Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Pós-Graduação em Matemática

Naamã Galdino da Silva Neris

Estudo Local de Curvas Singulares via Valorizações e Semigrupos

Juiz de Fora
2017

Naamã Galdino da Silva Neris

Estudo Local de Curvas Singulares via Valorizações e Semigrupos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Flaviana Andréa Ribeiro

Juiz de Fora

2017

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

Galdino da Silva Neris, Naamã.
Estudo Local de Curvas Singulares via Valorizações e Semigrupos / Naamã Galdino da Silva Neris. – 2017.
63 f. : il.

Orientadora: Flaviana Andréa Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2017.

1. Curvas. 2. Valorizações. 3. Semigrupos. I. Andréa Ribeiro, Flaviana, orient. II. Estudo Local de Curvas Singulares via Valorizações e Semigrupos.

Naamã Galdino da Silva Neris

Estudo Local de Curvas Singulares via Valorizações e Semigrupos

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em:

BANCA EXAMINADORA

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

Profª. Drª. Beatriz Casulari da Motta Ribeiro
Universidade Federal de Juiz de Fora

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

Dedico este trabalho
À minha avó, Maria Galdino, pelo exemplo de vida.

AGRADECIMENTOS

À Deus, em primeiro lugar, por ter me dado saúde, sabedoria e força no decurso destes dois anos de mestrado;

Aos meus pais, Nalberto Carlos e Márcia Cristina, pela confiança, dedicação e apoio dispensados e pelas inúmeras orações endereçadas a mim;

Aos meus irmãos, Naara Galdino e Naason Galdino, pelo apoio incondicional;

À toda minha família que sempre me apoiou e torceu por mim;

Aos irmãos de fé, Luíz e Alice, pela amizade, confiança, apoio e por terem me recebido de braços abertos em sua casa;

À minha amiga, Cida, pela amizade, companheirismo e pelas palavras de conforto nos momentos difíceis;

À professora doutora, Flaviana Andréa Ribeiro, pela amizade e por compartilhar comigo os seus conhecimentos e sabedoria. Como orientadora, conduziu-me com responsabilidade e competência na realização desta dissertação;

Às professoras doutoras, Beatriz Casulari da Motta Ribeiro e Lia Feital Fusaro Abrantes, por terem aceitado o convite para fazer parte da banca. Obrigado pela leitura minuciosa, pelas sugestões e comentários;

Aos Professores do Departamento de Matemática da Universidade Federal de Juiz de Fora, pela forma competente e dedicada com que atuaram;

Aos colegas e amigos de mestrado, pela amizade, conhecimento compartilhado e companheirismo nessa jornada;

À secretária da pós-graduação, Paula, pelo profissionalismo e pela amizade;

À capes, pelo apoio financeiro;

Em especial, um agradecimento ao Professor Dr. Renato Vidal da Silva Martins, pela sugestão dos exemplos nesta dissertação.

RESUMO

O objetivo principal desse trabalho é o estudo local de curvas planas singulares usando valorizações e semigrupos de valores. Vimos que os objetos algébricos que correspondem aos pontos da curva são as valorizações ou, equivalentemente, os anéis de valorização discreta. Mais precisamente, seja k um corpo algebricamente fechado, C uma curva plana projetiva irredutível e não singular e $k(C)$ o corpo das funções racionais de C. Então, existe uma bijeção entre os pontos da curva C e o conjunto das valorizações discretas da extensão $k(C)/k$. Vimos também que no caso de curvas singulares essa correspondência não é em geral uma bijeção. Estudamos semigrupos de valores associados aos anéis locais de algumas curvas planas e também usamos as noções de semigrupo e ideais relativos para caracterizar módulos livres de torção e posto 1 sobre dois exemplos de curvas singulares.

Palavras-chave: Curvas. Valorizações. Semigrupos.

ABSTRACT

The main of this work is the local study of singular plane curves using valuations and semigroups of values. We have seen that the objects that correspond to the points of the curve are the valuations or, equivalently, the discrete valution rings. More precisely, let k be an algebraically closed field, C an irreducible non-singular projective plane curve and $k(C)$ the rational function field of C. Then, there exists a bijection between the points of the curve C and the set of discrete valuations of the extension $k(C)/k$. We have also seen that in the case of singular curves this correspondence is not usually a bijection. We have studied semigroups of values associated with the local ring of some plane curves and we have also used the semigroup notions and relative ideals to characterize the torsion free modules of rank 1 on two examples of singular curves.

Key-words: Curves. Valuations. Semigroups.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A motivação inicial para a escolha do tema apresentado nesse trabalho foi o estudo de feixes de profundidade 1 sobre uma curva C, cujas singularidades são pontos duplos ordinários. Em [S], C. S. Seshadri mostra a existência de uma bijeção entre o conjunto das classes de equivalência desses feixes e o conjunto de classes de equivalência de fibrados vetoriais sobre $\tilde{C}$, a normalização de C, munidos de uma estrutura adicional.

Em [ALR], os autores dão uma outra prova dos resultados de C.S. Seshadri mostrando a propriedade funtorial dessa relação e estendendo a discussão para a estabilidade dos feixes. Em [ARM], mostra-se que os resultados continuam válidos para curvas cujas singularidades são cúspides.

Um ponto central destes trabalhos é certamente a Proposição 2 [p. 164] de [S] que descreve localmente os feixes sobre os pontos singulares da curva C. Por isso, nosso objetivo foi estudar os módulos livre de torção e posto 1 sobre os anéis locais de dois tipos de curvas singulares, usando as técnicas apresentadas em [BDF] e [BF] de associar a esses objetos semigrupos de valores e ideais relativos.

Mais especificamente, vimos em alguns exemplos particulares como associar aos R-módulos livre de torção e posto 1 ideais relativos de S, onde S é o semigrupo de valores de R.

No Capítulo 2, apresentamos alguns objetos básicos de Álgebra Comutativa como por exemplo, módulos, fecho inteiro de um anel, valorização discreta, anéis de valorização discreta e alguns resultados importantes para o desenvolvimento do trabalho.

No Capítulo 3, estudamos curvas planas irredutíveis via corpos de funções algébricas e vimos que os objetos algébricos que correspondem aos pontos das curvas são as valorizações (ou equivalentemente, os anéis de valorização discreta) do seu corpo de funções racionais. Mais precisamente, vimos que para uma curva plana projetiva irredutível C e não singular existe uma bijeção entre os pontos da curva e o conjunto das valorizações da extensão $k(C)/k$, onde $k(C)$ é o corpo de funções racionais de C (k é um corpo algebricamente fechado). Vimos também que para curvas singulares essa correspondência não é em geral uma bijeção.

No Capítulo 4, com o objetivo de estudar módulos livres de torção e posto 1 sobre anéis locais de dois tipos particulares de curvas singulares, estudamos a noção de semigrupos numéricos, semigrupos de valores e ideais relativos. Nesse capítulo também, apresentamos a noção de completamento de anéis e módulos que é uma ferramenta importante para o cálculo dos semigrupos de anéis e módulos.

2 RESULTADOS BÁSICOS

Neste capítulo apresentaremos os pré-requisitos de Álgebra Comutativa que serão necessários para a compreensão dos capítulos subsequentes e também para a familiarização com as notações.

2.1 ANÉIS E IDEAIS

Nesta seção, apresentaremos algumas propriedades e definições elementares de anéis e ideais, que é um dos conceitos básicos da Álgebra Comutativa. Em todo nosso trabalho, estaremos considerando anel comutativo com unidade.

Teorema 2.1. *Todo anel $R \neq \{0\}$ possui pelo menos um ideal maximal.*

Demonstração: Ver [AM], Teorema 1.3, pág. 4. ■

Corolário 2.1. *Cada elemento de um anel R que não é invertível, está contido em um ideal maximal.*

Demonstração: Seja $a \in R$ um elemento não invertível. Então, $R/\langle a\rangle \neq \{\overline{0}\}$ e, pelo Teorema 2.1, existe um ideal maximal $\overline{\mathfrak{m}} \subset R/\langle a\rangle$. A imagem inversa de $\overline{\mathfrak{m}}$ em R é um ideal maximal contendo a. ■

Definição 2.1. Um anel R que tem um único ideal maximal $\mathfrak{m}$ se denomina *anel local*. O corpo $k = R/\mathfrak{m}$ se denomina *corpo residual* de R.

Proposição 2.1. *(i) Sejam R um anel e $\mathfrak{m}$ um ideal de R, tal que cada $x \in R - \mathfrak{m}$ é invertível em R. Então, R é um anel local e $\mathfrak{m}$ é seu único ideal maximal.*

(ii) Sejam R um anel e $\mathfrak{m}$ um ideal maximal de R, tal que cada elemento de $1 + \mathfrak{m}$ é invertível em R. Então R é um anel local.

Demonstração:

(i) Suponha que exista um ideal J tal que $\mathfrak{m} \subsetneq J \subseteq R$. Então, existe $x \in J$ tal que $x \notin \mathfrak{m}$. Como x é invertível, $J = R$. Portanto, $\mathfrak{m}$ é maximal.

Agora suponhamos que exista outro ideal maximal $\mathfrak{m}' \subseteq R$. Como $\mathfrak{m}'$ é próprio e $\mathfrak{m}$ é formado pelos elementos de R que não são invertíveis, temos que $\mathfrak{m}' \subseteq \mathfrak{m} \subseteq R$. Mas, como $\mathfrak{m}'$ é maximal, temos que $\mathfrak{m}' = \mathfrak{m}$. Portanto, R é um anel local e $\mathfrak{m}$ seu ideal maximal.

(ii) Seja $x \in R - \mathfrak{m}$. Queremos mostrar que existe um y invertível em R. Como $x \in R - \mathfrak{m}$, então $x \notin \mathfrak{m}$ e $\mathfrak{m} + \langle x\rangle = \langle R\rangle$. Logo, existem $y \in R$ e $t \in \mathfrak{m}$ tais que $t + xy = 1$.

Então, $xy = 1 - t \in 1 + \mathfrak{m}$ e, portanto, é invertível em R. Logo y é invertível em R. Do item i) segue que R é um anel local.

■

Definição 2.2. Dado um ideal $\mathfrak{a}$ de um anel R, denotamos por $r(\mathfrak{a})$ o ideal radical de $\mathfrak{a}$, ou seja,

$$r(\mathfrak{a}) := \{r \in R;\ r^n \in \mathfrak{a},\ \text{para algum } n \in \mathbb{N}\}.$$

2.2 MÓDULOS

Esta seção apresenta definição de módulos e algumas de suas propriedades. Anéis e ideais são exemplos de módulos.

Definição 2.3. Seja R um anel. Um *R-módulo* M é um grupo abeliano junto com uma aplicação

$$\mu : R \times M \longrightarrow M \text{ representada por } \mu(r, x) = rx$$

tal que, para todo $x, y \in M$ e todo $r, s \in R$, as seguintes propriedades são satisfeitas:

(i) $r(x + y) = rx + ry$;

(ii) $(r + s)x = rx + sx$;

(iii) $(rs)x = r(sx)$;

(iv) $1x = x$.

Definição 2.4. Um subconjunto não vazio N de um R-módulo M é um *submódulo* de M se as seguintes condições são satisfeitas:

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

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

Definição 2.5. Se N, P são submódulos de M, definimos

$$(N : P) = \{r \in R;\ rP \subseteq N\},$$

que é um ideal de R.

Em particular, chamamos *anulador de M*, o conjunto

$$(0 : M) = \{r \in M;\ rM = 0\},$$

e este ideal será denotado por $\mathrm{Ann}(M)$.

Definição 2.6. Um R-módulo é *fiel* se $\mathrm{Ann}(M) = 0$. Se $\mathrm{Ann}(M) = \mathfrak{a}$, então M é fiel como $A/\mathfrak{a}$-módulo.

Se $M = \sum_{i \in I} Rx_i$, os x_i são chamados de *geradores* de M; isto significa que todo elemento de M pode ser expresso (não necessariamente de forma única) como uma combinação linear finita de x_i com coeficientes em R.

Definição 2.7. Dizemos que um R-módulo M é *finitamente gerado* se possui um conjunto finito de geradores.

Definição 2.8. Sejam R um domínio de integridade e M um R-módulo. Um elemento $m \in M$ é chamado um *elemento de torção* de M se $Ann\,(m) := \{a \in R;\ am = 0\} \neq \{0\}$, isto é, se m é anulado por algum elemento não nulo de R.

Proposição 2.2. *Sejam R um domínio de integridade e M um R-módulo. Os elementos de torção de M formam um submódulo de M, chamado o submódulo de torção de M, denotado por $T(M)$.*

Demonstração: De fato, seja

$$T(M) = \{m \in M;\, am = 0,\ \text{ para algum } a \in R \text{ não nulo}\}.$$

Sejam $m_1, m_2 \in T(M)$. Então, existem $a_1, a_2 \in R$, não nulos, tais que $a_1 m_1 = 0$ e $a_2 m_2 = 0$. Logo, $a_1 a_2 (m_1 + m_2) = (a_1 a_2) m_1 + (a_1 a_2) m_2 = a_2 (a_1 m_1) + a_1 (a_2 m_2) = 0$. Como R é um domínio de integridade, $a_1 a_2 \neq 0$ e $m_1 + m_2 \in T(M)$.

