UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Renata Vieira Costa

Anéis Gorenstein e Semigrupos

Juiz de Fora
2020

Renata Vieira Costa

Anéis Gorenstein e Semigrupos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra.

Orientadora: Profa. Dra. Flaviana Andréa Ribeiro

Coorientadora: Profa. Dra. Joana Darc Antonia Santos da Cruz

Juiz de Fora

2020

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Costa, Renata Vieira.
Anéis Gorenstein e Semigrupos / Renata Vieira Costa. -- 2020.
76 f.

Orientadora: Flaviana Andréa Ribeiro
Coorientadora: Joana Darc Antonia Santos da Cruz
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2020.

1. Curvas planas. 2. Valorização. 3. Semigrupos. 4. Anel Gorenstein. I. Ribeiro, Flaviana Andréa , orient. II. da Cruz, Joana Darc Antonia Santos , coorient. III. Título.

Renata Vieira Costa

Anéis Gorenstein e Semigrupos

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Álgebra

Aprovada em 21 de agosto de 2020

BANCA EXAMINADORA

Flaviana Andréa Ribeiro

Profª. Drª. Flaviana Andréa Ribeiro - Orientadora
Universidade Federal de Juiz de Fora

Joana Darc A S da Cruz

Profª. Drª. Joana Darc Antonia Santos da Cruz - Coorientadora
Universidade Federal de Juiz de Fora

Flaviana Andréa Ribeiro

p/ Profª. Drª. Lia Feital Fusaro Abrantes
Universidade Federal de Viçosa

Flaviana Andréa Ribeiro

p/ Prof. Dr. Renato Vidal da Silva Martins
Universidade Federal de Minas Gerais

Dedico este trabalho à minha família.

AGRADECIMENTOS

À Deus em primeiro lugar.

Aos meus pais e irmãos, pela confiança e pelo apoio incondicional.

À minha orientadora Flaviana Andréa Ribeiro, por ter aceitado compartilhar comigo seu tempo e seus conhecimentos, pela paciência e dedicação que teve durante a elaboração deste trabalho.

À minha coorientadora Joana Darc Antonia Santos da Cruz, por todo suporte e ensinamentos que contribuíram para elaboração deste trabalho, sempre com paciência e dedicação.

Aos membros da banca por aceitarem o convite e dedicarem à leitura e contribução deste trabalho.

À UFJF e em especial aos professores do Mestrado Acadêmico em Matemática.

À CAPES pelo apoio financeiro.

RESUMO

Este trabalho está dividido em duas partes. Na primeira delas, estudamos corpos de funções algébricas em uma variável e valorizações. Depois usamos esses conceitos para estudar a relação entre os pontos de uma curva plana irredutível C e as valorizações no seu corpo de funções racionais, $K(C)$. Um exemplo de um corpo de funções algébricas em uma variável é justamente o corpo $K(C)$. Na segunda parte, estudamos anéis Gorenstein e semigrupos numéricos. Mais especificamente, um anel local R noetheriano, domínio de integridade, unidimensional e integralmente fechado é um domínio de valorização discreta. Logo, existe uma valorização $v : \mathbb{K} \to \mathbb{Z} \cup \{\infty\}$, onde $\mathbb{K}$ é o corpo de frações de R, tal que

$$v(R) := \{v(x); x \in R \setminus \{0\}\}$$

é um semigrupo numérico. Algumas propriedades do anel R podem ser obtidas através do seu semigrupo $v(R)$. Por exemplo, vimos que um anel local R, analiticamente irredutível, residualmente racional e unidimensional é Gorenstein se e somente se $v(R)$ é um semigrupo simétrico. O fecho inteiro do anel local de uma curva algébrica plana C em um ponto p unirramificado, $\overline{\mathcal{O}_p(C)}$, é um exemplo de anel Gorenstein.

Palavras-chave: Curvas planas. Valorização. Semigrupos. Anel Gorenstein.

ABSTRACT

This work can be divided into two parts. In the first part we study algebraic function field of one variable and valuation. As an application of these concepts we investigate the relation between points of an irreducible algebraic plane curve C and the valuations in its rational function field, $K(C)$. An example of an algebraic functions field of one variable is $K(C)$. The second part is devoted to the study of Gorenstein rings and numeric semigroups. More specifically, an integrally closed one-dimensional local domain Noetherian ring R is discrete valuation domain. Therefore, there is a valuation $v : \mathbb{K} \to \mathbb{Z} \cup \{\infty\}$, where $\mathbb{K}$ is the field fractions fiel of R, such that

$$v(R) := \{v(x); x \in R \setminus \{0\}\}$$

is a numeric semigroup. Some properties can be obtained by of a ring R can revealed by its semigroup $v(R)$. For example, we have seen that an analytically irreducible local ring R which is residually rational is Gorenstein iff the value-semigroup $v(R)$ is simetric. The integral closure of the local ring of a plane algebraic curve C at an unibranch point p, $\overline{\mathcal{O}_p(C)}$, is an example of a Gorenstein ring.

Keywords: Plane curves. Valuations. Semigroups. Gorenstein ring.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem como principal referência o artigo *The Value-Semigroup of a One-Dimensional Gorenstein Ring* de E. Kunz, ver [K]. O estudo de singularidades de uma curva algébrica C pode ser feito através do semigrupo de valores do anel local, $\mathcal{O}_p(C)$ em cada singularidade $p \in C$. Propriedades de um dado anel R podem ser obtidas através do seu semigrupo $v(R)$. Por exemplo, vimos que um anel local R, analiticamente irredutível, residualmente racional e unidimensional é Gorenstein se, e somente, se $v(R)$ é um semigrupo simétrico. O fecho inteiro do anel local de uma curva algébrica plana C em um ponto p unirramificado, $\overline{\mathcal{O}_p(C)}$, é um exemplo de anel Gorenstein.

O trabalho foi organizado em cinco capítulos, como descritos a seguir.

No Capítulo 2 apresentamos alguns conceitos de álgebra comutativa que são necessários para o entendimento do trabalho.

No Capítulo 3 estabelecemos o ambiente no qual trabalharemos. Definimos corpos de funções algébricas em uma variável, anéis de valorização e domínios de valorização discreta. Também apresentamos alguns resultados necessários para nos capítulos seguintes relacionarmos anéis e semigrupos numéricos.

No Capítulo 4 fazemos um estudo de curvas planas irredutíveis via corpos de funções algébricas. Estabelecemos uma correspondência entre os pontos de uma curva plana afim irredutível e os anéis de valorização discreta dos seus corpos de funções racionais.

No Capítulo 5 estudamos os conceitos de semigrupos numéricos, anéis não ramificados e anéis Gorenstein, além da relação entre eles. Dado um anel local, noetheriano e unidimensional vimos que uma condição necessária e suficiente para que ele seja Gorenstein é que seu semigrupo numérico seja simétrico.

2 CONCEITOS E RESULTADOS BÁSICOS

Introduziremos, neste capítulo, alguns conceitos necessários de Álgebra Comutativa para a compreensão do trabalho.

2.1 ANÉIS E MÓDULOS

Nesta seção revisaremos rapidamente algumas definições e propriedades elementares de anéis, ideais primos, maximais e primários.

Definição 2.1. Um **Anel** R é um conjunto com duas operações binárias, soma e multiplicação, denotadas por $(+, \cdot)$ respectivamente e tais que:

(i) R é um grupo abeliano em relação a operação de soma (R tem um elemento nulo, 0, e todo $x \in R$ tem um inverso aditivo, $-x$).

(ii) A multiplicação é associativa e distributiva em relação à adição.

Neste trabalho consideraremos anéis comutativos e com unidade, isto é, tais que:

(iii) $x \cdot y = y \cdot x$, para todos $x, y \in R$.

(iv) Existe $1 \in R$ tal que $x \cdot 1 = 1 \cdot x = x$, para todo $x \in R$.

Definição 2.2. Um **ideal** é um subconjunto I não vazio de um anel R que é um subgrupo aditivo e é tal que $RI \subseteq I$, ou seja, se $x \in R$ e $y \in I$ tem-se $xy \in I$. Um ideal I é dito **ideal próprio** se $I \neq R$, ou seja, $1 \notin I$. Os múltiplos $a \cdot x$, para todo $a \in R$, de um elemento $x \in R$ formam um **ideal principal**, denotado por $\langle x \rangle$.

Definição 2.3. (i) Um **divisor de zero** num anel R é um elemento não nulo $x \in R$ o qual "divide 0", isto é, para o qual existe $0 \neq y \in R$ tal que $x \cdot y = 0$. Um anel sem divisores de zero não nulos (e no qual $1 \neq 0$) é chamado de **domínio de integridade**.

(ii) Um elemento **invertível** em R é um elemento $x \in R$ que "divide 1", isto é, para o qual existe $y \in R$ tal que $x \cdot y = 1$. O elemento y é determinado de maneira única por x e é denotado por x^{-1}. Os invertíveis em R formam um grupo abeliano (multiplicativo), denotado por $R^{\times}$. Um **corpo** é um anel k no qual $1 \neq 0$ e todo elemento não nulo tem inverso.

Definição 2.4. Um ideal $\mathfrak{p}$ de R é dito **primo** se $\mathfrak{p} \neq R$ e se $x \cdot y \in \mathfrak{p}$, então $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Um ideal $\mathfrak{m}$ é dito **maximal** se $\mathfrak{m} \neq R$ e se sempre que outro ideal I satisfazer $\mathfrak{m} \subseteq I \subseteq R$, então $R = I$ ou $I = \mathfrak{m}$.

Equivalentemente às definições acima temos:

Proposição 2.5. *(i)* $\mathfrak{p}$ *é um ideal primo se, e somente se,* $R/\mathfrak{p}$ *é um domínio de integridade.*

(ii) $\mathfrak{m}$ *é um ideal maximal se, e somente se,* $R/\mathfrak{m}$ *é um corpo.*

Demonstração. Ver [M], Proposição 1.3, página 20. ■

Teorema 2.6. *Todo anel não nulo* $R \neq 0$ *possui pelo menos um ideal maximal.*

Demonstração. Ver [AM], Teorema 1.3, página 3. ■

Definição 2.7. Um anel R que possui exatamente um ideal maximal $\mathfrak{m}$ é chamado **anel local**. O corpo $k = R/\mathfrak{m}$ é chamado de **corpo de resíduos** de R.

Definição 2.8. Um **domínio de ideais principais** (DIP) é um domínio de integridade no qual todo ideal é principal.

Definição 2.9. Sejam $I \subset R$ ideal. Dizemos que um ideal I é **irredutível** se sempre que $I = J \cap K$, então $I = J$ ou $I = K$, com J e K ideais de R.

Definição 2.10. Definimos o **radical** do ideal I de R como sendo

$$\sqrt{I} = \{x \in R;\ \ x^n \in I,\ \text{ para algum }\ n > 0\}\,.$$

Definição 2.11. Um ideal $\mathfrak{q}$ em um anel R é **primário** se $\mathfrak{q} \neq R$ e se $xy \in \mathfrak{q}$ então $x \in \mathfrak{q}$ ou $y^n \in \mathfrak{q}$, para algum $n > 0$.

Proposição 2.12. *Seja* $\mathfrak{q}$ *um ideal primário em* R*. Então* $\sqrt{\mathfrak{q}}$ *é o menor ideal primo de* R *contendo* $\mathfrak{q}$*.*

Demonstração. Ver [AM], Proposição 4.1, página 50. ■

Definição 2.13. Se $\mathfrak{q}$ é primário e $\mathfrak{p} = \sqrt{\mathfrak{q}}$ então dizemos que $\mathfrak{q}$ é **$\mathfrak{p}$-primário**.

Definição 2.14. Uma **decomposição primária** de um ideal I de um anel R é uma expressão de I como interseção finita de ideais primários,

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

Em geral, uma decomposição primária não precisa existir. Diremos que um ideal I é **decomponível** se I admite uma decomposição primária.

Se um ideal I for decomponível e ainda:

(i) todos os $\sqrt{\mathfrak{q}_i}$ são distintos, e

(ii) temos que $\bigcap_{j\neq i} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$, para $1 \leq i \leq n$

a decomposição primária é dita **minimal**.

Definição 2.15. Seja R um anel. Um R**-módulo** é um par (M, μ), onde M é um grupo abeliano e

$$\begin{array}{rcl} \mu : R \times M & \to & M \\ (r, m) & \mapsto & rm \end{array}$$

é uma função que satisfaz:

(i) $r\,(m+n) = rm + rn$;

(ii) $(r+p)\,m = rm + pm$;

(iii) $(rp)\,m = r\,(pm)$;

(iv) $1.m = m$.

Exemplo 2.16. Um ideal I de R é um R-módulo. Em particular, R é um R-módulo.

Definição 2.17. Um subconjunto N de um R-módulo M é um **submódulo** de M se satisfazem as seguintes condições:

(i) Para todo $m, n \in N$, tem-se $m + n \in N$;

(ii) Para todo $r \in R$, $m \in N$, tem-se $rm \in N$.

Se m é um elemento de M, o conjunto de todos os múltiplos rm, com $r \in R$, é um submódulo de M, denotado por Rm ou $\langle m \rangle$. Se $M = \sum_{i\in I} Rm_i$, onde os m_i's são elementos de M. Dizemos que os m_i's formam um **conjunto de geradores** de M. Neste caso, se todo elemento de M pode ser expresso (não necessariamente de maneira única) como uma combinação linear finita dos m_i's com coeficientes em R. Um R-módulo M é dito **finitamente gerado** se ele tem um conjunto finito de geradores.

Definição 2.18. Sejam N e M R-submódulos. A função $f : M \longrightarrow N$ é um R**-homomorfismo** se

$$f(x+y) = f(x) + f(y);$$
$$f(rx) = r \cdot f(x)$$

para todo $r \in R$ e para todo $x, y \in M$.

Definição 2.19. Uma sequência de R-módulos e R-homomorfismos

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

é dita **exata** em M_i se $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. A sequência é **exata** se é exata em cada M_i.

Em particular:

(i) $0 \to M' \xrightarrow{f} M$ é exata $\Leftrightarrow$ f é injetiva;

(ii) $M \xrightarrow{g} M'' \to 0$ é exata $\Leftrightarrow$ g é sobrejetiva;

(iii) $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ é exata $\Leftrightarrow$ f é injetiva, g é sobrejetiva e $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

2.2 ANÉIS E MÓDULOS DE FRAÇÕES

A formação de frações e o processo associado de localização são ferramentas importantes em Álgebra Comutativa. Nesta seção apresentaremos algumas definições e propriedades da formação de frações.

Definição 2.20. Seja R um anel. Um **sistema multiplicativo** de R é um subconjunto S de R, não vazio, tal que $1 \in S$ e S é fechado com respeito à multiplicação em R. Em $R \times S$, definimos a relação $\equiv$ por:

$$(x, s) \equiv (y, t) \Leftrightarrow (xt - ys)u = 0, \text{ para algum } u \in S.$$

Usaremos as notações x/s para a classe de equivalência $\overline{(x, s)}$ e $S^{-1}R$ para o conjunto das classes de equivalência.

O conjunto $S^{-1}R$ recebe um estrutura de anel quando definirmos em $S^{-1}R$ as seguintes operações:

$$\frac{x}{s} + \frac{y}{y} = \frac{xt + ys}{st} \text{ e}$$

$$\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st},$$

para todo $x, y \in R$ e para todo $s, t \in S$.

Definição 2.21. O anel $S^{-1}R$ é chamado de **anel de frações** de R em relação a S.

Observação 2.22. Em geral, existe um homomorfismo de anéis $f : R \longrightarrow S^{-1}R$ definido por $f(x) = x/1$, que em geral, não é injetivo.

Definição 2.23. Se R é um domínio de integridade e $S = R - \{0\}$, chamamos o conjunto $S^{-1}R$ de **corpo de frações** de R.

Exemplo 2.24. Seja $\mathfrak{p}$ um ideal primo de R. Então $S = R - \mathfrak{p}$ é um sistema multiplicativo e, nesse caso, escrevemos $R_{\mathfrak{p}}$ em vez de $S^{-1}R$.

Definição 2.25. O processo de passar de R a $R_{\mathfrak{p}}$ é chamado de **localização** de R em $\mathfrak{p}$.

Proposição 2.26. *Os ideais primos de $S^{-1}R$ estão em correspondência biunívoca com os ideais primos de R que não interceptam S.*

Demonstração. Ver [AM], Proposição 3.11, página 41. ■

A construção de $S^{-1}R$ pode ser estendida para um R-módulo M, definindo a relação $\equiv$ em $M \times S$ por:

$$(m,s) \equiv (m',s') \Leftrightarrow \exists\ t \in S \text{ ta quel } t(sm' - s'm) = 0,\ \forall\ m,m' \in M \text{ e } \forall\ s,s' \in S.$$

Definimos em $S^{-1}M$ as operações:

$$\begin{array}{rcl} + : S^{-1}M \times S^{-1}M & \longrightarrow & s^{-1}M \\ \left(\dfrac{m}{s}, \dfrac{m'}{t}\right) & \longmapsto & \dfrac{mt + m's}{st} \end{array}$$

$$\begin{array}{rcl} \cdot : S^{-1}M \times S^{-1}M & \longrightarrow & S^{-1}M \\ \left(\dfrac{x}{s}, \dfrac{m}{t}\right) & \longmapsto & \dfrac{xm}{st} \end{array}$$

para todo $m, m' \in M$ e $x, s, t \in S$. Então $S^{-1}M$ é um $S^{-1}R$-módulo.

Seja $u : M \longrightarrow N$ um homomorfismo de R-módulos. Então u induz um homomorfismo de $S^{-1}R$-módulos $S^{-1}u : s^{-1}M \longrightarrow S^{-1}N$, de maneira que $S^{-1}u$ aplica m/s em $u(m)/s$. Temos também que $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

Proposição 2.27. *A operação S^{-1} é exata, isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é uma sequência de R-módulos exata, então $S^{-1}M' \xrightarrow{s^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é uma sequência de $S^{-1}R$-módulos exata em $S^{-1}M$.*

Demonstração. Ver [AM], Proposição 3.3, página 39. ■

2.3 DEPENDÊNCIA INTEIRA

Definição 2.28. Seja $R \supseteq A$ uma extensão de anéis, isto é, R é um anel e A um subanel de R. Um elemento $r \in R$ é dito **inteiro** sobre A se r é raiz de um polinômio mônico com coeficientes em A, isto é, se satisfaz uma equação da forma

$$r^n + a_1 r^{n-1} + \cdots + a_n = 0, \tag{2.1}$$

onde os $a_i \in A$. Dizemos que a extensão $R \supseteq A$ é **inteira** se todo elemento $r \in R$ é inteiro sobre A.

Proposição 2.29. *Sejam $A \subseteq R$ uma extensão de anéis e $r \in R$. As seguintes afirmações são equivalentes:*

(i) *r é inteiro sobre A;*

(ii) *$A[r]$ é um A-módulo finitamente gerado;*

(iii) *$A[r]$ está contido em um subanel C de R tal que C é um A-módulo finitamente gerado.*

Demonstração. Ver [AM], Proposição 5.1, página 59. ■

Corolário 2.30. *Sejam $x_i \in R$, com $1 \leq i \leq n$, elementos inteiros sobre A. Então o anel $A[x_1, \ldots, x_n]$ é um A-módulo finitamente gerado.*

Demonstração. Ver [AM], Corolário 5.2, página 60. ■

Corolário 2.31. *Seja $R \supseteq A$ uma extensão de anéis. O conjunto C dos elementos de R que são inteiros sobre A é um subanel de R que contém A.*

Demonstração. Ver [AM], Corolário 5.3, página 60. ■

Definição 2.32. O anel C do Corolário 2.31 é chamado **fecho inteiro** de A em R. Se $C = A$, então A é dito **integralmente fechado** em R. Se $C = R$, o anel R é dito inteiro sobre A.

Corolário 2.33. *Se $A \subseteq R \subseteq C$ são anéis e R é inteiro sobre A e C é inteiro sobre R, então C é inteiro sobre A.*

Demonstração. Ver [AM], Corolário 5.4, página 60. ■

Definição 2.34. Um domínio de integridade é dito **integralmente fechado** se é integralmente fechado no seu corpo de frações.

Proposição 2.35. *Seja R um domínio de integridade. As seguintes condições são equivalentes:*

(i) *R é integralmente fechado;*

(ii) *$R_{\mathfrak{p}}$ é integralmente fechado para cada ideal primo $\mathfrak{p}$ de R;*

(iii) *$R_{\mathfrak{m}}$ é integralmente fechado para cada ideal maximal $\mathfrak{m}$ de R.*

Demonstração. Ver [AM], Proposição 5.13, página 63. ■

2.4 CONDIÇÕES DE CADEIA

Seja Ω um conjunto parcialmente ordenado por uma relação $\leq$.

Proposição 2.36. *As seguintes condições em Ω são equivalentes:*

(i) Toda sequência crescente $x_1 \leq x_2 \leq \cdots$ em Ω é estacionária, isto é, existe n tal que $x_n = x_{n+1} = \cdots$.

(ii) Todo subconjunto não vazio de Ω tem um elemento maximal.

Demonstração. $(i) \Rightarrow (ii)$ Sejam T um subconjunto não vazio de Ω e $x_1 \in T$. Se x_1 é maximal em T, acabou. Caso contrário existe $x_2 \in T$ tal que $x_1 < x_2$. Se x_2 é maximal em T acabou, caso contrário repetiremos o processo. Este processo termina, pois caso contrário obteríamos uma cadeia $x_1 < x_2 < x_3 < \cdots$ estritamente crescente, contradizendo a hipótese. Portanto, T tem um elemento maximal.

$(ii) \Rightarrow (i)$ Seja $x_1 \leq x_2 \leq \cdots$ uma sequência crescente em Ω, então o conjunto $(x_m)_{m\geq 1}$ tem um elemento maximal x_n. Logo, $x_m \leq x_n \leq x_{n+1} \leq x_{n+2} \leq \cdots$, para todo $m \geq 1$ donde segue que a sequência é estacionária. ■

Definição 2.37. Se Ω é o conjunto de submódulos de um R-módulo M, ordenado pela relação $\subseteq$, então (i) da proposição anterior é chamada **condição de cadeia ascendente** (cca) e (ii) é chamado de **condição maximal**. Um R-módulo M que satisfaz qualquer uma destas condições equivalentes é chamado de **noetheriano**.

