*** *de $|D|$ se, para todo $f \in V$, o coeficiente de P em $div(f)+D$ é estritamente positivo. Uma série linear $|D|$ é* ***livre de pontos de base*** *se nenhum $P \in X$ é ponto de base de $|D|$.*

Observação 3.60. *Se Q é um ponto de base de D, então $\ell(D) = \ell(D-Q)$.*

De fato, $\mathcal{L}(D) = \{f \in k(X); ord_P(f) \geq -D, \forall P \in X\}$ e $\mathcal{L}(D-Q) = \{f \in k(X); ord_P(f) \geq -D+Q, \forall P \in X\}$. Como $D \geq D-Q$, temos que $\mathcal{L}(D-Q) \subset \mathcal{L}(D)$. Agora, seja $f \in \mathcal{L}(D)$, então $ord_P(f) \geq -D, \forall P \in X$. Como Q é ponto de base temos $ord_Q(f) + D > 0$, daí $ord_Q(f) + D - Q \geq 0 \Rightarrow ord_Q(f) \geq -D+Q$, e daí $\mathcal{L}(D) = \mathcal{L}(D-Q) \Rightarrow \ell(D) = \ell(D+Q)$.x

Exemplo 3.61. *Se D é divisor de uma curva algébrica X de gênero g e $deg(D) \geq 2g$ então $|D|$ é livre de pontos de base.*

De fato, se $deg(D) \geq 2g-1$, pelo Teorema 2.24, o Teorema de Riemann-Roch se reduz a

$$\ell(D) = deg(D) + 1 - g$$

e

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

Portanto, $\ell(D) \neq \ell(D-Q)$ e $|D|$ é livre de pontos de base.

CAPÍTULO 4

SEMIGRUPOS NUMÉRICOS

Um semigrupo numérico é um subconjunto não vazio H de $\mathbb{N}$ fechado para a adição, que contém o 0 e cujo complemento em $\mathbb{N}$ é finito. A simplicidade deste conceito torna possível a compreensão de problemas cuja resolução nem sempre é trivial. Este fato atraiu, no fim do século XIX, vários matemáticos, como Frobenius e Silvester. Frobenius propôs o seguinte problema: Qual é a maior quantia que não podemos obter utilizando apenas moedas previamente determinadas? Por exemplo, qual é a maior quantia que não podemos obter utilizando apenas moedas de 5 e 7? A solução deste problema é 23, que é exatamente a maior lacuna do semigrupo numérico gerado por 5 e 7. Na segunda metade do século XX os semigrupos numéricos voltaram a ser estudados, principalmente devido às suas aplicações na Geometria Algébrica.

4.1 Propriedades de semigrupos numéricos

Denotaremos um semigrupo numérico por H. O número natural $g := g(H) := \#(\mathbb{N} \setminus H)$ é chamado **gênero de** H. Como g é finito existe $c \in H$ tal que $c - 1 \notin H$ e todo natural maior do que c pertence a H. Chamaremos este número c de **condutor de** H. Denotaremos por $L = L(H)$ o conjunto dos elementos que não pertencem a H, chamaremos seus elementos de **lacunas** e os denotaremos por $1 = \ell_1 < \ell_2 < \cdots < \ell_g$. Os elementos de H serão denotados por $0 = m_0 < m_1 < m_2 \cdots$, e $m_1 = m$ será chamado **multiplicidade de** H**.** Utilizaremos a notação $\rightarrow$ para representar que todo natural a partir do número que antecede a seta pertence ao semigrupo. Além disso, por simplicidade, chamaremos um semigrupo numérico apenas de semigrupo.

Exemplo 4.1. *Seja H um semigrupo de gênero g. Vamos analisar os semigrupos que existem de acordo com o gênero:*

1. *Se* $g = 0$ *então* $H = \{0, 1 \rightarrow\} = \mathbb{N}$.
2. *Se* $g = 1$ *então* $H = \{0, 2 \rightarrow\}$
3. *Se* $g = 2$ *então* $H = \{0, 2, 4 \rightarrow\}$ *ou* $H = \{0, 3 \rightarrow\}$
4. *Se* $g = 3$ *então* $H = \{0, 4 \rightarrow\}$; $H = \{0, 3, 5, 6 \rightarrow\}$; $H = \{0, 3, 4, 6 \rightarrow\}$; $H = \{0, 2, 4, 6 \rightarrow\}$

Definição 4.2. *Um semigrupo* H *é dito* ***hiperelíptico*** *se* $m = 2$. *Caso contrário* H *é dito não-hiperelíptico.*

Teorema 4.3. *Seja* H *um semigrupo de gênero* g.

(a) H *é hiperelíptico se, e somente se* $\ell_j = 2j - 1$, *para cada inteiro* $j = 1, \cdots, g - 1$.

(b) H *é não-hiperelíptico se, e somente se* $\ell_j \leq 2j - 2$, *para cada inteiro* $j = 2, \cdots, g - 1$ *e* $\ell_g \leq 2g - 1$.

Para demonstrar esse teorema vamos provar o seguinte lema:

Lema 4.4. *Seja* H *um semigrupo de gênero* g. *Então* $\ell_j \leq 2j - 1, \forall\ 1 \leq j \leq g$.

Demonstração: Para $j = 1$ temos $\ell_1 \leq 2 \cdot 1 - 1 = 1$.
Suponha $2 \leq j \leq g$. Considere os pares da forma $(\alpha, \ell_j - \alpha)$, com $1 \leq \alpha \leq \left[\frac{\ell_j}{2}\right]$, e $\left[\frac{\ell_j}{2}\right]$ é a parte inteira de $\frac{\ell_j}{2}$. Se $\alpha \in H$, então $\ell_j - \alpha \notin H$, pois, se isso acontecesse, teríamos $(\ell_j - \alpha) + \alpha = \ell_j \in H$, o que é absurdo. Portanto, em cada par $(\alpha, \ell_j - \alpha)$ existe pelo menos uma lacuna. Como existem $\left[\frac{\ell_j}{2}\right]$ pares, temos

$$\#\{\text{ lacunas entre 1 e } \ell_{j-1}\} \geq \left[\frac{\ell_j}{2}\right].$$

Por outro lado, temos

$$\#\{\text{ lacunas entre 1 e } \ell_{j-1}\} \leq j - 1.$$

Então temos

$$\left[\frac{\ell_j}{2}\right] \leq \#\{\text{ lacunas entre 1 e } \ell_{j-1}\} \leq j - 1 \Rightarrow \left[\frac{\ell_j}{2}\right] \leq j - 1.$$

Como

$$\left[\frac{\ell_j}{2}\right] \leq \frac{\ell_j}{2} < \left[\frac{\ell_j}{2}\right] + 1 \leq j,$$

segue que

$$\frac{\ell_j}{2} < j \Rightarrow \ell_j < 2j \Rightarrow \ell_j \leq 2j - 1.$$

□

A partir deste lema temos $l_g \leq 2g-1$. Daí o intervalo $[0, 2g]$ tem exatamente g lacunas e g não-lacunas, ou seja,

$$H = \{0, m_1, \cdots, m_g = 2g, 2g+1, \cdots\}.$$

Outra coisa que podemos concluir deste lema é que no intervalo $[1, 2j-1]$ existem pelo menos j lacunas, para cada $j \in \{1, \cdots, g\}$, pois $\ell_j \leq 2j-1$.

Observação 4.5. *Como $\ell_j \leq 2j-1$, com $1 \leq j \leq g$, então $m_j \geq 2j$.*

De fato, como comentamos acima, no intervalo $[1, 2j-1]$ existem pelo menos j lacunas, isto é,

$$\#\{\text{ lacunas entre 1 e } 2j-1\} \geq j.$$

Como existem $2j-1$ elementos entre 1 e $2j-1$ e pelo menos j elementos desse conjunto são lacunas, temos

$$\#\{\text{ não lacunas entre 1 e } 2j-1\} \leq j-1.$$

Mas

$$m_0 < m_1 < \cdots < m_{j-1} < m_j \Rightarrow m_j > 2j+1 \Rightarrow m_j \geq 2j.$$

Demonstração do Teorema 4.3:

(a) ($\Rightarrow$) Suponha H hiperelíptico. Já temos, para qualquer semigrupo numérico, $\ell_1 = 2 \cdot 1 - 1 = 1$. Como H é hiperelíptico, $2 \in H$, o que significa que as lacunas de H são ímpares. Pelo Lema 4.4, temos $\ell_j \leq 2j-1$. Mas como $2j \in H, \forall\, j \in \{1, \cdots, g\}$, temos $\ell_j = 2j-1$.