Sejam $a \in R$, $m \in T(M)$ e $b \in R$, não nulo, tal que $bm = 0$. Então, $b(am) = a(bm) = 0$ e $ab \neq 0$. Logo, $am \in T(M)$. ■

Definição 2.9. Um R-módulo M é dito *livre de torção* se $T(M) = \{0\}$.

Exemplo 2.1. Seja R um domínio de integridade. Todo R-módulo livre é livre de torção.

Definição 2.10. Seja R um domínio de integridade com o corpo de frações K e seja M um R-módulo. Definimos o posto de M, denotado por $\mathrm{rank}_R M$, por:

$$\mathrm{rank}_R M := \dim_K K \otimes_R M.$$

2.2.1 Sequências Exatas

Definição 2.11. Uma sequência de R-módulos e R-homomorfismos

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

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

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

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

(iii) $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ é exata $\Leftrightarrow$ f é injetora, g é sobrejetora e g induz um isomorfismo de $\mathrm{Coker}(f) = M/f(M')$ sobre M''.

Definição 2.12. Uma sequência de R-módulos e R-homomorfismos da forma

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

é chamada *sequência exata curta* de R-módulos e R-homomorfismos.

2.3 ANÉIS E MÓDULOS DE FRAÇÕES

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

Definição 2.13. 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 de 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 $\dfrac{x}{s}$ para a classe de equivalência $\overline{(x, s)}$ e $S^{-1}R$ para o conjunto das classes de equivalência.

Ao definirmos em $S^{-1}R$ as operações:

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

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

para todo $x, y \in R$ e todo $s, t \in S$, o conjunto $S^{-1}R$ passa a ter uma estrutura de anel.

O anel $S^{-1}R$ é chamado de *anel de frações* de R em relação a S. Também existe um homomorfismo de anéis $f : R \longrightarrow S^{-1}R$ definido por $f(x) = x/1$, que em geral, não é injetivo.

Observação 2.1. Se R for um domínio de integridade e $S = R - \{0\}$, chamamos o conjunto $S^{-1}R$ de *corpo de frações* de R.

O resultado a seguir é satisfeito para todos os anéis de frações.

Proposição 2.3. *(Propriedade Universal do Anel de Frações) Seja $g : R \longrightarrow R_1$ um homomorfismo de anéis tal que $g(s)$ é um invertível em R_1, para todo $s \in S$. Então existe um único homomorfismo de anéis $h : S^{-1}R \longrightarrow R_1$, tal que $g = h \circ f$.*

Demonstração: Ver [AM], Proposição 3.1, pág. 42. ■

Exemplo 2.2. 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 2.14. O processo de passar de R a $R_{\mathfrak{p}}$ é chamado de *localização* de R em $\mathfrak{p}$.

Proposição 2.4. *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.(iv), pág. 47. ■

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

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

Usaremos as notações $\dfrac{m}{s}$ para a classe de equivalência $\overline{(m, s)}$ e $S^{-1}M$ para o conjunto dessas classes.

Definimos em $S^{-1}M$ as operações:

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

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

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 $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

O seguinte resultado, é uma importante propriedade da operação S^{-1}.

Proposição 2.5. *A operação S^{-1} é exata, isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é uma sequência de R-módulos exata em M, 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, pág. 44. ■

2.4 DEPENDÊNCIA INTEIRA E ANEL DE VALORIZAÇÃO

Nesta seção, apresentaremos algumas propriedades relacionadas a dependência inteira. Também, apresentaremos alguns resultados importantes sobre anel de valorização.

2.4.1 **Dependência Inteira**

Sejam R um anel e B um subanel de R (tal que $1_R \in B$). Um elemento $x \in R$ é *inteiro* sobre B, se x é raiz de um polinômio mônico com coeficientes em B, isto é, se x satisfaz uma equação da forma

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

onde os $b_i's$ são elementos de B. Evidentemente, cada elemento de B é inteiro sobre B.

Proposição 2.6. *As seguintes afirmações são equivalentes:*

(i) $x \in R$ *é inteiro sobre* B*;*

(ii) $B[x]$ *é um* B*-módulo finitamente gerado;*

(iii) $B[x]$ *está contido em um subanel* C *de* R *tal que* C *é um* B*-módulo finitamente gerado;*

(iv) Existe um $B[x]$*-módulo fiel* M *que é finitamente gerado como* B*-módulo.*

Demonstração: Ver [AM], Proposição 5.1, pág. 66. ■

Corolário 2.2. *Sejam* x_i*, para* $1 \leq i \leq n$*, elementos de* R *inteiros sobre* B*. Então o anel* $B[x_1, \ldots, x_n]$ *é um* B*-módulo finitamente gerado.*

Demonstração: Ver [AM], Corolário 5.2, pág. 66. ■

Corolário 2.3. *O conjunto* C *de elementos de* R *que são inteiros sobre* B *é um subanel de* R *que contém* B*.*

Demonstração: Ver [AM], Corolário 5.3, pág. 66. ■

Definição 2.15. Denominamos o anel C do Corolário (2.3), o *fecho inteiro* de B em R. Se $C = B$, então dizemos que B é *integralmente fechado* em R. Se $C = R$, dizemos que o anel R é *inteiro* sobre B.

Corolário 2.4. *Se $B \subseteq R \subseteq C$ são anéis e se R é inteiro sobre B e C é inteiro sobre R, então C é inteiro sobre B.*

Demonstração: Ver [AM], Corolário 5.4, pág. 67. ■

Teorema 2.2. *Sejam $B \subseteq R$ anéis, R inteiro sobre B e, $\mathfrak{p}$ um ideal primo de B. Então existe um ideal primo de R tal que $\mathfrak{q} \cap B = \mathfrak{p}$.*

Demonstração: Ver [AM], Teorema 5.10, pág. 68. ■

2.4.2 Domínios de Integridade Integralmente Fechados

Definição 2.16. Um domínio de integridade é dito ser *integralmente fechado* se é integralmente fechado em seu corpo de frações.

Proposição 2.7. *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 $\mathfrak{p}$;*

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

Demonstração: Ver [AM], Proposição 5.13, pág. 70. ■

2.4.3 Anel de Valorização

Seja R um domínio de integridade e seja K seu corpo de frações.

Definição 2.17. Dizemos que R é um *anel de valorização* de K se, para cada $x \in K$ e $x \neq 0$, $x \in R$ ou $x^{-1} \in R$.

Proposição 2.8. *Seja R um anel de valorização.Então se cumprem as seguintes afirmações:*

(i) *R é um anel local;*

(ii) *Se R' é um anel tal que $R \subseteq R' \subseteq K$, então R' é um anel de valorização de K;*

(iii) *R é integralmente fechado em K.*

Demonstração:

(i) Seja $\mathfrak{m}$ o conjunto dos elementos de K que não são invertíveis em R, ou seja, $x \in \mathfrak{m}$ se, e somente se, $x = 0$ ou $x^{-1} \notin R$. Vamos mostrar que $\mathfrak{m}$ é um ideal de R. De fato, se $a \in R$ e $x \in \mathfrak{m}$ temos que $ax \in \mathfrak{m}$, pois caso contrário, $(ax)^{-1} \in R$ o que implica que $x^{-1} = a(ax)^{-1} \in R$.

Agora, sejam $x, y \in \mathfrak{m}$ não nulos. Como $xy^{-1} \in K$, então $xy^{-1} \in R$ ou $yx^{-1} \in R$. Se $xy^{-1} \in R$ então $x + y = (1 + xy^{-1})y \in R\mathfrak{m} \subseteq \mathfrak{m}$ e, se $yx^{-1} \in R$ então $x + y = (1 + yx^{-1})x \in R\mathfrak{m} \subseteq \mathfrak{m}$. Logo, $x + y \in \mathfrak{m}$. Em virtude da Proposição (2.1), R é um anel local e $\mathfrak{m}$ seu ideal maximal.

(ii) Como $x \in K$, então $x \in R \subseteq R'$ ou $x^{-1} \in R \subseteq R'$. Logo R' é um anel de valorização de K.

(iii) Seja $x \in K$ inteiro sobre R. Então temos

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

com $b_i \in R$. Se $x \in R$ já está provado. Agora, se $x \notin R$, então $x^{-1} \in R$, pois R é um anel de valorização. Assim, segue que:

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

Logo $x \in R$. Absurdo, pois supomos inicialmente que $x \notin R$.

Portanto R é integralmente fechado sobre K.

■

Nosso objetivo principal com os resultados apresentados a seguir é mostrar que o fecho inteiro de um domínio de integridade A no seu corpo de frações K é a interseção de todos os anéis de valorização de K que contém A.

Definição 2.18. Seja S um conjunto não vazio. Dizemos que S *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 $x, y \in T$, ou $x \leq y$ ou $y \leq x$. Dizemos que a cadeia T é limitada superiormente se, existe $z \in S$ tal que $t \leq z\ \ \forall\ t \in T$.

Lema 2.1. *(Lema de Zorn) Se toda cadeia $T \subseteq S$ tem uma cota superior em S, então existe um elemento maximal em S.*

Seja K um corpo, Ω um corpo algebricamente fechado. Seja Σ o conjunto de todos os pares (A, f), onde A é um subanel de K e f é um homomorfismo de A em Ω. O conjunto Σ é parcialmente ordenado, como segue:

$$(A, f) \leq (A', f') \Leftrightarrow A \subseteq A' \text{ e } f' \mid_A = f$$

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

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

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

Queremos construir o par (A, f) tal que

$$(A_i, f_i) \leq (A, f), \text{ isto é, tal que } A_i \subseteq A \text{ e } f \mid_{A_i} = f_i, \ \forall\, i \in I$$

Definimos $A = \bigcup_{i \in I} A_i \subseteq K$ um anel.

Considere $f : A \longrightarrow \Omega$ definida da seguinte maneira: dado $x \in A = \bigcup_{i \in I} A_i$, temos que $x \in A_i$, para algum $i \in I$. Então $f(x) := f_i(x)$, ou seja, $f \mid_{A_i} = f_i$.

Vejamos que 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, $f_j \mid_{A_i} = f_i$ ou $f_i \mid_{A_j} = f_j$ e $f_i(x) = f_j(x)$ ou $f_j(x) = f_i(x)$.

Agora, vejamos que 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 $f(x+y) = f_i(x+y) = f_i(x) + f_i(y)$ e $f(xy) = f_i(xy) = f_i(x)f_i(y)$, isto é, f é um homomorfismo de anéis.

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

Lema 2.2. *B é um anel local e $\mathfrak{m} = Ker(g)$ é seu ideal maximal.*

Demonstração: Como $g(B)$ é um subanel de um corpo, portanto um domínio de integridade, e $g(B) \simeq \dfrac{B}{ker(g)}$, temos que o ideal $\mathfrak{m} = Ker(g)$ é primo.

Podemos estender a função g a um homomorfismo

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

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

Vejamos que $\widetilde{g}$ está bem definida. Com efeito,

$$\frac{b}{s} = \frac{b_1}{s_1} \text{ em } \ B_{\mathfrak{m}} \Rightarrow \exists\ t \notin \mathfrak{m} \text{ tal que } t(bs_1 - sb_1) = 0 \in B.$$

Daí,

$$g(t)(g(b)g(s_1) - g(s)g(b_1)) = 0 \in K \Rightarrow g(b)g(s_1) - g(s)g(b_1) = 0\ (g(t) \neq 0).$$

Logo,

$$\widetilde{g}\left(\frac{b}{s}\right) = \frac{g(b)}{g(s)} = \frac{g(b_1)}{g(s_1)} = \widetilde{g}\left(\frac{b_1}{s_1}\right).$$

Além disso,

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

é homomorfismo injetor, pois B é domínio. Logo, $B_{\mathfrak{m}}$ contém uma cópia de B e (sem perda de generalidade $B \subseteq B_{\mathfrak{m}}$) $(B, g) \leq (B_{\mathfrak{m}}, \widetilde{g})$. 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 2.3. *Seja x um elemento não nulo de K. Seja $B[x]$ o subanel de K gerado por x sobre B e seja $\mathfrak{m}[x]$ 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:

$$u_0 + u_1x^1 + \cdots + u_mx^m = 1 \qquad (u_i \in m) \tag{2.1}$$

$$v_0 + v_1x^{-1} + \cdots + v_nx^{-n} = 1 \qquad (v_j \in m) \tag{2.2}$$

em que podemos supor que os graus m, n são os menores possíveis. Consideremos $m \geq n$ e multipliquemos (2.2) por x^n. Assim

$$v_0x^n + v_1x^{n-1} + \cdots + v_n = x^n$$
$$v_1x^{n-1} + \cdots + v_n = x^n - v_0x^n$$

$$v_1x^{n-1} + \cdots + v_n = x^n(1 - v_0) \tag{2.3}$$

Como $v_0 \in m$, B é um anel local e $\mathfrak{m} = Ker(g)$ é seu ideal maximal, pela Proposição (2.1) se deduz que $(1 - v_0)$ é um invertível em B, e a equação (2.3) pode ser escrita da seguinte forma:

$$x^n = w_1x^{n-1} + \cdots + w_n,$$

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

Portanto,

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

contrariando a minimalidade de m na equação (2.1).