Agora, se Ω é ordenado por $\supseteq$, (i) da proposição acima é chamada **condição de cadeia descendente** (ccd) e (ii) de **condição minimal**. Um R-módulo M que satisfaz qualquer uma dessas condições equivalentes é chamado de **artiniano**.

Proposição 2.38. *Um R-módulo M é noetheriano se, e somente se, todo submódulo de M é finitamente gerado.*

Demonstração. Sejam N um submódulo de M e Ω o conjunto de todos os submódulos finitamente gerados de N. Então Ω é um conjunto não vazio (pois $0 \in \Omega$) de submódulos M. Logo, tem um elemento maximal N_0, finitamente gerado, isto é, $N_0 = \sum_{i=1}^{n} Ra_i$. Se $N_0 \neq N$, considere o submódulo $N_0 + Ra$, onde $a \in N$ e $a \notin N_0$. Então, $N_0 + Ra = \sum_{i=1}^{n} Ra_i + Ra$ é finitamente gerado e contém estritamente N_0, contradição. Logo, $N = N_0$ e, portanto, N é finitamente gerado.

Reciprocamente, seja $M_1 \subseteq M_2 \subseteq \cdots$ uma cadeia ascendente de submódulos de M. Observe que $N = \bigcup_{n=1}^{\infty} M_n$ é um submódulo de M (usando a condição de cadeia) e logo é finitamente gerado. Sejam $x_1, \ldots, x_r$ os geradores de N. Suponha que $x_i \in M_{n_i}$ e seja $n = \max\{n_i; 1 \leq i \leq r\}$. Então cada $x_i \in M_n$. Logo $N = M_n$ e, portanto, a cadeia é estacionária. ■

Definição 2.39. Um anel R é dito **noetheriano** (resp. **artiniano**) se é noetheriano (resp. artiniano) como R-módulo, ou seja, se satisfaz a (cca) (resp. (ccd)) em ideais.

Proposição 2.40. *Seja*

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

uma sequência exata de A-módulos. Então

(i) M é noetheriano se, e somente se, M' e M'' são noetherianos;

(ii) M é artiniano se, e somente se, M' e M'' são artinianos.

Demonstração. $(i)(\Rightarrow)$ Uma cadeia ascendente de submódulos de M' (ou M'') dão origem a uma cadeia em M, e como M é noetheriano, essa cadeia é estacionário. Portanto, M' (ou M'') é noetheriano.

$(\Leftarrow)$ Seja $(L_n)_{n\geq 1}$ uma cadeia ascendente de M-submódulos, então $(\alpha^{-1}(L_n))$ é uma cadeia em M', e $(\beta(L_n))$ é uma cadeia em M''. Para n suficientemente grande, ambas as cadeias são estacionárias e, portanto, (L_n) é estacionária.

$(ii)(\Rightarrow)$ Uma cadeia descendente de submódulos de M' (ou M'') dão origem a uma cadeia em M, como M é artiniano, essa cadeia é estacionária. Portanto, M' ou M'' é artiniano.

$(\Leftarrow)$ Seja $(L_n)n \geq 1$ uma cadeia descendente de M-submódulos. Então $\alpha^{-1}(L_n)$ é uma cadeia em M', e $(\beta(L_n))$ é uma cadeia em M''. Para n suficientemente grande, ambas as cadeias são estacionárias e, portanto, (L_n) é estacionária. ■

Exemplo 2.41. Todo corpo k é noetheriano e artiniano, pois tem somente dois ideais $\langle 0\rangle$ e k.

Exemplo 2.42. Todo Domínio de Ideais Principais é noetheriano, pois todo ideal é finitamente gerado.

Exemplo 2.43. O anel $\mathbb{Z}$ é noetheriano, pois é um Domínio de Ideais Principais.

Proposição 2.44. *Sejam R um anel noetheriano (resp. artiniano) e I um ideal de R. Então R/I é um anel noetheriano (resp. artiniano).*

Demonstração. Pela Proposição 2.40, R/I é noetheriano (resp. artiniano) como R-módulo. Portanto, também é noetheriano (resp. artiniano) como R/I-módulo. ■

Uma **cadeia** de submódulos de um módulo M é uma sequência $(M_i)_{i=0}^n$ de submódulos de M tais que

$$M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0 \tag{2.2}$$

Definição 2.45. O **comprimento** da cadeia (2.2) é n. Uma **série de composição** de M é uma cadeia maximal, ou seja, uma cadeia no qual cada quociente M_{i+1}/M_i, com $0 \leq i \leq n$, é simples, isto é, não tem outros submódulos além do zero e dele mesmo.

Definição 2.46. Definimos o **comprimento** de um R-módulo M, denotado por $l_R(M)$, como sendo o mínimo entre todos os comprimentos das séries de composição de M ou ∞ se M não admite série de composição.

Proposição 2.47. *M tem uma série de composição se, e somente se, M satisfaz ambas as condições de cadeia.*

Demonstração. Ver [AM], Proposição 6.8, página 77. ■

A proposição anterior é equivalente a dizer que $l(M) < \infty$ se, e somente se, M é artiniano e noetheriano.

Definição 2.48. Um módulo que satisfaz ambas condições, (cca) e (ccd), é chamado de **módulo de comprimento finito**.

Teorema 2.49 (Teorema da Base de Hilbert)**.** *Se R é um anel noetheriano, então o anel de polinômios $R[x]$ é noetheriano.*

Demonstração. Ver [AM], Teorema 7.5, página 81. ■

Corolário 2.50. *Se R é um anel noetheriano então $R[x_1, \ldots, x_n]$ é noetheriano.*

Demonstração. Ver [AM], Corolário 7.6, página 81. ■

Definição 2.51. Definimos uma **cadeia de ideais primos** de um anel R como sendo uma sequência estritamente crescente e finita

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

onde cada $\mathfrak{p}_i$ é um ideal primo de R. O **comprimento** da cadeia é n. Definimos a **dimensão** ou **dimensão de Krull** de um anel $R \neq 0$ como sendo o supremo dos comprimentos de todas as cadeias de ideais primos de R.

Se existem cadeias arbitrariamente longas de ideais primos de R, então dizemos que $\dim R = \infty$.

Exemplo 2.52. Todo corpo K tem dimensão zero.

Exemplo 2.53. Um DIP tem dimensão 1.

Exemplo 2.54. $\dim k[x_1, \ldots, x_n] = n$.

Definição 2.55. Um **anel local regular** é um anel local noetheriano tal que o número mínimo de geradores de seu ideal maximal é igual à sua dimensão de Krull.

2.5 GRAU DE TRANSCENDÊNCIA

Definição 2.56. Seja $\mathbb{K}/k$ uma extensão de corpos. Um subconjunto finito $\{x_1, \ldots, x_n\} \subseteq F$ é **algebricamente independente** sobre k se não existe $f(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ satisfazendo $f(x_1, \ldots, x_n) = 0$. Um subconjunto arbitrário $S \subset \mathbb{K}$ é **algebricamente independente** sobre k se todos os subconjuntos finitos de S são algebricamente independentes sobre k.

Definição 2.57. Uma **base de transcendência** da extensão $\mathbb{K}/k$ é um subconjunto $\mathfrak{B}$ de k que satisfaz:

(i) $\mathfrak{B}$ é algebricamente independente.

(ii) $\mathfrak{B} \subseteq \mathfrak{B}'$ e $\mathfrak{B}'$ é um subconjunto algebricamente independente de $\mathbb{K}$, então $\mathfrak{B} = \mathfrak{B}'$.

Definição 2.58. Sejam $\mathbb{K}/k$ uma extensão de corpos e $\mathfrak{B}$ uma base de transcendência de $\mathbb{K}/k$. À cardinalidade de $\mathfrak{B}$ damos o nome de **grau de transcendência** de $\mathbb{K}/k$, e denotamos por $\text{trdeg}(\mathbb{K}/k)$.

Observação 2.59. $\mathbb{K}/k$ é uma extensão algébrica se, e somente se, $\text{trged}(\mathbb{K}/k) = 0$.

3 CORPOS DE FUNÇÕES E VALORIZAÇÕES

De agora em diante, assumiremos que k é um corpo algebricamente fechado de característica zero, $k[x]$ é o anel de polinômios em uma variável e $k(x)$ é o corpo de frações. Neste capítulo estamos interessados nos anéis de valorizações do corpo de funções algébricas em uma variável sobre k, denominados **domínios de valorização discreta**.

3.1 CORPOS DE FUNÇÕES EM UMA VARIÁVEL

Sejam $k[x]$ o anel de polinômios em uma variável e $k(x)$ o seu corpo de frações.

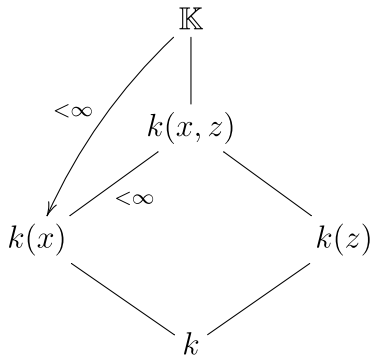
Definição 3.1. Um **corpo de funções algébricas em uma variável sobre** k é uma extensão $\mathbb{K}$ de k tal que $\mathbb{K}$ é uma extensão finita de $k(x)$, para algum elemento $x \in \mathbb{K}$ transcendente sobre k. O corpo k é chamado **corpo de constantes**.

Por simplicidade, chamaremos $\mathbb{K}/k$ de corpos de funções.

A extensão $\mathbb{K}/k$ é chamada **racional** se $\mathbb{K} = k(x)$ para algum $x \in \mathbb{K}$ transcendente sobre k.

Lema 3.2. *Seja $\mathbb{K}/k$ um corpo de funções. Um elemento $z \in \mathbb{K}$ é transcendente sobre k se, e somente se, $[\mathbb{K} : k(z)] < \infty$.*

Demonstração. $\mathbb{K}/k$ um corpo de funções, então $\mathbb{K}$ é uma extensão finita de $k(x)$, para algum $x \in \mathbb{K}$ transcendente sobre k. Agora, seja $z \in \mathbb{K}$ transcendente sobre k. Então o grau de transcendência de $k(z)$ sobre k é 1.



Também temos que o grau de transcendência de $k(x)/k$ é 1 e que $[\mathbb{K} : k(x)] < \infty$. Então $[k(x,z) : k(x)] < \infty$, pois

$$[\mathbb{K} : k(x)] = [\mathbb{K} : k(x,z)] \cdot [k(x,z) : k(x)].$$

Assim, $k(x,z)/k(x)$ é uma extensão algébrica, portanto, de grau de transcendência igual a 0. Como

$$\text{trdeg}(k(x,z)/k) = \text{trdeg}(k(x,z)/k(x)) + \text{trdeg}(k(x)/k),$$

temos que $\text{trdeg}(k(x,z)/k) = 1$. Agora,

$$\text{trdeg}(k(x,z)/k) = \text{trdeg}(k(x,z)/k(z)) + \text{trdeg}(k(z)/k)$$

nos dá que $\text{trdeg}(k(x,z)/k(z)) = 0$. Logo, x é algébrico sobre $k(z)$. Portanto, pelo diagrama, temos que $[\mathbb{K} : k(z)] < \infty$.

Por outro lado, seja $z \in \mathbb{K}$ um elemento algébrico sobre k. Então $k(z)/k$ é uma extensão finita. Mas como $\mathbb{K}/k$ é um corpo de funções e, portanto, uma extensão infinita, temos que $\mathbb{K}/k(z)$ é uma extensão infinita, pois

$$[\mathbb{K} : k] = [\mathbb{K} : k(z)][k(z) : k].$$

■

Definição 3.3. Um **anel de valorização** de um corpo de funções $\mathbb{K}/k$ é um anel $\mathcal{O} \subseteq \mathbb{K}$ com as seguintes propriedades:

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

(ii) Para qualquer $z \in \mathbb{K}$ tem-se $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Observação 3.4. As duas condições da Definição 3.3 nos diz que $\mathcal{O}$ é um domínio de integridade que não é um corpo. De fato, $\mathcal{O}$ fosse um corpo, então a condição (ii) nos daria que $\mathcal{O} = \mathbb{K}$, contrariando (i).

Exemplo 3.5. Seja $\mathbb{K} = k(x)$, com x transcendente sobre k. Dado $p(x) \in k[x]$ irredutível, defina:

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

Veja que $f(x)/g(x) \in k(x)$, se $f(x), p(x)$ são elementos não nulos de $k[x]$, mas tal elemento não pertence a $\mathcal{O}_{p(x)}$ se $p(x)$ não divide $f(x)$. Além disso, se $g(x) \in k[x]$ é tal que $g(x)$ é irredutível e $\text{mdc}(p(x), g(x)) = 1$, então $1/g(x) \in \mathcal{O}_{p(x)} \setminus k$. Portanto, $k \subsetneq \mathcal{O}_{p(x)} \subsetneq \mathbb{K}$.

Seja $z = f(x)/g(x) \in \mathbb{K} = k(x)$ um elemento não nulo tal que $\text{mdc}(f(x), g(x)) = 1$. Se $z \notin \mathcal{O}_{p(x)}$, então $p(x)|g(x)$ e $p(x)$ não divide $f(x)$. Logo, $z^{-1} = g(x)/f(x) \in \mathcal{O}_{p(x)}$. Portanto, $\mathcal{O}_{p(x)}$ é um anel de valorização de $k(x)$.

Note ainda que se $p(x)$ e $g(x)$ são polinômios irredutíveis distintos de $k[x]$, temos

$$\mathcal{O}_{p(x)} \neq \mathcal{O}_{g(x)},$$

pois $1/g(x) \in \mathcal{O}_{p(x)}$ e $1/g(x) \notin \mathcal{O}_{g(x)}$.

Proposição 3.6. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K}/k$. Então*

(i) $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ possui um único ideal maximal $\mathfrak{m} = \mathcal{O} \setminus \mathcal{O}^\times$, onde

$$\mathcal{O}^\times = \{z \in \mathcal{O}; \exists \ v \in \mathcal{O} \ \ com \ \ zv = 1\}$$

é o grupo dos elementos invertíveis de $\mathcal{O}$.

(ii) Para $0 \neq x \in \mathbb{K}/k$, tem-se $x \in \mathfrak{m}$ se, e somente se, $x^{-1} \notin \mathcal{O}$.

Demonstração. (i) Primeiro vamos mostrar que $\mathfrak{m}$ tal como definido acima é um ideal. Se $x \in \mathfrak{m}$ e $z \in \mathcal{O}$, então $xz \notin \mathcal{O}^\times$, pois caso contrário, teríamos que x é invertível, o que seria uma contradição, pois $x \notin \mathcal{O}^\times$. Logo, $xz \in \mathcal{O} \setminus \mathcal{O}^\times = \mathfrak{m}$.

Agora, sejam $x, y \in \mathfrak{m} \setminus \{0\}$. Então, xy^{-1} e $yx^{-1} \in \mathbb{K}$, de modo que $xy^{-1} \in \mathcal{O}$ ou $yx^{-1} \in \mathcal{O}$. Sem perda de generalidade, suponhamos que $xy^{-1} \in \mathcal{O}$. Então, $1 + xy^{-1} \in \mathcal{O}$, de modo que, $x + y = y(1 + xy^{-1}) \in \mathfrak{m}$, pois como já vimos $\mathcal{O}\mathfrak{m} \subset \mathfrak{m}$.

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

Agora, se P é um ideal maximal de $\mathcal{O}$, então P não possui elementos invertíveis, de modo que $P \subseteq \mathfrak{m} \subsetneq \mathcal{O}$. Logo, $P = \mathfrak{m}$, ou seja, $\mathfrak{m}$ é o único ideal maximal.

(ii) $(\Rightarrow)$ Se $0 \neq x \in \mathfrak{m}$, então x^{-1} não pertence a $\mathcal{O}$, pois caso contrário, teríamos que x seria invertível em $\mathcal{O}$, o que seria uma contradição.

$(\Leftarrow)$ Se $x^{-1} \notin \mathcal{O}$, então $x \in \mathcal{O}$ não é invertível em $\mathcal{O}$. Logo, $x \in \mathfrak{m} = \mathcal{O} \setminus \mathcal{O}^\times$. ■

Lema 3.7. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K}/k$. Sejam $\mathfrak{m}$ seu ideal maximal e $0 \neq x \in m$. Sejam $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ tais que $x_1 = x$ e $x_i \in x_{i+1}\mathfrak{m}$, com $i = 1, 2, \ldots, n-1$. Então o grau da extensão $[\mathbb{K} : k(x)]$ é maior ou igual a n.*

Demonstração. Como $0 \neq x \in \mathfrak{m}$, segue da definição de $\mathfrak{m} = \mathcal{O}/\mathcal{O}^\times$ que $x \notin k$. Além disso, como k é algebricamente fechado, pelo Lema 3.2, temos que $[\mathbb{K} : k(x)] < \infty$.

Basta então provarmos que $x_1, \ldots, x_n$ são linearmente independentes sobre $k(x)$. Suponha, por absurdo, que exista uma combinação linear não trivial $\sum_{i=1}^{n} \alpha_i(x)x_i = 0$, com $\alpha_i(x) \in k(x)$. Podemos assumir sem perda de generalidade, que $\alpha_i(x) \in k[x]$ e que x não divide $\alpha_i(x)$, para algum i. Seja $a_i := \alpha_i(0)$ o termo constante de $\alpha_i(x)$. E escolha j de forma que $a_j \neq 0$ e que $a_i = 0$ sempre que $i > j$. Escreva

$$-\alpha_j(x)x_j = \sum_{i \neq j} \alpha_i(x)x_i = \sum_{i<j} \alpha_i(x)x_i + \sum_{i>j} \alpha_i(x)x_i,$$

e observe que $\alpha_i(x) \in \mathcal{O}$, para todo $i = 1, \ldots, n$ (já que $x = x_1 \in \mathfrak{m}$), $x_i \in x_j\mathfrak{m}$ para $i < j$ e $\alpha_i(x) = xg_i(x)$, para $i > j$, onde $g_i(x) \in k[x]$. Assim

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

com $p_j \in \mathfrak{m}$. Logo, o lado direito da igualdade anterior pertence à $\mathfrak{m}$.

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

$$a_j = \alpha_j(x) - xg_j(x) \in \mathfrak{m} \cap k = \{0\}.$$

Contradição, pois $a_j \neq 0$. Portanto, $x_1, \ldots, x_n$ são linearmente independentes. ■

Teorema 3.8. *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K}/k$ e $\mathfrak{m}$ seu ideal maximal. Então:*

(i) $\mathfrak{m}$ *é um ideal principal.*

(ii) Se $\mathfrak{m} = t\mathcal{O}$*, então todo elemento* $0 \neq z \in \mathbb{K}$ *possui uma representação única na forma* $z = t^n u$*, para* $n \in \mathbb{Z}$ *e* $u \in \mathcal{O}^\times$*.*

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

Demonstração. (i) Suponha que $\mathfrak{m}$ não é principal e tome $0 \neq x_1 \in \mathfrak{m}$. Assim, $\mathfrak{m} \neq x_1\mathcal{O}$, ou seja, existe $x_2 \in \mathfrak{m} \setminus x_1\mathcal{O}$. Então $x_2x_1^{-1} \notin \mathcal{O}$ e $x_1x_2^{-1} \in \mathfrak{m}$, pelo item (ii) da Proposição 3.6. Dessa forma, $x_1 \in x_2\mathfrak{m}$. Continuando o processo, obtemos uma sequência infinita de elementos $x_1, x_2, \ldots$ de $\mathfrak{m}$ tais que $x_i \in x_{i+1}\mathfrak{m}$, para todo $i \geq 1$, o que é um absurdo segundo o Lema 3.7. Portanto, $\mathfrak{m}$ é principal.

(ii) (Existência) Seja $z \in \mathbb{K}$. Da definição de $\mathcal{O}$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Suponha $z \in \mathcal{O}$. Se $z \in \mathcal{O}^\times$, então $z = t^0 z$ e fica provado. Suponha, agora, $z \in \mathfrak{m} = t\mathcal{O}$. Então $z = tx_2$, com $x_2 \in \mathcal{O}$. Se x_2 é invertível, nada mais temos a fazer. Se $x_2 \in \mathfrak{m} = t\mathcal{O}$, então $x_2 = tx_3$, com $x_3 \in \mathcal{O}$. Continuando o processo, temos uma sequência

$$x_1 = z, x_2, \ldots, x_n \in \mathfrak{m}; \;\; x_i \in x_{i+1}\mathfrak{m}, \;\; \forall i.$$

Mas pelo Lema 3.7 essa sequência não pode ser infinta. Logo, existe um inteiro maximal $r \geq 1$ tal que $z = t^r u$ com u invertível em $\mathcal{O}$.

(Unicidade) Suponha $z = ut^{n_1} = vt^{n_2}$, com u, v invertíveis em $\mathcal{O}$ e $n_1 \geq n_2$. Então $ut^{n_1-n_2} = v$ é invertível em $\mathcal{O}$. Como t é não invertível, então $n_1 = n_2$ e $u = v$.

(iii) $\mathcal{O}$ é um domínio por definição. Seja $I \subseteq \mathcal{O}$ um ideal não nulo. O conjunto $C = \{r \in \mathbb{N}; \;\; t^r \in I\}$ é não vazio, pois se $0 \neq x \in I$, então $x = t^r u$, com $u \in \mathcal{O}^\times$ e $r \geq 0$.

Daí $t^r = xu^{-1} \in I$. Pelo Princípio da Boa Ordenação, o conjunto C possui um menor elemento, de modo que podemos definir $n = \min(C)$. Afirmamos que $I = t^n\mathcal{O}$. De fato, como $t^n \in I$, segue que, $I \supset t^n\mathcal{O}$.

Por outro lado, seja $0 \neq y \in I$. Temos $y = t^s w$, com $w \in \mathcal{O}^\times$ e $s \geq 0$. Como $t^s = w^{-1}y \in I$ e $n = \min(C)$, temos que ter $s \geq n$, de modo que $t^n | t^s$ e, desse modo $t^n | y$, o que mostra que $y \in t^n\mathcal{O}$. Portanto, $t^n\mathcal{O} = I$. ■

Um subanel $\mathcal{O}$ de um corpo $\mathbb{K}$ que satisfaz as propriedades do Teorema 3.8 é chamado de **anel de valorização discreta**.