($\Leftarrow$) Seja $j \in \{1, \cdots, g-1\}$ tal que $\ell_j = 2j-1$. Seja $k = max\{i \in \{1, \cdots, g\} | \ell_i = 2i-1\}$. Se $k = 2$, então $\ell_2 = 2 \cdot 2 - 1 = 3$, e daí $2 \in H$.
Tome $k \geq 3$. Então ℓ_{k+1} não é da forma $2(k+1)-1$, isto é, $\ell_{k+1} \neq 2(k+1)-1 = 2k+1$. Pelo Lema 4.4 temos $\ell_{k+1} \leq 2(k+1)-1 = 2k+1$, mas como $\ell_{k+1} \neq 2k+1$ segue $\ell_{k+1} < 2k+1 \Rightarrow \ell_{k+1} \leq 2k$. Por outro lado, como $\ell_k < \ell_{k+1}$ e $\ell_k = 2k-1$, temos $\ell_{k+1} = 2k$, e disso concluímos que k é lacuna de H, pois se isso não acontecesse teríamos $k + k = 2k = \ell_{k+1} \in H$, o que é absurdo.
Considere o intervalo $[1, 2k]$. Como $\ell_{k+1} = 2k$ pertence a esse intervalo, $[1, 2k]$ possui $k+1$ lacunas e $k-1$ elementos de H. Considere todos os $k-1$ pares da forma $(\alpha, \ell_{k+1} - \alpha), \alpha \in \{1, \cdots, k-1\}$. Temos que $2k$ e k não se encontram entre esses pares. De fato, $2k$ não pertence pois o maior elemento é $2k-1$ e k não pertence pois $\alpha \in \{1, \cdots, k-1\}$. Assim temos que cada par é constituido de uma lacuna e uma não lacuna, pois se α for lacuna então $2k-\alpha$ é não lacuna. Considere o par $(1, 2k-1)$. Vimos que se $k \geq 3$ então $2k-1$ é uma lacuna. Mas daí teríamos $1 \in H$, o que é absurdo. Portanto $k = 2$ e H é hiperelíptico.

(b) ($\Rightarrow$) Seja H um semigrupo não hiperelíptico. Do Lema 4.4, tomando $j = g$ temos $\ell_g \leq 2g-1$. Como H é não hiperelíptico, $2 \notin H$, ou seja, $\ell_2 = 2$, e

daí $\ell_2 \leq 2 \cdot 2 - 2 = 2$. Considere agora $g \geq 3$. Do Lema 4.4 temos que, dado $j \in \{3, \cdots, g-1\}$, temos $\ell_j \leq 2j - 1$. Como H é não hiperelíptico, pelo item (a) temos $\ell_j < 2j - 1$, ou seja, $\ell_j \leq 2j - 2$, para todo $2 \leq j \leq g - 1$.

($\Leftarrow$) Para mostrar que H é não-hiperelíptico basta mostrar que $\ell_2 = 2$. Sabemos que $\ell_1 = 1$. Por hipótese $\ell_2 \leq 2 \cdot 2 - 2 = 2$. Como $\ell_1 < \ell_2$, temos $\ell_2 = 2$ e H é não-hiperelíptico.

□

Como já vimos, para todo $j \in \{1, \cdots, g\}$, temos $\ell_j \leq 2g - 1$.

Definição 4.6. *Se $\ell_g = 2g - 1$, H é dito um **semigrupo simétrico.***

Exemplo 4.7. *O semigrupo $\{0, 4, 5, 8, 9, 10, 12 \rightarrow\}$ é simétrico pois $g = 6$ e $\ell_g = 11 = 2 \cdot 6 - 1$.*

A simetria pode ser caracterizada da seguinte forma: *Seja H um semigrupo simétrico de gênero g. Para cada $n \in \mathbb{N}$ temos $n \in H \Leftrightarrow \ell_g - n \notin H$.* De fato, suponha $\ell_g - n \in H$. Como H é fechado para a soma teríamos $(\ell_g - n) + n = \ell_g \in H$, o que é absurdo. Reciprocamente, como H é simétrico, temos $\ell_g = 2g - 1$. Daí:

- Se $\ell_g - n < 0$ teríamos $2g - 1 - n < 0$, ou seja, $n > 2g - 1$, e daí $n \in H$.
- Suponha então $0 < \ell_g - n < 2g - 1$. Considere os pares da forma $(\alpha, \ell_g - \alpha)$, com $1 \leq \alpha \leq g - 1$, tendo ao todo $g - 1$ pares. Como $2g - 1$ é uma lacuna que não pertence aos pares acima, estes contém $g - 1$ lacunas. Dessa forma os pares são formados por uma lacuna e uma não lacuna e, como $\ell_g - n \notin H$, temos $n \in H$.

Proposição 4.8. *Seja H um semigrupo de gênero g tal que $\ell_g = 2g - 2$. Então $g - 1 \notin H$ e, para cada inteiro $n \neq g - 1$, temos $n \in H$ se, e somente se $\ell_g - n \notin H$.*

Demonstração: Se $g - 1 \in H$, teríamos $(g - 1) + (g - 1) = 2g - 2 = \ell_g \in H$, o que é absurdo. Assim $g - 1 \notin H$. Seja agora $n \neq g - 1$. Tome os $g - 2$ pares da forma $(n, \ell_g - n)$, com $1 \leq n \leq g - 2$. Como o gênero do semigrupo é g segue que existem g lacunas no intervalo $[1, 2g - 2]$. Como $2g - 2$ e $g - 1$ são lacunas e não pertencem aos pares, estes possuem $g - 2$ lacunas, e daí cada par é constituído por uma lacuna e uma não-lacuna. Portanto, $n \in H$ se, e somente se $\ell_g - n \notin H$.

□

Teorema 4.9. *Se H é um semigrupo não-hiperelíptco de gênero g, então cada inteiro r, com $2 \leq r \leq 2g$, é a soma de duas lacunas de H, com exceção apenas de ℓ_g, se H é simétrico.*

Demonstração: Seja $r \geq 2$ um inteiro tal que r não é a soma de duas lacunas de H. Considere os pares $(i, r - i)$, com $1 \leq i \leq \left[\frac{r}{2}\right]$. Como r não é a soma de duas lacunas e $i + (r - i) = r$, cada par possui pelo menos uma não-lacuna de H, e daí o número de não-lacunas entre 1 e $r - 1$ é pelo

menos $\left[\frac{r}{2}\right]$, pois existem $\left[\frac{r}{2}\right]$ pares. Denotando por j o número de lacunas menores do que r temos $j \leq r-1-\left[\frac{r}{2}\right] \Rightarrow 2j+1 \leq r$. De fato, se r é par, $j \leq r-1-\frac{r}{2} \Rightarrow j+1 \leq \frac{r}{2} \Rightarrow 2j+2 \leq r \Rightarrow 2j+1 \leq r$. Se r é ímpar, $j \leq r-1-\left(\frac{r}{2}-\frac{1}{2}\right) \Rightarrow j+\frac{1}{2} \leq \frac{r}{2} \Rightarrow 2j+1 \leq r$. Como $r \leq 2g$ temos $2j+1 \leq 2g \Rightarrow 2j < 2g \Rightarrow j < g$. Como j denota o número de lacunas menores do que r temos a desigualdade

$$2j+1 \leq r \leq \ell_{j+1}. \tag{4.1}$$

Por hipótese, H é não-hiperelíptico. Daí, pelo Teorema 4.3, temos $\ell_j \leq 2j-2$, para todo $j \in \{1, \cdots, g-1\}$ e $\ell_g \leq 2g-1$. Se $j+1 \in \{1, \cdots, g-1\}$ temos, por (4.1), $2j+1 \leq \ell_{j+1} \leq 2j$, o que é absurdo. Então $g = j+1$. Por (4.1) temos $r \leq \ell_g \leq 2g-1$. Por outro lado temos $2j+1 = 2j+2-1 = 2(j+1)-1 = 2g-1 \leq r$. Então $r = 2g-1 = \ell_g$, ou seja, o único inteiro $2 \leq r \leq 2g$ que não é soma de duas lacunas é ℓ_g, se H for simétrico.

□

Proposição 4.10. *Se H é um semigrupo não-hiperelíptico de gênero g tal que $\ell_{g-1} = 2g-4$ ou $\ell_g \geq 2g-2$, então $\#(L+L) = 3g-3$.*

Demonstração: Seja $\ell_g \geq 2g-2$. Pelo Teorema 4.3, $\ell_g \leq 2g-1$. Assim $\ell_g = 2g-2$ ou $\ell_g = 2g-1$. Pelo Teorema 4.9, temos que os elementos do conjunto

$$A = \{2, 3, \cdots, 2g-2, \ell_g+\ell_1, \cdots, \ell_g+\ell_g\}$$

são somas de duas lacunas. Note que $\#A = 3g-3$. Vamos mostrar que a soma de quaisquer duas lacunas de H é um elemento de A. Pelo Teorema 4.9, todos os elementos de 2 a $2g-2$ são somas de lacunas. Considere então $u > 2g-2$ tal que $u = \ell_i + \ell_j$, com $\ell_j > g-1$ (pois como $u > 2g-2$, um deles deve ser maior que $g-1$). Como $u > 2g-2$, temos $\ell_g \leq u$, e daí podemos escrever $u = \ell_g + s$, com $s \geq 0$. Assim temos

$$u = \ell_g + s = \ell_i + \ell_j \Rightarrow \ell_i = (\ell_g - \ell_j) + s.$$

1º caso: Suponha $\ell_g = 2g-1$, ou seja, que H é simétrico.
Se $s \in H$ temos $\ell_g - \ell_j \notin H$, pois ℓ_i é lacuna. Daí $\ell_g - \ell_j = \ell_k \Rightarrow \ell_g = \ell_k + \ell_i$, ou seja, ℓ_g é soma de duas lacunas, o que contradiz o Teorema 4.9. Então $s \notin H$.