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

Teorema 2.3. *Seja (B, g) um elemento maximal de Σ. Então B é um anel de valorização do corpo K.*

Demonstração: Pela definição de anel de valorização, devemos mostrar que se $x \neq 0$ é um elemento de K, então $x \in B$ ou $x^{-1} \in B$. Pelo lema anterior, suponhamos que o ideal $\mathfrak{m}[x]$ é um ideal próprio do anel $B' = B[x]$. Então, $\mathfrak{m}[x]$ está contido em um ideal $\mathfrak{m}' \in B'$ e tem-se que $\mathfrak{m}' \bigcap B = \mathfrak{m}$ (pois $\mathfrak{m} \subseteq \mathfrak{m}' \bigcap B \subseteq B$).

Portanto, a inclusão $B \hookrightarrow B'$ induz uma inclusão $k = B/\mathfrak{m} \hookrightarrow k' = B'/\mathfrak{m}'$. Então $k' = k[\overline{x}]$ onde $\overline{x}$ é a imagem de x em k'. De fato , como $\overline{x} \in k'$ e $k \subseteq k'$ então $k[\overline{x}] \subseteq k'$. Agora, para ver a inclusão contrária, seja $y \in k'$. Como $k' = B'/\mathfrak{m}' = B[x]/\mathfrak{m}'$, temos que $y = \overline{f(x)}$, onde $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in B[x]$. Isso implica que $\overline{f(x)} = \overline{a_0} + \overline{a_1}\overline{x} + \cdots + \overline{a_n}\overline{x^n} \in k[\overline{x}]$. 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, $\forall\ y \in k', \exists\ h(T) \in k[T]$ mônico tal que $h(y) = 0$.

Agora, 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 $k[T] \longrightarrow \Omega[T]$ dada por $\overline{g}(h(t)) = h'(t)$, temos que $h(y) = 0$ implica que $h'(y) = 0$. 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 $B' = B$. Logo $x \in B$.

Portanto, B é um anel de valorização do corpo K. ■

Corolário 2.5. *Seja A um subanel de um corpo K. Então o fecho inteiro $\overline{A}$ de A em K é a interseção de todos os anéis de valorização de K que contém A.*

Demonstração: Sejam $A \subseteq K$ subanel e B um anel de valorização de K tal que $A \subseteq B$. Vamos mostrar que $\overline{A} = \bigcap B$.

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 $x \in K$. Se $x \notin \overline{A}$, vamos mostrar que $x \notin \bigcap B$, ou seja, que $x \notin B$, para nenhum anel de valorização B de 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 $A[x^{-1}]$, o que implica que $x^{-1} \in \mathfrak{m}' \subseteq A'$, para algum ideal maximal $\mathfrak{m}'$ de $A' = A[x]$.

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

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

onde $f : A' \to k'$ é o homomorfismo natural e, usando o Teorema 2.3, temos que existe $B \subseteq k'$ elemento maximal de Σ' e $g : B \longrightarrow \Omega$ um homomorfismo tal que B é um anel de valorização de k' e $A \subseteq B$.

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

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

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

Portanto $\overline{A} = \bigcap B$ ■

2.5 VALORIZAÇÃO DISCRETA E ANÉIS DE VALORIZAÇÃO DISCRETA

Nesta seção, apresentaremos o conceito de valorização discreta e anéis de valorização discreta, juntamente com suas principais propriedades.

2.5.1 **Valorização Discreta**

Definição 2.19. Sejam K um corpo e $K^* = K\backslash\{0\}$. Uma *valorização discreta* em K é uma função $v : K^* \longrightarrow \mathbb{Z}$ sobrejetiva que satisfaz:

(i) $v(xy) = v(x) + v(y), \ \ \forall\ x, y \in K^*$;

(ii) $v(x + y) \geq min\,\{v(x), v(y)\} \quad se\ x, y \in K^*$.

Convencionamos definir: $v(0) = \infty$.

Se $\forall\ n \in \mathbb{Z},\ \infty + n = \infty$ e $\infty + \infty = \infty$ temos que (i) e (ii), definidos acima, valem $\forall x, y \in K$.

É fácil ver que: $v(1) = 0,\ v(-x) = v(x)$ e $v(x^{-1}) = -v(x)$.

Proposição 2.9. *Sejam $x_1, x_2, \ldots, x_n \in K$. Então*

(i) $v(x_1 + x_2 + \cdots + x_n) \geq min\{v(x_1), \ldots, v(x_n)\}$ *e a igualdade se verifica se o* $min\{v(x_1), \ldots, v(x_n)\}$ *é atingido só uma vez.*

(ii) Se $x_1, x_2, \ldots, x_n$ *não são todos nulos e* $x_1+x_2+\cdots+x_n = 0$*, então* $min\{v(x_1), \ldots, v(x_n)\}$ *não é atingido só uma vez.*

Demonstração:

(i) Fazendo indução em n e usando a propriedade (ii) da Definição 2.19 mostramos que

$$v(x_1 + x_2 + \cdots + x_n) \geq \min\{v(x_1), \ldots, v(x_n)\}.$$

Vamos supor, sem perda de generalidade, que $\min\{v(x_1), \ldots, v(x_n)\} = v(x_1)$ e $v(x_1) < v(x_i),\ \forall\ i = 2, \ldots, n$, Então devemos mostrar que

$$v(x_1 + x_2 + \cdots + x_n) = v(x_1).$$

Por hipótese, sabemos que $v(x_1+x_2+\cdots+x_n) \geq v(x_1)$. Para mostrar a desigualdade contrária, note que:

$$\begin{aligned} v(x_1) &= v(x_1 + x_2 + \cdots + x_n - x_2 - x_3 - \cdots - x_n) \\ &\geq \min\{v(x_1 + x_2 + \cdots + x_n), v(-x_2 - \cdots - x_n)\} \\ &= \min\{v(x_1 + x_2 + \cdots + x_n), v(x_2 + \cdots + x_n)\}. \end{aligned}$$

Se $\min\{v(x_1 + x_2 + \cdots + x_n), v(x_2 + \cdots + x_n)\} = v(x_1 + x_2 + \cdots + x_n)$, temos que

$$v(x_1) \geq v(x_1 + x_2 + \cdots + x_n) \geq v(x_1).$$

Se $\min\{v(x_1 + x_2 + \cdots + x_n), v(x_2 + \cdots + x_n)\} = v(x_2 + \cdots + x_n)$, então

$$\begin{aligned} v(x_1) &\geq v(x_2 + \cdots + x_n) \geq \min\{v(x_2, \ldots, x_n)\} \\ &= v(x_i). \end{aligned}$$

para todo $i \neq 1$.

Então $v(x_1) \geq v(x_i)$, mas por hipótese $v(x_1) < v(x_i)$ para todo $i \neq 1$.

Portanto, $v(x_1 + x_2 + \cdots + x_n) = v(x_1)$.

(ii) Se $\min\{v(x_1 + x_2 + \cdots + x_n)\}$ fosse atingido uma vez, então pelo item anterior, teríamos que:

$$v(x_1 + x_2 + \cdots + x_n) = \min\{v(x_1, x_2, \ldots, x_n)\} = v(x_1).$$

Mas,

$$v(x_1 + x_2 + \cdots + x_n) = v(0) = \infty \Rightarrow v(x_1) = \infty.$$

Absurdo.

■

O conjunto $R = \{x \in K;\ v(x) \geq 0\}$ é um anel de valorização, chamado de anel de valorização v de K. De fato, dado $x \notin R$, temos que $v(x) < 0$. Como $v(1) = 0$, temos que

$$0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \Rightarrow v(x^{-1}) = -v(x).$$

Então $v(x^{-1}) > 0$. Logo, $x^{-1} \in R$.

Portanto o conjunto R é um anel de valorização v de K.

Exemplo 2.3. Para cada primo fixo p, definimos

$$\begin{array}{rccc} v_p: & \mathbb{Q} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & n \\ & 0 & \longmapsto & \infty \end{array}$$

onde $x = p^n \dfrac{c}{d}$ com $c, d \in \mathbb{Z}$, $p \nmid c$ e $p \nmid d$.

Então v_p é uma valorização discreta de $\mathbb{Q}$. De fato, dados

$$x = p^m \frac{a}{b} \text{ com } p \nmid a \text{ e } p \nmid b \text{ e } y = p^n \frac{c}{d} \text{ com } p \nmid c \text{ e } p \nmid d,$$

temos que $v_p(x) = m$, $v_p(y) = n$ e:

(i) $v_p(xy) = v_p\left(p^{m+n}\dfrac{ac}{cd}\right) = m + n = v_p(x) + v_p(y)$ pois $p \nmid ac$ e $p \nmid cd$;

(ii) Se $m < n$, $v_p(x+y) = v_p\left(p^m\left(\dfrac{ad + p^{n-m}bc}{bd}\right)\right) = m = v_p(x)$, pois $p \nmid (ad + p^{n-m}bc)$ e $p \nmid bd$, e se $m > n$
$v_p(x+y) = v_p\left(p^n\left(\dfrac{p^{m-n}ad + bc}{bd}\right)\right) = n = v_p(y)$, pois $p \nmid (p^{m-n}ad)$ e $p \nmid bc$.

Assim;

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

Portanto, a função v_p é uma valorização discreta de K.

O anel de valorização de v_p é o anel local $\mathbb{Z}_{(p)} = \left\{\dfrac{a}{b};\ a, b \in \mathbb{Z},\ p \nmid b\right\}$.

2.5.2 Anéis de Valorização Discreta

Definição 2.20. Seja R um domínio que não é um corpo. R é dito um *anel de valorização discreta*, se existe um elemento irredutível $t \in R$ tal que todo elemento $z \in R - \{0\}$, pode ser escrito de maneira única como $z = ut^n$, onde u é invertível e n é um inteiro não negativo. O elemento irredutível t é dito parâmetro de uniformização de R ou uniformizante local em R.

Observação 2.2. A condição de R ser um anel de valorização discreta (AVD) é equivalente à R ser noetheriano, local, cujo único ideal maximal é principal (ver [WF], Proposição 4, pág. 34).

Observação 2.3. Qualquer outro parâmetro de uniformização de R é da forma ut, onde u é invertível.

Proposição 2.10. *Dada uma valorização discreta de K, $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$, consideremos o conjunto $R = \{x \in K;\ v(x) \geq 0\}$. Então R é um anel de valorização discreta, chamado o anel de valorização discreta de v, que tem K como corpo de frações. Reciprocamente, todo anel de valorização discreta que tem K como corpo de frações é dessa forma para alguma valorização v de K.*

Demonstração:

Temos que R é um domínio pois $R \subset K$ e K é um corpo. Além disso, se $z \in R$ e $v(z) > 0$ então $v(1/z) = -v(z) < 0$. Logo, R é um domínio que não é um corpo.

Devemos mostrar que existe $t \in R$, irredutível, tal que $\forall z \in R - \{0\}$, $z = ut^n$, $n \geq 0$ e u invertível em R.

Primeiro devemos observar que uma consequência imediata do fato de $v(1/u) = -v(u)$ é que, $u \in R$ é invertível (em R) se, e somente se, $v(u) = 0$. Sendo v uma aplicação sobrejetiva, existe $t \in K$ tal que $v(t) = 1$. Suponhamos $t = ab$ com $a, b \in R$. De $1 = v(a) + v(b)$ temos $v(a) = 0$ ou $v(b) = 0$. Portanto, ou a ou b é invertível em R e t é irredutível.

Dado $z \in R$, sejam $n = v(z) \geq 0$ e $u = zt^{-n} \in K$. Então $v(u) = 0$ e $z = ut^n$ com u invertível em R. Além disso, se $z = u_1 t^{n_1} = u_2 t^{n_2}, n_1 v(t) = n_2 v(t)$ e $n_1 = n_2$. Portanto, a menos de multiplicação por invertíveis, temos unicidade.

Observe que K é o corpo de frações de R pois, se $z \in K - \{0\}$, então $z \in R$ ou $z^{-1} \in R$.

Reciprocamente, seja $R \subset K$ um anel de valorização discreta que tem K como corpo de frações. Então fixado t (parâmetro de uniformização em R) é verdade que todo $z \in K - \{0\}$ pode ser escrito de maneira única como $z = ut^n$ onde $n \in \mathbb{Z}$. Defina $ord(z) = n$ e $ord(0) = \infty$. É fácil ver que

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

é uma valorização discreta de K. ■

Se R é o anel de valorização correspondente à valorização v, denotaremos às vezes R por $\mathcal{O}_v$ e seu ideal maximal por $\mathcal{M}_v$.