Definição 3.9. Seja $\mathcal{O}$ um anel de valorização de um corpo de funções $\mathbb{K}/k$ e $\mathfrak{m}$ seu ideal maximal. Um elemento $t \in \mathfrak{m}$ tal que $\mathfrak{m} = t\mathcal{O}$ é chamado **parâmetro local** de $\mathcal{O}$.

3.2 VALORIZAÇÃO DISCRETA

Definição 3.10. Uma **valorização discreta** de corpo $\mathbb{K}$ é uma função

$$v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

satisfazendo as seguintes propriedades:

(i) $v(x) = \infty \Leftrightarrow x = 0$.

(ii) $v(xy) = v(x) + v(y)$, para todo $x, y \in \mathbb{K}$.

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

(iv) Existe um elemento $z \in \mathbb{K}$ tal que $v(z) = 1$.

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

Observação 3.11. É fácil ver: $v(-x) = v(x)$ e $v(x^{-1}) = -v(x)$.

Observação 3.12. Dos itens (ii) e (iv) acima, temos que $v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$ é sobrejetora.

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

Se $j \in \mathbb{Z}$ e $j \neq 0$, por (iv), existe $z \in \mathbb{Z}$ tal que $v(z) = 1$. Assim, se $j > 0$, $v(z^j) = jv(z) = j$. Caso, $j < 0$, fazendo $q = -j,\ \ q > 0$ e

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

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

Definição 3.13. O conjunto consistindo de 0 e todos os elementos $x \in \mathbb{K}^*$ tais que $v(x) \geq 0$ é um anel, chamado **anel de valorização** de v.

Definição 3.14. Uma **valorização discreta em uma extensão de corpos** $\mathbb{K}/k$ é uma valorização discreta v de $\mathbb{K}$ que satisfaz a condição:

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

Lema 3.15. *Sejam v uma valorização discreta de $\mathbb{K}$ e $x, y \in \mathbb{K}$ tais que $v(x) \neq v(y)$. Então $v(x+y) = min\ (v(x), v(y))$.*

Demonstração. Inicialmente observe que $v(ax) = v(a) + v(x) = v(x)$, para todo $0 \neq a \in k$. Em particular, temos $v(-y) = v(y)$. Como $v(x) \neq v(y)$, suponha, sem perda de generalidade, $v(x) < v(y)$.

Assuma, $v(x+y) \neq \min\{v(x), v(y)\}$, ou seja, $v(x+y) > v(x)$. Dessa forma

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

o que é uma contradição. Portanto, $v(x+y) = \min\{v(x), v(y)\}$ se $v(x) \neq v(y)$. ■

Veremos a seguir exemplos de valorizações da extensão $k(t)/k$, onde $k(t)$ é o corpo de frações de $k[t]$, o anel de polinômios em uma variável com coeficientes em k.

Exemplo 3.16. Fixado $a \in k$, podemos escrever todo elemento $f(t) \in k[t]$ na forma $f(t) = (t-a)^n f_1(t)$, com $n \in \mathbb{N}, n \geq 0$ e $c \in k$ não nulo e tal que $(t-a) \nmid f_1(t)$. Logo, todo elemento de $k(t)$ tem a forma

$$\frac{f(t)}{g(t)} = (t-a)^m \frac{f_1(t)}{g_1(t)},$$

com $m \in \mathbb{Z}$ e tal que $(t-a) \nmid f_1(t)$ e $(t-a) \nmid g_1(t)$.

A função $v_a : k(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ definida por:

$$v_a\left((t-a)^m \frac{f_1(t)}{g_1(t)}\right) = m,$$

onde $(t-a) \nmid f_1(t)$ e $(t-a) \nmid g_1(t)$ e $v_a(0) = \infty$, é uma valorização de $k(t)/k$.

Exemplo 3.17. Como no exemplo anterior, podemos escrever um elemento arbitrário de $k(t)$ na forma

$$\frac{f(t)}{g(t)} = t^m \frac{f_1(t)}{g_1(t)},$$

com $m \in \mathbb{Z}$ e tal que $t \nmid f_1(t)g_1(t)$. A função $v : k(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ definida por:

$$v\left(t^m \frac{f_1(t)}{g_1(t)}\right) = -m,$$

onde $t \nmid f_1(t)g_1(t)$ e $v(0) = \infty$, é uma valorização de $k(t)/k$ tal que $v(t) = -1$ e $v(1/t) = 1$. Essa valorização será denotada por v_∞.

A próxima proposição mostra que as valorizações definidas nos Exemplos 3.16 e 3.17 são as únicas valorizações de $k(t)/k$.

Proposição 3.18. *Seja $v : k(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ uma valorização de $k(t)/k$ tal que $v(0) = \infty$. Se $v(t) \geq 0$, então $v = v_a$, para um único $a \in k$. Além disso, se $v(t) < 0$ então $v = v_\infty$.*

Demonstração. Suponha que $v(t) \geq 0$. Então $v(f) \geq 0$, para todo $f \in k[t]$.

De fato, todo $f \in k[t]$ é da forma

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n, \text{ com } a_0, a_1, \ldots, a_n \in k \text{ e } a_n \neq 0.$$

Logo, $v(f) \geq \min\{v(a_0), v(a_1) + v(t), \ldots, v(a_n) + nv(t)\} \geq 0$.

Usando que v é sobrejetiva temos que existe $f \in k[t]$ tal que $v(f) > 0$. Escreva $f = c \prod_{i=1}^{r} (t - c_i)$, com $c, c_i \in k$, $\forall i = 1, \ldots, r$, e $c \neq 0$. De $v(f) = \sum_{i=1}^{r} v(t - c_i) > 0$, temos que $v(t - c_i) > 0$, para algum $i \in \{1, \ldots, r\}$. Fazendo $c_i = a$, veremos que $v = v_a$.

Observe que se $b \in k$ e $b \neq a = c_i$, então

$$v(t - b) \geq \min\{v(t - c_i), v(b - c_i)\} = 0. \tag{3.1}$$

Pelo Lema 3.15, como o $\min\{v(t - c_i), v(b - c_i)\} = \min\{v(t - c_i), 0\}$ só acontece uma vez, já que $v(t - c_i) > 0$, vale a igualdade em (3.1), ou seja,

$$v(t - b) = \min\{v(t - c_i), 0\} = 0.$$

Além disso, dado $z \in k(t)$ arbitrário, escrevemos $z = (t - a)^e g(t)/h(t)$ com $e \in \mathbb{Z}, g(t), h(t) \in k[t], h(t) \neq 0$ e tais que $(t - a) \nmid g(t)h(t)$. Então

$$v(z) = ev(t - a) + \cancelto{0}{v(g(t))} - \cancelto{0}{v(h(t))} = ev(t - a).$$

Como v é sobrejetora, temos $v(t - a) = 1$ e $v = v_a$.

Para unicidade, observe que $v(a-t) = v(t-a) > 0$ e $v(t-b) > 0$, com $a \neq b$, implicaria $0 = v(a-b) = v(-t+a+t-b) \geq \min\{v(t - a), v(t - b)\} = \min\{v(t - a), v(t - b)\} > 0$.

Agora, suponha $v(t) < 0$. Então, $v(1/t) > 0$ e para $b \neq 0$,

$$v\left(1 - \frac{b}{t}\right) \geq \min\{v(1), v(b/t)\} = \min\{v(1), v(b) + v(1/t)\} = \min\{0, v(1/t)\} = 0.$$

Pelo Lema 3.15, como o $\min\{v(1), v(b/t)\} = \min\{0, v(1/t)\}$ só acontece uma vez, já que $v(1/t) > 0$, vale a igualdade e segue que

$$v\left(1 - \frac{b}{t}\right) = \min\{0, v(1/t)\} = 0.$$

Logo, para todo $f(t) \in k[t]$, temos que $f(t) = t^m \prod_{i=1}^{r}(1 - c_i/t)$, com $r \in \mathbb{N}$, $m \in \mathbb{Z}$, $m \geq 0$, $c_i \in k$ não nulo. Portanto, $v(f(t)) = mv(t)$. A sobrejetividade de v implica que $v(t) = -1$. Assim

$$v\left(t^m \frac{f_1(t)}{g_1(t)}\right) = -m,$$

se $m \in \mathbb{Z}$ e $t \nmid f_1(t)g_1(t)$. Logo, $v = v_\infty$. ■

Definição 3.19. Seja $\mathcal{O}$ um domínio de integridade. $\mathcal{O}$ é chamado de **domínio de valorização discreta (DVD)** se $\mathcal{O}$ é um anel de valorização de uma valorização discreta v do corpo de frações de $\mathcal{O}$. Neste caso, denotaremos $\mathcal{O}$ por $\mathcal{O}_v$

Pela Proposição 3.6, $\mathcal{O}$ é um anel local, e o seu ideal maximal $\mathfrak{m}$ é o conjunto de todos $x \in \mathbb{K}$ tal que $v(x) > 0$.

Se $I \neq 0$ é um ideal de $\mathcal{O}$, existe n, menor número inteiro tal que $v(x) = n$, para algum $x \in I$. Logo, I contém todo $y \in \mathcal{O}$ tal que $v(y) \geq n$ e, portanto, os únicos ideais em $\mathcal{O}$ diferentes de zero são os ideais $\mathfrak{m}_n = \{y \in \mathcal{O};\ \ v(y) \geq n\}$. Dessa forma, os ideais formam uma cadeia de ideais, $\mathfrak{m} \supseteq \mathfrak{m}_2 \supseteq \mathfrak{m}_3 \supseteq \cdots$, e portanto $\mathcal{O}$ é noetheriano.

Definição 3.20. Seja $\mathcal{O}_v$ um DVD de $\mathbb{K}$. Definimos

$$\begin{array}{rccc} v_{\mathcal{O}}: & \mathbb{K} & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & t^n u & \longmapsto & n \\ & 0 & \longmapsto & \infty \end{array}$$

onde t é um parâmetro local de $\mathcal{O}$.

Esta função $v_{\mathcal{O}}$ está bem definida, pois não depende da escolha do parâmetro local. De fato, seja t' outro parâmetro local. Então $\mathfrak{m} = t\mathcal{O} = t'\mathcal{O}$, logo $t = t'w$, para algum $w \in \mathcal{O}^\times$. Portanto, $t^n u = ((t')^n w^n)\, u = (t')^n (w^n u)$, com $w^n u \in \mathcal{O}^\times$.

Proposição 3.21. *Sejam $\mathcal{O}$ um anel de valorização. Então $\mathcal{O}$ é integralmente fechado em $\mathbb{K}$.*

Demonstração. Seja $x \in \mathbb{K}$ inteiro sobre $\mathcal{O}$. Então temos

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

com $b_i \in \mathcal{O}$ e $n \in \mathbb{N}$. Se $x \in \mathcal{O}$ não há o que fazer. Agora, se $x \notin \mathcal{O}$, então $x^{-1} \in \mathcal{O}$, pois $\mathcal{O}$ é um anel de valorização. Assim, segue que:

$$\begin{aligned} x^n &= -(b_1 x^{n-1} + \cdots + b_n) \\ \frac{x^n}{x^{n-1}} &= -\frac{(b_1 x^{n-1} + \cdots + b_n)}{x^{n-1}} \\ x &= -(b_1 + b_2 x^{-1} + \cdots + b_n x^{1-n}) \in \mathcal{O}. \end{aligned}$$

Logo $x \in \mathcal{O}$. Absurdo, pois supomos inicialmente que $x \notin \mathcal{O}$. Portanto, $\mathcal{O}$ é integralmente fechado sobre $\mathbb{K}$. ■

Teorema 3.22. *Seja $\mathbb{K}/k$ um corpo de funções algébricas em uma variável. Então são válidas as seguintes afirmativas:*

(i) Para qualquer domínio de valorização discreta $\mathcal{O}_v$ com ideal maximal $\mathfrak{m}$ a função v definida em (3.20) é uma valorização discreta de $\mathbb{K}/k$. Além disso,

$$\mathcal{O}_v = \{z \in \mathbb{K};\ \ v(z) \geq 0\},$$

$$\mathcal{O}_v^{\times} = \{z \in \mathbb{K};\ \ v(z) = 0\},$$

$$\mathfrak{m} = \{z \in \mathbb{K};\ \ v(z) > 0\}.$$

Um elemento $t \in \mathbb{K}$ é um parâmetro local de $\mathcal{O}_v$ se, e somente se, $v(t) = 1$.

(ii) Reciprocamente, suponha que v seja uma valorização discreta de $\mathbb{K}/k$. Então o conjunto $\mathcal{O}_v = \{z \in \mathbb{K};\ \ v(z) \geq 0\}$ é um domínio de valorização discreta de $\mathbb{K}/k$.

Demonstração. (i) Faremos a demonstração em etapas.

Etapa 1. v é uma valorização discreta.

Seja t um parâmetro local em $\mathcal{O}_v$. Então dados $x, y \in \mathbb{K} \setminus \{0\}$, temos que $x = t^n u$ e $y = t^m w$, com $n, m \in \mathbb{Z}$, $u, w \in \mathcal{O}_v^{\times}$.

Segue da definição que $v(z) = \infty$ se, e somente se, $z = 0$. Além disso,

$$v(0 + 0) = v(0) = \infty = \min\{\infty, \infty\} = \{v(0), v(0)\},$$

$$v(x + 0) = v(x) = n = \min\{n, \infty\} = \min\{v(x), v(0)\}$$

$$v(0.0) = v(0) = \infty = \infty + \infty = v(0) + v(0),$$

$$v(x.0) = v(0) = \infty = \infty + n = v(0) + v(x) \text{ e}$$

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

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

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

Assim, $v(x + y) = n$, se $u + t^{m-n} w \in \mathcal{O}_v^{\times}$, ou $v(x + y) > n$, se $u + t^{m-n} \notin \mathcal{O}_v^{\times}$ (este último caso abrange a situação na qual $x + y = 0$). Logo, sempre temos que

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

Finalmente, $v(t) = 1$ (por definição) e, como $k \setminus \{0\} \subseteq \mathcal{O}_v^\times$, temos que $v(a) = 0$, para todo $a \in k \setminus \{0\}$. Portanto, a função v é uma valorização discreta de $\mathbb{K}/k$.

Etapa 2. $\mathcal{O}_v = \{z \in \mathbb{K};\ \ v(z) \geq 0\}$.

De fato, seja $x \in \{z \in \mathbb{K};\ \ v(z) \geq 0\}$, temos que $v(x) \geq 0$. Se $v(x) = \infty$, então $x = 0$ e assim $x \in \mathcal{O}_v$. Caso contrário, $x = t^n u$, onde $n = v(x) \geq 0$ e $u \in \mathcal{O}_v^\times$. Isso nos dá que $x \in \mathcal{O}_v$, pois $\mathcal{O}_v^\times \subseteq \mathcal{O}_v$, se $n = 0$, ou $x \in t\mathcal{O}_v = \mathfrak{m} \subseteq \mathcal{O}_v$, se $n > 0$. Por outro lado, a demonstração da Proposição 3.8 (ii) nos dá que se $z \in \mathcal{O}_v \setminus \{0\}$, então existem $n \in \mathbb{Z}_+$ e $u \in \mathcal{O}_v^\times$ tais que $z = t^n u$, onde $v(z) \geq 0$. Ainda, se $z = 0$, então $v(z) = \infty > 0$, o que mostra que $\mathcal{O}_v = \{z \in \mathbb{K};\ \ v(z) \geq 0\}$.

Etapa 3. $\mathcal{O}_v^\times = \{z \in \mathbb{K};\ \ v(z) = 0\}$.

Análogo a demonstração da Etapa 2.

Etapa 4. $\mathfrak{m} = \{z \in \mathbb{K};\ \ v(z) > 0\}$.

Das Etapas 2 e 3, temos $\mathfrak{m} = \mathcal{O}_v \setminus \mathcal{O}_v^\times = \{z \in \mathbb{K};\ \ v(z) > 0\}$

Etapa 5. $t \in \mathbb{K}$ é um parâmetro local de $\mathcal{O}_v$ se, e somente se, $v(t) = 1$

De fato, se t é um parâmetro local então pela definição de v, temos $v(t) = 1$. Por outro lado, se $z \in \mathbb{K}$ tal que $v(z) = 1$, então $z = tu$, onde $u \in \mathcal{O}_v^\times$. Assim, $\mathfrak{m} = t\mathcal{O}_v = z\mathcal{O}_v$ e z é um parâmetro local.

(ii) Seja v uma valorização discreta. Então

$$\mathcal{O}_v = \{z \in \mathbb{K};\ \ v(z) \geq 0\}$$

é um anel de valorização de $\mathbb{K}/k$.

Com efeito, $\mathcal{O}_v$ é um subanel de $\mathbb{K}$, pois $0 \in \mathcal{O}_v$, pois $v(0) = \infty > 0$. E, dados $x, y \in \mathcal{O}_v$, temos que $v(x) \geq 0$ e $v(y) \geq 0$, donde

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

de modo que xy e $x - y \in \mathcal{O}_v$. Além disso, como existe $z \in \mathbb{K}$ tal que $v(z) = -1$, temos que $z \notin \mathcal{O}_v$, o que mostra que $\mathcal{O}_v \subseteq \mathbb{K}$ é uma inclusão estrita. Ainda, $v(a) = 0$, para todo $a \in k \setminus \{0\}$. Logo, $k \subseteq \mathcal{O}_v$. Como existe $z \in \mathcal{O}_v$ tal que $v(z) = 1$, temos que $z \notin k$, então $k \subsetneq \mathcal{O}_v$.

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

Portanto, $\mathcal{O}_v$ é um anel de valorização. ■

Nosso objetivo agora é mostrar que o fecho inteiro de um domínio de integridade A no seu corpo de frações $\mathbb{K}$ é a interseção de todos os anéis de valorização de $\mathbb{K}$ que contém A. Para isto, precisamos dos resultados apresentados a seguir.

Definição 3.23. Seja S um conjunto não vazio. Dizemos que S é **parcialmente ordenado** e escrevemos $(S, \leq)$ se:

(i) $x \leq x$; $\forall x \in S$ (Reflexiva);

(ii) $x \leq y$ e $y \leq x \Rightarrow x = y$, $\forall x, y \in S$ (Anti-simétrica);

(iii) $x \leq y$ e $y \leq z \Rightarrow x \leq z$, $\forall x, y, z \in S$ (Transitiva).

Um subconjunto $T \subseteq S$ é uma cadeia em S se, para todo $x, y \in T$ vale que ou $x \leq y$ ou $y \leq x$. Dizemos que a cadeia T é limitada superiormente se existe $z \in S$ tal que $t \leq z$, para todo $t \in T$.

Lema 3.24 (Lema de Zorn)**.** *Se toda cadeia $T \subseteq S$ tem uma cota superior em S, então existe um elemento maximal em S.*

Sejam $\mathbb{K}$ um corpo, Ω um corpo algebricamente fechado, Σ o conjunto de todos os pares $(A.f)$, onde A é subanel de $\mathbb{K}$ e f é um homomorfismo de A em Ω. O conjunto Σ é parcialmente ordenado, com a relação

$$(A, f) \leq (A', f') \Leftrightarrow A \subseteq A' \quad \text{e} \quad f'|_A = f.$$

Vamos provar que o conjunto Σ satisfaz as condições do Lema de Zorn.

Seja $T \subseteq \Sigma$ uma cadeia, isto é,

$$T = \{(A_i, f_i)_{i \in I};\ (A_i, f_i) \in \Sigma\ (A_i, f_i) \leq (A_j, f_j)\ \text{ou}\ (A_j, f_j) \leq (A_i, f_i),\ \forall i, j \in I\}.$$

Queremos construir um par (A, f) tal que $(A_i, f_i) \leq (A, f)$, isto é, tal que $A_i \subseteq A$ e $f|_{A_i} = f_i$, para todo $i \in I$.

Definimos $A = \bigcup_{i \in I} A_i \subseteq K$ subanel, e consideremos $f : A \longrightarrow \Omega$ dada por: se $x \in A = \bigcup_{i \in I}$, temos que $x \in A_i$, para algum $i \in I$. Então $f(x) := f_i(x)$, ou seja, $f|_{A_i} = f_i$.

A função f está bem definida. De fato, se $x \in A_i \bigcap A_j$, como $(A_i, f_i) \leq (A_j, f_j)$ ou $(A_j, f_j) \leq (A_i, f_i)$, pois T é uma cadeia, temos que $A_i \subset A_j$ e $f_j|_{A_i} = f_i$ ou $A_j \subset A_i$ e $f_i|_{A_j} = f_j$. Logo, $f_j|_{A_i} = f_i$ ou $f_i|_{A_j} = f_i$ e $f_i(x) = f_j(x)$ ou $f_j(x) = f_i(x)$.

A função f é um homomorfismo. Dados $x \in A_i$ e $y \in A_j$, podemos supor, sem perda de generalidade, que $A_j \subseteq A_i$. Então $x, y \in A_i$. Logo, $x + y \in A_i$ e $xy \in A_i$. Daí segue que

$$f(x + y) = f_i(x + y) = f_i(x) + f_i(x)\ \text{ e }\ f(xy) = f_i(xy) = f_i(x)f_i(y).$$

Portanto, f é um homomorfismo de anéis.

Logo, o conjunto Σ satisfaz as condições do Lema de Zorn. Portanto, Σ possui pelo menos um elemento maximal, que denotaremos por (B, g).

Lema 3.25. *B é um anel e $\mathfrak{m} = Ker(g)$ é seu ideal maximal.*

Demonstração. Como $g(B)$ é um subanel de um corpo. Segue que ele é um domínio de integridade. Além disso, $g(B) \simeq \dfrac{B}{Ker(g)}$ implica que o ideal $\mathfrak{m}$=Ker(g) é ideal primo.

Podemos estender a função g a $B_{\mathfrak{m}}$ e obter o homomorfismo

$$\begin{array}{ccc} \tilde{g} : B_{\mathfrak{m}} & \longrightarrow & \Omega \\ \dfrac{b}{s} & \longmapsto & \dfrac{g(b)}{g(s)} \end{array}$$

onde $b \in B$, $s \notin \mathfrak{m}$ =Ker(g).