2º caso: $\ell_g = 2g-2$. Como supomos $\ell_j > g-1$, temos $\ell_j \neq g-1$. Da igualdade $u = \ell_i + \ell_j = \ell_g + s$ temos $\ell_i - s = \ell_g - \ell_j$. Suponha $s \in H$. Pela Proposição 4.8 temos $\ell_g - \ell_j \in H$. Daí $\ell_i - s \in H \Rightarrow \ell_i - s = N \in H$. Então $\ell_j = N + s \in H$, o que é absurdo. Portanto, $s \notin H$.

Dessa forma concluímos que a soma de quaisquer duas lacunas pertence ao conjunto A.

Vamos analisar o caso em que $\ell_{g-1} = 2g-4$. Podemos considerar apenas o caso em que $\ell_g = 2g-3$, pois o caso em que $\ell_g \geq 2g-2$ foi provado acima. Neste caso, temos que cada par $(r, \ell_g - r)$, com $r \in \{2, \cdots, g-2\}$,

tem uma lacuna e uma não lacuna de H. De fato, não podem haver duas não-lacunas, pois $r + (\ell_g - r) = \ell_g$ e não podem haver duas lacunas pois existem $g-3$ pares e as lacunas $1, 2g-3$ e $2g-4$ não pertencem a esses pares. Como $g-2 \notin H$, pois $(g-2)+(g-2) = 2g-4 = \ell_{g-1} \notin H$, temos $g-1 = (2g-3)-(g-2) = \ell_g - (g-2)$ é uma não lacuna devido ao par $(g-2, g-1)$ e daí, como $(g-1)+(g-3) = 2g-4 = \ell_{g-1}$, temos $g-3 \notin H$. Da mesma forma concluímos que os elementos $1, \cdots, g-2 \notin H$. Pelo Teorema 4.9 já temos que qualquer r, com $2 \leq r \leq 2g$, é soma de duas lacunas, e assim já temos $2g-1$ elementos. Os demais elementos que são somas de duas lacunas são:

$$\begin{aligned}
&\ell_g + 4 = 2g - 3 + 4 = 2g + 1\\
&\ell_g + 5 = 2g - 3 + 5 = 2g + 2\\
&\vdots\\
&\ell_g + g - 2 = 2g - 3 + g - 2 = 3g - 5\\
&\ell_{g-1} + \ell_{g-1} = 2g - 4 + 2g - 4 = 4g - 8\\
&\ell_g + \ell_{g-1} = 2g - 3 + 2g - 4 = 4g - 7\\
&\ell_g + \ell_g = 2g - 3 + 2g - 3 = 4g - 6
\end{aligned}$$

que são, ao todo, $g-2$ elementos. Assim o número total de elementos que são soma de duas lacunas é $2g-1+g-2 = 3g-3$.

□

Teorema 4.11. *Se H é um semigrupo simétrico não-hiperelíptico de gênero g então, para cada inteiro $n \geq 2$, temos*

$$nL = \{n, n+1, \cdots (n-1)(2g-1)-1\} \cup \{(n-1)(2g-1) + \ell_j | j = 1, \cdots, g\},$$

onde nL denota o conjunto de todas as somas de n lacunas de H. Em particular,

$$\#(nL) = (2n-1)(g-1), \text{ para cada } n \geq 2.$$

Demonstração: Denote

$$A := \{n, n+1, \cdots (n-1)(2g-1)-1\} \cup \{(n-1)(2g-1) + \ell_j | j = 1, \cdots, g\}.$$

$(nL \subseteq A)$: Seja $u \in nL$, ou seja, $u = \ell_{i_1} + \cdots + \ell_{i_n}$. O menor valor que u pode assumir é n, pois nesse caso será a soma de 1 n vezes. Se u for qualquer valor entre n e $(n-1)(2g-1)-1$ o resultado segue trivialmente. Vamos assumir então que $u = (n-1)\ell_g + s$, com $s \geq 0$ e vamos mostrar que s é uma lacuna. Temos

$$u = \ell_{i_1} + \cdots + \ell_{i_n} = (n-1)\ell_g + s$$

$$\Rightarrow \ell_{i_n} = (\ell_g - \ell_{i_1}) + (\ell_g - \ell_{i_2}) + \cdots + (\ell_g - \ell_{i_{n-1}}) + s.$$

Como H é simétrico ℓ_g é sempre a soma de uma lacuna e uma não-lacuna, e assim $\ell_g - \ell_{i_k} \in H$. Como ℓ_{i_n} é lacuna temos $s \notin H$ e o resultado segue.

$(A \subseteq nL)$: Para qualquer $n \geq 2$ já temos que os elementos do conjunto $\{(n-1)(2g-1) + \ell_j | j = 1, \cdots, g\}$ são somas de n lacunas. Vamos provar por

indução que os elementos do conjunto $\{n, n+1, \cdots, (n-1)(2g-1)-1\}$ também o são. O caso em que $n = 2$ já está provado no Teorema 4.9. Suponha que qualquer elemento k, com $n \leq k \leq (n-1)(2g-1)-1$, seja soma de n lacunas. Tome um inteiro r tal que $n+1 \leq r \leq n(2g-1)-1$. Se encontrarmos uma lacuna ℓ tal que

$$n \leq r - \ell \leq (n-1)(2g-1) - 1, \tag{4.2}$$

provaremos o resultado, pois r será a soma de $n+1$ lacunas. Vamos analisar três casos:

1º caso: $r \geq n + 2g - 1$. Neste caso tome $\ell = 2g-1$. Então temos

$$n + 2g - 1 \leq r \Rightarrow n + 2g - 1 - (2g-1) \leq r - (2g-1) \Rightarrow n \leq r - \ell$$

$r \leq n(2g-1)-1 \Rightarrow r-(2g-1) \leq (n-1)(2g-1)-1 \Rightarrow r-\ell \leq (n-1)(2g-1)-1.$

Portanto, para este caso encontramos uma lacuna que satisfaz (4.2)

2º caso: $r = n+2g-2$. Neste caso tome $\ell = 2$. Então temos $r-2 = n+2g-4$. Como o gênero é maior ou igual a 2, pois H é não-hiperelíptico, temos $r-2 \geq n$. Por outro lado, precisamos mostrar $r-2 \leq (n-1)(2g-1)-1$, o que é o mesmo que provar que $n+2g-4 \leq (n-1)(2g-1)-1$. Temos $(n-1)(2g-1)-1 = 2ng-n-2g = n+2g+(2ng-2n-4g)$. Basta então provar que $-4 \leq 2ng-2n-4g$, o que é equivalente a provar $n+2g-ng \leq 2$. Como $g \geq 2, -g \leq -2$, e daí temos

$$n + 2g - ng = n - g(n-2) \leq n - 2(n-2) = -n - 4 \leq -2 - 4 = 2,$$

pois $n \geq 2$. Com isso provamos que $r-2 \leq (n-1)(2g-1)-1$ e também conseguimos uma lacuna que satisfaz (4.2).

3º caso: $r \leq n + 2g - 3$. Neste caso tome $\ell = 1$. Como $r \geq n+1$, então $r-1 \geq n$. Podemos provar agora que $r-1 \leq (n-1)(2g-1)-1$ usando $r-1 \leq n+2g-4$, o que é o mesmo que mostrar que

$$n + 2g - 4 \leq (n-1)(2g-1) - 1,$$

e isso já foi provado no 2º caso.

Dessa forma encontramos lacunas para todos os valores de r e o resultado segue por indução.

Como consequência desse resultado temos $\#(nL) = (2n-1)(g-1)$, para $n \geq 2$.

□

Definição 4.12. *Um semigrupo é* ***quase-simétrico*** *se* $\ell_g = 2g-2$.

Exemplo 4.13. *Considere o semigrupo numérico* $\{0, 3, 5 \rightarrow\}$. *Este semigrupo tem gênero* $g = 3$ *e* $\ell_g = 4 = 2 \cdot 3 - 2$, *portanto é quase-simétrico.*

Teorema 4.14. *Sejam H um semigrupo quase-simétrico de gênero g e n um inteiro positivo. Então*

$$nL = \{n, n+1, \cdots, (n-1)(2g-2)\} \cup \{\ell_i + (n-1)(2g-2); i = 1, \cdots, g\}$$

e, em particular, $\#(nL) = (2g-3)n - g - 3$.

Demonstração: Vamos denotar $B = nL = \{n, n+1, \cdots, (n-1)(2g-2)\} \cup \{\ell_i + (n-1)(2g-2); i = 1, \cdots, g\}$

- $nL \subseteq B$: Seja $u \in nL$. Então $u = \ell_{i_1} + \cdots + \ell_{i_n}, \ell_{i_1} \leq \cdots \leq \ell_{i_n}$. O menor valor que u pode assumir é n, que é a soma de 1 n-vezes. Se n for qualquer valor entre n e $(n-1)(2g-2)$ já temos o resultado. Suponha $u = (n-1)\ell_g + s,$ para $s \geq 0$. Vamos mostrar que s é uma lacuna. Temos

$$\ell_{i_1} + \cdots + \ell_{i_n} = s + (n-1)\ell_g$$

$$\Rightarrow \ell_{i_1} = (\ell_g - \ell_{i_n}) + \cdots + (\ell_g - \ell(i_2)) + s,$$

  com $\ell_i > g - 1$ para todo i. Pela Proposição 4.8, temos que cada $\ell_g - \ell_i \in H$ logo $s \notin H$, pois caso contrário $\ell_{i_1} \in H$, o que é absurdo.