Definição 2.21. Seja R um domínio de integridade. Se R é um anel de valorização discreta, então R é um anel de valorização de v. Logo, R é um anel local e, o conjunto

$$\mathcal{M}_v = \{x \in K;\ v(x) > 0\}$$

é seu ideal maximal.

2.6 CORPOS DE FUNÇÕES ALGÉBRICAS EM UMA VARIÁVEL

Definição 2.22. Seja K/k uma extensão de corpos. Chamaremos K/k corpo de funções algébricas em uma variável, com k como corpo de constantes, se k for algebricamente fechado em K e, se existir $z \in K - k$ tal que $[K : k(z)] < \infty$.

A partir desse ponto, estaremos considerando k um corpo *algebricamente fechado*.

Exemplo 2.4. Sejam k um corpo algebricamente fechado, $k[t]$ o anel de polinômios em uma variável com coeficiente em k e $K = k(t)$ o corpo de frações de $k[t]$. Então K/k é um corpo de funções algébricas em uma variável.

Lema 2.4. *Sejam R um anel de valorização discreta do corpo de funções algébricas em uma variável K/k, $\mathcal{M}$ o ideal maximal de R e $x \in \mathcal{M}$ não nulo. Sejam $x_1, x_2, \ldots, x_n \in \mathcal{M}$ tais que $x_1 = x$ e $x_i \in x_{i+1}\mathcal{M}$, para todo $i = 1, 2, \ldots, n-1$. Então $[K : k(x)] \geq n$.*

Demonstração: Como $[K : k(x)]$ é a dimensão de K visto como $k(x)$-espaço vetorial, basta provarmos que o conjunto $\{x_1, \ldots, x_n\}$ é linearmente independente sobre $k(x)$. Daí, teremos que $[K : k(x)] \geq n$.

Suponha, por absurdo, que exista uma combinação linear $\sum_{i=1}^{n} \varphi_i x_i = 0$ não trivial com $\varphi_i \in k(x)$. Podemos assumir que todos os φ_i's são polinômios em x e que x não divide todos eles. Defina $a_i = \varphi_i(0)$, o termo constante de φ_i e escolha $j \in \{1, \ldots, n\}$ tal que $a_j \neq 0$ e que $a_i = 0$, para $i > j$. Assim obtemos:

$$\sum_{i=1}^{n} \varphi_i x_i = 0 \Rightarrow -\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \tag{2.4}$$

Observe que $\varphi_i \in R$ para qualquer i, pois $x \in \mathcal{M},\ x_i \in x_j\mathcal{M}$, para $i < j$ e $\varphi_i = xg_i$, para $i > j$, onde g_i são polinômios em x.

Dividindo (2.4) por x_j, temos:

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

Uma vez que $\frac{x_i}{x_j}$, $\frac{x}{x_j} \in \mathcal{M}$, pois $x_i \in x_j\mathcal{M}$, se $i < j$, o lado direito desta igualdade pertence a $\mathcal{M}$. Então, $\varphi_j \in \mathcal{M}$. Por outro lado, $\varphi_j = a_j + xg_j$, com $g_j \in k[x] \subseteq R$ e $x \in \mathcal{M}$. Então, $a_j = \varphi_j - xg_j \in \mathcal{M}$. Mas $a_j = \varphi_j(0) \in k$ e $\mathcal{M} \cap k = \{0\}$. Contradição, pois pela escolha de j devemos ter $a_j \neq 0$.

Logo, o conjunto $\{x_1, \ldots, x_n\}$ é linearmente independente e, portanto, concluímos que $[K : k(x)] \geq n$. ■

O resultado a seguir nos dá algumas propriedades básicas de anéis de valorização discreta de um corpo de funções algébricas em uma variável.

Proposição 2.11. *Sejam R um anel de valorização do corpo de funções algébricas em uma variável K/k e $\mathcal{M}$ o ideal maximal de R. Então:*

(i) $\mathcal{M}$ é um ideal principal.

(ii) R é um domínio de ideais principais. Mais precisamente, se $\mathcal{M} = \langle t \rangle$ e $I \subseteq R$ for um ideal não nulo, então $I = t^n R$, para algum $n \in \mathbb{N}$.

Demonstração:

(i) Suponha, por absurdo, que $\mathcal{M}$ não seja principal e tome $x_1 \in \mathcal{M}$ não nulo. Como $\mathcal{M} \neq x_1 R$, existe $x_2 \in \mathcal{M} \backslash x_1 R$. Então, $x_1^{-1} x_2 \notin R$, pois, caso contrário, teríamos que $x_2 \in x_1 R$. Logo, $x_2^{-1} x_1 \in \mathcal{M}$, donde temos que $x_1 \in x_2 \mathcal{M}$.

Continuando com essa construção, obtemos por indução, uma sequência infinita de elementos $x_1, x_2, \ldots \in \mathcal{M}$, tais que $x_i \in x_{i+1}\mathcal{M}$, para todo $i \geq 1$. Mas, pelo lema 2.4, isso nos leva a uma contradição.

Portanto, $\mathcal{M}$ é um ideal principal.

(ii) Segue-se por definição que R é um domínio de ideais principais. Agora, seja $I \subseteq R$ 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 $u \in R^*$ e $r \geq 0$, daí $t^r = xu^{-1} \in I$.

Seja $n = min(C)$. Vamos provar que $I = t^n R$.

De fato, como $t^n \in I$, então $I \supset t^n R$. Por outro lado, seja $y \in I$ com $y \neq 0$. Temos que $y = t^s w$, com $w \in R^*$ e $s \geq 0$, então $t^s = yw^{-1}$ e $s \geq n$. Logo, $y = t^n \cdot t^{s-n} w \in t^n R$. Portanto, $I = t^n R$.

■

3 CURVAS ALGÉBRICAS

O nosso estudo de curvas será via o estudo de corpos de funções algébricas em uma variável. Os objetos algébricos que corresponderão aos pontos da curva, serão as valorizações (ou equivalentemente, os anéis de valorização discreta) do seu corpo de funções racionais.

3.1 VARIEDADES ALGÉBRICAS

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

Definição 3.1. 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 3.2. Dizemos que um subconjunto $X \subset \mathbb{A}^n(k)$ é *fechado* se $X = V(S)$ para algum $S \subset k[X_1, \ldots, X_n]$.

Observação 3.1. Os subconjuntos fechados de $\mathbb{A}^n(k)$ são também chamados de conjuntos algébricos afins.

Definição 3.3. Se $f \in k[X_1, \ldots, X_n]$ é um polinômio não constante, o conjunto de zeros de f se denomina *hipersuperfície* definida por f.

Definição 3.4. As hipersuperfícies em $\mathbb{A}^2$, 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 Curvas Algébricas planas.

Exemplo 3.1. O conjunto $H = \{(t, t^2, t^3);\ t \in k\}$ é um conjunto algébrico.

De fato, consideremos os polinômios $f(X, Y, Z) = X^2 - Y$ e $g(X, Y, Z) = X^3 - Z$. É claro que para $p = (t, t^2, t^3)$ e $t \in k$, temos $f(p) = 0$ e $g(p) = 0$. Logo, o conjunto $H = \{(t, t^2, t^3; t \in k\} \subset V(f, g)$. Reciprocamente, se $p = (x, y, z) \in V(f, g)$, então

$$y = x^2 \ \text{ e } \ z = x^3 \Rightarrow p = (x, y, z) = (x, x^2, x^3) \in H.$$

Portanto H é um conjunto algébrico.

Definição 3.5. Definimos a *topologia de Zariski* em $\mathbb{A}^n(k)$ escolhendo para abertos os subconjuntos de $\mathbb{A}^n(k)$ que são complementares de conjuntos fechados.

Definição 3.6. 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 3.7. 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 3.1. *(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 qualquer 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 algebricamente fechado. Para qualquer ideal $\mathfrak{a} \subseteq k[x_1 \ldots, x_n]$, $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, 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 1.2, pág. 3. ■

O resultado a seguir, relaciona conjuntos algébricos irredutíveis e ideais primos, o que facilita a caracterização de tais conjuntos.

Proposição 3.2. *Seja X um subconjunto de $\mathbb{A}^n(k)$. Então X é irredutível se, e somente se, $I(X)$ é um ideal primo.*

Demonstração: Se X é irredutível, vamos mostrar que $I(X)$ é primo. De fato, se $fg \in I(X)$, então $X \subseteq V(fg) = V(f) \cup V(g)$. Assim, $X = (X \cap V(f)) \cup (X \cap V(g))$. 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 $I(X_2) \supsetneq I(X)$ e desta forma 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. ■

Exemplo 3.2. $\mathbb{A}^n(k)$ é irredutível para todo n, pois o ideal $I(\mathbb{A}^n(k)) = \langle 0 \rangle$ é primo.

Definição 3.8. Dado $X \subseteq \mathbb{A}^n(k)$ um subconjunto fechado, definimos o *anel de coordenadas* de X, denotado por $\Gamma(X)$, por

$$\Gamma(X) = \frac{k[X_1, \ldots, X_n]}{I}.$$

Definição 3.9. 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

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

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

Usualmente, chamamos de *pontos finitos* os pontos do conjunto

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

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

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

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 3.10. Um ponto $p = (a_0 : \ldots : a_n) \in \mathbb{P}^n(k)$ é *zero* de um polinômio $F \in k[X_0, \ldots, X_n]$, se $F(p) = 0$ para qualquer escolha de coordenadas homogêneas. Neste caso, $F \in k[X_0, \ldots, X_n]$ deve um polinômio homogêneo de grau d, isto é,

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

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 zero* de S.

Definição 3.11. 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.

Observação 3.2. Os subconjuntos fechados de $\mathbb{P}^n(k)$ são também chamados de conjuntos algébricos projetivos.

Definição 3.12. 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 3.13. 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*.

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

$$I(X) := \{F \in k[X_0, \ldots, X_n];\ F(p) = 0\ \forall\ p \in X\}.$$

Definição 3.14. 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 $\mathbb{A}^n(k)$ com 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 3.15. Dado $X \subseteq \mathbb{P}^n(k)$ um fechado projetivo, definimos o *anel de coordenadas homogêneas* de X, denotado por $\Gamma(X)$, por

$$\Gamma(X) = \frac{k[X_0, \ldots, X_n]}{I(X)}.$$

3.2 CURVAS ALGÉBRICAS E CORPOS DE FUNÇÕES ALGÉBRICAS

Dada uma $V \subset \mathbb{A}^n(k)$ uma variedade algébrica, sejam $I \subset K[X_1, X_2, \ldots, X_n]$ 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 e $k(V)$, seu corpo de frações, é chamado *corpo de funções racionais* de V.

Definição 3.16. A *dimensão* de V é o grau de transcendência da extensão $K(V)/k$. Uma variedade de dimensão um é chamada curva.

Observação 3.3. É possível mostrar que em $\mathbb{A}^2(k)$ as definições 3.4 e 3.16 coincidem.

Assim, no caso de curvas, $K(V)/k$ é um corpo de funções algébricas em uma variável (com k como corpo de constantes).

Observação 3.4. Se K/k é um corpo de funções algébricas, podemos mostrar que $[K : k(x)] < \infty$, para todo $x \in K \backslash k$. Além disso, se k for algebricamente fechado, existe $x \in K \backslash k$ tal que $K/k(x)$ é separável e portanto $K = k(x)(y)$. Como $[K : k(x)] < \infty$, existe $f \in k[X, Y]$ irredutível tal que $f(x, y) = 0$. Logo, se C é a curva plana irredutível definida por $f(X, Y) = 0$, teremos K isomorfo ao corpo de funções racionais de C.

Definição 3.17. Seja K/k uma extensão de corpos. Uma valorização de K/k é uma valorização de K tal que $v(a) = 0, \ \ \forall\ a \in k\backslash\{0\}$.

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

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

Veremos a seguir exemplos de valorização 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 3.3. Fixado $a \in k$, podemos escrever todo elemento $f(t) \in k[t]$ na forma $f(t) = c(t-a)^n f_1(t)$, com $n \in \mathbb{N}$, $c \in k$ não nulo e tal que $(t-a) \not| f_1(t)$. Consequentemente, todo elemento de $k(t)$ tem a forma

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

com $m \in \mathbb{Z}$, $c \in k$ não nulo e tal que $(t-a) \not| f_1(t)$ e $(t-a) \not| g_1(t)$.

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

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

onde $c \in k$ é não nulo, $(t-a) \not| f_1(t)$ e $(t-a) \not| g_1(t)$ e $v_a(0) = \infty$, é uma valorização de $k(t)/k$.

Exemplo 3.4. Como no exemplo anterior, podemos escrever um elemento arbitrário de $k(t)$ na forma

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

com $m \in \mathbb{Z}$, $c \in k$ não nulo e tal que $t \not| f_1(t)g_1(t)$. A função $v : k(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ definida por:

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

onde $c \in k$ é não nulo, $t \not| f_1(t)g_1(t)$ e $v(0) = \infty$, é uma valorização de $k(t)/k$ tal que $v(t) = -1$ e $v(1/t) = 1$. Tal valorização será denotada por v_∞.