De fato, a função $\tilde{g}$ está bem definida pois, se $b/s = b_1/s_1 \in B_{\mathfrak{m}}$, então existe $t \notin \mathfrak{m}$ tal que $t(bs_1 - sb_1) = 0 \in B$. Daí, $g(t)(g(b)g(s_1) - g(s)g(b_1)) = 0 \in \mathbb{K}$. Então $g(b)g(s_1) - g(s)g(b_1) = 0 (g(t) \neq 0)$. Logo,

$$\tilde{g}\Big(\frac{b}{s}\Big) = \frac{g(b)}{g(s)} = \frac{g(b_1)}{g(s_1)} = \tilde{g}\Big(\frac{b_1}{s_1}\Big).$$

Além disso,

$$\begin{array}{ccc} \varphi : B & \longrightarrow & B_{\mathfrak{m}} \\ b & \longmapsto & \dfrac{b}{1} \end{array}$$

é um homomorfismo injetor, pois B é domínio. Logo, $B_{\mathfrak{m}}$ contém uma cópia de B e (sem perda de generalidade $B \subseteq B_{\mathfrak{m}}$) $(B, g) \leq (B_{\mathfrak{m}}, \tilde{g})$. Como (B, g) é um elemento maximal de Σ, concluímos que $B = B_{\mathfrak{m}}$.

Portanto, B é um anel local e $\mathfrak{m}$ seu ideal maximal.

■

Lema 3.26. *Sejam x um elemento não nulo de $\mathbb{K}$, $B[x]$ o subanel de $\mathbb{K}$ gerado por x sobre B e $\mathfrak{m}[x]$ a extensão de $\mathfrak{m}$ em $B[x]$. Então ou $\mathfrak{m}[x] \neq B[x]$ ou $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.*

Demonstração. Suponhamos que $\mathfrak{m}[x] = B[x]$ e $\mathfrak{m}[x^{-1}] = B[x^{-1}]$. Então, temos as seguintes equações:

$$u_0 + u_1 x + \cdots + u_m x^m = 1 \quad (u_i \in m) \tag{3.2}$$

$$v_0 + v_1 x^{-1} + \cdots + v_n x^{-n} = 1 \quad (v_j \in n) \tag{3.3}$$

em que podemos supor que os graus m e n são os menores possíveis. Considerando $m \geq n$ e multiplicando (3.3) por x^n, obtemos

$$v_0 x^n + v_1 x^{n-1} + \cdots + v_n = x^n \Rightarrow v_1 x^{n-1} + \cdots + v_n = x^n - v_0 x^n$$

$$\Rightarrow v_1 x^{n-1} + \cdots + v_n = x^n (1 - v_0) \tag{3.4}$$

Como $v_0 \in n$, B é um anel local e $\mathfrak{m}$ =Ker(g) é seu ideal maximal, temos $(1 - v_0)$ é um invertível em B e a equação (3.4) pode ser escrita da seguinte forma:

$$x^n = w_1 x^{n-1} + \cdots + w_n,$$

onde $w_j = \dfrac{v_j}{(1 - v_0)} \in B$. Portanto,

$$x^n - w_1 x^{n-1} - \cdots - w_n = 0,$$

contrariando a minimalidade de m na equação (3.2).

Portanto, $\mathfrak{m}[x] \neq B[x]$ ou $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$. ■

Teorema 3.27. *Seja (B, g) um elemento maximal de Σ. Então B é um anel de valorização do corpo $\mathbb{K}$.*

Demonstração. Para mostrar que B é um anel de valorização de $\mathbb{K}$, devemos mostrar que para todo $x \in \mathbb{K}$, $x \in B$ ou $x^{-1} \in B$. Pelo lema anterior, podemos supor, sem perda de generalidade que o ideal $\mathfrak{m}[x]$ é um ideal próprio do anel $B' = B[x]$. Então $\mathfrak{m}[x]$ está contido em um ideal $\mathfrak{m}' \subset B'$ e tem-se que $\mathfrak{m}' \bigcap B = \mathfrak{m}$ (pois $\mathfrak{m}$ é maximal e $\mathfrak{m} \subseteq \mathfrak{m}' \bigcap B \subseteq B$).

Portanto, a inclusão $B \hookrightarrow B'$ induz uma inclusão $k := B/\mathfrak{m} \hookrightarrow k' = B'/\mathfrak{m}'$. Afirmamos que $k' = k[\overline{x}]$, onde $\overline{x}$ é a imagem de x em k'. De fato, como $\overline{x} \in k'$ e $k \subseteq k'$, então $k[\overline{x}] \subseteq k'$. Para inclusão contrária, seja $y \in k'$, como $k' = B'/\mathfrak{m}' = B[x]/\mathfrak{m}'$, temos que $y = \overline{f(x)}$, onde $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in B[x]$. Logo,

$$\overline{f(x)} = \overline{a_0} + \overline{a_1}\ \overline{x} + \cdots + \overline{a_n}\ \overline{x}^n \in k[\overline{x}].$$

Logo, $k' = k[x]$. Como k' é corpo, $\overline{x}$ é algébrico sobre k e, portanto, k' é uma extensão algébrica finita de k. Assim, para todo $y \in k'$, existe $h(T) \in k[T]$ mônico tal que $h(y) = 0$.

O homomorfismo $g : B \longrightarrow \Omega$ induz uma inclusão $\overline{g} : k = B/\mathfrak{m} \longrightarrow \Omega$, onde $\mathfrak{m}$ =Ker(g). Considerando a inclusão induzida $\overline{g} : k[T] \longrightarrow \Omega[T]$ dada por $\overline{g}(h(t)) = p(t)$, temos que $h(y) = 0$ implica $p(y) = 0$. Como Ω é algebricamente fechado, segue que $y \in \Omega$. Então podemos estender $\overline{g} : k = B/\mathfrak{m} \longrightarrow \Omega$ a uma inclusão $\overline{g'} : k' = B/\mathfrak{m}' \longrightarrow \Omega$.

Compondo $\overline{g'}$ com o homomorfismo natural $f : B' \longrightarrow k' = B/\mathfrak{m}'$, temos que $\overline{g'} \circ f = g' : B' \longrightarrow \Omega$ estende g.

Então (B, g) e (B', g') são tais que $B \subseteq B'$ e $g'|_B = g$, ou seja, $(B, g) \leq (B', g') \in \Sigma$. Como (B, g) é um elemento maximal de Σ, temos que $(B, g) = (B', g')$ e $B' = B$. Como $x \in B$. Portanto, B é um anel de valorização de $\mathbb{K}$. ■

Corolário 3.28. *Seja A um subanel de um corpo $\mathbb{K}$. Então o fecho inteiro $\overline{A}$ de A em $\mathbb{K}$ é a interseção de todos os anéis de valorização de $\mathbb{K}$ que contém A.*

Demonstração. Seja B um anel de valorização de $\mathbb{K}$ tal que $A \subseteq B$. Como B é integralmente fechado, temos que:

$$A \subseteq B \Rightarrow \overline{A} \subseteq \overline{B} = B \Rightarrow \overline{A} \subseteq B.$$

Logo, $\overline{A} \subseteq \bigcap B$.

Reciprocamente, seja $x \in \mathbb{K}$. Se $x \notin \overline{A}$, vamos mostrar que $x \notin \bigcap B$, ou seja, que $x \notin B$, para algum anel de valorização B de $\mathbb{K}$. Como $x \notin \overline{A}$, então $x \notin A[x^{-1}]$, pois caso contrário, x seria raiz de um polinômio mônico com coeficientes em A, ou seja, $x \in \overline{A}$. Logo, $x^{-1} \in A[x^{-1}]$ e x^{-1} não é unidade em $A[x^{-1}]$, implicando que $x^{-1} \in \mathfrak{m}' \subseteq A'$, para algum ideal maximal $\mathfrak{m}'$ de $A' = A[x^{-1}]$.

Seja Ω o fecho algébrico de $k' = A'/\mathfrak{m}'$. Aplicando o Lema de Zorn à coleção:

$$\Sigma' = \{(C, h); C \text{ subanel de } \mathbb{K}, A' \subset C \text{ e } h : C \longrightarrow \Omega \text{ homomorfismo tal que } g|_{A'} = f\},$$

onde $f : A' \to k'$ é o homomorfismo natural, temos, pelo Teorema 3.27, que existe $B \subseteq \mathbb{K}$ elemento maximal de Σ' (anel e valorização) e $g : B \longrightarrow \Omega$, tais que $A' \subseteq B$ e $g|_{A'} = f$.

Então $x^{-1} \in \mathfrak{m}'$ e $f(x^{-1}) = \overline{0}$ em Ω. Se $x \in B$, então $g(x) \in \Omega$. Logo,

$$g(x) \cdot f(x^{-1}) = 0 \Rightarrow g(x) \cdot g(x^{-1}) = 0 \Rightarrow g(x \cdot x^{-1}) = 0 \Rightarrow 1 = 0.$$

Absurdo. Logo, $x \notin B$ e $\bigcap B \subseteq \overline{A}$.

Portanto, $\overline{A} = \bigcap B$.

■

4 CURVAS ALGÉBRICAS

O estudo das curva será via corpos de funções de algébricas em uma variável. Estabeleceremos uma correspondência entre os pontos de uma curva e os anéis de valorização discreta do seu corpo de funções racionais.

4.1 VARIEDADES ALGÉBRICAS AFINS

Nesta seção, apresentaremos os conceitos básicos da Geometria Algébrica que serão usados neste trabalho.

Definição 4.1. O **espaço afim** de dimensão n sobre um corpo k, denotado por $\mathbb{A}_k^n$ ou simplesmente por $\mathbb{A}^n(k)$, é o conjunto de todas as n-uplas de elementos de k. Um elemento $p = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ será chamado **ponto** e os a_i's serão chamados de **coordenadas** de p.

Considere o anel de polinômios $k[x_1, \ldots, x_n]$ nas variáveis $x_1, \ldots, x_n$ com coeficientes em k. Seja $S \subset k[x_1, \ldots, x_n]$ um subconjunto. Denotamos por

$$V(S) := \{p \in \mathbb{A}^n(k); f(p) = 0, \forall\ f \in S\}$$

o **conjunto de zero** de S.

Definição 4.2. Dizemos que um subconjunto $X \subset \mathbb{A}^n(k)$ é **fechado** se $X = V(S)$ para algum $S \subset k[x_1, \ldots, x_n]$.

Os subconjuntos fechados de $\mathbb{A}^n(k)$ são também chamados de conjuntos algébricos afins.

Definição 4.3. Seja $f \in k[x_1, \ldots, x_n]$ um polinômio não constante. O conjunto de zeros de f se denomina **hipersuperfície** definida por f.

As hipersuperfícies em $\mathbb{A}^2(k)$, isto é, o conjunto solução de $f(x_1, x_2) = 0$, onde f é um polinômio não constante em duas variáveis, são também chamadas de **curvas algébricas afins planas**.

Exemplo 4.4. O conjunto $H = \{(t, t^2, t^3); t \in k\}$ é um conjunto algébrico. Mas precisamente, $H = V(f, g)$, onde $f, g \in k[x, y, z]$ são definidos por $f(x, y, z) = x^2 - y$ e $g(x, y, z) = x^3 - z$.

Exemplo 4.5. Os subconjuntos algébricos de $\mathbb{A}^2(k)$ definidos por $C_1 = V(y^2 - x^2 - x^3)$ e $C_2 = V(y^2 - x^3)$ são exemplos de curvas algébricas afins planas.

Definição 4.6. Definimos a **topologia de Zariski** em $\mathbb{A}^n(k)$ escolhendo para os abertos os subconjuntos de $\mathbb{A}^n(k)$ que são complementares de conjuntos fechados.

Definição 4.7. Um subconjunto Y de um espaço topológico X é **irredutível** se ele não puder ser escrito como a união $Y = Y_1 \cup Y_2$ de dois subconjuntos fechados (de Y, com a topologia induzida) próprios.

Definição 4.8. Uma **variedade afim** é um subconjunto fechado irredutível de $\mathbb{A}^n(k)$. Um subconjunto aberto de uma variedade afim é uma **variedade quase afim**.

Seja $X \subset \mathbb{A}^n(k)$ um subconjunto qualquer. Definimos o ideal de X por

$$I(X) := \{f \in k[x_1, \ldots, x_n]; f(p) = 0, \forall p \in X\}.$$

Proposição 4.9. *(i) Sejam T_1, T_2 subconjuntos de $k[x_1, \ldots, x_n]$. Se $T_1 \subseteq T_2$, então $V(T_1) \supseteq V(T_2)$.*

(ii) Se $X_1 \subseteq X_2$ são subconjuntos de $\mathbb{A}^n(k)$, então $I(X_1) \supseteq I(X_2)$.

(iii) Para quaisquer dois subconjuntos X_1, X_2 de $\mathbb{A}^n(k)$, temos

$$I(X_1 \cup X_2) = I(X_1) \cap I(X_2).$$

(iv) Seja k um corpo algebricamente fechado. Para qualquer ideal $\mathfrak{a} \subseteq k[x_1, \ldots, x_n]$, tem-se $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, onde $\sqrt{\mathfrak{a}}$ é o radical de $\mathfrak{a}$.

(v) Para qualquer subconjunto $X \subseteq \mathbb{A}^n(k)$, $V(I(X)) = \overline{X}$, onde $\overline{X}$ é o fecho de X, isto é, a interseção de todos os subconjuntos fechados de $\mathbb{A}^n(k)$ contendo X.

Demonstração. Ver [HR], Proposição 1.3, página 3. ■

Proposição 4.10. *Seja X um subconjunto de $\mathbb{A}_n(k)$. Então X é irredutível se, e somente se, $I(X)$ é um ideal primo.*

Demonstração. Supondo que X é irredutível, vamos mostrar que X é um ideal primo. Se $fg \in I(X)$, como $X \subseteq V(I(X))$ e, pela proposição anterior, $V(I(X)) \subseteq V(\langle fg \rangle) = V(fg)$ e $V(fg) = V(f) \cup V(g)$, temos $X \subset V(f) \cup V(g)$. Logo, $X = (X \cap V(f)) \cup (X \cap V(g))$. Como X é irredutível, então $X = X \cap V(f)$ ou $X = X \cap V(g)$. Logo, $X \subset V(f)$ ou $X \subset V(g)$. Portanto, $f \in I(X)$ ou $g \in I(X)$, isto é, $I(X)$ é primo.

Reciprocamente, suponha que $I(X)$ é primo e que $X = X_1 \cup X_2$, com $X_1 \subsetneq X$ e $X_2 \subsetneq X$. Assim, $I(X_1) \supsetneq I(X)$ e $I(X_2) \supsetneq I(X)$. Logo existem $f \in I(X_1)$ e $g \in I(X_2)$ tais que $f, g \notin I(X)$. Por outro lado, $fg \in I(X_1 \cup X_2) = I(X)$, o que é um absurdo, pois $I(X)$ é primo. Portanto, X é irredutível. ■

Definição 4.11. Dado $X \subseteq \mathbb{A}^n(k)$ um subconjunto fechado, definimos o **anel de coordenadas** de X, denotado por $\Gamma(X)$, por

$$\Gamma(X) = \frac{k[x_1, \ldots, x_n]}{I(X)}.$$

4.2 VARIEDADES ALGÉBRICAS PROJETIVAS

Para definir variedades projetivas, procedemos de maneira análoga à definição de variedades afins, exceto que trabalhamos no espaço projetivo.

Definição 4.12. O **espaço projetivo** de dimensão n sobre um corpo k, denotado por $\mathbb{P}^n_k$ ou simplesmente por $\mathbb{P}^n(k)$, é o conjunto das classes de equivalência de $(n+1)$-uplas $(a_0, \ldots, a_n)$ de elementos de k, não todos nulos, sob a relação de equivalência dada por

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \Leftrightarrow \exists\ \lambda \in k \setminus \{0\};\ \ (b_0, \ldots, b_n) = (\lambda a_0, \ldots, \lambda a_n).$$

Um ponto $p \in \mathbb{P}^n(k)$ será denotado por $p = (a_0 : ... : a_n)$ e os a_i's serão chamados de **coordenadas homogêneas** de p.

Chamamos de **pontos finitos** os pontos do conjunto

$$\{(x_0 : ... : x_n) \in \mathbb{P}^n(k);\ \ x_0 \neq 0\} = \{(1 : x_1 : ... : x_n);\ \ (x_1, \ldots, x_n) \in \mathbb{A}^n(k)\}$$

e chamamos de **pontos no infinito** os pontos do conjunto

$$\{(x_0 : ... : x_n) \in \mathbb{P}^n(k);\ \ x_0 = 0\} = \left\{(0 : x_1 : ... : x_n);\ \ (x_1 : ... : x_n) \in \mathbb{P}^{n-1}(k)\right\}.$$

Note que o conjunto dos pontos finitos de $\mathbb{P}^n(k)$ pode ser identificado com $\mathbb{A}^n(k)$ e o conjunto dos pontos no infinito pode ser identificado com $\mathbb{P}^{n-1}(k)$.

Em particular, temos

$$\mathbb{P}^1(k) = \text{reta afim dos pontos finitos} \cup \{(0 : 1)\},$$

e assim $\mathbb{P}^1(k)$ tem um único ponto no infinito. E temos

$$\mathbb{P}^2(k) = \text{plano afim dos pontos finitos} \cup \text{reta projetiva dos pontos no infinito.}$$

Definição 4.13. Um ponto $p = (a_0 : ... : a_n) \in \mathbb{P}^n(k)$ é **zero** de um polinômio qualquer $F \in k[x_1, \ldots, x_n]$, se $F(p) = 0$ para qualquer escolha de coordenadas homogêneas de p. Neste caso, $F \in k[x_1, \ldots, x_n]$ deve ser um polinômio homogêneo de grau d, isto é,

$$F(ta_0, \ldots, ta_n) = t^d F(a_0, \ldots, a_n), \forall\ t \in k \setminus \{0\}.$$

Seja $S \subset k[x_0, \ldots, x_n]$ um conjunto de polinômios homogêneos. Denotamos por

$$V(S) := \{p \in \mathbb{P}^n(k);\ \ F(p) = 0, \forall F \in S\}$$

o **conjunto de zeros** de S.

Definição 4.14. Dizemos que um subconjunto $X \subset \mathbb{P}^n(k)$ é **fechado** se $X = V(S)$, para algum conjunto $S \subset k[x_0, \ldots, x_n]$ de polinômios homogêneos. Os subconjuntos fechados de $\mathbb{P}^n(k)$ são também chamados de conjuntos algébricos projetivos.

Definição 4.15. Definimos a **topologia de Zariski** em $\mathbb{P}^n(k)$ escolhendo para abertos os subconjuntos de $\mathbb{P}^n(k)$ que são complementares de fechados projetivos.

Definição 4.16. Uma **variedade projetiva** é um subconjunto fechado irredutível de $\mathbb{P}^n(k)$ (com uma topologia induzida). Um subconjunto aberto de uma variedade projetiva é uma **variedade quase projetiva**.

Observação 4.17. A definição de conjunto algébrico projetivo irredutível é análoga ao caso afim.

Seja $X \subset \mathbb{P}^n(k)$ um subconjunto. Definimos o **ideal homogêneo** de X por

$$I(X) := \{F \in k[x_1, \ldots, x_n];\ \ F(p) = 0, \forall\ p \in X\}.$$

Definição 4.18. Dado um subconjunto $Y \subset \mathbb{P}^n(k)$ definimos $\overline{Y} \subset \mathbb{P}^n(k)$, o **fecho projetivo** de Y, como sendo a interseção de todos os subconjuntos fechados de $\mathbb{P}^n(k)$ que contém Y.

Para qualquer subconjunto $Y \subset \mathbb{P}^n(k)$ temos que $V(I(Y)) = \overline{Y}$. Se $Y \subset \mathbb{A}^n(k)$ for um fechado afim, identificamos $\mathbb{A}^n(k)$ como o aberto $U_0 \subset \mathbb{P}^n(k)$ e falamos do fecho de Y em $\mathbb{P}^n(k)$, o qual chamamos fecho projetivo de Y.

Definição 4.19. Dado $X \subseteq \mathbb{P}^n(k)$ um fechado projetivo, definimos o **anel de coordenadas homogêneas** de X, denotado por $\Gamma(X)$, por

$$\Gamma(X) = \frac{k[x_0, \ldots, x_n]}{I(X)}.$$

4.3 CURVAS ALGÉBRICAS E VALORIZAÇÕES

Sejam $V \subset \mathbb{A}^n(k)$ uma variedade algébrica, $I \subset k[x_1, x_2, \ldots, x_n]$ o ideal primo de V e $\Gamma(V) = k[x_1, x_2, \ldots, x_n]/I$. Então, $\Gamma(V)$ é um domínio de integridade (pois V é irredutível se, e somente se, $I(V)$ é primo) e $k(V)$, seu corpo de frações, é chamado **corpo de funções racionais** de V.

Definição 4.20. A **dimensão** de V é o grau de transcendência da extensão $k(V)/k$. Uma variedade de dimensão um é chamada curva.

No caso de curvas, $k(V)/k$ é um corpo de funções algébricas em uma variável (com k como corpo de constantes), pois o grau de transcendência igual a 1 implica que existe $t = x_i \in K(V) = k(x_1, \ldots, x_n)$, transcendentes sobre k, tal que $[k(V) : k(t)] < \infty$.

Definição 4.21. Seja $\mathbb{K}/k$ uma extensão de corpos. Uma valorização de $\mathbb{K}/k$ é uma valorização de $\mathbb{K}$ tal que $v(a) = 0$, para todo $a \in k \setminus \{0\}$.

O conjunto das valorizações de $\mathbb{K}/k$ será denotado por $S_{\mathbb{K}/k}$, isto é,

$$S_{\mathbb{K}/k} = \{v : \mathbb{K} \to \mathbb{Z} \cup \{\infty\};\ \ v \text{ é uma valorização de } \mathbb{K} \text{ e } v(a) = 0, \forall a \in k \setminus \{0\}\}.$$

Agora veremos como associar pontos de uma curva plana irredutível afim C à valorizações de $k(C)/k$.

Começaremos com um exemplo onde essa associação é bem natural.