- $B \subseteq nL$: os elementos do conjunto $\{\ell_i + (n-1)\ell_g; i = 1, \cdots, g\}$ já são somas de n lacunas. Vamos analisar os elementos do conjunto $\{n, n+1, \cdots, (n-1)(2g-2)\}$. Seja $u \in \{n, n+1, \cdots, (n-1)(2g-2)\}$. Então podemos escrever

$$u - n = (r-2) + i(2g-3), r \in \{2, \cdots, 2g-2\} \quad \text{e} \quad i \in \{0, \cdots, n-2\}.$$

  Daí temos

$$\begin{aligned} u &= r - 2 + n + i(2g-2) - i \\ &= (n-2-i) + i(2g-2) + r \\ &= (n-2-i)\ell_1 + i\ell_g + r. \end{aligned}$$

  Para mostrar que u é soma de n lacunas basta mostrar que r é a soma de duas lacunas. Como $\ell_g = 2g - 2 = 2(g-1), 2$ deve ser lacuna de H e, portanto, H é não-hiperelíptico. Daí, pelo Teorema 4.9, o resultado segue.

□

Exemplo 4.15. *Considere o semigrupo numérico*

$$H = \{0, 13, 14, 15, 16, 17, 18, 20, 22, 23, 26 \rightarrow\}.$$

Vamos calcular L_2. Temos que o gênero de H é 16 e que o conjunto de lacunas é dado por

$$L = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 19, 21, 24, 25\}.$$

Pelo Teorema 4.9, todo número entre 2 e 32 pertence a L_2, e daí já temos $\#L_2 \geq 30$. Como a maior lacuna é 25, o maior elemento de L_2 é 50. Precisamos então verificar os valores de r, para $33 \leq r \leq 49$.

Note que $33 = 25 + 8$; $34 = 25 + 9$; $35 = 25 + 10$; $36 = 25 + 11$; $37 = 25 + 12$; $38 = 19 + 19$; $40 = 19 + 21; 42 = 21 + 21$; $43 = 19 + 24$; $44 = 19 + 25$; $45 = 21 + 24$; $46 = 21 + 24$; $48 = 24 + 24$; $49 = 24 + 25$. *Os elementos* $39, 41$ *e* 47 *não são escrito como a soma de duas lacunas. Portanto,* $\#L_2 = 46$. *Observe que, pelo Teorema 4.11, podemos concluir que* H *não é um semigrupo simétrico, pois* $3g - 3 = 3 \cdot 16 - 3 = 45$ *e* $\#L_2 = 46$.

Em [4], Komeda cita que todo semigrupo numérico H tal que $g \leq 15$ satisfaz $\#L_2(H) \leq 3g-3$. Além disso, temos a seguinte tabela de semigrupos com gênero até 37, onde n_g representa o número de semigrupos numéricos de gênero g e m_g representa o número de semigrupos numéricos de gênero g, com $\#L_2 > 3g - 3$:

g	n_g	m_g
16	2806	2
17	8045	6
18	13467	15
19	22464	31
20	37396	67
21	62194	145
22	103246	293
23	170963	542
24	282828	1053
25	467224	1944
26	770832	3591
27	1270267	6584
28	2091030	11871
29	3437839	20987
30	5646773	37598
31	9266788	66330
32	15195070	116501
33	24896206	203300
34	40761087	323978
35	66687201	615762
36	109032500	1058418
37	178158289	1819323

4.2 Semigrupos γ-hiperelípticos

Nesta seção vamos apresentar propriedades de um tipo particular de semigrupo: os semigrupos γ-hiperelípticos.

Definição 4.16. *Seja* $\gamma \in \mathbb{N}$. *Um semigrupo numérico* H *é dito* $\gamma-$***hiperelíptico*** *se as seguintes condições são satisfeitas:*

(a) H *tem exatamente* γ *elementos pares no intervalo* $[2, 4\gamma]$*;*

(b) $4\gamma + 2 \in H$.

Um semigrupo hiperelíptico é equivalente a um semigrupo 0-hiperelíptico.

Exemplo 4.17. *Considere o semigrupo numérico*

$$H = \{0, 4, 8, 12 \rightarrow\},$$

onde $g = 9$. *H possui 3 elementos pares no intervalo* $[2, 12]$, *a saber 4,8 e 12, e* $14 = 4 \cdot 3 + 2 \in H$. *Portanto H é um semigrupo 3-hiperelíptico.*

Para $i = 1, \cdots, m-1$, seja $s_i = s_i(H)$ o menor elemento de H que é congruente a i módulo m e defina $e_i = e_i(H)$ como

$$s_i = e_i m + i.$$

Exemplo 4.18. *Seja o semigrupo* $\{0, 4, 5, 8, 9, 10, 12 \rightarrow\}$. *Como* $m = 4$ *temos* $i = 1, 2, 3$. *Daí,*

- $s_1 = 5$, *pois* $5 \equiv 1 \ (mod\ 4)$;
- $s_2 = 10$, *pois* $10 \equiv 2 \ (mod\ 4)$;
- $s_3 = 15$, *pois* $15 \equiv 3 \ (mod\ 4)$.

Neste caso temos $e_1 = 1, e_2 = 2$ *e* $e_3 = 3$, *respectivamente.*

Proposição 4.19. *Os* $e_i's$ *definidos acima satisfazem:*

(a) $g = \sum_{i=1}^{m-1} e_i$.

(b) $\begin{cases} e_i + e_j \geq e_{i+j}, & \text{se} \quad i + j < m \\ e_i + e_j + 1 \geq e_{i+j-m}, & \text{se} \quad i + j > m \end{cases}$

Demonstração:

(a) Como $s_i \in H$, para todo $i \in \{1, \cdots, m-1\}$, temos $\{s_i + jm_1, j \in \mathbb{N}\} \subset H$. Note também que $mj + i \notin H$, para todo $i \in \{1, \cdots, m-1\}$ e para todo $j \leq e_i - 1$. De fato, como $s_i = e_i m + i$ é o menor elemento de H congruente a i módulo m, todos os elementos $mj + i$ tais que $i = 1, \cdots, m-1$ e $j \leq e_i - 1$ não pertencem a H, pois são menores que s_i. Logo as lacunas ℓ tais que $\ell \equiv i \ (mod\ m)$ são

$$\{mj + i; i = 0, \cdots, e_i - 1\}.$$

Isso significa que as lacunas que são congruentes a i são e_i. Portanto, temos

$$g = \sum_{i=1}^{m-1} e_i.$$

(b) Suponha $i + j < m$. Temos

$$s_i + s_j = (e_i m + i) + (e_j m + j) = (e_i + e_j)m + (i + j) \equiv i + j \ (mod\ m).$$

Como s_{i+j} é o menor elemento de H que é congruente a $i + j$ segue que $s_i + s_j \geq s_{i+j}$. Daí temos

$$(e_i + e_j)m + (i + j) \geq (e_{i+j})m + (i + j)$$

$$\Rightarrow (e_i + e_j)m \geq (e_{i+j})m$$

$$\Rightarrow e_i + e_j \geq e_{i+j}.$$

Suponha $i + j > m$. Note que, como $i < m$ e $j < m$, então $i + j < 2m$. Assim

$$s_i+s_j = (e_i m+i)+(e_j m+j) = (e_i+e_j)m+(i+j) \equiv i+j \equiv i+j-m \ (mod\ m).$$

Daí temos $s_i + s_j \geq s_{i+j-m}$. Então

$$(e_i + e_j)m + (i + j) \geq (e_{i+j-m})m + (i + j - m)$$

$$\Rightarrow (e_i + e_j)m + (i + j) \geq (e_{i+j-m} - 1) + (i + j)$$

$$\Rightarrow (e_i + e_j)m \geq (e_{i+j-m} - 1)m$$

$$\Rightarrow e_i + e_j + 1 \geq e_{i+j-m}.$$

□

Exemplo 4.20. *Seja H um semigrupo de gênero g e multiplicidade $m = 4$. Tome $\gamma = e_2$ e note que e_2 representa o número de lacunas pares de H (pois representa o número de elementos que deixam resto 2 na divisão por 4). Note ainda que, como o conjunto de lacunas é dado por $\{mj + i; j = 0, \cdots, e_i - 1\}$, temos $4(\gamma - 1) + 2 \leq 2g - 2 \Rightarrow 4\gamma \leq 2g$. Assim,*

$$\{4, \cdots, 4\gamma, 4\gamma + 2, \cdots, 2g\}$$

é o conjunto de elementos pares de H no intervalo $[2, 2g]$. Em particular, existem γ elementos pares no intervalo $[2, 4\gamma]$ e $4\gamma + 2 \in H$, logo H é γ-hiperelíptico.

Consideremos $\tilde{m}_1 < \tilde{m}_2 < \cdots$ os elementos pares do semigrupo.

Observação 4.21. *Se H é um semigrupo $\gamma-$hiperelíptico, então $\tilde{m}_\gamma = 4\gamma$. De fato, suponha que 4γ seja uma lacuna. No intervalo $[2, 4\gamma]$ existem 2γ números pares, sendo que γ deles pertencem a H, pois H é $\gamma-$hiperelíptico. Dessa forma existem γ lacunas pares no intervalo $[2, 4\gamma]$. Os números $4\gamma - \tilde{m}_i, i = 1, \cdots, \gamma$, são lacunas pares de H menores que 4γ. Dessa forma existem $\gamma+1$ lacunas pares no intervalo $[2, 4\gamma]$, o que é absurdo. Portanto $4\gamma \in H$*

Vamos agora caracterizar os semigrupos $\gamma-$hiperelípticos.