A proposição a seguir mostra que as valorizações definidas nos Exemplos 3.3 e 3.4 são as únicas valorizações de $k(t)/k$.

Proposição 3.3. *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: *i*) Suponhamos $v(t) \geq 0$. Afirmamos que $v(f) \geq 0, \ \forall \ f \in k[t]$.

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,

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

Usando que v é sobrejetiva temos que existe $f \in k[t]$ tal que $v(f) > 0$.

Escreva $f = c\prod_{i=0}^{r}(t - c_i)$, com $c, c_i \in k, \forall \ i = 1, \ldots, r$, e $c \neq 0$.

De $v(f) > 0$ obtém-se que $v(t - c_i) > 0$, para algum $i \in \{0, \ldots, r\}$. Fazendo $c_i = a$, veremos que $v = v_a$.

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

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

Além disso, dado $z \in k(t)$ arbitrário, escrevemos $z = c(t - a)^e g(t)/h(t)$ com $e \in \mathbb{Z}$, $c \in k$ não nulo, $g(t), h(t) \in k[t]$, $h(t) \neq 0$ e tais que $(t - a) \nmid g(t)h(t)$. Então $v(z) = e$. Como v é sobrejetora, $v(t - a) = 1$ e $v = v_a$.

Para a unicidade, observe que $v(t - a) > 0$ e $v(t - b) > 0$, com $a \neq b$, implicaria

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

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

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

Pela Proposição 2.9, 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

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

Logo, para todo $f(t) \in k[t]$, temos $f(t) = ct^m \prod_{i=1}^{r}(1 - c_i/t)$, com $m \in \mathbb{N}$, $c, c_i \in k$ e não nulos, e portanto $v(f(t)) = m$. Mais ainda,

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

se $m \in \mathbb{Z}$, $c \in k$ é não nulo e $t \nmid f_1(t)g_1(t)$. Assim, $v = v_\infty$. ■

3.3 CURVAS ALGÉBRICAS E VALORIZAÇÕES

Nesta seção veremos como associar pontos de uma curva plana irredutível afim à valorizações de $k(C)/k$. Veremos primeiramente em um exemplo particular.

Exemplo 3.5. Seja C a curva afim dada por $F(X,Y) = X = 0$, cujo fecho projetivo é $\mathbb{P}^1(k)$. Então existe uma bijeção entre o conjunto de valorizações de $k(C)$ e os pontos de $\mathbb{P}^1(k)$.

De fato, se C é dada por $F(X,Y) = X = 0$, temos

$$\Gamma(C) = \frac{k[X,Y]}{\langle F(X,Y)\rangle} = \frac{k[X,Y]}{\langle X\rangle} = k[t], \text{ onde } t = \overline{Y} \in \frac{k[X,Y]}{\langle X\rangle},$$

$\overline{Y}$ é a classe residual de Y em $k[X,Y]/\langle F\rangle$ e

$$k(C) = k(t).$$

Então segue dos Exemplos 3.3 e 3.4 e da Proposição 3.3 que existe uma bijeção entre os seguintes conjuntos

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

Definição 3.18. Sejam C uma curva plana afim dada por $F(X,Y) = 0$ e $p = (a,b) \in C$. Dizemos que p é um *pontos 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 não singular*.

Veremos que o exemplo anterior pode ser generalizado no seguinte sentido: dada uma curva plana afim irredutível e não singular C, existe uma bijeção entre um subconjunto das valorizações de $k(C)/k$ e os pontos de C. Para isso, precisaremos de alguns resultados que serão apresentados a seguir.

Proposição 3.4. *Seja K/k corpo de funções algébricas em uma variável. Sejam v uma valorização de K/k e $f \in K$ tal que $v(f) \geq 0$. Então existe um único $c \in k$ tal que $v(f-c) > 0$.*

Demonstração:

Se $f \in k$ então $v(f-f) = v(0) = \infty$ e $c = f$.

Agora, se $f \notin k$ então $[K : k(f)] < \infty$ e, como v é sobrejetiva, existem $z \in K$ 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.

Fatorando $b_i(f)$ temos que $b_i(f) = a\prod_{j=0}^{s}(f - c_j)^{e_j}$ e $v(f - c_j) > 0$ para algum $j = 0, \ldots, s$, pois $v(b_i(f)) > 0$. Denotemos tal c_j por c.

Resta mostrarmos a unicidade. Suponhamos que exista $b \in k$, $b \neq c$ tal que $v(f - b) > 0$. Então,

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

Absurdo. Logo, $c \in k$ é único. ■

Definição 3.19. Seja K/k corpo de funções algébricas em uma variável. Dados $f \in K$, v uma valorização de K/k com $v(f) \geq 0$ e $c \in k$ tal que $v(f - c) > 0$, definimos c o valor de f em v e denotamos $f(v) = c$. Se $v(f) < 0$, dizemos que f tem um pólo em v e denotamos $f(v) = \infty$. Se $v(f) > 0$ dizemos que f tem um zero em v.

Assim cada $f \in K/k$ define uma função

$$f : \{v \text{ é uma valorização de } K/k\} \longrightarrow k \cup \{\infty\}.$$

Lema 3.1. *Seja v uma valorização de K/k.*

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

$$(fg)(v) = f(v)g(v), \tag{3.1}$$

$$(f + g)(v) = f(v) + g(v). \tag{3.2}$$

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

$$\frac{hf(v)}{hg(v)} = \frac{f}{g}(v). \tag{3.3}$$

Demonstração:

(i) Mostremos inicialmente que $(fg)(v) = f(v)g(v)$.

Se $f(v) = c$ e $g(v) = e$, segue da definição que $v(f - c) > 0$ e $v(g - e) > 0$. Então. devemos mostrar que $v(fg - ce) > 0$. Com efeito,

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

Agora, para mostramos que $(f+g)(v) = f(v)+g(v)$ vamos ver que $v[(f+g)-(c+e)] > 0$. Mas,

$$\begin{aligned} v[(f+g)-(c+e)] = v[(f-c)+(g-e)] &\geq \min\{v(f-c),\ v(g-e)\} \\ &> 0. \end{aligned}$$

(ii) Suponhamos $hf(v) = c$ 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,

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

■

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

Seja V uma variedade afim e seja $p \in V$. 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 $b(p) \neq 0$.

Definimos $\mathcal{O}_p(V)$ como sendo o conjunto de todas as funções racionais de V que estão definidas em p. Então, $\mathcal{O}_p(V)$ é um subanel de $k(V)$ contendo $\Gamma(V)$, ou seja,

$$\mathcal{O}_p(V) = \{f \in k(V);\ f \text{ está definida em } p\}.$$

É fato que $\mathcal{O}_p(V)$ é um anel local noetheriano, chamado anel local de V em p, cujo o único ideal maximal é:

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

O anel local é o objeto que traduz propriedades locais. Por exemplo, se C é uma curva plana, temos:

Teorema 3.1. *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: [WF] Teorema 1, pág. 49. ■

Proposição 3.5. *Seja K/k corpo de funções algébricas em uma variável com k como corpo de constantes. Seja R um anel local com $k \subset R \subset K$.*

Então existe B, anel de valorização discreta com K como corpo de frações, tal que $k \subset R \subset B \subset K$ 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 K.

Demonstração: [EO] Corolário 9,7, pág. 62.

■

Veremos agora como associar 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 as classes residuais de X e Y em $K[X,Y]/\langle F\rangle$.

Proposição 3.6. *Se* $S'_{k(C)/k}=\left\{v\in S_{k(C)/k};\ v(x)\geq 0 \text{ e } v(y)\geq 0\right\}$ *e*

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

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

Demonstração: Segue das igualdades (3.1) e (3.2) 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 3.5, existe v valorização de $k(C)/k$ tal que

$$\mathcal{O}_p(C)\subset\mathcal{O}_v \text{ e } \mathcal{M}_p=\mathcal{O}_p(C)\cap\mathcal{M}_v.$$

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

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

Para concluir, 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 3.5,

$$\mathcal{O}_p(C)=\mathcal{O}_v$$

donde concluímos que existe um único $v\in S'_{k(C)/k}$ tal que $p=\varphi(v)$. Portanto, se C é não singular teremos $\varphi: S'_{k(C)/k}\longrightarrow C$ uma bijeção. ■

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

Exemplo 3.6. 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 $t = y/x$, temos $x = t^2 - 1$, $y = t(t^2-1)$ e

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

Nesse caso, pela Proposição 3.3, $S_{k(C)/k} = \{v_c;\ c \in k\} \cup \{v_\infty\}$.

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,

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

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

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

Observe 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 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* $y = w^3-3w^2+2w$.

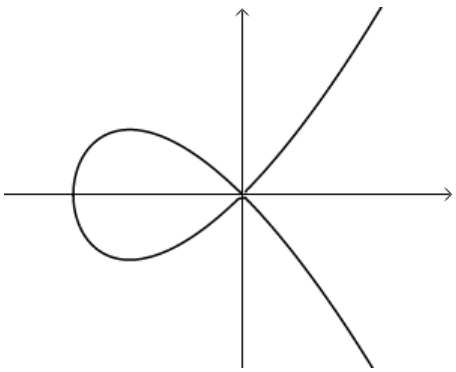


Figura 1 – Curva $X^2+X^3-Y^2 = 0$

Exemplo 3.7. Seja C a curva afim sobre $k = \mathbb{C}$ dada por $F(X, Y) = Y^2 - X^n = 0$, onde $n = 2l + 1$ é um inteiro positivo ímpar. Como no exemplo anterior, 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 $t = y/x^l$, temos $x = t^2$, $y = tx^l = t(t^2)^l = t^{2l+1} = t^n$ e

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

Então, pela Proposição 3.3, $S_{k(C)/k} = \{v_c;\ c \in k\} \cup \{v_\infty\}$.

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

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

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

Portanto,

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

Novamente $p = (0, 0)$ é o único ponto singular de C e $\varphi(v_c) = (0, 0)$ se, e somente se, $c = 0$. Com isso, podemos ver que na origem, a curva C admite uma única valorização v_0 cujo uniformizante local é $u = t$. Nesse caso, $x = u^2$ $y = u^n$.

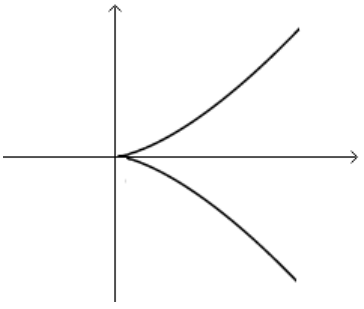


Figura 2 – Curva $Y^2 - X^3 = 0$

Exemplo 3.8. Seja C uma curva afim sobre $k = \mathbb{C}$ dada por $F(X, Y) = Y^3 - X^3 - X^4 = 0$. Fazendo $t = y/x$, temos que $x = t^3 - 1$, $y = t(t^3 - 1)$ e $K(C) = k(t)$. Então,

$$S_{k(C)/k} = \{v_c;\ c \in k\} \cup \{v_\infty\}$$

e $v(x) \geq 0$ e $v(y) \geq 0$ se, e somente se, $v = v_c$ para algum $c \in k$.

Dado $v_c \in S_{k(C)/k}$, temos

$$x(v_c) = t(v_c)^2 = c^3 - 1 \text{ e } y(v_c) = t(v_c)^3 = c(c^3 - 1).$$

Portanto,

$$\begin{array}{rccc} \varphi: & S'_{k(c)/k} & \longrightarrow & k^2 \\ & v_c & \longmapsto & (c^3 - 1, c(c^3 - 1)) \end{array}$$

Novamente, $p = (0, 0)$ é o único ponto singular de C e

$$\varphi(v_c) = (0, 0) \Leftrightarrow c = 1, \frac{\sqrt{3}}{2}i - \frac{1}{2}, -\frac{\sqrt{3}}{2}i - \frac{1}{2}.$$

Então, na origem, a curva C admite três valorizações.

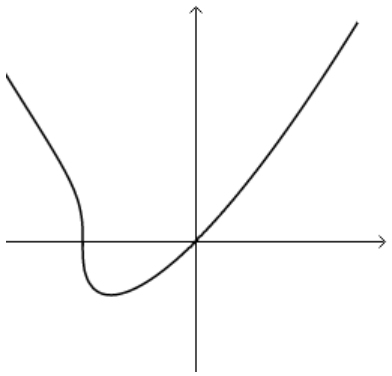


Figura 3 – Curva $Y^3 - X^3 - X^4 = 0$

4 SEMIGRUPOS DE VALORES

4.1 SEMIGRUPO NUMÉRICO

Definição 4.1. Um *semigrupo numérico* S é um subconjunto dos 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) $\mathbb{N}\backslash S$ é finito.

Denotaremos um semigrupo numérico da seguinte forma

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

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

Dizemos que s_1 é a *multiplicidade de* S e o denotamos por $m(S)$, s_n é o *condutor* de S e será denotado por $\beta(S)$, ou simplesmente β.