Exemplo 4.22. Seja C a curva afim dada por $f(x, y) = x = 0$, cujo fecho projetivo é $\mathbb{P}^1(k)$. Neste caso,

$$\Gamma(C) = \frac{k[x, y]}{\langle f(x, y)\rangle} = \frac{k[x, y]}{\langle x\rangle} = k[t], \text{ onde } t = \overline{y} \in \frac{k[x, y]}{\langle x\rangle},$$

$\overline{y}$ é a classe residual de y em $k[x, y]/\langle f\rangle$ e $k(C) = k(t)$.

Então segue dos Exemplos 3.16 e 3.17 e da Proposição 3.18 que existe uma bijeção natural entre os seguintes conjuntos

$$\begin{array}{ccc} \{v; v \text{ é uma valorização de } k(t)/k\} & \longleftrightarrow & k \cup \{\infty\} = \mathbb{P}^1(k) \\ v = v_a & \longleftrightarrow & a \\ v_\infty & \longleftrightarrow & \infty \end{array}$$

Para curvas gerais vamos precisar antes de algumas definições e resultados.

A próxima proposição é um resultado semelhante à Proposição 3.18, porém considerando o caso mais geral em $\mathbb{K}/k$ é um corpo de funções algébricas em uma variável.

Proposição 4.23. *Seja $\mathbb{K}/k$ um corpo de funções algébricas em uma variável. Sejam v uma valorização de $\mathbb{K}/k$ e $f \in \mathbb{K}$ tal que $v(f) \geq 0$. Então existe um único $c \in k$ tal que $v(f - c) > 0$.*

Demonstração. (Existência) Seja $f \in k$, então $v(f - f) = v(0) = \infty$. Tome $c = f$. Agora, se $f \notin k$, então $[\mathbb{K} : k(f)] < \infty$. Como v é sobrejetiva, existem $z \in \mathbb{K}$ e $g(x) \in k[f][x]$ não nulos, tais que $v(z) > 0$ e $g(z) = 0$. Considere $g(x) = \sum_{i=0}^{r} b_i(f)x^i$, com $b_0(f) \neq 0$. Afirmamos que $v(b_i(f)) > 0$, para algum $i = 0, \ldots, r$.

De fato, se $v(b_i(f)) = 0$, para todo $i = 0, \ldots, r$ tal que $b_i(f) \neq 0$, então

$$\infty = v(0) = v\left(\sum_{i=0}^{r} b_i(f)z^i\right) = v(b_0(f)),$$

contradição (pois $b_0(f) \neq 0$).

Suponha que $b_i(f) \neq 0$ e que $v(b_i(f)) > 0$. Se $b_i(f) = a\prod_{j=0}^{s}(f - c_j)^{e_j}$ concluímos que $v(f - c_j) > 0$ para algum $j = 0, \ldots, s$, pois $v(b_i(f)) > 0$. Denote c_j por c.

(Unicidade) Suponha que exista $b \in k,\ b \neq c$ tal que $v(b-f) = v(f-b) > 0$. Então,

$$0 = v(b-c) = v\Big((f-c)-(f-b)\Big) \geq \min\{v(f-c), v(f-b)\} > 0.$$

Absurdo. Logo, $c \in k$ é único. ■

Definição 4.24. Sejam $\mathbb{K}/k$ um corpo de funções algébricas em uma variável, dados $f \in \mathbb{K}$ e v uma valorização de $\mathbb{K}/k$ com $v(f) \geq 0$. Dizemos que o único elemento $c \in k$ tal que $v(f-c) > 0$ é o **valor** de f em v e escrevemos $f(v) = c$. Se $v(f) < 0$, dizemos que f tem **polo** em v e escrevemos por $f(v) = \infty$. Se $v(f) > 0$, dizemos que f tem um **zero** em v.

Assim cada $f \in \mathbb{K}$ define uma função

$$\begin{array}{rcl} f : \{v;\ v \text{ é uma valorização de } \mathbb{K}/k\} & \longrightarrow & k \cup \infty \\ v & \longmapsto & c, \text{ se } v(f-c) > 0 \text{ e } v(f) \geq 0 \\ v & \longmapsto & \infty, \text{ se } v(f) < 0 \end{array}$$

Lema 4.25. *Seja v uma valorização de $\mathbb{K}/k$.*

(i) Se $f, g \in \mathbb{K}$ são tais que $v(f) \geq 0$ e $v(g) \geq 0$, então:

$$(fg)(v) = f(v)g(v); \tag{4.1}$$

$$(f+g)(v) = f(v) + g(v). \tag{4.2}$$

(ii) Se $g \in \mathbb{K} - \{0\}$ e $f, h \in \mathbb{K}$ são tais que $v(hf) \geq 0, v(hg) \geq 0$ e $v(f/g) \geq 0$, então:

$$\frac{hf(v)}{hg(v)} = \frac{f}{g}(v). \tag{4.3}$$

Demonstração. (i) Segue da definição que $f(v) = c$ e $g(v) = e$ implicam $v(f-c) > 0$ e $v(g-e) > 0$ $(fg)(v) = f(v)g(v)$.

Sejam $f(v) = c$ e $g(v) = e$, segue da definição que $v(f-c) > 0$ e $v(g-e) > 0$. Então temos que mostrar que $v(fg-ce) > 0$. De fato,

$$\begin{array}{rcl} v(fg-ce) & = & v(fg-cg+cg-ce) = v\Big((f-c)g + c(g-e)\Big) \\ & \geq & \min\{v(f-c)+v(g), v(c)+v(g-e)\} \\ & > & 0. \end{array}$$

Agora, para mostramos que $(f+g)(v) = f(v) + g(v)$, temos que mostrar que $v\Big((f+g)-(c+e)\Big) > 0$. Temos

$v\Big((f+g)-(c+e)\Big) = v\Big((f-c)+(g-e)\Big) \geq \min\{v(f-c), v(g-e)\} > 0.$

(ii) Suponhamos que $hf(v) = c$ e $hg(v) = d$, ou seja, $v(hf-c) > 0$ e $v(hg-d) > 0$. Vamos mostrar que $v(f/g - c/d) > 0$.

De fato,

$$\begin{aligned} v(f/g - c/d) = v(hf/hg - c/d) &= v\Big((hf/hg - c/hg + c/hg - c/d)\Big) \\ &= v\Big((hf-c)/hg + c(d-hg)/hgd\Big) \\ &\geq \min\{v(hf-c) - v(hg), v(d-hg) - v(hg)\} \\ &= \min\{v(hf-c), v(d-hg)\} > 0. \end{aligned}$$

Na última igualdade acima usamos que $v(hg) = 0$, pois $v(hg) > 0$ implicaria $d = 0$, já que $d \in k$ é único tal que $v(hg-d) > 0$. Entretanto, $d \neq 0$ porque está no denominador da fração $hf(v)/hg(v)$. ■

Na sequência, para associarmos valorizações aos pontos de uma curva precisaremos definir anel local de uma curva em um ponto.

Sejam V uma variedade afim e $p \in V$. Dizemos que uma função racional $f \in k(V)$ está definida em p se existirem $a, b \in \Gamma(V)$ tais que $f = a/b$ e $b(p) \neq 0$.

Definição 4.26. Se p é um ponto de uma curva plana afim C, definimos o **anel local** de C em p, denotado por $\mathcal{O}_p(C)$, como sendo o anel de todas as funções racionais de V que estão definidas em p.

Observação 4.27. $\mathcal{O}_p(C)$ é um subanel de $k(C)$ contendo $\Gamma(C)$.

De fato, sejam $g_1, g_2 \in K(C)$ definidas em p, isto é, $g_1 = a_1/b_1$ e $g_2 = a_2/b_2$, onde $a_i, b_i \in \Gamma(C)$, para $i = 1, 2$, e $g_1(p) \neq g_2(p)$. Então:

$$g_1 + g_2 = \frac{a_1b_2 + a_2b_1}{b_1b_2} \text{ e } g_1 \cdot g_2 = \frac{a_1a_2}{b_1b_2},$$

com $b_1(p)b_2(p) \neq 0$, pois $\Gamma(C)$ é domínio.

Observe que em geral g_1/g_2 não é definida em p, pois podemos ter $g_2(p) = 0$.

Logo, $\mathcal{O}_p(C)$ é um subanel de $k(C)$. Além disso, os elementos de $\Gamma(C)$ são da forma a/b e, portanto, estão contidos em $\mathcal{O}_p(C)$, para todo $p \in C$.

Observação 4.28. $\mathcal{O}_p(C)$ é um anel noetheriano.

Seja I um ideal de $\mathcal{O}_p(C)$ e defina $J = I \cap \Gamma(C)$. Como $\Gamma(V)$ é noetheriano (Corolário 3.3 e Proposição 2.44), J é finitamente gerado, isto é, $J = \langle f_1, \ldots, f_m \rangle$. Afirmamos que $f_1, \ldots, f_m$ geram I.

De fato, dado $g \in I \subseteq \mathcal{O}_p(C)$, como g é definida em p, então existem $a, b \in \Gamma(C)$, com $g = \dfrac{a}{b}$ e $b(p) \neq 0$. Logo, $bg \in \Gamma(C) \cap I = J$ e, assim, $bg = r_1f_1 + \cdots + r_mf_m$, com

$r_i \in \Gamma(C)$. Então

$$g = \frac{\sum r_i f_i}{b} = \sum \frac{r_i}{b} f_i,$$

onde $r_j/b \in \mathcal{O}_p(C)$.

Observação 4.29. $\mathcal{O}_p(C)$ é um anel cujo único ideal maximal é

$$\mathcal{M}_p(C) = \{f \in \mathcal{O}_p(C);\ \ f(p) = 0\}.$$

De fato, vamos mostrar que $\mathcal{M}_p(C)$ é um ideal maximal. Considere a função definida por

$$\begin{array}{ccc} \varphi : \mathcal{O}_p(C) & \longrightarrow & k \\ f & \longmapsto & \varphi(f) = f(p) \end{array},$$

uma valorização.

Vamos mostrar que φ é um homomorfismo de anéis. Para isto, sejam $f, g \in \mathcal{O}_p(C)$. Então

$$\begin{aligned} \varphi(f+g) = (f+g)(p) = f(p) + g(p) = \varphi(f) + \varphi(g) \\ \varphi(fg) = (fg)(p) = f(p)g(p) = \varphi(f)\varphi(g). \end{aligned}$$

Portanto, φ é um homomorfismo de anéis. Além disso,

$$Ker(\varphi) = \{f \in \mathcal{O}_p(C);\ \ \varphi(f) = 0\} = \{f \in \mathcal{O}_p(C);\ \ f(p) = 0\} = \mathcal{M}_p(C).$$

Como φ é sobrejetiva temos, pelo primeiro Teorema de isomorfismo,

$$\frac{\mathcal{O}_p(C)}{Ker(\varphi)} \simeq \varphi(\mathcal{O}_p(C)) = k.$$

Como k é corpo, então $\mathcal{M}_p(C)$ é um ideal maximal.

Agora, mostraremos que $\mathcal{M}_p(C)$ é único. Seja $f \in \mathcal{O}_p(C)$ um elemento invertível, então $f(p) \neq 0$, logo, $f \notin \mathcal{M}_p(C)$. Portanto, $\mathcal{M}_p(C)$ contém todos os elementos não invertíveis de $\mathcal{O}_p(C)$. Logo, todos os outros ideais próprios de $\mathcal{O}_p(C)$ estão contidos em $\mathcal{M}_p(C)$, ou seja, $\mathcal{M}_p(C)$ é o único ideal maximal de $\mathcal{O}_p(C)$.

Veremos no próximo teorema que o anel local de uma curva em um ponto é o objeto que traduz propriedades locais da curva.

Definição 4.30. Sejam C uma curva plana afim dada por $F(x, y) = 0$ e $p = (a, b) \in C$. Dizemos que p é um **ponto simples** de C se $F_x(p) \neq 0$ ou $F_y(p) \neq 0$. Um ponto $p \in C$ que não é simples é chamado **ponto singular**. Uma curva que só possui pontos simples se denomina uma **curva plana afim não singular.**

Teorema 4.31. *Um ponto $p \in C$ é simples se, e somente se, $\mathcal{O}_p(C)$ é um anel de valorização discreta. Neste caso, se $L = ax + by + c$ é uma reta que passa por p mas não é tangente a C em p, então a imagem l de L em $\mathcal{O}_p(C)$ é um parâmetro de uniformização de $\mathcal{O}_p(C)$.*

Demonstração. Ver [WF], Teorema 1, página 49. ■

Proposição 4.32. *Seja $\mathbb{K}/k$ um corpo de funções algébricas em uma variável com k como corpo de constantes. Seja R um anel local com $k \subset R \subset \mathbb{K}$. Então existe um anel de valorização discreta B tendo $\mathbb{K}$ como corpo de frações, tal que $k \subset R \subset B \subset \mathbb{K}$ e $\mathcal{M}_R = R \cap \mathcal{M}_B$, onde $\mathcal{M}_R$ é o ideal maximal de R e $\mathcal{M}_B$ é o ideal maximal de B.*

Além disso, se R é um anel de valorização discreta, então R não está contido propriamente em nenhum outro anel de valorização discreta de $\mathbb{K}$.

Demonstração. Ver [EO], Corolário 9.7, página 62. ■

Veremos agora como relacionar os pontos de uma curva afim irredutível C dada por $F(X, Y) = 0$ com valorizações.

Seja $k(C)$ o corpo de funções racionais de C. Então $k(C) = k(x, y)$, onde $x = \overline{X}$ e $y = \overline{Y}$ são classes residuais de X e Y em $k[X, Y]/\langle F \rangle$.

Proposição 4.33. *Se $S'_{k(C)/k} = \left\{ v \in S_{k(C)/k};\ \ v(x) \geq 0 \ \ e \ \ v(y) \geq 0 \right\}$ e*

$$\begin{array}{rccc} \varphi: & S'_{k(C)/k} & \longrightarrow & \mathbb{A}^2_k \\ & v & \longmapsto & (x(v), y(v)), \end{array}$$

então $\varphi(S'_{k(C)/k}) = C$. Além disso, se C for não singular, φ é uma bijeção.

Demonstração. Das igualdades (4.1) e (4.2) temos que

$$F(x(v), y(v)) = F(x, y)(v) = 0(v) = 0.$$

Ou seja, $\varphi(S'_{k(C)/k}) \subset C$.

Reciprocamente, dado $p \in C$, temos que $\mathcal{O}_p(C)$ é um anel local e $k \subset \mathcal{O}_p(C) \subset k(C)$. Então pela Proposição 4.32, existe v valorização de $k(C)/k$ tal que $\mathcal{O}_p(C) \subset \mathcal{O}_v$ e $\mathcal{M}_p = \mathcal{O}_p(C) \cap \mathcal{M}_v$.

Mas se $p = (a, b)$, então $(x - a),\ \ (y - b) \in \mathcal{M}_p$, logo, $(x - a),\ \ (y - b) \in \mathcal{M}_v$, ou seja, $v(x - a) > 0$ e $v(y - b) > 0$. Assim, $x(v) = a,\ \ y(v) = b$ e

$$p(x(v), y(v)) = \varphi(v) \in \varphi(S'_{k(C)/k}).$$

Observe que se $p = (a, b) = (x(v), y(v))$, então $v(x - a) > 0$ e $v(y - b) > 0$ e, portanto, o anel local de C em p, $\mathcal{O}_p(C)$, está contido no anel de valorização discreta

correspondente a v, isto é, $\mathcal{O}_p(C) \subset \mathcal{O}_v$. Então se p é um ponto não singular de C, pela Proposição 4.31, $\mathcal{O}_p(C) = \mathcal{O}_v$. Logo, concluímos que existe um único $v \in {S'}_{k(C)/k}$ tal que $p = \varphi(v)$. Portanto, se C é não singular temos que $\varphi : {S'}_{k(C)/k} \longrightarrow C$ é uma bijeção. ■

Veremos nos exemplos a seguir a construção da correspondência φ em curvas singulares.

Exemplo 4.34. Seja C uma curva afim sobre $k = \mathbb{C}$ dada por

$$F(X, Y) = X^2 + X^3 - Y^2 = 0.$$

Sejam $x = \overline{X}$ e $y = \overline{Y}$ as classes residuais de X e Y em $k[X, Y]/\langle X^2 + X^3 - Y^2 \rangle$. Então

$$y^2 = x^2 + x^3 = x^2(1 + x) \Rightarrow \left(\frac{y}{x}\right)^2 = 1 + x.$$

Fazendo $t = \dfrac{y}{x}$, temos $x = t^2 - 1$, $y = t(t^2 - 1)$ e

$$k(C) = k(x, y) = k(t^2 - 1, t(t^2 - 1)) = k(t).$$

Pela Proposição 3.18, $S_{k(C)/k} = \{v_c;\ c \in k\} \cup \{\infty\}$. Além disso, como x e y são polinômios em t, temos que $v(x) \geq 0$ e $v(y) \geq 0$ se, e somente se, $v(t) \geq 0$. Logo,

$${S'}_{k(C)/k} = \left\{v \in S_{k(C)/k};\ v(x) \geq 0 \text{ e } v(y) \geq 0\right\} = \{v_c;\ c \in k\}.$$

Para $v_c \in S_{k(C)/k}$, temos $v_c(t - c) = 1$ e $t(v_c) = c$. Logo,

$$x(v_c) = t(v_c)^2 - 1(v_c) = c^2 - 1 \text{ e } y(v_c) = t(v_c)(t(v_c)^2 - 1(v_c)) = c(c^2 - 1).$$

Portanto,

$$\begin{array}{ccc} \varphi : {S'}_{k(C)/k} & \longrightarrow & k^2 \\ v_c & \longmapsto & (c^2 - 1, c(c^2 - 1)) \end{array}.$$

Note que $p = (0, 0)$ é o único ponto singular de C e $\varphi(v_c) = (0, 0)$ se, e somente se, $c = 1$ ou $c = -1$. Ou seja, na origem, a curva C admite duas valorizações v_1 e v_{-1}, cujos os uniformizantes locais são $u = t - 1$ e $w = t + 1$, respectivamente.

Em $\mathcal{O}_{v_1}$, $x = u(u + 2)$ e $y = u(u^2 + 3u + 2) = u^3 + 3u^2 + 2u$.

Analogamente, mostra-se que em $\mathcal{O}_{v_{-1}}$, $x = (w(w - 2))$ e $y = w^3 - 3w^2 + 2w$.

Exemplo 4.35. Seja C a curva afim sobre $k = \mathbb{C}$, dada por

$$F(X, Y) = Y^2 - X^n = 0,$$

onde $n = 2l + 1$, l é um inteiro positivo. Sejam $x = \overline{X}$ e $y = \overline{Y}$ as classes residuais de X e Y em $k[X, Y]/\langle Y^2 - X^n \rangle$. Então

$$y^2 = x^n = x^{2l+1} \Rightarrow \left(\frac{y}{x^l}\right)^2 = x.$$

Fazendo, $t = \dfrac{y}{x^l}$, temos $x = t^2, y = tx^l = t(t^2)^l = t^{2l+1} = t^n$ e

$$k(C) = k(x, y) = k(t^2, t^{2l+1}) = k(t).$$

Pela Proposição 3.18, $S_{k(C)/k} = \{v_c;\ \ c \in k\} \cup \{v_\infty\}$. Como $x = t^2$ e $y = t^n$ temos que $v(x) \geq 0$ e $v(y) \geq 0$ se, e somente se, $v(t) \geq 0$, ou ainda, se e somente se, $v = v_c$ para algum $c \in k$. Logo, $S'_{k(C)/k} = \{v(x) \geq 0 \text{ e } v(y) \geq 0\} = \{v_c;\ \ c \in k\}$.

Segue da definição que para $v_c \in S_{k(C)/k}$, $v_c(t - c) = 1$ e $t(v_c) = c$. Logo,

$$x(v_c) = t(v_c)^2 = c^2 \quad \text{e} \quad y(v_c) = t(v_c)^n = c^n.$$

Portanto

$$\begin{array}{ccc} \varphi : S'_{k(C)/k} & \longrightarrow & \mathbb{A}^2_k \\ v_c & \longmapsto & (c^2, c^n) \end{array}.$$

Note que $p = (0, 0)$ é o único ponto singular de C e $\varphi(v_c) = (0, 0)$ se, e somente se, $c = 0$. Ou seja, na origem, a curva C admite uma única valorização v_0 cujo uniformizante local é $u = t$. Portanto, $x = u^2$ e $y = u^n$.

5 SEMIGRUPOS E ANÉIS GORENSTEIN

Neste capítulo introduzimos os conceitos de semigrupos, semigrupos simétricos e de anéis Gorenstein, além da relação entre anéis Gorenstein e semigrupos.

Vamos considerar em todo capítulo que $0 \in \mathbb{N}$.

5.1 SEMIGRUPOS NUMÉRICOS

Definição 5.1. Um **semigrupo numérico** S é um subconjunto de números naturais $\mathbb{N}$, que satisfaz as seguintes condições:

(i) $0 \in S$;

(ii) Se $a, b \in S$, então $a + b \in S$;

(iii) $\mathbb{N} \setminus S$ é finito.

Escreve-se:

$$S = \{0, s_1, s_2, \ldots, s_n, \longrightarrow\}$$

onde $s_i > s_j$, para $i > j$. A seta significa que todos os elementos de $\mathbb{N}$ a partir de s_n pertencem a S.

O menor elemento de S diferente de zero, s_1, é chamando de **multiplicidade** de S e o denotamos por $m(S)$. O menor inteiro positivo $s_n \in S$ a partir do qual todo mundo pertence a S é chamado o **condutor** de S e será denotado por $\beta(S)$, ou simplesmente de β. O **número de Frobenius** de um semigrupo numérico S, que vamos denotar por $F(S)$, é o maior inteiro que não pertence ao semigrupo numérico. Observe que $F(S) = \beta - 1$. Os elementos do conjunto $G(S) = \mathbb{N} \setminus S$ são chamados de **lacunas** de S e a cardinalidade, $g(S)$, de $G(S)$ é chamada **gênero** de S.

Exemplo 5.2. $S = \{0, 5, 8, 10, 11, 13, 15, 16, 18, \longrightarrow\}$ é um semigrupo numérico com condutor $\beta = 18$, número de Frobenius $F(S) = 17$ e gênero $g(S) = 10$.