Lema 4.22. *Seja H um semigrupo e $\gamma \in \mathbb{N}$. Então H é $\gamma-$hiperelíptico se, e somente se γ é o número de lacunas pares de H. Neste caso*

$$\{4\gamma + 2i; i \in \mathbb{N}\} \subseteq H,$$

e para $i \in \mathbb{N}, \tilde{m}_{\gamma+i} = 4\gamma + 2i$.

Demonstração: ($\Rightarrow$) Seja H um semigrupo $\gamma-$hiperelíptico. Vamos mostrar que $\mathcal{G} := \{4\gamma + 2i; i \in \mathbb{N}\} \subseteq H$, pois com isso provaremos que γ é o número de lacunas pares de H. Suponha $\mathcal{G} \nsubseteq H$. Seja $\ell = 4\gamma + 2i$ o menor elemento de $\mathcal{G}$ que não pertence a H. Pelas propriedades de semigrupo temos que $4\gamma + 2i - \widetilde{m}_j$ é lacuna de H, para todo $j \in \{1, \cdots, \gamma\}$. Como $4\gamma + 2i$ é o menor elemento de $\mathcal{G}$ que não pertence a H, temos $4\gamma + 2i - \widetilde{m}_1 \leq 4\gamma$. Tome a sequência

$$0 < 4\gamma + 2i - \widetilde{m}_\gamma < \cdots < 4\gamma + 2i - \widetilde{m}_1 \leq 4\gamma.$$

Como no intervalo $[2, 4\gamma]$ existem γ elementos pares e γ lacunas pares temos $\widetilde{m}_\gamma \leq 4\gamma \Rightarrow 4\gamma - \widetilde{m}_\gamma \geq 0 \Rightarrow 4\gamma + 2i - \widetilde{m}_\gamma \geq 2i$, para todo $i \geq 2$, pois $4\gamma + 2 \in H$ e $4\gamma + 2i \notin H$. Assim temos, para todo $j \in \{1, \cdots, \gamma\}$,

$$2i \leq 4\gamma + 2i - \widetilde{m}_j \leq 4\gamma, i \geq 2.$$

Como no intervalo $[2i, 4\gamma]$ existem γ lacunas pares, que são os elementos da forma $4\gamma + 2i - \widetilde{m}_j$, temos que $2 \in [2, 4\gamma]$ deve ser um elemento de H, logo não pode existir i. Portanto

$$\{4\gamma + 2i; i \in \mathbb{N}\} \subseteq H.$$

($\Leftarrow$) Seja γ o número de lacunas pares de H e seja ℓ sua maior lacuna par. Então $\ell < \widetilde{m}_\gamma$, pois caso contrário teríamos $\gamma + 1$ lacunas de H dadas por $\ell - \widetilde{m}_\gamma, \cdots, \ell - \widetilde{m}_1, \ell$. Como $\widetilde{m}_{\gamma+i} = 4\gamma + 2i$, para $i \in \mathbb{N}, \widetilde{m}_\gamma \leq 4\gamma$, temos $4\gamma + 2 \in H$, e daí H é $\gamma-$hiperelíptico.

□

Corolário 4.23. *Seja H um semigrupo de gênero g e γ o número de suas lacunas pares. Então:*

1. *Um elemento ímpar de H é limitado inferiormente por $2g - 4\gamma + 1$.*
2. *Se $g \geq 4\gamma$ então $m_i = \widetilde{m}_i, \forall i = 1, \cdots, \gamma$.*
3. *Se $g \geq 4\gamma$ e $h \in H$ tal que $h \leq g$ então h é par.*

Demonstração: Pelo teorema anterior sabemos que H é $\gamma-$hiperelíptico.

1. Como H é γ-hiperelíptico, H possui exatamente γ elementos pares no intervalo $[2, 4\gamma]$. Pelo Teorema 4.3, $\ell_j \leq 2j - 1, 1 \leq j \leq g$. Em particular temos $\ell_j \leq 2g-1$, ou seja, todas as lacunas de H estão no intervalo $[1, 2g-1]$. Como γ lacunas são pares o número de lacunas ímpares é $g-\gamma$, e no intervalo

$[1, 2g-1]$ existem g elementos ímpares. Assim, o número de elementos ímpares de H é $g-(g-\gamma)=\gamma$.

Afirmação: Seja h um número ímpar de H. Então $h+\widetilde{m}_\gamma \geq 2g$.
De fato, suponha $h+\widetilde{m}_\gamma < 2g$. Então $h+\widetilde{m}_\gamma \leq 2g-1$. Nesse caso teríamos $h, h+\widetilde{m}_1, \cdots, h+\widetilde{m}_\gamma$ elementos ímpares de H no intervalo $[1, 2g-1]$, o que é absurdo. Como $\widetilde{m}_\gamma = 4\gamma$, temos

$$h+\widetilde{m}_\gamma \geq 2g \Rightarrow h+4\gamma \geq 2g \Rightarrow h \geq 2g-4\gamma \Rightarrow h \geq 2g-4\gamma+1,$$

pois h é ímpar e $2g-4\gamma$ é par.

2. Seja h um elemento ímpar de H. Por (1) temos $h \geq 2g-4\gamma+1$. Como $g \geq 4\gamma$ temos $h \geq 4\gamma+1$, ou seja, todos os elementos ímpares de H são maiores que $4\gamma = \widetilde{m}_\gamma$. Daí $m_i = \widetilde{m}_i$, para todo $i \in \{1, \cdots, \gamma\}$.

3. Suponha h ímpar. Então por (1) e pela hipótese temos

$$g \geq h \geq 2g-4\gamma+1$$

$$\Rightarrow g \geq 2g-4\gamma+1 \Rightarrow g \leq 4\gamma-1,$$

o que contradiz a hipótese.

□

Vamos mostrar como construir um semigrupo γ-hiperelíptico simétrico a partir de um semigrupo de gênero γ.

Proposição 4.24. *Seja $\widetilde{H}$ um semigrupo de gênero γ e $g \geq 3\gamma$ um inteiro. O conjunto*

$$H = \{2h | h \in \widetilde{H}\} \cup \{2g-1-2s | s \in \mathbb{Z} \setminus \widetilde{H}\}$$

é um semigrupo simétrico γ-hiperelíptico de gênero g.

Para facilitar a notação, denotamos $H_1 = \{2h; h \in \widetilde{H}\}$ e $H_2 = \{2g-1-2s; s \in \mathbb{Z} \setminus \widetilde{H}\}$. Assim $H = H_1 \cup H_2$. Vamos mostrar que H é um semigrupo numérico. Temos $0 \in H$, pois $0 \in \widetilde{H}$, já que $\widetilde{H}$ é um semigrupo numérico.

Sejam $x_1, x_2 \in H$.

- Se $x_1, x_2 \in H_1$ então $x_1 = 2h_1$ e $x_2 = 2h_2$, para $h_1, h_2 \in \widetilde{H}$, e como $\widetilde{H}$ é semigrupo temos $x_1+x_2 = 2(h_1+h_2) \in H$.

- Suponha $x_1 \in H_1$ e $x_2 \in H_2$. Então $x_1 = 2h$, para $h \in \widetilde{H}$ e $x_2 = 2g-1-2s$, com $s \in \mathbb{Z} \setminus \widetilde{H}$. Assim, temos $x_1+x_2 = 2h+2g-1-2s = 2g-1-2(s-h)$. Agora note que $s-h$ é lacuna, pois caso contrário teríamos $s-h+h = s \in \widetilde{H}$, o que é absurdo. Assim $x_1+x_2 \in H$.

- Suponha $x_1, x_2 \in H_2$. Como os elementos de H_2 são números ímpares, a soma de dois desses elementos é um número par. Como $\widetilde{H}$ tem gênero γ, todo elemento maior que $2\gamma-1$ pertence a $\widetilde{H}$. Assim, se n é um número

par tal que $n > 2(2\gamma - 1)$, então $n \in \widetilde{H}$. Dessa forma, basta provar a desigualdade $x_1 + x_2 > 2(2\gamma - 1)$.
Seja $s \in \mathbb{Z} \setminus \widetilde{H}$. Então $s \leq 2\gamma - 1 \Rightarrow 2g - 1 - 2s \geq 2g - 1 - 2(2\gamma - 1)$. Como $g \geq 3\gamma$ temos $2g \geq 6\gamma$, daí $2g - 1 - 2s \geq 6\gamma - 1 - 4\gamma + 2 \geq 2\gamma + 1$. Assim $x_1 + x_2 \geq 4\gamma + 2 > 4\gamma - 2$ e, portanto, $x_1 + x_2 \in H$.