Definimos $F(S) = \max(\mathbb{N}\backslash S)$ o *número de Frobenius* de S. Observe que $F(S) = \beta - 1$. Os elementos do conjunto $G(S) = \mathbb{N}\backslash S$ são chamados *lacunas* de S e a cardinalidade, $g(S)$, de $G(S)$ é chamada de *gênero* de S.

Exemplo 4.1. $S = \{0, 3, 6, 9, \longrightarrow\}$ é um semigrupo numérico com $F(S) = 8$, $G(S) = \{1, 2, 4, 5, 7, 8\}$ e $g(S) = 6$.

Sejam S um semigrupo numérico e $H \subseteq S$. Dizemos que S é gerado por H se $\forall\ s \in S$, existem $h_1, \ldots, h_n \in H$ e $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$ tais que $s = \sum_{i=1}^{n} \lambda_i h_i$.

Todo semigrupo numérico é finitamente gerado. De fato, note que

$$S = \langle s_1, \ldots, s_n = \beta, \beta + 1, \ldots, \beta + s_1 - 1\rangle, \tag{4.1}$$

Consideremos $H = \{s_1, \ldots, s_n = \beta, \beta + 1, \ldots, \beta + s_1 - 1\}$.

Como $S = \{0, s_1, s_2, \ldots, s_n, \longrightarrow\}$, é fácil ver que todos os elementos de H estão contidos em S. Por outro lado,

$$0, s_1, \ldots, s_n \in \langle s_1, \ldots, s_n = \beta, \beta + 1, \ldots, \beta + s_1 - 1\rangle.$$

Agora, seja um elemento $a \in S$ tal que $a > s_n = \beta$. Pelo algoritmo de Euclides existem $q, r \in \mathbb{N}$ tais que $a = q\beta + r$, com $q \geq 1$ e $0 \leq r < \beta$.

Se $r = 0$, temos que $a = q\beta$. Logo, $a \in \langle s_1, \ldots, s_n = \beta, \beta + 1, \ldots, \beta + s_1 - 1\rangle$. Agora, se $0 < r < \beta$, dividimos r por s_1 e encontramos $q_1, r_1 \in \mathbb{N}$ tal que $r = q_1 r_1 + r_1$ com $0 \leq r_1 < s_1$. Então

$$a = (q\beta + r) = q\beta + q_1 s_1 + r_1 = (q-1)\beta + q_1 s_1 + \beta + r_1 \Rightarrow$$

$$a \in \langle s_1, \ldots, s_n = \beta, \beta + 1, \ldots, \beta + s_1 - 1\rangle,$$

pois $(q-1) \in \mathbb{N}$.

Chamaremos conjunto minimal de geradores de S o conjunto de elementos de S que geram S e tal que nenhum elemento desse conjunto pode ser obtido, como combinação linear com coeficientes lineares, a partir de outros. Pela fórmula (4.1), para encontrar o conjunto minimal de geradores de S, basta tirar do conjunto de geradores aqueles que são soma de dois anteriores.

Proposição 4.1. *O conjunto minimal de geradores de S é único.*

Demonstração: Suponha por absurdo que existam dois conjuntos geradores distintos de S. Sejam estes conjuntos $G_1 = \{g_1, \ldots, g_n\}$ e $G_2 = \{h_1, \ldots, h_m\}$. Suponhamos G_1 e G_2 distintos e que existe $g' \in G_1 \backslash G_2$. Daí $g' \in S$. Além disso, como G_2 é um conjunto gerador de S, temos que $g' = \sum_{i=1}^{m} a_i h_i$, onde $a_i \in \mathbb{N}^*$ e $h_i \in G_2$, $\forall i = 1, \ldots, m$. Agora, como $h_i \in S$ e G_1 é conjunto gerador de S, então $h_i = \sum_{j=1}^{n} b_{ij} g_j$ com $b_{ij} \in \mathbb{N}^*$ e $g_j \in G_1$, $\forall j = 1, \ldots, n$. Logo,

$$g' = \sum_{i=1}^{m} a_i (\sum_{j=1}^{n} b_{ij} g_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_{ij} g_j,$$

isto é, g' é combinação linear com coeficientes positivos de outros elementos do conjunto G_1. Absurdo, pois G_1 é conjunto gerador minimal. Portanto $G_1 \subset G_2$. Analogamente, mostramos que $G_2 \subset G_1$. ■

Lema 4.1. *Seja $H = \langle a_1, a_2, \ldots, a_n\rangle$. Então H é um semigrupo numérico se, e somente se, $mdc(a_1, a_2, \ldots, a_n) = 1$.*

Demonstração: Suponhamos que $\text{mdc}(a_1, a_2, \ldots, a_n) = d \neq 1$. Pela propriedade do mdc, temos que $d | a_i$ para cada $1 \leq i \leq n$, ou seja, $a_i = dk_i$ para cada $1 \leq i \leq n$.

Tome $h \in H$. Então, $h = a_1 x_1 + \cdots + a_n x_n$. Daí, segue que,

$$h = dk_1 x_1 + dk_2 x_2 + \cdots + dk_n x_n \Rightarrow h = d(k_1 x_1 + k_2 x_2 + \cdots + k_n x_n),$$

ou seja, $H \subseteq \langle d\rangle = \{kd;\ k \in \mathbb{N}\}$. Assim, $\mathbb{N}\backslash\langle d\rangle \subseteq \mathbb{N}\backslash H$.

Se $d \neq 1$, existe $e \in \mathbb{N}$ com $d < e < 2d$ tal que

$$\{e + n;\ n \in \mathbb{N}\} \subseteq \mathbb{N}\backslash\langle d\rangle \subseteq \mathbb{N}\backslash H.$$

Isso implica que $\mathbb{N}\backslash\langle d\rangle$ não é finito. Absurdo, pois como H é um semigrupo numérico, $\mathbb{N}\backslash H$ é finito. Logo, $d = 1$.

Para mostrar a recíproca, é suficiente provar que $\mathbb{N}\backslash H$ é finito.

Como $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, existem inteiros $z_1, \ldots, z_n$ e $a_1, \ldots, a_n \in H$ tais que $z_1a_1 + \cdots + z_na_n = 1$. Movendo esses termos com z_i negativo para o lado direito, podemos encontrar $i_1, \ldots, i_k, j_1, \ldots, j_l \in \{1, \ldots, n\}$ tais que $z_{i_1}a_{i_1} + \cdots + z_{i_k}a_{i_k} = 1 - z_1a_{j_1} - \cdots - z_{j_l}a_{j_l}$. Seja $h = -z_1a_{j_1} - \cdots - z_{j_l}a_{j_l}$. Então $h \in \langle a_1, \ldots, a_n\rangle$ e $h + 1 = z_{i_1}a_{i_1} + \cdots + z_{i_k}a_{i_k} \in \langle a_1, \ldots, a_n\rangle$.

Provaremos que se $n \in \mathbb{N}$ for tal que $n \geq (h-1)h + (h-1)$, então $n \in \langle a_1, \ldots, a_n\rangle$. De fato, dado $n \geq (h-1)h + (h-1)$, sejam $q, r \in \mathbb{N}$ tais que $n = qh + r$, com $0 \leq r \leq h-1$.

Como por hipótese $n \geq (h-1)h + (h-1)$, temos que

$$qh + r > (h-1)h + (h-1) \Rightarrow q \geq h - 1 \geq r.$$

Logo

$$n = (rh + r) + (q - r)h = r\underbrace{(h+1)}_{\in H} + (q-r)\underbrace{h}_{\in H}.$$

■

Definição 4.2. A cardinalidade do conjunto minimal de geradores de S, é chamada de *dimensão de mergulho* de S e denotamos por $e(S)$.

Observação 4.1. Se $e(S) = 1$, então $S = \mathbb{N}$.

Exemplo 4.2. Se m é um inteiro positivo, então $S = \{0, m, \longrightarrow\}$ é um semigrupo numérico com multiplicidade m. Pela fórmula (4.1), temos que $S = \langle m, m+1, \ldots, 2m-1\rangle$.

Exemplo 4.3. Seja $S = \{0, 5, 7, 9, 10, 12, 14, \longrightarrow\}$. Temos que $S = \langle 5, 7, 9\rangle$. Logo, $m(S) = 5$, $F(S) = 13$, $G(S) = \{1, 2, 3, 4, 6, 8, 11, 13\}$ e $g(S) = 8$.

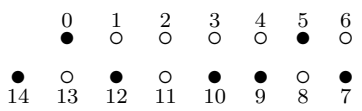


Figura 4 – Diagrama do semigrupo $S = \langle 5, 7, 9\rangle$

O diagrama acima, usado para representar semigrupos, é construído da seguinte forma: na primeira coluna coloca-se o condutor de S e em cada coluna a partir da segunda coloca-se 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 a S e bolinhas brancas indicam os elementos de $\mathbb{N}\backslash S$.

Exemplo 4.4. Seja $S = \{0, 4, 7, 8, 9, 11, \longrightarrow\}$. Temos que $S = \langle 4, 7, 9\rangle$. Logo, $m(S) = 4,\ F(S) = 10,\ G(S) = \{1, 2, 3, 5, 6, 10\}$ e $g(S) = 6$.

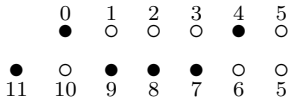


Figura 5 – Diagrama do semigrupo $S = \langle 4, 7, 9\rangle$

Definição 4.3. Seja $E, F \subset \mathbb{Z}$, definimos as seguintes operações:

(i) $E + F = \{a + b;\ a \in E,\ b \in F\}$,

(ii) $E + n = \{a + n;\ a \in E,\ n \in \mathbb{Z}\}$,

(iii) $nE = E + E + ... + E$, n vezes, $n \in \mathbb{N}^*$,

(iv) $E - F = \{a \in \mathbb{Z};\ a + F \subset E\}$.

Definição 4.4. Um *ideal relativo* de S é um subconjunto não vazio I de $\mathbb{Z}$ tal que:

(i) $I + S \subseteq I$

(ii) $I + s \subseteq S$, para algum $s \in \mathbb{Z}$.

Um ideal relativo de S que está contido em S é um *ideal* de S.

4.2 ANÉIS LOCAIS DE CURVAS E SEMIGRUPOS

Sejam C uma curva plana irredutível dada por $F(X, Y) = 0$ e $k(C)/k$ o corpo de funções racionais de C.

Dado $p \in C$, temos que $\mathcal{O}_p(C) \subset k(C)$ é um anel local noetheriano e que $\overline{\mathcal{O}_p(C)}$ é a interseção de todos os anéis de valorização de $k(C)$ que contém $\mathcal{O}_p(C)$ (ver Corolário 2.5). Observe que pela Proposição 2.11, como $k(C)/k$ é um corpo de funções algébricas em uma variável, os anéis de valorizações de $k(C)$ são anéis de valorização discreta.

Além disso, temos que $\overline{\mathcal{O}_p(C)}$ é um $\mathcal{O}_p(C)$-módulo finito e portanto $\mathcal{O}_p(C)$-ideal fracionário (ver [R], Teorema 8.11, pág. 122). Como consequência temos que

$$0 \neq (\mathcal{O}_p(C) : \overline{\mathcal{O}_p(C)}).$$

Definição 4.5. Dizemos que $p \in C$ é um ponto *unirramificado* se existir uma única valorização v de $k(C)/k$ tal que $\mathcal{O}_p(C) \subseteq \mathcal{O}_v$. Nesse caso, temos que $\overline{\mathcal{O}_p(C)} = \mathcal{O}_v$. Caso contrário, dizemos que $p \in C$ é um ponto *multirramificado*.

Definição 4.6. Dado $p \in C$ unirramificado e $v : k(C) \to \mathbb{Z} \cup \{\infty\}$ valorização tal que $\mathcal{O}_p(C) \subset \mathcal{O}_v$, definimos:

$$v(\mathcal{O}_p(C)) = \{v(x);\ x \in \mathcal{O}_p(C)\}.$$

Proposição 4.2. *$S = v(\mathcal{O}_p(C))$ é um semigrupo numérico.*

Demonstração: De fato,

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

(ii) Dados $a, b \in S$, existem $x, y \in \mathcal{O}_p(C)$ tais que $a = v(x)$ e $b = v(y)$. Daí, segue que:

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

pois $xy \in \mathcal{O}_p(C)$.

(iii) Para concluir, devemos mostrar que $\mathbb{N}\backslash S$ é finito. Para isso, observe que sendo $p \in C$ unirramificado temos $\mathcal{O}_v = \overline{\mathcal{O}_p(C)}$. Então, dado $z \in (\mathcal{O}_p(C) : \mathcal{O}_v)$, temos que $z\mathcal{O}_v \subseteq \mathcal{O}_p(C)$. Seja t o parâmetro local de $\mathcal{O}_v$. Como $(\mathcal{O}_p(C) : \mathcal{O}_v)$ é um $\mathcal{O}_v$-módulo, temos $t^i z \in (\mathcal{O}_p(C) : \mathcal{O}_v)$ para todo $i \in \mathbb{N}$. Assim,

$$v(t^i z) = v(t^i) + v(z) = i + v(z) \in S,$$

para todo i. Logo, $\mathbb{N}\backslash S$ é finito.