Definição 5.3. Sejam S um semigrupo numérico e A um subconjunto não vazio de S. Dizemos que S é **gerado** por A, e escrevemos $S = \langle A \rangle$, se para todo $s \in S$, existem $a_1, \ldots, a_n \in A$ e $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$ tais que $s = \sum_{i=1}^{n} \lambda_i a_i$. Quando A é finito, $A = \{a_1, a_2, \ldots, a_n\}$, dizemos que S é **finitamente gerado** e escrevemos

$$S = \langle a_1, a_2, \ldots, a_n \rangle .$$

Exemplo 5.4. O conjunto gerador do semigrupo

$$S = \{0, 5, 7, 9, 10, 12, 14, \longrightarrow\}$$

é $\{5, 7, 9\}$.

Exemplo 5.5. O conjunto $\{4, 7, 9\}$ é um conjunto de geradores do semigrupo

$$S = \{0, 4, 7, 8, 9, 11, \longrightarrow\}.$$

Dizemos que um conjunto A de geradores de S é **minimal** se nenhum elemento de A puder ser obtido como combinação linear, com coeficientes naturais, a partir de outros elementos do conjunto.

Observamos que

$$S = \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n;\ x_1, \ldots, x_n \in \mathbb{N}\}$$

é o conjunto das combinações lineares com coeficientes inteiros não negativos que podemos formar com os geradores. Para encontrar o conjunto minimal de geradores de S, basta tirar do conjunto de geradores os elementos que são soma de dois outros.

Proposição 5.6. *Todo semigrupo numérico admite um único sistema de geradores minimal que é finito.*

Demonstração. Seja S um semigrupo numérico. Denotaremos por S^* o conjunto dos elementos do semigrupo S com exceção do elemento zero. Observe que $S^* + S^*$ é o conjunto dos elementos em S que são soma de dois elementos, diferentes de zero, em S. Primeiro mostraremos que $\bar{S} = S^* \setminus (S^* + S^*)$ é um sistema de geradores de S. Seja $s \in S^*$, se $s \notin \bar{S}$ então existem $a, b \in S^*$, menores do que s, tais que $s = a + b$. Novamente, se algum destes últimos elementos, eventualmente os dois, não pertencer a $\bar{S}$, podemos escreve-lo como soma de dois elementos em S^* menores do que ele. Ou seja, supondo que $a \notin \bar{S}$ então existem $c, d \in S^*$, menores do que a tais que $s = c + d + b$. De novo, se algum dos elementos b, c, d não pertencer a $S^* \setminus (S^* + S^*)$ conseguimos também escreve-lo como soma de dois elementos menores pertencentes a S^*, fazendo assim uma descida no conjunto dos números naturais. É claro que, como estamos no conjunto dos inteiros não negativos, esta descida é finita e portanto conseguimos encontrar $s_1, \cdots, s_n \in \bar{S}$ tais que $s_1, s_2, ..., s_n \in \bar{S} = S^* \setminus (S^* + S^*)$ e $s = s_1 + \cdots + s_n$. Logo, $\bar{S}$ é um sistema de geradores.

Seja m a multiplicidade de S. Então por definição, $m \in \bar{S}$ e é o menor elemento em $\bar{S}$. Vejamos que $\bar{S}$ não pode ter mais do que m elementos. Suponhamos que existam $a, b \in \bar{S}$ tais que $a < b$ e b é congruente com a módulo m. Portanto, $b = km + a$ para algum $k \in \mathbb{N}$. Absurdo! Então, existe em $\bar{S}$ no máximo um elemento por cada classe de congruência módulo m.

Seja agora $A = \{a_1, \ldots, a_n\}$ um sistema de geradores para S. Afirmamos que $\bar{S}$ está contido neste sistema de geradores. Seja $s \in \bar{S}$, então existem $\lambda_1, \ldots, \lambda_n$ inteiros não negativos, não todos nulos, tais que $s = \lambda_1 a_1 + \cdots + \lambda_n a_n$. Mas, como $s \notin (S^* + S^*)$, temos que $s = a_i$, para algum $i \in \{1, \ldots, n\}$. E portanto, qualquer elemento que está em $\bar{S}$ pertence também ao conjunto de geradores A. Logo, $\bar{S}$ está contido em qualquer

sistema de geradores de S, ou seja, $\bar{S} \subseteq A$. Em particular, no caso em que A é um sistema minimal de geradores temos a igualdade. ■

Observação 5.7. Quando $S = \langle a_1, a_2, \ldots, a_n \rangle$ e não for dito o contrário, assumiremos que $\{a_1, a_2, \ldots, a_n\}$ é um **conjunto minimal** de geradores. Os elementos $a_1, a_2, \ldots, a_n$ serão chamados **geradores minimais** de S.

Lema 5.8. *Seja $S = \langle a_1, a_2, \ldots, a_n \rangle$. Então A é um semigrupo numérico se, e somente se, $mdc(a_1, a_2, \ldots, a_n) = 1$.*

Demonstração. Suponha que $\text{mdc}(a_1, a_2, \ldots, a_n) = d \neq 1$. Dado um elemento $s \in S$, existem $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$, tais que

$$s = a_1 x_1 + \cdots + a_n x_n.$$

Como $d | a_i$, para todo i, temos $d|s$, ou seja, $S \subseteq \langle d \rangle = \{kd;\ \ k \in \mathbb{N}\}$. Logo, $\mathbb{N} \setminus \langle d \rangle \subseteq \mathbb{N} \setminus S$. Sendo $d \neq 1$, existe $e \in \mathbb{N}$ tal que $d < e < 2d$. Então,

$$d \not| (nd + e),\ \forall n \in \mathbb{N} \Rightarrow \{nd + e;\ \ n \in \mathbb{N}\} \subseteq \mathbb{N} \setminus \langle d \rangle \subseteq \mathbb{N} \setminus S.$$

Logo, $\mathbb{N} \setminus S$ não é finito. Absurdo, pois S é um semigrupo numérico. Portanto $d = 1$.

Para a recíproca, é suficiente provar que $\mathbb{N} \setminus S$ é finito. Como $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, existem inteiros $\lambda_1, \ldots, \lambda_n$ tais que $\lambda_1 a_1 + \cdots + \lambda_n a_n = 1$. Passando os termos com λ_i's negativos para o lado direito, podemos encontrar $i_1, \ldots, i_k, j_1, \ldots, j_l \in \{1, \ldots, n\}$ tais que

$$\lambda_{i_1} a_{i_1} + \cdots + \lambda_{i_k} a_{i_k} = 1 - \lambda_1 a_{j_1} - \cdots - \lambda_{j_l} a_{j_l}.$$

Seja $s = -\lambda_1 a_{j_1} - \cdots - \lambda_{j_l} a_{j_l}$. Então, $s,\ s + 1 \in S = \langle a_1, \ldots, a_n \rangle$. Mostraremos que se $n \in \mathbb{N}$ é tal que $n \geq (s-1)s + (s-1)$, então $n \in S$. De fato, dado $n \in \mathbb{N}$ sejam $q,\ r \in \mathbb{N}$ tais que $n = qs + r$ com $0 \leq r \leq s - 1$. Se $n \geq (s-1)s + (s-1)$, então

$$n = qs + r \geq (s-1)s + (s-1) \Rightarrow q \geq s - 1 \geq r.$$

Logo, $n = (rs + r) + (q - r)s = r \underbrace{(s+1)}_{\in S} + (q - r) \underbrace{s}_{\in S}$. ■

Um semigrupo pode ser representado através de um diagrama formado por duas linhas da seguinte forma: na primeira coluna e segunda linha coloca-se o condutor de S e nas colunas seguintes, dois inteiros cuja soma é o número de Frobenius, listados em ordem crescente na linha superior e decrescente na inferior. Bolinhas pretas indicam os elementos que pertencem ao semigrupo S e as bolinhas brancas indicam os elementos de $\mathbb{N} \setminus S$:

	0	1	2	3	4	5	6	7	8
	●	○	○	○	○	●	○	○	●
●	○	●	●	○	●	○	●	●	○
18	17	16	15	14	13	12	11	10	9

Figura 1 – Diagrama do semigrupo $S = \langle 5, 8, 11\rangle$

Exemplo 5.9. Seja $S = \{0, 6, 7, 8, 11, \longrightarrow\}$. Temos que $S = \langle 6, 7, 8, 11\rangle$. Logo $m(s) = 6$, $F(S) = 10$, $G(S) = \{1, 2, 3, 4, 5, 9, 10\}$ e $g(S) = 7$.

	0	1	2	3	4	5
	●	○	○	○	○	○
●	○	○	●	●	●	○
11	10	9	8	7	6	5

Figura 2 – Diagrama do Semigrupo $S = \langle 6, 7, 8, 11\rangle$

5.1.1 **Semigrupos Simétricos**

Uma propriedade fundamental dos semigrupos associados aos anéis locais de curvas em pontos singulares é a simetria. Esta propriedade é dada pelo Teorema de Kunz que será provado mais adiante.

Definição 5.10. Um semigrupo numérico S é chamado **simétrico** se existe um número inteiro n tal que a função

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & z & \longmapsto & n - z \end{array}$$

leva elementos de S em elementos que não pertencem à S e, leva elementos que não pertencem à S em elementos que pertencem a S.

Observação 5.11. Seja S é um semigrupo simétrico gerado pelos números naturais $a_1, \ldots, a_k$, com $\text{mdc}(a_1, \ldots, a_k) = 1$. Então, existe um inteiro positivo $n \notin S$ (o número de Frobenius) tal que $n + i \in S$, para $i = 1, 2, \ldots$. Para cada $s \in S$ temos que $n - s \notin S$ pois, caso contrário, $n = (n - s) + s \in S$. Então, a quantidade de elementos de S pertencentes ao conjunto $\{0, 1, 2, \ldots, n\}$ é sempre menor ou igual que a quantidade de não elementos de S contidos neste mesmo conjunto.

Segue diretamente da Observação 5.11 que o diagrama de um semigrupo simétrico possui bolinha preta em toda coluna, e obviamente esta deve ser única, uma vez que a soma dos dois elementos de uma mesma coluna é o número de Frobenius do semigrupo.

Exemplo 5.12. O semigrupo $S = \langle 4, 6, 11\rangle = \{0, 4, 6, 8, 10, 11, 12, 14, \longrightarrow\}$ é simétrico e possui o seguinte diagrama:

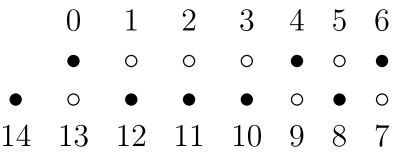


Figura 3 – Diagrama do Semigrupo $S = \langle 4, 6, 11\rangle$

Proposição 5.13. *O semigrupo S é simétrico se, e somente se, o conjunto $\{0, 1, \ldots, n\}$, onde n é número de Frobenius de S, possui tantos elementos de S quanto não elementos de S.*

Demonstração. ($\Leftarrow$) Suponhamos que o conjunto $\{0, 1, \ldots, n\}$ tem tantos elementos de S quanto nõ elementos de S, onde n é o número de Frobenius de S. Então, dado $z \notin S$, temos que $n - z \in S$ pois, caso contrário, teríamos mais elementos em $\{0, 1, \ldots, n\}$ fora de S do que em S. Além disso, $z \in S$ implica $n - z \notin S$, porque $n \notin S$. Logo, S é simétrico.

($\Rightarrow$) Se S é um semigrupo simétrico, então n é inteiro positivo da definição de semigrupo simétrico. De fato, seja m um inteiro positivo tal que a função

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ z & \longmapsto & m - z \end{array}$$

leva elementos de S em elementos que não pertencem à S e elementos que não pertencem à S em elementos que pertencem a S. Se $m > n$, então $m \in S$. Absurdo, pois $0 \in S$, implica $m \notin S$. Por outro lado, se $m < n$, então $\varphi(n) = m - n \in S$. Absurdo, pois $m - n < 0$. Logo, $m = n$ Como $\varphi(z) = n - z$ mapeia o conjunto $\{0, 1, \ldots, n\}$ nele mesmo, existem nesse conjunto tantos elementos de S e quanto não elementos de S. ■

5.2 ANÉIS NÃO RAMIFICADOS

Nesta seção apresentaremos diferentes caracterização de um anel que será mais tarde definido como anel Gorenstein. Os resultados apresentados aqui podem ser encontrados em [B].

Considere R um anel comutativo com unidade. O **anel total de frações** de R é definido por:

$$Q(R) = \left\{ \frac{a}{b};\ \ a, b \in R,\ b \text{ não é divisor de zero em } R \right\},$$

onde $a/b = c/d$ se, e somente se, $ad - bc = 0$ em R.

O anel $Q(R)$ é o menor anel contendo R tal que todos os elementos não divisores de zeros são invertíveis.

Definição 5.14. Um **ideal** I em $Q(R)$ é um R-módulo para o qual existe um não divisor de zero $t \in R$ tal que

$$t \cdot I := \{ta;\ \ a \in I\} \subseteq R.$$

O ideal I é chamado **inteiro** se $I \subseteq R$.

Observação 5.15. Se o anel R é noetheriano, os ideais de $Q(R)$ são R-módulos finitamente gerados. De fato, para $I \subset Q(R)$ ideal, existe $t \in R$, não divisor de zero, tal que $t \cdot I \subset R$. Como R é noetheriano temos $tI = \langle a_1, a_2, \ldots, a_n \rangle$, ou seja,

$$I = \left\langle \frac{a_1}{t}, \frac{a_2}{t}, \ldots, \frac{a_n}{t} \right\rangle$$

como R-módulo.

Definição 5.16. Seja I um ideal de $Q(R)$. Definimos o **inverso** de I, denotado por I^{-1}, como:

$$I^{-1} = \{x \in Q(R);\ \ x \cdot I \subseteq R\}.$$

Observe que se I contém um elemento de R não divisor de zero, então I^{-1} é um ideal.

Definição 5.17. Sejam I e J ideais em $Q(R)$. O **ideal quociente** de I por J é o ideal de R definido por:

$$(I : J) = \{x \in R;\ \ x \cdot J \subseteq I\}.$$

Definição 5.18. Seja $a \in Q(R)$. Denotamos por $\langle a \rangle := a \cdot R$, o **ideal gerado** por a.

Proposição 5.19. *Sejam I e J ideais em $Q(R)$. Então:*

1. *Se $I \supseteq J$, então $I^{-1} \subseteq J^{-1}$.*
2. *$I \subseteq (I^{-1})^{-1}$ e $\left((I^{-1})^{-1}\right)^{-1} = I^{-1}$.*
3. *Se $a \in Q(R)$ é um não divisor de zero, então $\langle a \rangle^{-1} = \langle a^{-1} \rangle$ e $(a \cdot I)^{-1} = a^{-1} \cdot I^{-1}$.*
4. *Se $a \in Q(R)$ é não divisor de zero e $a \in I$, então $\langle a \rangle : I = a \cdot I^{-1}$.*

Demonstração.

1. Se $x \in I^{-1}$, então $x \cdot I \subseteq R$. Como $I \supseteq J$, então $x \cdot J \subseteq R$, ou seja, $x \in J^{-1}$. Portanto, $I^{-1} \subseteq J^{-1}$.

2. Primeiro vamos mostrar que $I \subseteq (I^{-1})^{-1}$. Por definição,

$$I^{-1} = \{x \in Q(R);\ \ x \cdot I \subseteq R\} \Rightarrow I^{-1} I \subseteq R \Rightarrow I \subseteq \left(I^{-1}\right)^{-1}.$$

Agora vamos mostrar que $\left((I^{-1})^{-1}\right)^{-1} = I^{-1}$. Pela primeira parte deste item temos $I \subseteq (I^{-1})^{-1}$ e, pelo item anterior, temos

$$\left(\left(I^{-1}\right)^{-1}\right)^{-1} \subseteq I^{-1}.$$

Novamente, pela primeira parte deste item, temos $I^{-1} \subseteq \left((I^{-1})^{-1}\right)^{-1}$. Logo,

$$I^{-1} = \left(\left(I^{-1}\right)^{-1}\right)^{-1}.$$

3. Vamos mostrar que $\langle a\rangle^{-1} = \langle a^{-1}\rangle$, onde $a \in Q(R)$ é não divisor de zero. Seja $x \in \langle a\rangle^{-1}$. Então

$$x \cdot \langle a\rangle \subseteq R \Rightarrow xa \in R \Rightarrow xa = r \in R \Rightarrow x = a^{-1}r \Rightarrow x \in \left\langle a^{-1}\right\rangle.$$

Por outro lado, se $x \in \langle a^{-1}\rangle$, então $x = a^{-1}r$, com $r \in R$. Como $xa = r \in R$, temos $x \in \langle a^{-1}\rangle$, isto é, $\langle a^{-1}\rangle \subseteq \langle a\rangle^{-1}$.

Mostraremos agora que $(a \cdot I)^{-1} = a^{-1} \cdot I^{-1}$. Temos que

$$x \in (a \cdot I)^{-1} \Leftrightarrow x(a \cdot I) \subseteq R \Leftrightarrow (xa)I \subseteq R \Leftrightarrow x \in a^{-1} \cdot I^{-1}.$$

4. Seja $a \in Q(R)$ um não divisor de zero. Então

$$a \cdot I^{-1} = \{x \in Q(R);\ \ x = ay \ \text{ e } \ yI \subseteq R\} = \left\{x \in Q(R);\ \ \frac{x}{a} \cdot I \subseteq R\right\} = \\ = \{x \in Q(R);\ \ x \cdot I \subseteq \langle a\rangle\}.$$

Logo, $(a \cdot I^{-1}) \bigcap R = \langle a\rangle : I$. Se $a \in I$, então $a \cdot I^{-1} \subseteq R$ e $(a \cdot I^{-1}) \bigcap R = a \cdot I^{-1}$. Portanto, $\langle a\rangle : I = a \cdot I^{-1}$. ■

De agora em diante vamos supor que R é um anel local, unidimensional e noetheriano, cujo o ideal maximal será denotado por $\mathfrak{m}$.

Proposição 5.20. *Todo ideal inteiro ($I \subset R$) que contém um não divisor de zero é um ideal $\mathfrak{m}$-primário.*

Demonstração. Se R é um anel noetheriano e $D(R)$ é o conjunto de divisores de zero de R. Então,

$$D(R) = \bigcup_{i=1}^{m} p_i, \ \text{ onde } \ p_i's \ \text{ são os ideais primos pertencentes ao ideal } \ \langle 0\rangle.$$

A demonstração desta afirmação pode ser encontrada em [AM], Cap. 4, Prop. 4.7. Se o ideal $I \subset R$ tem um elemento x não divisor de zero, então $x \notin p_j$, para todo primo pertencente ao $\langle 0\rangle$. Em particular, x não pertence a nenhum ideal primo minimal de R.

Sejam $I = \bigcap_{j=1}^{n} I_j$, uma decomposição primária (minimal) de I e q_j o radical de I_j, para todo $j = 1, 2, \ldots, n$. Então q_j é um ideal primo de R, para todo $j = 1, 2, \ldots, n$ e, como $\langle 0 \rangle \subset q_j$, para todo $j = 1, 2, \ldots, n$, temos que $p_i \subset q_j$, para algum p_i primo minimal de R (isto é, algum primo minimal dentre os ideais primos pertencentes ao $\langle 0 \rangle$). Agora, usando que R é um anel local com ideal maximal $\mathfrak{m}$, temos $p_i \subset q_j \subseteq \mathfrak{m}$. Finalmente, usando que R tem dimensão 1 e que $p_i \neq q_j$, pois $x \in I \subset q_j$ e $x \neq p_i$, concluímos que $q_j = \mathfrak{m}$, para todo $j = 1, 2, \ldots, n$. Logo, $j = 1$ e I é $\mathfrak{m}$-primário. ■

Observação 5.21. Nos casos em que estaremos interessados, o anel R será o anel local de uma curva irredutível em um ponto singular. Portanto, será um domínio de integridade e a Proposição 5.20 será verdadeira para todo ideal I de R.

Proposição 5.22. *Para todo ideal inteiro I de R, contendo um não divisor de zero, o anel R/I é um R-módulo de comprimento finito. Além disso, também tem comprimento finito o R-módulo J/I, onde J é um ideal inteiro contendo I.*

Demonstração. Seja I um ideal inteiro de R. Como R é noetheriano, R/I também é (Proposição 2.44). Vamos mostrar que R/I é um anel artiniano. Pela Proposição 5.20, I é $\mathfrak{m}$-primário. Seja $P \subset R$ ideal primo tal que $I \subset P$. Então $\sqrt{I} = \mathfrak{m} \subset \sqrt{P} = P$, e como $\mathfrak{m}$ é maximal, segue que $P = \mathfrak{m}$. Logo, $\overline{\mathfrak{m}} \subset R/I$ é o único ideal primo (e também maximal) de R/I, donde concluímos que R/I tem dimensão zero. Pelo Teorema 8.5 de [AM], temos que R/I é artiniano. Por fim, segue da Proposição 2.47 que R/I tem comprimento finito. Como todo submódulo de um módulo de comprimento finito também tem comprimento finito, se J for um ideal inteiro contendo I, então $J/I \subset R/I$ tem comprimento finito. ■

Para o próximo teorema é útil observar que se c é um divisor de zero em $Q(R)$, a função

$$\begin{array}{rccc} \varphi : Q(R) & \to & Q(R) \\ x & \mapsto & cx \end{array}$$

é um isomorfismo de R-módulos em $Q(R)$. Em particular, para ideias $I \subseteq J \subseteq Q(R)$, temos

$$\frac{I}{J} \simeq \frac{c \cdot I}{c \cdot J}.$$

Teorema 5.23. *Seja R um anel local unidimensional, noetheriano e local, cujo o ideal maximal $\mathfrak{m}$ contém um elemento não divisor de zero. As seguintes condições são equivalentes:*

(i) O comprimento de $\mathfrak{m}^{-1}/R$, denotado por $l(\mathfrak{m}^{-1}/R)$ é igual a 1.

(ii) Para todo $\alpha \in \mathfrak{m}$ não divisor de zero, tem-se $l\left(\dfrac{\langle \alpha \rangle : \mathfrak{m}}{\langle \alpha \rangle}\right) = 1$.

(iii) Para todo $\alpha \in \mathfrak{m}$ não divisor de zero, o ideal $\langle\alpha\rangle$ é irredutível.

(iv) Para todo ideal $I \subset Q(R)$, contendo um não divisor de zero, tem-se $I = (I^{-1})^{-1}$.