Vamos mostrar agora que o gênero de H é g. Temos que todo número par maior que $2(2\gamma - 1)$ pertence a H. Como $g \geq 3\gamma$, todo elemento par maior que $2g$ pertence a H. Vamos analisar os elementos de H_2. Todos os inteiros negativos pertencem a $\mathbb{Z} \setminus \widetilde{H}$. Tome, por exemplo, $y = -1 \in \mathbb{Z} \setminus \widetilde{H}$. Então $2g - 1 - 2(-1) = 2g - 1 \in H$. Se considerarmos todos os inteiros negativos concluiremos que todos os números ímpares maiores que $2g$ pertencem a H. Portanto, todo natural maior ou igual a $2g$ pertence ao semigrupo, ou seja, qualquer lacuna de H é menor ou igual a $2g - 1$. Os elementos pares de H são da forma $2h$, para $h \in \widetilde{H}$. Como $\widetilde{H}$ é γ-hiperelíptico, H possui γ lacunas pares. Vamos analisar agora as lacunas ímpares. Os elementos ímpares de H são da forma $2g - 1 - 2s$, onde s pertence ao conjunto de lacunas de $\widetilde{H}$. Como $\widetilde{H}$ tem gênero γ e no intervalo $[1, 2g - 1]$ existem g números ímpares, temos $g - \gamma$ lacunas ímpares no intervalo $[1, 2g - 1]$. Portanto o gênero de H é $g - \gamma + \gamma = g$. Como $0 \in \widetilde{H}$, temos $0 \notin \mathbb{Z} \setminus \widetilde{H}$ e, portanto, $2g - 1 \notin H$. Disso segue que H é simétrico. Além disso, como H possui γ lacunas pares, pelo Lema 4.22, temos que H é $\gamma-$hiperelíptico.

□

Exemplo 4.25. *Considere o semigrupo* $\widetilde{H} = \{0, 4, 6 \rightarrow\}$. *Vamos construir um semigrupo* H *simétrico,* 4*-hiperelíptico de gênero* 12 *a partir de* $\widetilde{H}$. *Sabemos que existem exatamente* 4 *lacunas pares em* H. *Então*

$$H \supset \{0, 8, 12, 14, 16, 18, 20, 22, 24 \rightarrow\}.$$

Vamos analisar agora quem são os elementos do conjunto $\{2g-1-2s; s \in \mathbb{Z}\setminus\widetilde{H}\}$. *Temos* $\mathbb{Z}_+ \setminus \widetilde{H} = \{1, 2, 3, 5\}$ *Assim, os elementos ímpares de* H *são* $13, 17, 19, 21$. *Portanto,*

$$H = \{0, 8, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 24 \rightarrow\}.$$

CAPÍTULO 5

SEMIGRUPOS NÃO-WEIERSTRASS

Neste capítulo chamaremos de X uma curva algébrica, não singular, projetiva e definida sobre um corpo k algebricamente fechado. No Capítulo 3 estabelecemos uma correspondência biunívoca entre pontos de uma curva e lugares do corpo de funções $k(X)$. Como k é algebricamente fechado todo lugar possui grau 1, e portanto é possível transferir o Teorema das Lacunas de Weierstrass para o estudo de curvas, que pode ser enunciado da seguinte forma:

"Seja X uma curva de gênero g e seja P um ponto de X. Então existem exatamente g números $0 < n_1 < n_2 < \cdots < n_g < 2g$ tais que não existe $z \in k(X)$ com polo de ordem $n_i, i \in \{1, \cdots, g\}$, em P."

Utilizando também o que provamos no Capítulo 2 para lugares, podemos concluir que o conjunto de números polos de um ponto $P \in X$ é fechado para a soma e como, o número de lacunas é finito, este conjunto é um semigrupo numérico.

Dessa forma, com a demonstração do Teorema de Weierstrass, provado por Weierstrass em meados de 1860, foi possível concluir que dada uma curva X algébrica, não singular, projetiva e definida sobre um corpo k algebricamente fechado, a todo $P \in X$ podemos associar um semigrupo numérico. Esse semigrupo é chamado **Semigrupo de Weierstrass em** P e é denotado por $H(P)$. Então podemos definir:

Definição 5.1. *Um número natural $n \in H(P)$ se, e somente se existe uma função racional sobre X regular em $X \setminus P$ e tem em P um polo de ordem n.*

Em 1893, o matemático alemão Hurwitz questionou a recíproca do resultado enunciado acima: *Dado um semigrupo H, existe uma curva X tal que, para*

algum ponto P de X, se tenha $H = H(P)$? Essa questão só foi resolvida, depois de algumas respostas equivocadas, em 1980, por Buchweitz, que construiu um semigrupo que não é de Weierstrass. Oliveira [6] observou que o método de Buchweitz não se aplica a semigrupos simétricos. Em 1993, baseado nos resultados de Torres [11], Oliveira e Stohr construíram um semigrupo simétrico que não é de Weierstrass. Neste capítulo apresentamos esses resultados.

5.1 Semigrupos não-Weierstrass obtidos por Buchweitz

O método de Buchweitz serve para construir semigrupos numéricos que não são de Weierstrass e se baseia na caracterização das lacunas do semigrupo.

Seja F/K um corpo de funções e P um lugar.

Proposição 5.2 (Método de Buchweitz)**.** *Um número inteiro positivo n é uma lacuna de P se, e somente se existe uma diferencial de Weil regular com $v_P(\omega) = n - 1$.*

Demonstração: Pelo Teorema de Riemann-Roch, temos

$$\begin{aligned} \ell(nP) &= n\, degP + 1 - g + \ell(W - nP) \\ \ell((n-1)P) &= (n-1)degP + 1 - g + \ell(W - (n-1)P) \end{aligned}$$

onde W é um divisor canônico. Destas desigualdades segue

$$\begin{aligned} \ell(nP) - \ell((n-1)P) &= degP + \ell(W - nP) - \ell(W - (n-1)P) \\ &= 1 + \ell(W - nP) - \ell(W - (n-1)P). \end{aligned}$$

Como n é lacuna e $\mathcal{L}((n-1)P) \subseteq \mathcal{L}(nP)$, temos $\ell(nP) = \ell(n-1)$, e daí n é lacuna se, e somente se

$$\ell(W - (n-1)P) - \ell(W - nP) = 1.$$

Como $\ell(W - (n-1)P) = dim\Omega_F(n-1)P$ e $\ell(W - nP) = dim\Omega_F(nP)$, temos que n é lacuna se, e somente se $\Omega_F(nP) \subsetneq \Omega_F(n-1)P$, ou seja, n é lacuna se, e somente se existe uma diferencial de Weil regular ω, com $v_P(\omega) = n - 1$.

□

Utilizando a linguagem de curvas, o método de Buchweitz pode ser enunciado da seguinte forma:

Seja X uma curva, $P \in X$ e $n \in \mathbb{Z}^+$. Então n é lacuna de $H(P)$ se, e somente se existe uma diferencial regular ω sobre X tal que $v_p(\omega) = n - 1$.

Para cada divisor $A \in Div(F)$ e para cada n inteiro, denotamos por $\Omega_F^n(A)$ o espaço das n-ésimas diferenciais de Weil, de forma que se $\omega \in \Omega_F^n(A)$, então

$(\omega) - A$ é um divisor positivo. Dessa forma, se $\omega \in \Omega_F(A)$, então $\omega^2 \in \Omega_F^2(A)$. $\Omega_F^n(0)$ é chamado **espaço das n-ésimas diferenciais de Weil regulares.**

Vamos calcular $dim_k\Omega_F^2(0) = \ell(2W)$, usando o Teorema de Riemann-Roch:

$$\begin{aligned}\ell(2W) &= deg2W + 1 - g + \ell(-W)\\ &= 2degW + 1 - g\\ &= 2(2g-2) + 1 - g\\ &= 3g - 3.\end{aligned}$$

Sejam n, n' lacunas de H. Então, pelo método de Buchweitz, existem diferenciais ω, ω' regulares sobre X, de ordem $n-1, n'-1$, respectivamente. Assim temos

$$n + n' = v_P(\omega \cdot \omega') = v_P(\omega) + v_P(\omega') = 2(n + n') - 2,$$

ou seja, X tem diferenciais quadráticas de ordem $k-2$ para cada $k \in L_2(P)$. Dessa forma, concluímos que o semigrupo H é de Weierstrass se

$$\#L_2 \leq dim\Omega_k^2(0) = 3g - 3.$$

Usando essa técnica, Buchweitz obteve em [1] o primeiro exemplo de semigrupo numérico que não é um semigrupo de Weierstrass:

Seja H o semigrupo numérico de gênero 16

$$H = \{0, 13, 14, 15, 16, 17, 18, 20, 22, 23, 26 \rightarrow\}.$$

No exemplo 4.15 mostramos que $\#L_2 = 46$. Pelo método de Buchweitz, se H fosse um semigrupo de Weierstrass, deveríamos ter $\#L_2 \leq 45$.

Como a dimensão do espaço das n-ésimas diferenciais de Weil regulares é $(2n-1)(g-1)$, qualquer semigrupo que satisfizer a propriedade $\#L_n > (2n-1)(g-1)$ não é um semigrupo de Weierstrass. Na tabela de semigrupos do Capítulo 4 temos o número exato de semigrupos com gênero $16 \leq g \leq 37$ que satisfazem $\#L_2 > 3g - 3$. Dessa forma, com a técnica de Buchweitz é possível encontrar vários semigrupos numéricos que não são de Weierstrass.