Portanto, $S = v(\mathcal{O}_p(C))$ é um semigrupo numérico. ■

Observação 4.2. Se $p \in C$ for simples, $\mathcal{O}_p(C) = \mathcal{O}_v$ para uma única valorização $v : k(C) \longrightarrow \mathbb{Z} \cup \{\infty\}$. Sendo v um aplicação sobrejetiva, existe $x \in k(C)$ tal que $v(x) = 1$. Como

$$\mathcal{O}_p(C) = \{z \in k(C);\ v(z) \geq 0\},$$

temos que $x \in \mathcal{O}_p(C)$ e $1 \in v(\mathcal{O}_p(C))$. Logo, $v(\mathcal{O}_p(C)) = \mathbb{N}$.

Exemplo 4.5. Seja C a curva plana irredutível dada por $Y^2 = X^n$, onde n é ímpar e seja $p = (0, 0)$ o único ponto singular de C. Seja R o anel local de C em p. Então, como vimos no Exemplo 3.7, $k(C) = k(t)$ e existe uma única valorização v de $k(C)/k$ tal que

$$k \subset R = \mathcal{O}_p(C) \subset \mathcal{O}_v.$$

A saber, $v = v_0$, onde $v_0 : k(t) \to \mathbb{Z} \cup \{\infty\}$ é tal que $v_0(t) = 1$ (ver Exemplo 3.3).

Neste caso,

$$k \subset k[t^2, t^n] \subset R = k[t^2, t^n]_{\langle t^2, t^n \rangle} \subset \overline{R} = k[t]_{\langle t \rangle}.$$

Seja $S = v(R)$. Afirmamos que $S = \langle 2, n \rangle = \{0, 2, 4. \ldots, n-3, n-1, \longrightarrow\}$.

De fato,

i) $v(t^2) = 2$, $v(t^n) = n$ e $t^2, t^n \in R$. Logo, $2, n \in S$ e

$$\langle 2, n \rangle = \{0, 2, 4. \ldots, n-3, n-1, \longrightarrow\} \subset S.$$

ii) Suponhamos $n = 2l + 1$. Um elemento genérico de R é da forma

$$z = \frac{f(t^2, t^n)}{g(t^2, t^n)}$$

onde $f(T_1, T_2), g(T_1, T_2) \in k[T_1, T_2]$ são polinômos não nulos e $g(t^2, t^n) \notin \langle t^2, t^n \rangle$, isto é, o termo constante de $g(T_1, T_2)$ é não nulo.

Façamos $f(T_1, T_2) = \sum_{i+j=0}^{s} a_{ij} T_1^i T_2^j \in k[T_1, T_2]$. Então

$$f(t^2, t^n) = \sum_{i+j=0}^{s} a_{ij} (t^2)^i (t^n)^j = (a_{00} + a_{10} t^2 + \cdots + a_{l0} t^{(2l)} + a_{01} t^n + \text{ termos de grau maior }),$$

onde $a_{ij} \in k$, para todo i, j. Daí segue que

$$v(f(t^2, t^n)) = \begin{cases} 0, & \text{se } a_{00} \neq 0; \\ 2k, & \text{se } a_{00} = a_{10} = \cdots = a_{(k-1)0} = 0 \text{ e } a_{k0} \neq 0, \text{ para } 0 < k < l; \\ a, & \text{com } a \geq n, \text{ se } a_{00} = a_{10} = \cdots = a_{l0} = 0. \end{cases}$$

podendo ser qualquer inteiro maior que 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

$$g(t^2, t^n) = \sum_{i+j=0}^{r} b_{ij} (t^2)^i (t^n)^j = (b_{00} + b_{10} t^2 + \cdots + a_{l0} t^{(2l)} + b_{01} t^n + \text{ termos de grau maior })$$

e, como $b_{00} \neq 0$, $v(g(t^2, t^n)) = 0$.

Logo, $v(z) = v(f(t^2, t^n)) - v(g(t^2, t^n)) = v(f(t^2, t^n))$ e daí segue que

$$S \subset \{0, 2, 4. \ldots, n-3, n-1, \longrightarrow\} = \langle 2, n \rangle.$$

No caso de $p \in C$ ser multirramificado, trabalharemos no completamento dos anéis locais e os objetos associados serão os semigrupos de valores.

4.3 COMPLETAMENTO

Apresentaremos agora alguns resultados que serão usados para definirmos o $\mathfrak{m}$-ádico completamento de um anel, onde $\mathfrak{m} \subseteq R$ é o ideal maximal.

4.3.1 **Sistema Inverso e Limite Inverso**

Definição 4.7. Um conjunto parcialmente ordenado I é chamado um *conjunto dirigido* se, para cada par $i, j \in I$, existe $k \in I$ tal que $i \leq k$ e $j \leq k$.

Lema 4.2. *Seja I um conjunto dirigido. Dado $\{\lambda_1, \ldots, \lambda_n\} \subset I$, existe $\lambda \in I$ tal que $\lambda_i \leq \lambda$ para todo $i \in \{1, \ldots, n\}$.*

Demonstração: Faremos indução em n.

Para $n = 2$, pela definição de conjunto dirigido, existe $\lambda \in I$ tal que $\lambda_1 \leq \lambda$ e $\lambda_2 \leq \lambda$.

Para $n = 3$, sejam $\lambda_1, \lambda_2, \lambda_3 \in I$. Então existe $\lambda' \in I$ tal que $\lambda_1 \leq \lambda'$ e $\lambda_2 \leq \lambda'$. E também existe $\lambda'' \in I$ tal que $\lambda' \leq \lambda''$ e $\lambda_3 \leq \lambda''$. Logo $\lambda_1 \leq \lambda'', \lambda_2 \leq \lambda''$ e $\lambda_3 \leq \lambda''$.

Suponhamos verdadeiro para n elementos de I, isto é, dado $\{\lambda_1, \ldots, \lambda_n\} \subset I$, existe $\lambda \in I$ tal que $\lambda_1 \leq \lambda, \ldots, \lambda_n \leq \lambda$. Mostraremos que a afirmação é verdadeira para $\{\lambda_1, \ldots, \lambda_n, \lambda_{n+1}\} \subset I$. De fato, por hipótese de indução, existe $\lambda \in I$ tal que $\lambda_1 \leq \lambda, \ldots, \lambda_n \leq \lambda$. Como I é um conjunto dirigido, existe $\lambda' \in I$ tal que $\lambda \leq \lambda'$ e $\lambda_n + 1 \leq \lambda'$. Portanto, $\lambda_1 \leq \lambda \leq \lambda', \ldots, \lambda_n \leq \lambda \leq \lambda'$ e $\lambda_n + 1 \leq \lambda'$. ■

Definição 4.8. Sejam R um anel e I um conjunto dirigido. Um *sistema inverso* de R-módulos sobre I, consiste de uma família de R-módulos $(M_i)_{i \in I}$ e, uma família de R-homomorfismos $\{\mu_{ij} : M_i \longrightarrow M_j;\ i, j \in I\}$ definidos sempre que $j \leq i$, satisfazendo os seguintes axiomas:

(i) μ_{ii} é a aplicação identidade de M_i, para todo $i \in I$;

(ii) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ sempre que $k \leq j \leq i$.

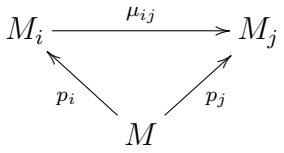
Em outras palavras, os diagramas como abaixo, quando definidos, são comutativos.

$$\begin{array}{ccc} M_i & \xrightarrow{\mu_{ij}} & M_j \\ {\scriptstyle \mu_{ik}}\downarrow & \swarrow {\scriptstyle \mu_{jk}} & \\ M_k & & \end{array}$$

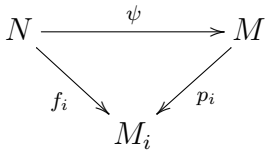
Denotamos um sistema inverso por $\mathbb{M} = (M_i, \mu_{ij})_{i \in I}$.

Definição 4.9. Seja $\mathbb{M} = (M_i, \mu_{ij})_{i\in I}$ um sistema inverso de R-módulos. Um *limite inverso* desse sistema é um par $(M, \{p_i\}_{i\in I})$, onde M é um R-módulo e $\{p_i : M \longrightarrow M_i\}_{i\in I}$ é uma família de R-homomorfismos de módulos que satisfaz as seguintes condições:

(i) $p_j = \mu_{ij} \circ p_i$, para todo $j \leq i$;



(ii) (Propriedade Universal do Limite Inverso) Dado qualquer par $(N, \{f_i\})_{i\in I}$, onde N é um R-módulo e $\{f_i : N \longrightarrow M_i\}_{i\in I}$ é uma família de R-homomorfismos tal que $f_j = \mu_{ij} \circ f_i$, para todo $j \leq i$, existe um único R-homomorfismo $\psi : N \longrightarrow M$ tal que $f_i = p_i \circ \psi$, para todo $i \in I$.



Observação 4.3. As aplicações p_i do limite inverso são chamadas *projeções*, porém não são necessariamente sobrejetivas.

Definição 4.10. Definimos $\prod_{i\in I} M_i$, o *produto direto* de R-módulos, com as operações usuais de soma e multiplicação por escalar, isto é, para todo $x = (x_i)_{i\in I}, y = (y_i)_{i\in I} \in \prod_{i\in I} M_i$ e para todo $a \in R$,

$$x + y = (x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \text{ e}$$

$$ax = a(x_i)_{i\in I} = (ax_i)_{i\in I}.$$

Teorema 4.1. *Seja $\mathbb{M} = (M_i, \mu_{ij})_{i\in I}$ um sistema inverso de R-módulos. Então:*

(i) Existe $(M, \{p_i\}_{i\in I})$ limite inverso de $\mathbb{M}$, denotado por $\varprojlim M_i$.

(ii) Se (M, p_i) e (N, q_i) são limites inversos de $\mathbb{M}$, então existe um único R-homomorfismo $\gamma : M \longrightarrow N$ tal que $q_i \circ \gamma = p_i$, para todo $i \in I$.

Demonstração:

(i) Sejam $\prod_{i\in I} M_i$ o produto direto de R-módulos e, para cada $i \in I$, π_i a aplicação projeção do produto direto em M_i. Defina

$$M = \left\{(x_i)_{i\in I} \in \prod_{i\in I} M_i \ ; \ \mu_{ij}(x_i) = x_j, \text{ para todo } i \geq j\right\},$$

e $p_i = \pi_i|_M$: $M \longrightarrow M_i$ as restrições das projeções canônicas a M.

Afirmamos que $(M, \{p_i\}_{i\in I})$ é limite inverso de $\mathbb{M}$.

Vamos verificar que M é um submódulo do produto direto $\prod_{i\in I} M_i$.

Com efeito, dados $x = (x_i)_{i\in I}, y = (y_i)_{i\in I} \in M$ e $a \in R$, temos que $\mu_{ij}(x_i) = x_j$ e $\mu_{ij}(y_i) = y_j$. Assim:

(i) $x - y = (x_i - y_i)_{i\in I}$ e $\mu_{ij}(x_i - y_i) = \mu_{ij}(x_i) - \mu_{ij}(y_i) = x_j - y_j \in M_j$.

(ii) $ax = (ax_i)_{i\in I}$ e $\mu_{ij}(ax_i) = a\mu_{ij}(x_i) = ax_j \in M_j$.

Logo, M é um submódulo do produto direto.

Agora, sejam $p_k : M \longrightarrow M_k$ e $p_l : M \longrightarrow M_l$ as projeções canônicas de M em M_k e M_l, respectivamente. Se $k \leq l \in I$, então:

$$(\mu_{lk} \circ p_l)((x_i)_{i\in I}) = \mu_{lk}(p_l(x_i)_{i\in I}) = \mu_{lk}(x_l) = x_k = p_k((x_i)_{i\in I}).$$

Portanto, $p_k = \mu_{lk} \circ p_l$, para todo $k \leq l$.

Agora, suponhamos que N é um R-módulo e que $\{f_i : N \longrightarrow M_i\}_{i\in I}$ é uma família de R-homomorfismos tal que $f_j = \mu_{ij} \circ f_i$, para todo $j \leq i$. Vamos mostrar que existe um único R-homomorfismo $\psi : N \longrightarrow M$ tal que $f_i = p_i \circ \psi$, para todo $i \in I$.