(v) Para todo ideal inteiro $I \subset R$, contendo um não divisor de zero tem-se

$$l(I^{-1}/R) = l(R/I).$$

Demonstração. $(i) \Rightarrow (ii)$ Seja $\alpha \in \mathfrak{m}$ um não divisor de zero. Pelo item *4* da Proposição 5.19 temos $\langle\alpha\rangle : \mathfrak{m} = \alpha \cdot \mathfrak{m}^{-1}$. Como $l(\mathfrak{m}^{-1}/R) = 1$ por hipótese e

$$\frac{\alpha \cdot \mathfrak{m}^{-1}}{\langle\alpha\rangle} = \frac{\alpha \cdot \mathfrak{m}^{-1}}{\alpha \cdot R} \simeq \frac{\mathfrak{m}^{-1}}{R}$$

temos

$$l\left(\frac{\langle\alpha\rangle : \mathfrak{m}}{\langle\alpha\rangle}\right) = l\left(\frac{\alpha \cdot \mathfrak{m}^{-1}}{\langle\alpha\rangle}\right) = l\left(\frac{\mathfrak{m}^{-1}}{R}\right) = 1.$$

$(ii) \Rightarrow (iii)$ Pela Proposição 5.20, o ideal $q = \langle\alpha\rangle$, onde $\alpha \in \mathfrak{m}$ é um não divisor de zero, é um ideal $\mathfrak{m}$-primário. Suponhamos $l\left(\dfrac{q : \mathfrak{m}^{-1}}{q}\right) = 1$. Vamos mostrar que q é irredutível.

Primeiro mostraremos que a condição $l((q : \mathfrak{m})/q) = 1$, onde q é $\mathfrak{m}$-primário, implica que o conjunto de todos os ideais de R que contém q propriamente possui o ideal $(q : \mathfrak{m})$ como menor elemento. Seja I um ideal de R tal que $q \subsetneq I$. Afirmamos que q está contido estritamente em $(q : \mathfrak{m}) \cap I$. De fato, segue da definição de $q : \mathfrak{m}$ que

$$q \subset q : \mathfrak{m} \Rightarrow q \subset (q : \mathfrak{m}) \cap I.$$

Além disso, se q é $\mathfrak{m}$-primário, como todo ideal em R é finitamente gerado (R é noetheriano), existe $s \geq 1$ tal que $\mathfrak{m}^s \subseteq q$ ($\mathfrak{m} = \sqrt{q}$) e, portanto, $I\mathfrak{m}^s \subseteq q$. Escolha s tal que $I\mathfrak{m}^s \subseteq q$ mas $I\mathfrak{m}^{s-1} \nsubseteq q$. Então, existe $\beta \in I\mathfrak{m}^{s-1} \subset I$ tal que $\beta \notin q$ e $\beta\mathfrak{m} \subset I\mathfrak{m}^s \subset q$. Donde segue que

$$\beta \notin q, \;\; \beta \in I \;\text{ e }\; \beta\mathfrak{m} \subset q \Rightarrow \beta \in (q : \mathfrak{m}) \cap I \;\text{ e }\; \beta \notin q.$$

Logo, $q \subsetneq (q : \mathfrak{m}) \cap I$ e assim, $q \subsetneq (q : \mathfrak{m}) \cap I \subseteq (q : \mathfrak{m})$. Mas $l(q : \mathfrak{m}/q) = 1$ significa que não existem ideais entre q e $(q : \mathfrak{m})$, ou seja, $(q : \mathfrak{m}) \cap I = (q : \mathfrak{m})$. Logo, $(q : \mathfrak{m}) \subseteq I$ e $(q : \mathfrak{m})$ é o menor ideal que contém q propriamente.

Agora mostraremos que q é irredutível. Suponhamos $q = I_1 \cap I_2$, onde I_1 e I_2 são ideais de R tais que $q \subsetneq I_1$ e $q \subsetneq I_2$. Então, pelo que mostramos no parágrafo anterior, $(q : \mathfrak{m}) \subseteq I_1$ e $(q : \mathfrak{m}) \subseteq I_2$, isto é,

$$(q : \mathfrak{m}) \subseteq I_1 \cap I_2 = q \Rightarrow (q : \mathfrak{m}) = q.$$

Contradição. Pois $l((q : \mathfrak{m})) = 1$. Logo, $q = I_1$ ou $q = I_2$.

$(iii) \Rightarrow (iv)$ Segue da definição que para cada ideal $I \subset Q(R)$, existe $t \in R$, não divisor de zero, tal que $J = tI \subset R$. Neste caso, $(I^{-1})^{-1} = t^{-1}(J^{-1})^{-1}$. Então, sem perda de generalidade, podemos assumir que $I \subseteq R$. Seja $\alpha \in I$ um não divisor de zero. Do item *(iii)*, segue que $\langle\alpha\rangle$ é irredutível e de [G], Teorema 7, temos $I = \langle\alpha\rangle : (\langle\alpha\rangle : I)$. Pelo item *4* da Proposição 5.19, temos $\langle\alpha\rangle : I = \alpha \cdot I^{-1}$ e, portanto,

$$I = \langle\alpha\rangle : (\langle\alpha\rangle : I) = \langle\alpha\rangle : (\alpha \cdot I^{-1})^{-1} = \alpha \cdot (\alpha \cdot I^{-1})^{-1} = \alpha\alpha^{-1}(I^{-1})^{1} = (I^{-1})^{-1}.$$

Na penúltima igualdade usamos o item 3 da Proposição 5.19. Logo, $I = (I^{-1})^{-1}$.

$(iv) \Rightarrow (v)$ Seja

$$I = I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_r = R$$

uma série de composição. Invertendo a série, obtemos

$$I^{-1} = I_0^{-1} \supseteq I_1^{-1} \supseteq \cdots \supseteq I_r^{-1} = R.$$

Se $I_i^{-1} = I_{i+1}^{-1}$, para algum i, invertendo novamente a cadeia temos

$$I_i = \left(I_i^{-1}\right)^{-1} = \left(I_{i+1}^{-1}\right)^{-1} = I_{i+1},$$

contradizendo a hipótese dos I_j's formarem uma série de composição. Então

$$I^{-1} = I_0^{-1} \supsetneq I_1^{-1} \supsetneq \cdots \supsetneq I_r^{-1} = R,$$

e, portanto, $l(I^{-1}/R) \geq l(R/I)$.

Por outro lado, começando com uma série de composição entre I^{-1} e R, obtemos, como feito anteriormente, uma cadeia entre I e R e $l(R/I) \geq l(I^{-1}/R)$.

Portanto, $l(R/I) = l(I^{-1}/R)$.

$(v) \Rightarrow (i)$ Como o ideal $\mathfrak{m}$ contém um não divisor de zero e, por hipótese, $l(\mathfrak{m}^{-1}/R) = l(R/\mathfrak{m}) = 1$, concluímos que $l(\mathfrak{m}^{-1}/R) = 1$, já que $l(R/\mathfrak{m}) = 1$ ($R/\mathfrak{m}$ é um corpo). ■

Nosso objetivo agora é dar alguns exemplos de anéis satisfazendo as propriedades do Teorema 5.23. Para isso, vamos apresentar mais alguns resultados.

Teorema 5.24. *Sejam R um anel local, noetheriano, unidimensional e $I \subset R$ um ideal inteiro. Suponha que I contém um não divisor de zero e é gerado por dois elementos. Então*

$$l(I^{-1}/R) = l(R/I).$$

Demonstração. Vamos supor inicialmente que $I = \langle a, b\rangle$, com $a, b \in R$ não divisores de zero. Considere as inclusões $R \supseteq I \supseteq \langle a\rangle$. Como a é um não divisor de zero, $R/\langle a\rangle$ tem comprimento finito e, da sequência exata

$$0 \longrightarrow \frac{I}{\langle a\rangle} \longrightarrow \frac{R}{\langle a\rangle} \longrightarrow \frac{R}{I} \longrightarrow 0,$$

segue que $l(R/I) = l(R/\langle a\rangle) - l(I/\langle a\rangle)$. A função

$$\begin{array}{rccc} \phi: & R & \longrightarrow & I/\langle a\rangle \\ & x & \mapsto & xb + \langle a\rangle \end{array}$$

é claramente um R-homomorfismo sobrejetor, cujo núcleo é o ideal

$$\mathrm{Ker}(\phi) = \{x \in R;\ \ xb \in \langle a\rangle\} = \{x \in R;\ \ x \cdot I \subseteq \langle a\rangle\} = \langle a\rangle : I = a \cdot I^{-1}.$$

A última igualdade segue do item 4 da Proposição 5.19. Logo, $R/a \cdot I^{-1} \simeq I/\langle a\rangle$.

Então

$$l(R/I) = l(R/\langle a\rangle) - l(I/\langle a\rangle) = l(R/\langle a\rangle) - l(R/a \cdot I^{-1}).$$

Além disso, $I^{-1} \supseteq R$, $R \supseteq a.I^{-1} \supseteq \langle a\rangle$ e a sequência

$$0 \longrightarrow \frac{a \cdot I^{-1}}{\langle a\rangle} \longrightarrow \frac{R}{\langle a\rangle} \longrightarrow \frac{R}{a \cdot I^{-1}} \longrightarrow 0,$$

é exata. Portanto, $l(a \cdot I^{-1}/a \cdot R) = l(R/\langle a\rangle) - l(R/a \cdot I^{-1})$. Assim, temos

$$l(R/I) = l(R/\langle a\rangle) - l(R/a.I^{-1}) = l(a.I^{-1}/a.R) = l(I^{-1}/R).$$

A demonstração de que podemos supor que I é gerado por dois elementos não divisores de zero será feita no lema a seguir. ■

Lema 5.25. *Nas condições do Teorema 5.24, o ideal I pode ser gerado por dois elementos não divisores de zero.*

Demonstração. Suponhamos inicialmente que $I = \langle a, b\rangle$ com a ou b não divisor de zero. Sem perda de generalidade, podemos supor que a é não divisor de zero. Vamos mostrar que existe $b' \in R$, não divisor de zero, da forma $b' = b_1 a + b$, para algum $b_1 \in R$. Neste caso, $I = \langle a, b\rangle = \langle a, b'\rangle$ como desejamos.

Seja $D(R)$ o conjunto de divisores de R. Como R é um anel noetheriano, temos

$$D(R) = \bigcup_{i=1}^{m} P_i;\ \ P_i\text{'s são ideais primos de } R, \text{pertencentes ao ideal } \langle 0\rangle .$$

Suponhamos $b \in D(R)$. Se $b \in P_i$, para todo $i = 1, \ldots, m$, tomamos $b_1 = 1$. Então, $b' = a + b \notin D(R)$ pois, caso contrário, $a + b \in P_j$, para algum j e, neste caso, $a \in P_j$. Absurdo, pois a não é divisor de zero. Se $b \in P_1, \ldots, P_l$ e $b \notin P_{l+1}, \ldots, P_m$. Seja $b_1 \in \bigcap_{i=l+1}^{m} P_i$ tal que $b_1 \notin \bigcup_{i=1}^{l} P_i$. Observe que só não existiria tal elemento b_1 se

$$\bigcap_{i=l+1}^{m} P_i \subset \bigcup_{i=1}^{l} P_i$$

o que implicaria $\bigcap_{i=l+1}^{m} P_i \subset P_k$, para algum $1 \leq k \leq l$ e consequentemente, $P_t \subset P_k$ para algum $l+1 \leq t \leq m$. Mas R é local e os P_i's são primos distintos. Assim,

$$P_t \subsetneq P_k \subsetneq \mathfrak{m}, \tag{5.1}$$

onde a última inclusão é estrita porque $\mathfrak{m}$ não pode ser igual a nenhum dos P_i's já que, por hipótese, $\mathfrak{m} \not\subset D(R)$. A cadeia (5.1) contradiz o fato de R ser unidimensional. Afirmamos que $b' = b_1 a + b \notin D(R)$. De fato, se $b' \in D(R)$, então $b' = b_1 a + b \in P_r$, para algum $r = 1, \ldots, m$. Se $r \leq l$, temos $b_1 a \in P_r$, pois $b \in P_1, \ldots, P_l$. Mas isto é impossível uma vez que P_r é primo e $a, b_1 \notin \bigcup_{i=1}^{l} P_i$. Por outro lado, se $r \geq l+1$, então $b = b' - b_1 a \in P_r$, absurdo pois $b \notin P_{l+1}, \ldots, P_m$.

Agora, suponhamos $a, b \in D(R)$ e seja $c \in I$ não divisor de zero. Tal elemento existe por hipótese. Então $I = \langle c, a, b \rangle$. Aplicando o raciocínio anterior, podemos encontrar $a' = a_1 c + a$, $b' = b_1 c + b \in R$, não divisores de zero, de modo que $I = \langle c, a', b' \rangle$. Seja $\mathfrak{m}$ o ideal maximal de R. Então, $I/\mathfrak{m}I$ é um $R/\mathfrak{m}$-espaço vetorial de dimensão menor ou igual a 2, já que I pode ser gerado por dois elementos. Então $\{c + \mathfrak{m}I, a' + \mathfrak{m}I, b' + \mathfrak{m}I\}$ gera $I/\mathfrak{m}I$ e é LD. Excluindo o elemento que é combinação dos outros dois, temos que $I/\mathfrak{m}I$ é gerado por dois deles. Sem perda de generalidade, $I/\mathfrak{m}I$ é gerado por $\{c + \mathfrak{m}I, a' + \mathfrak{m}I\}$, ou seja, $I = \langle c, a' \rangle + \mathfrak{m}I$. Usando um dos corolários do Lema de Nakayama (ver [AM], Corolário 2.7) temos $I = \langle c, a' \rangle$.

■

Corolário 5.26. *Seja R um anel noetheriano, local de dimensão 1, cujo o ideal maximal $\mathfrak{m}$ contém não divisor de zero e tal que $\mathfrak{m}$ é gerado por dois elementos. Então $l(\mathfrak{m}/R) = 1$.*

Demonstração. Como $l(R/\mathfrak{m}) = 1$, o resultado segue do Teorema 5.24. ■

A próxima proposição nos dá exemplos de anéis locais satisfazendo as condições do Corolário 5.26 e por conseguinte o Teorema 5.23.

Proposição 5.27. *O conjunto dos anéis noetherianos, locais e unidimensionais tais que o ideal maximal é gerado por dois elementos e contém um não divisor de zero, incluem os seguintes tipos de anéis:*

(i) $R = A/I$ é um anel local regular de dimensão 2 e $I \subset A$ é um ideal principal de A diferente de $\langle 0 \rangle$ e $\langle 1 \rangle$.

(ii) R é o anel local de uma curva algébrica plana C em um ponto simples p.

Demonstração. Ver [B], Teorema 4, página 101. ■

5.3 ANÉIS GORENSTEIN

Sejam R um anel local, noetheriano, unidimensional, com ideal maximal $\mathfrak{m}$ e $Q(R)$ o seu anel total de frações.

Definição 5.28. Dizemos que R é um anel **Gorenstein** se existe $a \in \mathfrak{m}$, não divisor de zero, tal que o ideal gerado por a é irredutível.

Teorema 5.29. *Seja R um anel local, noetheriano, unidimensional e com ideal maximal $\mathfrak{m}$. Suponha que $\mathfrak{m}$ contém um não divisor de zero. As seguintes afirmações são equivalentes:*

(i) *R é um anel Gorenstein.*

(ii) *Todo ideal principal de R, gerado por um elemento não divisor de zero é, irredutível.*

(iii) *O comprimento do R-módulo $\mathfrak{m}^{-1}/R$ é 1;*

(iv) *Para todo ideal $I \subset R$, contendo um não divisor de zero, vale $(I^{-1})^{-1} = I$*

Demonstração. Seja $\alpha \in \mathfrak{m}$ tal que $\langle\alpha\rangle$ é irredutível. Então, $\mathfrak{m} = \langle\alpha\rangle : (\langle\alpha\rangle\,;\mathfrak{m})$ e, pelo item *4* da Proposição 5.19, temos $\mathfrak{m} = (\mathfrak{m}^{-1})^{-1}$. Como $\mathfrak{m} \subset R$ é uma série de composição maximal, temos que $\mathfrak{m} \subset R \subset \mathfrak{m}^{-1}$ também é maximal. Logo, o comprimento de $\mathfrak{m}^{-1}/R$ é igual a 1. As equivalências então seguem direto do Teorema 5.23. ■

Definição 5.30. Seja $\bar{R}$ o fecho integral de R em $Q(R)$. O **ideal condutor** de R em $\bar{R}$ é definido por

$$\mathcal{C} := R : \bar{R} = \{r \in R;\ \ r\bar{R} \subseteq R\}.$$

Lema 5.31. *$\mathcal{C}$ é um ideal de R (e também de $\bar{R}$). Além disso, $\mathcal{C}$ é o maior ideal de $\bar{R}$ contido em R.*

Demonstração. Sejam $c_1, c_2 \in \mathcal{C}$ e $r \in R$. Então,

$$\begin{gathered}(c_1 + c_2)\bar{R} = c_1\bar{R} + c_2\bar{R} \subset R + R = R \text{ e} \\ (rc)\bar{R} = r(c\bar{R}) \subset rR \subset R.\end{gathered}$$

Logo, $\mathcal{C}$ é um ideal de R. Além disso, se $\alpha \in \bar{R}$ e $c \in \mathcal{C}$, então

$$(\alpha c)\bar{R} = \alpha(c\bar{R}) \subset \alpha R \subset \bar{R}.$$

Portanto, $\mathcal{C}$ é também um ideal de $\bar{R}$. Para terminar, seja I um ideal de $\bar{R}$ contido em R. Então, $\bar{R}I \subset I \subset R$, e, portanto, $I \subset \mathcal{C}$. ■

Suponhamos agora que $\bar{R}$ é um R-módulo finitamente gerado. Então $\mathcal{C}$ contém um não divisor de zero. De fato, se

$$\bar{R} = R\frac{m_1}{s_1} + R\frac{m_2}{s_2} + \cdots + R\frac{m_n}{s_n},$$

onde $\dfrac{m_i}{s_i} \in \bar{R} \subset Q(R)$ e s_i é um não divisor de zero, para todo $1 \leq i \leq n$, então $s = s_1 s_2 .... s_n \in R$ é não divisor de zero e $s\bar{R} \subset Rm_1 + \cdots + Rm_n \subset R$.

Proposição 5.32. *Se R é um anel Gorenstein tal que $\bar{R}$ é finitamente gerado como R-módulo, então o comprimento do R-módulo $\bar{R}/\mathcal{C}$ é $2d$, onde d é o comprimento de $R/\mathcal{C}$.*

Demonstração. Seja

$$\mathcal{C} = \mathfrak{a}_0 \subset \cdots \subset \mathfrak{a}_{d-1} \subset R$$

uma cadeia maximal de ideais em R. Afirmamos que

$$\mathcal{C} = \mathfrak{a}_0 \subset \cdots \subset \mathfrak{a}_{d-1} \subset R \subset \mathfrak{a}_{d-1}^{-1} \subset \cdots \subset \mathfrak{a}_0^{-1} = \mathcal{C}^{-1} = \bar{R}$$

é uma cadeia maximal de R-submódulos de $\bar{R}$.

Primeiro vamos mostrar que $\mathcal{C}^{-1} = \bar{R}$. De fato,

$$\bar{R}^{-1} = \{x \in Q(R);\ \ x\bar{R} \subset R\} \Rightarrow x \cdot 1_{\bar{R}} \in R,\ \ \forall x \in \bar{R}^{-1} \Rightarrow \bar{R}^{-1} \subset R.$$

Como $\bar{R}^{-1}\bar{R} \subset R$, concluímos que $\bar{R}^{-1} \subset \mathcal{C}$. Da definição de $\mathcal{C}$ segue que $\mathcal{C}\bar{R} \subset R$, o que implica que $\mathcal{C} \subset \bar{R}^{-1}$. Logo, $\mathcal{C} = \bar{R}^{-1}$.

Agora, usando que $\bar{R}$ é um R-módulo finitamente gerado, existe $t \in R$, não divisor de zero, tal que $t\bar{R} = I \subset R$ e, como R é Gorenstein, temos

$$I = (I^{-1})^{-1} = ((t\bar{R})^{-1})^{-1} = (t^{-1}\bar{R}^{-1})^{-1} = t(\bar{R}^{-1})^{-1} \Rightarrow \bar{R} = (\bar{R}^{-1})^{-1}.$$

Concluímos então que $\mathcal{C}^{-1} = (\bar{R}^{-1})^{-1} = \bar{R}$.

Finalmente, $(\mathfrak{a}_i^{-1})^{-1} = \mathfrak{a}_i$, para todo $i = 0, 1, \ldots, d-1$, pois R é Gorenstein, implica que $R \subset \mathfrak{a}_{d-1}^{-1} \subset \cdots \subset \mathfrak{a}_0^{-1} = \mathcal{C}^{-1} = \bar{R}$ é uma cadeia maximal. Portanto, o comprimento $l(\bar{R}/\mathcal{C}) = 2d$. ■

5.4 SEMIGRUPOS DE VALORES DE ANÉIS GORENSTEIN

Veremos agora como a teoria dos semigrupos numéricos pode ser usada para caracterizar anéis Gorenstein.

Na próxima definição usaremos o conceito de $\mathfrak{m}$-ádico completamento de um anel local R cuja definição e principais resultados podem ser encontrados com detalhes em [AM]. Porém, não os apresentaremos aqui porque o completamento será usado somente para caracterizar o fecho inteiro do anel R

Definição 5.33. Seja R um anel local, noetheriano, unidimensional e tal que seu ideal maximal $\mathfrak{m}$ contém um não divisor de zero. Dizemos R é **analiticamente irredutível** se seu $\mathfrak{m}$-ádico completamento $\hat{R}$ é um domínio de integridade.

Observação 5.34. Se um anel R é analiticamente irredutível, então R é um domínio de integridade, pois $R \subset \hat{R}$. Neste caso, o anel total de frações de R, $Q(R)$, é um corpo.