Pela Proposição 4.11, um semigrupo H de gênero g é simétrico se, e somente se $\#L_n = (2n-1)(g-1)$, para cada $n \geq 2$ e pelo Teorema 4.14, se H é quase-simétrico, então $\#L_n = (2g-3)n - g - 3$. Dessa forma, o método de Buchweitz não pode ser aplicado para semigrupos simétricos e quase-simétricos, pois a cardinalidade do conjunto de somas de n lacunas nunca será maior que $(2n-1)(g-1)$. Dessa forma, outra pergunta ficou sem resposta: *Existe um semigrupo de Weierstrass simétrico?* Essa pergunta foi respondida em 1993 por Stöhr, utilizando um resultado de [11], que apresentamos agora.

5.2 Semigrupos de Weierstrass em recobrimento duplo de curvas

Nesta seção vamos considerar X uma curva algébrica projetiva, irredutível, não-singular de gênero $g \geq 2$, definida sobre um corpo K algebricamente fechado de característica zero.

Dado $P \in X$, denotaremos por $H(P)$ o semigrupo de Weierstrass de X em P.

Definição 5.3. *Uma curva X é chamada **hiperelíptica** se é um recobrimento duplo da reta projetiva, isto é, o morfismo $f : X \to \mathbb{P}^1$ possui grau 2.*

Vamos generalizar essa definição para curvas de gênero $\gamma \geq 1$.

Definição 5.4. *Uma curva X é chamada $\gamma-$hiperelíptica se é um recobrimento duplo de uma curva Y de gênero γ, ou seja, existe um recobrimento $f : X \to Y$ de grau 2.*

Observação 5.5. *Pelo Corolário 1.29, existe uma bijeção entre o corpo de funções racionais e $K \cup \{\infty\}$. No Capítulo 3 vimos que $K \cup \{\infty\}$ é a reta projeitiva $\mathbb{P}^1$. Dessa forma concluímos que o corpo de funções de $\mathbb{P}^1$ é $K(x)$. Além disso, no Exemplo 2.4, provamos que o gênero do corpo de funções racionais é zero, e dessa forma concluímos também que o gênero de $\mathbb{P}^1$ é zero.*

Note que a definição de curva 0-hiperelíptica está de acordo com a definição de curva $\gamma-$hiperelíptica já que a reta projetiva tem gênero zero.

Seja $f : X \to Y$ um recobrimento duplo e $P \in X$ tal que $f(P) = Q \in Y$. Suponha que P seja totalmente ramificado, isto é, se $t \in \mathcal{O}_Q(Y)$ é um parâmetro, temos $e(P) = \text{ord}_P(t) > 1$. Como o recobrimento é duplo, se P é totalmente ramificado, então $e(P) = 2$.

Proposição 5.6. *As seguintes afirmações são equivalentes:*

(a) A curva X é hiperelíptica.

(b) Existe $P \in X$ tal que $H(P)$ é um semigrupo hiperelíptico.

Demonstração:

(a)⇒(b): Suponha que a curva X seja hiperelíptica. Então, por definição, existe um morfismo $f : X \to \mathbb{P}^1$ de grau 2. Pelo Teorema de Riemann-Hurwitz, temos

$$\begin{aligned} & 2g-2 = [K(X) : K(\mathbb{P}^1)](2\widetilde{g}-2) + \textstyle\sum_{P\in X}(e(P)-1) \\ \Rightarrow\ & 2g-2 = 2(-2) + \textstyle\sum_{P\in X}(e(P)-1) \\ \Rightarrow\ & \textstyle\sum_{P\in X}(e(P)-1) = 2g+2 \end{aligned}$$

Como $e(P) = 2$ para pontos totalmente ramificados, existem $2g + 2$ pontos totalmente ramificados em X. Portanto, nesses pontos, o semigrupo $H(P)$ terá 2 como não-lacuna, ou seja, $H(P)$ é hiperelíptico.

(b)⇒(a): Seja $x \in K(X)$ tal que $(x)_\infty = 2P$. Pelo Teorema 1.41, temos

$$[K(X) : K(x)] = 2.$$

Como $K(x)$ é o corpo de funções de $\mathbb{P}^1$, existe um morfismo $f : X \to \mathbb{P}^1$ de grau 2, ou seja, X é hiperelíptica.

□

Observação 5.7. *Para demonstrar o lema a seguir vamos demonstrar uma afirmação feita em [3]:*

"Seja X uma curva hiperelíptica e $\pi : X \longrightarrow \widetilde{X}$ um recobrimento duplo. Se $P \in X$ é um ponto totalmente ramificado e $\widetilde{P} = f(P)$, então, para cada $n \in \mathbb{Z}^+$, as seguintes afirmações são equivalentes:

(a) existe $\tilde{f} \in K(\widetilde{X})$ tal que $(\widetilde{f})_\infty = n\widetilde{P}$;

(b) existe $f \in K(X)$ tal que $(f)_\infty = 2nP$

Demonstração: Vamos provar a implicação (a)⇒(b). A recíproca segue da mesma forma. Seja $\widetilde{f} \in K(\widetilde{X})$ tal que $(\widetilde{f})_\infty = n\widetilde{P}$. Então, se z é um parâmetro de $\widetilde{P}$, temos $\widetilde{f} = u_1 z^{-n}$, onde u_1 é uma unidade de $\mathcal{O}_{\widetilde{P}}(\widetilde{X})$. Como P é totalmente ramificado, $ord_P(z) = 2$, ou seja, se t é um parâmetro de P, então $z = u_2 t^2$, onde u_2 é uma unidade de $\mathcal{O}_P(X)$. Assim temos $\widetilde{g} = u_1 z^{-1} = u_1 (u_2 t^2)^{-n} = u t^{-2n} \in K(X)$. Assim, definindo $f = u t^{-2n}$, temos $(f)_\infty = 2nP$ e o resultado segue.

Lema 5.8. *Seja P um ponto totalmente ramificado de uma curva γ-hiperelíptica X. Então $H(P)$ é $\gamma-$hiperelítico.*

Demonstração: Seja $f : X \to Y$ um recobrimento duplo, onde o gênero de Y é γ. Suponha que o semigrupo de Weierstrass do ponto $f(P)$ seja $0 < n_1 < n_2 < \cdots < n_\gamma = 2\gamma, 2\gamma + 1, \cdots$ (note que faz sentido considerar o semigrupo dessa forma, pois, como existem γ lacunas, o $\gamma-$ésimo elemento do semigrupo é 2γ.) Então, pela observação anterior, $H(P)$ é dado por $\{0, 2n_1, \cdots, 2n_\gamma = 4\gamma, 4\gamma + 2, \cdots\}$. Daí segue que $H(P)$ tem exatamente γ elementos pares no intervalo $[2, 4\gamma]$ e $4\gamma + 2 \in H(P)$, logo $H(P)$ é $\gamma-$hiperelíptico.

□

Provaremos agora o Teorema de Castelnuovo, que estabelece um limite para o gênero de uma curva. Para isso vamos apresentar algumas definições e resultados necessários.

Suponha que $p_1, \cdots, p_d$ sejam pontos distintos do espaço projetivo $\mathbb{P}^{n-1}$ com coordenadas homogêneas $[x_0 : \cdots : x_n]$. Considere o espaço vetorial $\mathcal{P}(n-1, k)$ de polinômios homogêneos de grau k nas n variáveis $x_1, \cdots, x_n$. Dizer que um polinômio F se anula em um ponto é o mesmo que dizer que existe uma hipersuperfície definida por $F = 0$ que passa por esse ponto. Para demonstrar o Teorema de Castelnuovo, vamos utilizar o seguinte lema, cuja demonstração está na página 227 de [5]:

Lema 5.9. *Seja X uma curva projetiva não singular em $\mathbb{P}^n$ de grau d que não está contida em nenhum hiperplano. Seja P um ponto de X. Então*

$$dim\mathcal{L}(kP) - dim\mathcal{L}((k-1)P) \geq \begin{cases} 1+k(n-1), & se\ 1+k(n-1) \leq d \\ d, & se\ 1+k(n-1) \geq d. \end{cases}$$

Teorema 5.10 (Teorema de Castelnuovo)**.** *O gênero de uma curva munida de uma série linear simples g_d^n satisfaz*

$$g \leq (n-1)\frac{m(m-1)}{2} + m\varepsilon,$$

onde $d-1 = m(n-1)+\varepsilon$, com $m \geq 1$ e $0 \leq \varepsilon \leq n-1$.

Demonstração: Denotemos

$$m = \left[\frac{d-1}{n-1}\right].$$

Com essa notação o lema acima pode ser reescrito na forma

$$dim\mathcal{L}(kP) - dim\mathcal{L}((k-1)P) \geq \begin{cases} 1+k(n-1), & \text{se } k \leq m \\ d, & \text{se } k \geq m. \end{cases}$$

Para c suficientemente grande, podemos formar a série

$$dim\mathcal{L}(cP) - dim\mathcal{L}(0) = \sum_{k=1}^{c}[dim\mathcal{L}(kP) - dim\mathcal{L}((k-1)P)].$$

Utilizando as desigualdades acima e o fato de que $dim\mathcal{L}(0) = 1$, temos

$$\begin{aligned} dim(cP) &\geq 1 + \sum_{k=1}^{m}[1+k(n-1)] + \sum_{k=m+1}^{c} d \\ &= 1 + m + (n-1)m(m+1)/2 + d(c-m) \end{aligned}$$

Agora, para c suficientemente grande podemos aplicar o Teorema de Riemann-Roch da seguinte forma:

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

onde g é o gênero de X. Escrevendo

$$d-1 = m(n-1)+\varepsilon,\ \text{com } 0 \leq \varepsilon \leq n-1,$$

temos

$$\begin{aligned} g &= deg\ cP + 1 - dim\mathcal{L}(cP) \\ &\leq dc + 1 - [1 + m + (n-1)m(m+1)/2 + d(c-m)] \\ &= -m - (n-1)m(m+1)/2 + [1 + m(n-1) + \varepsilon]m \\ &= (n-1)m(m-1)/2 + m\varepsilon, \end{aligned}$$

o que prova o teorema de Castelnuovo.

Teorema 5.11. *Seja $\gamma \in \mathbb{N}$ e X uma curva de gênero g tal que $g \geq 6\gamma + 4$. Então as seguintes afirmações são equivalentes:*

1. *A curva X é $\gamma-$hiperelíptica.*
2. *Existe $P \in X$ tal que $H(P)$ é γ-hiperelíptico.*
3. *Existe uma série linear livre de pontos de base em X com dimensão projetiva $2\gamma + 1$ e grau $6\gamma + 2$.*

Demonstração:
(1)⇒(2): Como X é γ-hiperelíptica existe um recobrimento duplo $f : X \to Y$, onde Y tem gênero γ. Pelo Teorema de Riemann-Hurwitz, temos

$$2g - 2 = (2\gamma - 2)2 + \sum_{P \in X} (e(P) - 1)$$

$$\Rightarrow \sum_{P \in X} (e(P) - 1) = 2g - 4\gamma + 2 \geq 12\gamma + 8 - 4\gamma + 2 = 8\gamma + 10 > 0,$$

ou seja, existem pontos totalmente ramificados em X. Se P é um desses pontos, pelo Lema 5.8, temos $H(P)$ um semigrupo $\gamma-$hiperelíptico.

(2)⇒(3): Seja $P \in X$ tal que $H(P)$ é um semigrupo $\gamma-$hiperelíptico.
Afirmação: $n_{2\gamma+1} = 6\gamma + 2$. De fato, como $H(P)$ é $\gamma-$hiperelíptico, pelo Lema 4.22, sendo $\widetilde{n}_i$ os elementos pares de $H(P)$, temos

$$\widetilde{n}_{\gamma+(\gamma+1)} = 4\gamma + 2(\gamma + 1) = 6\gamma + 2.$$

Se h for uma não-lacuna ímpar de $H(P)$, então, pelo Corolário 4.23, temos

$$h \geq 12\gamma + 8 - 4\gamma + 1 \Rightarrow s \geq 8\gamma + 9,$$

portanto $n_{2\gamma+1} = \widetilde{n}_{2\gamma+1} = 6\gamma + 2$. (Note que a hipótese $g \geq 5\gamma + 1$ seria suficiente para demonstrar essa implicação, porém a hipótese $g \geq 6\gamma + 4$ é necessária na implicação que provaremos a seguir.) Isso significa que existe $f \in K(X)$ tal que $(f)_\infty = 6\gamma + 2$ e, como existem $2\gamma + 2$ elementos do semigrupo menores ou iguais a $6\gamma + 2$, segue $\ell((6\gamma + 2)P) = 2\gamma + 2$. Portanto a série linear $|(6\gamma + 2)P|$ tem dimensão projetiva $2\gamma + 1$ e daí basta definir $g^{2\gamma+1}_{6\gamma+2}$.

(3)⇒(1): Seja $g^{2\gamma+1}_{6\gamma+2}$ um sistema linear livre de pontos de base na curva X de gênero $g \geq 6\gamma + 4$. Se esse sistema é simples então, pelo Teorema de Castelnuovo temos

$$g \leq \frac{m(m-1)}{2}(n-1) + m\varepsilon,$$

onde $m = \left[\frac{6\gamma + 1}{2\gamma}\right] = 3$ e $\varepsilon = 6\gamma + 1 - 3 \cdot 2\gamma = 1$. Então

$$g \leq \frac{3 \cdot 2 \cdot 2\gamma}{2} + 3 \Rightarrow g \leq 6\gamma + 3,$$

o que é impossível, pois, por hipótese, $g \geq 6\gamma + 4$. Dessa maneira temos que o sistema linear não é simples, ou seja, $g^{2\gamma+1}_{6\gamma+2}$ induz um sistema linear $\widetilde{g}^{2\gamma+1}_{(6\gamma+2)/t}$ livre de pontos de base em uma curva Y e um morfismo $f : X \to Y$ onde t é o grau de f. Como $2\gamma + 1 \leq \dfrac{6\gamma+2}{t}$ temos $t = 2$. Portanto o sistema é $\widetilde{g}^{2\gamma+1}_{3\gamma+1}$. Seja D um divisor pertencente a $\widetilde{g}^{2\gamma+1}_{3\gamma+1}$. Temos que D é um divisor não-especial pois, caso contrário, teríamos, pelo Teorema de Clifford,

$$2\gamma + 2 \leq 1 + \frac{3\gamma+1}{2} \Rightarrow 4\gamma + 4 \leq 3\gamma + 3,$$

o que é absurdo. Então, pelo Teorema de Riemann-Roch, temos

$$\ell(D) = deg(D) + 1 - g \Rightarrow g = 3\gamma + 1 + 1 - 2\gamma - 2 = \gamma,$$

ou seja, o gênero de Y é γ e X é uma curva $\gamma-$hiperelíptica.

□

Corolário 5.12. *Para cada inteiro $g \geq 100$ existe um semigrupo simétrico 16-hiperelíptico de gênero g que não é um semigrupo de Weierstrass.*

Demonstração: Seja $\widetilde{H} = \{0, 13, 14, 15, 16, 17, 18, 20, 22, 23, 26 \rightarrow\}$ o semigrupo de Buchweitz, que mostramos na primeira seção deste capítulo que não é de Weierstrass. Seja H o semigrupo simétrico obtido a partir de $\widetilde{H}$ como na Proposição 4.24, com gênero $g \geq 100$. Portanto H é um semigrupo 16-hiperelíptico, pois $\widetilde{H}$ tem gênero 16. Suponha que H seja um semigrupo de Weierstrass. Então existe uma curva X não-singular de gênero g definida sobre um corpo K algebricamente fechado e um ponto $P \in X$ tal que $H = H(P)$. Pelo Teorema 5.11 temos que X é 16-hiperelíptica, ou seja, existe uma curva $\widetilde{X}$ de gênero 16 e um recobrimento duplo $\pi : X \to \widetilde{X}$. Pela Observação 5.7 segue que o semigrupo associado a $\pi(X)$ é o semigrupo de Buchweitz, o que é contradição, pois como esse semigrupo não é de Weierstrass, ele não está associado a nenhuma curva.

□

Note que precisamos da hipótese $g \geq 100$ pois 16 é o menor gênero de um semigrupo que não é de Weierstrass e, para aplicar o Teorema 5.11, devemos ter $g \geq 6\gamma + 4$. Além disso, como esse resultado vale para todo $\gamma \geq 16$, concluímos que existem infinitos semigrupos simétricos que não são de Weierstrass.

Até hoje não são conhecidas as condições gerais de um semigrupo numérico para que este não seja de Weierstrass. Todos os estudos realizados até hoje impõe condições sobre os elementos do semigrupo, seus geradores ou seu peso e, portanto, a condição para que um semigrupo não seja de Weierstrass ainda é um problema em aberto.

CONSIDERAÇÕES FINAIS

A partir deste trabalho podemos concluir que nem todo semigrupo é um semigrupo de Weierstrass e apresentamos exemplos de semigrupos que não estão associados a uma curva algébrica. Apesar de termos concluído que existem infinitos semigrupos que não são de Weierstrass, todos os estudos nessa área ainda impõe condições sobre o gênero do semigrupo ou sobre seus elementos, logo não existe uma generalização para que um semigrupo não seja de Weierstrass, sendo ainda um problema em aberto.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Buchweitz, R. O., *On Zariski's criterion for equisingularity and non smoothable monomial curves*, Thése, Paris VII (1981).

[2] Fulton, W., *Algebraic Curves: an introduction to Algebraic Geometry*, Benjamin, New York, 1969.

[3] Kato, T., *On the order of a zero of the Theta Function*, Kodai Math. Sem. Rep. **28** (1977), 390-407.

[4] Komeda, J., *Non-Weierstrass numerical semigroups*, Semigroup Forum **57** (1998), 157-185.

[5] Miranda, R., *Algebraic curves and Riemann Surfaces*, Graduate Studies in Mathematics, Vol.5.

[6] Oliveira, G., *Numerical semigroups and the canonical ideal of nontrigonal curves*, Manusc. **71** (1991), 431-450.

[7] Oliveira, G., *Numerical semigroups whose last gap is large*, Semigroup Forum, Vol.**69**(2004), 423-430.

[8] Oliveira, G. e Stöhr, K.O, *Gorenstein curves with quasi-symmetric Weierstrass semigroups*, Geometriae Dedicata **67** (1997), 45-63.

[9] Stichtenoth, H., *Algebraic Function Fields and codes*, Universitext, Springer Berlin - Heidelberg - New York, 1993.

[10] Torres, F., *Weierstrass semigroups*, Pro Mathematica: Vol. X, nº19-20, 1996.

[11] Torres, F., *Weierstrass points and double covering of cuves with application: symmetric numerical semigroups which cannot be realized as weierstrass semigroups*, Manusc. Math. **83** (1994), 39-58.