Teorema 5.35. *O anel R é analiticamente irredutível se, e somente se, $\bar{R}$ é um domínio de valorização discreta e um R-módulo finitamente gerado.*

Demonstração. Ver [M], Teorema 7.1, página 68. ■

O Teorema 5.35 garante que existe uma valorização

$$v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

tal que $\bar{R} = \{x \in \mathbb{K};\ v(x) \geq 0\}$ e $\mathbb{K}$ é o corpo de frações de R. Como $R \subseteq \bar{R}$, podemos definir o conjunto de valores de R por

$$v(R) = \{v(x);\ x \in R \setminus \{0\}\} \subset \mathbb{N}.$$

Proposição 5.36. *Sejam R um anel analiticamente irredutível, $\bar{R}$ seu fecho inteiro e $\mathbb{K}$ o corpo de frações de R. Seja $v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$ a valorização definida por $\overline{R}$. Então $S = v(R)$ é um semigrupo numérico.*

Demonstração. Temos:

(i) $0 \in S$, pois $v(1) = 0$;

(ii) Sejam $a, b \in S$. Então existem $x, y \in R$ tais que $a = v(x)$, $b = v(y)$. Logo,

$$a + b = v(x) + v(y) = v(xy) \in S.$$

(iii) Sejam $\mathcal{C} = \{x \in R;\ x\bar{R} \subset R\}$ o ideal condutor de R em $\bar{R}$ e

$$c = \min\{v(x);\ x \in \mathcal{C} \text{ e } x \neq 0\}.$$

Afirmamos que $S = v(R) \supset \{c + n;\ \forall n \in \mathbb{N}\}$. De fato, se $z \in \mathbb{K}$ é tal que $v(z) = c + n$, para algum $n \in \mathbb{N}$, e se $c = v(x)$, com $x \in \mathcal{C} \setminus \{0\}$, então

$$v(z) = c + n = v(x) + n \Rightarrow v(z) - v(x) = n \geq 0 \Rightarrow v(z/x) \geq 0$$
$$\Rightarrow z/x \in \bar{R} \Rightarrow z = x\bar{r};\ \bar{r} \in \bar{R} \Rightarrow z \in R\ (x \in \mathcal{C}) \Rightarrow v(z) = c + n \in v(R).$$

Concluímos assim $\mathbb{N} \setminus S$ é finito e $S = v(R)$ é um semigrupo numérico. ■

Definição 5.37. O semigrupo $v(R)$ é denominado **semigrupo de valores** do anel R.

Queremos uma condição necessária e suficiente para que o anel R seja Gorenstein em termos de semigrupo de valores de R. Antes disso faremos uma ligação entre o ideal condutor de R em $\bar{R}$ e o condutor numérico do seu semigrupo $v(R)$.

Observação 5.38. No que segue vamos supor que R é um anel **local, noetheriano, unidimensional e analiticamente irredutível**. Sejam $\mathbb{K}$ o corpo de frações de R e $\bar{R}$ o fecho inteiro de R. Também vamos supor que R e $\bar{R}$ possuem o **mesmo corpo residual**, isto é, $R/\mathfrak{m} \simeq \bar{R}/\mathfrak{M}$, onde $\mathfrak{m}$ e $\mathfrak{M}$ são os ideais maximais de R e $\bar{R}$, respectivamente. Esse é o caso sempre que o corpo residual de R for algebricamente fechado.

O próximo lema explicita a importância de supor que R e $\bar{R}$ possuem o mesmo corpo residual.

Lema 5.39. *Sejam R um anel como na Observação 5.38 e $\mathbb{K}$ o corpo de frações de R. Suponhamos $v(x) = v(y)$, para $x, y \in \mathbb{K} \setminus \{0\}$. Então, $v(x - ey) > v(y)$ para algum $e \in R$ invertível.*

Demonstração. Sejam $x, y \in \mathbb{K} \setminus \{0\}$ tais que $v(x) = v(y)$. Então,

$$0 = v(x) - v(y) = v(x/y) \Rightarrow x/y = u \in \bar{R} \text{ com } v(u) = 0.$$

Logo, $x = uy$, com $u \in \bar{R}$ invertível. Além disso, $u \in \bar{R}$ invertível significa que $u \notin \mathfrak{M}$, onde $\mathfrak{M}$ é o ideal maximal de $\bar{R}$. Usando que R e $\bar{R}$ possuem o mesmo corpo residual, temos que

$$\begin{aligned}\bar{0} \neq \bar{u} \in \bar{R}/\mathfrak{M} \simeq R/\mathfrak{m} \Rightarrow \exists\, e \in R \setminus \mathfrak{m};\ \bar{u} = \bar{e} \in \bar{R}/\mathfrak{M} \Rightarrow \\ u - e = m \in \mathfrak{M} \Rightarrow u = e + m \Rightarrow x = uy = (e + m)y \Rightarrow \\ x - ey = my \Rightarrow v(x - ey) = v(my) = v(m) + v(y) > v(y),\end{aligned}$$

pois $m \in \mathfrak{M}$ implica que $v(m) > 0$. ■

Proposição 5.40. *Seja $\mathcal{C} = \{x \in R;\ x\bar{R} \subset R\}$ o ideal condutor de R em $\bar{R}$ e*

$$c = \ min\{v(x);\ x \in \mathcal{C} \ \text{ e } \ x \neq 0\}.$$

Então,

$$\mathcal{C} = \{z \in \mathbb{K};\ v(z) \geq c\}$$

e c é o condutor do semigrupo $S = v(R)$.

Demonstração. A inclusão $\mathcal{C} \subset \{z \in \mathbb{K};\ v(z) \geq c\}$ segue da definição de c.

Agora sejam $z \in \mathbb{K}$ tal que $v(z) \geq c$ e $x \in \mathcal{C} \setminus \{0\}$ tal que $c = v(x)$. Então,

$$v(z) \geq v(x) \Rightarrow v(z) - v(x) \geq 0 \Rightarrow v(z/x) \geq 0$$

$$\Rightarrow z/x \in \bar{R} \Rightarrow z = x\,\bar{r};\ \bar{r} \in \bar{R} \Rightarrow z \in R\ (x \in \mathcal{C}).$$

Além disso, $z = x\bar{r}$, com $x \in \mathcal{C}$ e $\bar{r} \in \bar{R}$, implica

$$z\bar{R} \subset x\,\bar{r}\,\bar{R} \subset x\,\bar{R} \subset R \Rightarrow z \in \mathcal{C}.$$

Logo, $\mathcal{C} = \{z \in \mathbb{K};\ v(z) \geq c\}$. Observe que $\mathcal{C}$ sendo um ideal de $\bar{R}$ e $\bar{R}$ DVD e, portanto, um domínio de ideais principais, implicam que $\mathcal{C} = t^c\,\bar{R}$, para algum $t \in \bar{R}$ tal que $v(t) = 1$.

Agora devemos mostrar que c é o condutor de $S = v(R)$. Vimos na demonstração da Proposição 5.36, item *(iii)*, que

$$S = v(R) \supset \{c + n;\ \forall n \in \mathbb{N}\}.$$

Para terminar a demonstração, devemos mostrar que $c-1 \notin S = v(R)$. Suponhamos por absurdo que $c - 1 = v(r)$, para algum $r \in R$. Então, $v(r) = v(t^{(c-1)})$. Pelo Lema 5.39, existe $e \in R$ invertível, tal que

$$v(t^{(c-1)} - er) > v(r) = c - 1 \Rightarrow v(t^{(c-1)} - er) \geq c.$$

Portanto,

$$t^{(c-1)} - er \in \mathcal{C} \subset R \Rightarrow t^{(c-1)} \in R.$$

Afirmamos que $t^{(c-1)} \in R$ implica que $t^{(c-1)} \in \mathcal{C}$. De fato, dado $y \in \bar{R}$, seja $x \in R$, tal que $\bar{y} = \bar{x} \in R/\mathfrak{m} \simeq \bar{R}/\mathfrak{M}$. Então, $y - x \in \mathfrak{M}$ e $v(y - x) > 0$. Logo,

$$y\,t^{(c-1)} = \underbrace{(y - x)\,t^{(c-1)}}_{\in\,\mathcal{C}} + \underbrace{x\,t^{(c-1)}}_{\in\,R} \in R \Rightarrow t^{(c-1)} \in \mathcal{C}.$$

Absurdo, pois c é o menor valor dos elementos de $\mathcal{C}$. ■

Corolário 5.41. *Sejam R um anel como na Observação 5.38 e $\mathbb{K}$ o corpo de frações de R. Seja $x \in \mathbb{K}$, tal que $v(x - r) \in v(R)$, para todo $r \in R$. Então, $x \in R$.*

Demonstração. Seja $x \in \mathbb{K}$, tal que $v(x - r) \in v(R)$, para todo $r \in R$. Dado $r_1 \in R$ temos que $v(x - r_1) \in v(R)$, ou seja, existe $r_1' \in R$, tal que $v(x - r_1) = v(r_1')$. Pelo Lema 5.39, existe $e_1 \in R$, tal que

$$v(x - r_1 - e_1 r_1') = v(x - (r_1 + e_1 r_1')) > v(r_1').$$

Como $r_1 + e_1 r_1' \in R$ e $v(x - r) \in v(R)$, para todo $r \in R$, podemos aplicar o Lema 5.39 uma quantidade finita vezes para achar $r'' \in R$, tal que $v(x - r'') \geq c$, onde c é o condutor de $v(R)$. Logo, pela Proposição 5.40,

$$x - r'' \in \mathcal{C} \subset R \Rightarrow x \in R.$$

■

Teorema 5.42 (Teorema de Kunz)**.** *Sejam R um anel local, noetheriano, unidimensional e analiticamente irredutível, com ideal maximal $\mathfrak{m}$, $\bar{R}$ o fecho inteiro de R no seu corpo de frações $\mathbb{K}$ e $v : \mathbb{K} \to \mathbb{Z}$ a valorização correspondente. Suponha que R e $\bar{R}$ possuem o mesmo corpo de classe residual. Então R é um anel Gorenstein se, e somente se, o semigrupo de valor $v(R)$ é simétrico.*

Demonstração. ($\Rightarrow$) Suponhamos que $v(R)$ é um semigrupo simétrico, isto é, se c é o condutor de $v(R)$ e $n = c - 1$, então para $z \in v(R)$, temos que $n - z \notin v(R)$ e se $z \notin v(R)$ então $n - z \in v(R)$. Vamos mostrar que $\mathfrak{m}^{-1}/R$ é um R-módulo de comprimento 1 e, portanto, é Gorenstein. Afirmamos que

$$v(\mathfrak{m}^{-1}) = \{n\} \cup v(R). \tag{5.2}$$

Seja $x \in \mathfrak{m}^{-1}$, tal que $x \notin R$. Se $v(x) \in v(R)$ nada temos a fazer. Se $v(x) \notin v(R)$ então, $v(x) \leq n = c - 1$, pois c é o condutor de $v(R)$. Suponhamos por absurdo que $v(x) < n$. Como $v(R)$ é simétrico e $v(x) \notin v(R)$, temos que $n - v(x) \in v(R)$. Seja $r_1 \in R$ tal que $v(r_1) = n - v(x) > 0$. Observe que $v(x) < n$ implica que $v(r_1) > 0$ e, consequentemente, que $r_1 \in R \cap \mathfrak{M} = \mathfrak{m}$. Como $v(r_1 x) = n$ e $n \notin v(R)$ temos que $r_1 x \notin R$. Mas isto é uma contradição com o fato de

$$x \in \mathfrak{m}^{-1} = \{y \in \mathbb{K};\ y\,\mathfrak{m} \subset R\}.$$

Logo, $v(x) = n$, para todo $x \in \mathfrak{m}^{-1} \setminus R$.

Agora vamos usar a igualdade (5.2) para provar que

$$l(\mathfrak{m}^{-1}/R) = 1.$$

Seja N um submódulo de $\mathfrak{m}^{-1}$ tal que $R \subsetneq N \subset \mathfrak{m}^{-1}$. Afirmamos que $N = \mathfrak{m}^{-1}$. De fato, dados $x \in \mathfrak{m}^{-1} \setminus R$ e $y \in N \setminus R$, sejam $r, r' \in R$, tais $v(x-r), v(y-r') \notin v(R)$. A existência desses elementos é garantida pelo Corolário 5.41. Então, $v(x - r) = n = v(y - r')$ e, pela Proposição 5.39, existe $e \in R$ invertível, tal que

$$v((x - r) - e(y - r')) > v(y - r') = n = c - 1 \Rightarrow v((x - r) - e(y - r')) \geq c.$$

Pela Proposição 5.40, temos que

$$(x - r) - e(y - r') \in \mathcal{C} \subset R \subset N \Rightarrow x \in N,\ \text{pois } r, r', e \in R \text{ e } y \in N.$$

Logo, $N = \mathfrak{m}^{-1}$ e, portanto, $l(\mathfrak{m}^{-1}/R) = 1$.

($\Leftarrow$) Suponhamos que R é um anel Gorenstein e que

$$v_0 < v_1 < \cdots < v_{d-1}$$

são os números no conjunto $\{0, 1, \ldots, n\}$ que são valores de elementos de R, onde $n = c-1$ e c é o condutor de $v(R)$. Defina $I_i = \{r \in R;\ \ v(r) \geq v_i\}$, para $i = 0, \ldots, d-1$. Então

$$R = I_0 \supset I_1 \supset \cdots \supset I_{d-1} \supset \mathcal{C}$$

é uma cadeia de ideais de R estritamente decrescente. Afirmamos que essa cadeia é máxima pois, para todo $r \in R \setminus \{0\}$ tal que $v(r) = v_{i-1}$, temos $I_i + Rr = I_{i-1}$. De fato, dado $y \in I_{i-1}$ temos que $v(y) \geq v_{i-1} = v(r)$. Então, $y = ur$ para algum $u \in \bar{R}$ invertível. Pelo Lema 5.39, existe $e \in R$ tal que $v(y - er) > v(r) = v_{i-1}$, donde concluímos que $y - er \in I_i$, ou seja, $y \in I_i + Rr$. A inclusão contrária segue da definição dos $I_i's$ e de r. Logo, $l(R/\mathcal{C}) = d$. Como R é Gorenstein, temos pela Proposição 5.32 que $l(\bar{R}/\mathcal{C}) = 2d$. Além disso, como $\mathcal{C} = \bar{R}t^c$, onde $t \in \bar{R}$ é tal que $v(t) = 1$ e $c = n + 1$, temos que $l(\bar{R}/\mathcal{C}) = n + 1$. Logo, $n + 1 = 2d$ e, pela Proposição 5.13, $v(R)$ é simétrico. ■

Corolário 5.43. *Seja R um anel local noetheriano, unidimensional e analiticamente irredutível. Suponha que seu corpo residual é algebricamente fechado e seu ideal maximal é gerado por dois elementos. Então o semigrupo de valores de R é simétrico.*

Demonstração. Segue do Corolário 5.26 que $l(m^{-1}/R) = 1$. Logo, R é Gorenstein e, portanto, pelo Teorema 5.42 o semigrupo de valores de R é simétrico. ■

Observe que os anéis da Proposição 5.27 são também exemplos de anéis de Gorenstein.

Exemplo 5.44. Seja C a curva plana irredutível dada por $Y^2 = X^n$, onde $n = 2l + 1$. Sejam $p = (0, 0)$ o único ponto singular de C, $x = \overline{X}$ e $y = \overline{Y}$ as classes residuais de X e Y em $\mathbb{K}[X, Y]/\langle Y^2 - X^n \rangle$ e $R = k[x, y]_{\langle x,y \rangle}$ o anel local de C em p. Então, como vimos no Exemplo 4.35, $k(C) = k(t)$, onde $t = y/x^l$ e

$$k \subset R = k[t^2, t^n]_{\langle t^e, t^n \rangle} \subset k(t).$$

Considere $v = v_0 : k(t) \to \mathbb{Z} \cup \{\infty\}$ a úncia valorização de $k(t)/k$ tal que $\bar{R} = \mathcal{O}_v$. Então $v(t) = 1$ e

$$k \subset k[t^2, t^n] \subset R = k[t^2, t^n]_{\langle t^2, t^n \rangle} \subset \bar{R} = k[t]_{\langle t \rangle}.$$

Seja $S = v(R)$. Afirmamos que $S = \langle 2, n \rangle = \langle 0, 2, 4, \ldots, n-3, n-1, \longrightarrow \rangle$.

De fato, temos:

(i) $v(t^2) = 2$ e $v(t^n) = n$. Logo, $2, n \in S$ e

$$\langle 2, n \rangle = \langle 0, 2, 4, \ldots, n-3, n-1, \longrightarrow \rangle \subset S.$$

(ii) Como $n = 2l + 1$, um elemento genérico de R é da forma $z = f(t^2, t^n)/g(t^2, t^n)$, onde $f(T_1, T_2), g(T_1, T_2) \in k[T_1, T_2]$ são polinômios não nulos e $g(t^2, t^n) \notin \langle t^2, t^n \rangle$, ou seja, o termo constante de $g(T_1, T_2)$ é não nulo. Escreva

$$f(T_1, T_2) = \sum_{i+j=0}^{s} a_{ij} T_1^i T_2^j \in k[T_1, T_2] \text{ e}$$

$$f(t^2, t^n) = \sum_{i+j=0}^{s} a_{ij}(t^2)^i (t^n)^j = a_{00} + a_{10}t^2 + \cdots + a_{l0}t^{(2l)} + a_{01}t^n + \text{ termos de grau maior,}$$

onde $a_{ij} \in k$, para todo i, j. Daí segue que

$$v(f(t^2, t^n)) = \begin{cases} 0, & \text{se} \quad a_{00} \neq 0; \\ 2k, & \text{se} \quad a_{00} = a_{10} = \cdots = a_{(k-1)0} = 0 \text{ e } a_{k0} \neq 0, \text{ para } 0 < k < l; \\ a, & \text{com } a \geq n, \text{ se } a_{00} = a_{10} = \cdots = a_{l0} = 0 \end{cases}$$

e então $v(f(t^2, t^n))$ pode assumir qualquer valor inteiro positivo da forma k, com $0 < k < l$, ou qualquer $a \geq n$.

Analogamente, fazendo $g(T_1, T_2) = \sum_{i+j=0}^{r} = b_{ij} T_1^i T_2^j \in k[T_1, T_2]$, temos

$$g(t^2, t^n) = b_{ij}(t^2)^i (t^n)^j = b_{00} + b_{10}t^2 + \cdots + a_{l0}t^{(2l)} + b_{01}t^n + \text{ termos de grau maior.}$$

Como $b_{00} \neq 0, v(g(t^2, t^n)) = 0$. Logo,

$$v(z) = v(f(t^2, t^n)) - v(g(t^2, t^n)) = v(f(t^2, t^n)).$$

Então, $S \subset \{0, 2, 4, ..., n-3, n-1, \longrightarrow\} = \langle 2, n \rangle$. Logo,

$$S = \langle 2, n \rangle = \langle 0, 2, 4, ..., n-3, n-1, \longrightarrow \rangle .$$

Pelo diagrama da Figura 4 concluímos que S é simétrico.

	0	1	2	3	4	5	6	...	l
	●	○	●	○	●	○	●	...	●
●	○	●	○	●	○	●	○	...	○
$2l+1$	$2l$	$2l-1$	$2l-2$	$2l-3$	$2l-4$	$2l-5$	$2l-6$	...	l

Figura 4 – Diagrama do semigrupo $S = \langle 2, n = 2l + 1 \rangle$ e l par.

REFERÊNCIAS

[AM] ATIYAH, M. F., MACDONALD, I. G. **Introduction to Commutative Algebra**. University Oxford: Addison-Wesley Publishing Company, Inc, Massachusetts, 1969.

[B] BERGER, R. **Über eine Klasse unvergabelter lokaler Ringe**. Math. Ann. 146, 1962, 98-102, MR 27 #175.

[B1] BERGER, R. **Über den Singularitätsgrad von Teilringen in Funktionenkörpern**. Math. Z. 77, 1961, 228-240. MR24#A730.

[BDF] BARUCCI, V.; D'ANNA, M.; FRÖBERG, R. **Analytically unramified one-dimensional semilocal rings and their value groups**. Journal of Pure and Applied Algebra 144, 2000, 215-254.

[BF] BARUCCI, V.; FRÖBERG, R. **One-Dimensional Almmost Gorenstein Rings**. Journal of Algebra 188, 1997, 418-442.

[CDK] CAMPILLO, V.; DELGADO, F.; KIYEK, K. **Gorenstein property and symmetry for one-dimensional local Coehn-Macaulay ring**. Manuscripta Math. 83, 1994, 405-423.

[CS] COHEN, I. S.; SEIDENBERG, A. **Prime ideals and integral dependence**. Bull. Am. Math. Soc. 52, 252-262, 1946.

[D] D'ANNA, M. **The canonical module of a one-dimensional reduced ring**. Comm. Alegbra 25, 1997, 2939-2965.

[EO] ENDLER, O. **Valuation Theory**. New York: Springer-Verlag, 1972

[G] GRÖBNER, W. **Über irreduzible Ideale in kommutativen Ringen**. Math. Ann. 110, 197-222, 1934

[HR] HARTSHORNE, R. **Algebraic Geometry**. New York: Springer-Verlag, 1977.

[HT] HUNGERFORD, T. W. **Algebra**. New York: Springer-Verlag, 1974

[K] KUNZ, E. **The Value-Semigroup of a One-Dimensional Goresntein Ring**. Proceedings of The American Mathematical Society, 25, 748-751, 1970.

[Ka] KATZ, D. **On the number of minimal prime ideals in the completion of a local domain**. Rocky Montain J. Math. 16, nº 3, 575-578, 1986.

[M] MATLIS, E. **One Dimensional Local Cohen-Macaulay Rings**, Lecture Notes in Mathematics, Vol. 327, Springer-Verlag, 1973.

[N] NERIS, N. G. S. **Estudo Local de Curvas Singulares via Valorizações e Semigrupos**. Dissertação (Mestrado em Matemática). Universidade Federal de Juiz de Fora, Juiz de Fora, 2017.

[R] REID, M. **Undergraduate Commutative Algebra**. Cambridge: Cambridge University Press, London Mathematical Society Texts 29, 1995.

[RS] ROSALES, J. C.; GARCIA-SÁNCHEZ, P. A. **Numerical semigroups**. Springer Science+Business Media, 2009.

[S] STICHTENOTH, H. **Algebric Function Fields and Codes**.Springer-Verlag, 2009.

[WF] FULTON, W. **Algebric Curves**. An Introduction To Algebric Geometry. W.A.Benjamin, Inc., New York, 1969.