Seja $\psi : N \longrightarrow \prod_{i\in I} M_i$, definida por $\psi(y) = (f_i(y))_{i\in I}$. Como cada f_i é homomorfismo, temos que ψ é homomorfismo. De $f_j = \mu_{ij} \circ f_i$, sempre que $j \leq i$, segue que $\psi : N \longrightarrow M \subset \prod_{i\in I} M_i$ e que

$$p_i \circ \psi(y) = \pi_i(\psi(y)) = \pi_i((f_i(y))_{i\in I}) = f_i(y) \Rightarrow p_i \circ \psi = f_i.$$

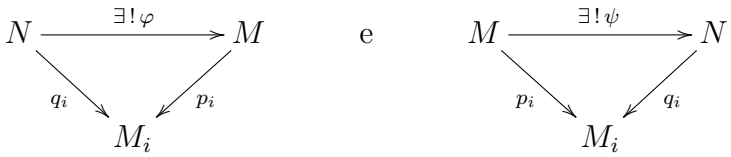
Por fim, para mostrar a unicidade, suponhamos que exista outro R-homomorfismo $\psi' : N \longrightarrow M$ tal que $f_i = p_i \circ \psi'$, para todo $i \in I$. Então, para todo $y \in N$

$$p_i(\psi'(y)) = f_i(y), \forall\, i \in I \Rightarrow p_i(\psi(y)) = p_i(\psi'(y)), \forall\, i \in I$$

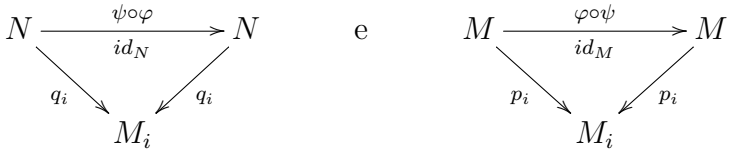
$$\Rightarrow \psi(y) = \psi'(y), \forall\, y \in N \Rightarrow \psi = \psi'.$$

Portanto, $(M, \{p_i\}_{i\in I})$ é limite inverso de $\mathbb{M}$.

(ii) Sejam $(M, \{p_i\}_{i\in I})$ e $(N, \{q_i\}_{i\in I})$ limites inversos de $(M_i, \{\mu_{ij}\}_{i\in I})$. Aplicando a propriedade universal de $(M, \{p_i\}_{i\in I})$, existe um único R-homomorfismo $\varphi : N \longrightarrow M$ tal que $p_i \circ \varphi = q_i$. De forma análoga, aplicando a propriedade universal de $(N, \{q_i\}_{i\in I})$, existe um único R-homomorfismo $\psi : M \longrightarrow N$ tal que $q_i \circ \psi = p_i$.



Assim, $q_i \circ (\psi \circ \varphi) = p_i \circ \varphi = q_i$ e $p_i \circ (\varphi \circ \psi) = q_i \circ \psi = p_i$, para todo $i \in I$. Ou seja, os diagramas



são comutativos. Logo, pela unicidade da aplicação dada na definição do limite inverso temos que $\psi \circ \varphi = id_N$ e $\varphi \circ \psi = id_M$.

■

4.3.2 **Completamento**

Sejam R um anel e M um R-módulo. Para um conjunto dirigido I, seja $\mathbb{F} = \{M_\lambda\}_{\lambda \in I}$ uma família de submódulos de M, indexada por I, tal que para todo $\lambda, \mu \in I$ e $\lambda < \mu$ temos $M_\lambda \supset M_\mu$. Em seguida, tome $\mathbb{F}$ como um sistema de vizinhanças de 0. Mais especificamente, defina

$$U \subset M \text{ é aberto} \iff \forall x \in U,\ \exists\ \lambda \in I \text{ tal que } x + M_\lambda \subseteq U.$$

Então, M é um grupo topológico.

De fato:

(i) $\emptyset$ é aberto por vacuidade e M é aberto pois, $\forall\ x \in M$ e $\forall\ M_\lambda \in \mathbb{F}$ tem-se que $x + M_\lambda \subset M$.

(ii) Seja $\{U_\alpha\}_{\alpha \in \wedge}$ uma coleção arbitrária de abertos. Dado $x \in \bigcup_{\alpha \in \wedge} U_\alpha$ temos que $x \in U_\alpha$ para algum $\alpha \in \wedge$. Como U_α é aberto, então existe $\lambda \in I$ tal que $x + M_\lambda \subset U_\alpha$. Daí $x + M_\lambda \subset \bigcup_{\alpha \in \wedge} U_\alpha$. Logo $\bigcup_{\alpha \in \wedge} U_\alpha$ é aberto.

(iii) Seja $U_1, U_2, \ldots, U_n$ uma coleção finita de abertos. Dado $x \in \bigcap_{i=1}^{n} U_i$ temos que $x \in U_i$ para todo $i = 1, \ldots, n$. Então existe $\lambda_i \in I$ tal que $x + M_{\lambda_i} \subset U_i$ para cada $i \in \{1, \cdots, n\}$, tais que:

$$\begin{aligned} x + M_{\lambda_1} &\subseteq U_1 \\ x + M_{\lambda_2} &\subseteq U_2 \\ &\vdots \\ x + M_{\lambda_n} &\subseteq U_n \end{aligned}$$

Seja $\lambda \in I$ tal que $\lambda_i \leq \lambda\ \forall i \in \{1, \ldots, n\}$. Assim, $M_{\lambda_i} \supseteq M_\lambda\ \forall i \in \{1, \ldots, n\}$.

Logo

$$\begin{array}{ccccc} x+M_\lambda & \subseteq & x+M_{\lambda_1} & \subseteq & U_1 \\ x+M_\lambda & \subseteq & x+M_{\lambda_2} & \subseteq & U_2 \\ & & & \vdots & \\ x+M_\lambda & \subseteq & x+M_{\lambda_n} & \subseteq & U_n \end{array}$$

Portanto, $x+M_\lambda \subseteq \bigcap_{i=1}^{n} U_i$.

Logo, M é um *grupo topológico*.

Definição 4.11. Uma topologia definida a partir de um sistema de vizinhanças de 0 é chamada de *topologia linear*.

Lema 4.3. *M_λ é um subconjunto aberto e fechado.*

Demonstração: De fato, cada $M_\lambda \subset M$ é um conjunto aberto, cada classe $m+M_\lambda$ é novamente aberto e o complementar $M-M_\lambda$ *de* M_λ é uma união de classes, que também é aberto. ■

Segue do lema anterior que o módulo quociente M/M_λ é discreto na topologia quociente.

Além disso, para $\lambda < \mu$, a inclusão $M_\lambda \supset M_\mu$ induz um homomorfismo natural $\varphi_{\lambda\mu} : M/M_\mu \longrightarrow M/M_\lambda$. Esses homomorfismos fazem do conjunto $\{M/M_\lambda; \varphi_{\lambda\mu}\}$ um sistema inverso de R-módulos sobre o conjunto dirigido I.

Definição 4.12. O limite inverso $\varprojlim M/M_\lambda$ do sistema inverso $\{M/M_\lambda, \varphi_{\lambda\mu}\}_{\lambda\in I}$ é chamado o *completamento* de M e será denotado por $\hat{M}$.

Segue da construção do limite inverso que

$$\hat{M} = \left\{ (x_\lambda)_{\lambda\in I} \in \prod_{i=1}(M/M_\lambda);\ \varphi_{\lambda\mu}(x_\mu) = x_\lambda \text{ para todo } \lambda \leq \mu \right\}$$

e que existe um R-homomorfismo natural $\psi : M \longrightarrow \hat{M}$ que é contínua.

Definição 4.13. Dizemos que M é *completo* quando o homomorfismo $\psi : M \longrightarrow \hat{M}$ é um isomorfismo.

Exemplo 4.6. Sejam R um anel, $\mathfrak{m} \subseteq R$ ideal e M um R-módulo. Para cada $i \in \mathbb{N}$, sejam $R_i = R/\mathfrak{m}^i$ e $M_i = M/\mathfrak{m}^i M$ e, para $j \leq i$, considere a aplicação canônica $\phi_{ij} : R/\mathfrak{m}^i \longrightarrow R/\mathfrak{m}^j$. Então $(M_i, \phi_{ij})_{i\in\mathbb{N}}$ é um sistema inverso de R-módulos. O $\mathfrak{m}$-*ádico* completamento de R é o anel

$$\hat{R} = \varprojlim \frac{R}{\mathfrak{m}^i}.$$

O $\mathfrak{m}$-ádico completamento de M é o R-módulo

$$\hat{M} = \varprojlim \frac{M}{\mathfrak{m}^i M}.$$

Exemplo 4.7. Sejam k um corpo, $R = k[t]$ o anel de polinômios em uma variável e $\mathfrak{m} = \langle t \rangle$. Para cada inteiro positivo i, seja

$$R_i = \frac{k[t]}{\mathfrak{m}^i} = \frac{k[t]}{\langle t^i \rangle}.$$

Então, $\hat{R} = \varprojlim \frac{k[t]}{\mathfrak{m}^i} \simeq k[[t]]$, o anel das séries de potências formais em uma variável.

Para ver isso, observe que, por construção

$$\hat{R} = \left\{ (\overline{p_i(t)})_{i \in \mathbb{N}^*}; \overline{p_i(t)} \in \frac{k[t]}{\langle t^i \rangle} \text{ e } \overline{p_i(t)} = \overline{p_j(t)} \in \frac{k[t]}{\langle t^j \rangle}, \forall\, j \leq i \right\}.$$

Ou seja, os polinômios $p_i(t)$ e $p_j(t)$ coincidem até a potência j, sempre que $j \leq i$. Desse modo, existe um homomorfismo natural de $\hat{R}$ em $k[[t]]$ que associa o elemento $(\overline{p_i(t)})_{i \in \mathbb{N}^*}$ de $\hat{R}$ à série de potências $\sum_{i=1}^{\infty} a_i t^i$ tal que $p_i(t) = a_0 + a_1 t + \cdots + a_i t^i$, para todo $i > 0$. Esse homomorfismo é claramente bijetor, portanto é um isomorfismo.

Exemplo 4.8. Sejam k um corpo, $R = k[t_1, \ldots, t_n]$ o anel de polinômios em n variáveis com coeficiente em k e $\mathfrak{m} = \langle t_1, \ldots, t_n \rangle$. Então, o completamento de R com respeito a $\mathfrak{m}$ é $\widehat{R} = k[[t_1, \ldots, t_n]]$, o anel das séries de potências formais em n variáveis.

Teorema 4.2. *Sejam R um anel, M um R-módulo com uma topologia linear e $N \subset M$ um submódulo. Considere em N a topologia induzida de M e em M/N a topologia quociente. Então, estas topologias são lineares e:*

(i) $0 \to \widehat{N} \to \widehat{M} \to \widehat{M/N}$ *é uma sequência exata e* $\widehat{N}$ *é o fecho de* $\psi(N)$ *em* $\widehat{M}$*, onde* $\psi : M \longrightarrow \widehat{M}$ *é uma aplicação natural.*

(ii) Se, além disso, a topologia de M é definida por uma cadeia decrescente de submódulos $M_1 \supset M_2 \supset \ldots$, então

$$0 \to \widehat{N} \to \widehat{M} \to \widehat{M/N} \to 0$$

é uma sequência exata. Em outras palavras, $\widehat{M/N} \simeq \widehat{M}/\widehat{N}$.

Demonstração: [MR] Teorema 8.1, pág. 56. ■

Como consequência desse último resultado temos:

Teorema 4.3. *Seja R um anel Noetheriano e $\mathfrak{m} = \langle a_1, \ldots, a_n \rangle$ um ideal de R. Então, $\hat{R}$, o $\mathfrak{m}$-ádico completamento de R é tal que:*

$$\hat{R} \simeq \frac{R[[X_1, \ldots, X_n]]}{(X_1 - a_1, \ldots, X_n - a_n)}.$$

Logo, $\hat{R}$ é um anel Noetheriano.

Demonstração: [MR] Teorema 8.12, pág. 61. ■

Teorema 4.4. *Seja R um anel semilocal com ideais maximais $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ e seja $\mathfrak{m} = rad(R) = \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_r$ o nilradical de R. Então, o $\mathfrak{m}$-ádico completamento $\hat{R}$ de R se decompõe como um produto direto*

$$\hat{R} = \hat{R}_1 \times \ldots \times \hat{R}_r,$$

onde $R_i = R_{\mathfrak{m}_i}$ e $\hat{R}_i$ é o $\mathfrak{m}_i$-ádico completamento do anel local R_i.

Demonstração: [MR] Teorema 8.15, pág. 62. ■

4.4 SEMIGRUPOS DE VALORES

Nesta seção veremos como associar aos anéis locais de curvas em pontos singulares multirramificados o conceito de semigrupos de valores.

Seja R um anel local, noetheriano, reduzido e unidimensional, tal que seu fecho inteiro $\overline{R}$, no anel total de frações $Q(R)$, é um R-módulo finito. Sejam $\mathfrak{p}_i,\ i = 1, \ldots, n$ primos minimais de R. Se $\overline{R/\mathfrak{p}_i}$ é o fecho inteiro de $R/\mathfrak{p}_i$ no seu corpo quociente $Q(R/\mathfrak{p}_i)$, veremos que o diagrama a seguir é válido, onde todos os homomorfismos são injetivos.

$$\begin{array}{ccc} R & \longrightarrow & R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n \\ \downarrow & & \downarrow \\ \overline{R} & \xrightarrow{\simeq} & \overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n} \\ \downarrow & & \downarrow \\ Q(R) & \xrightarrow{\simeq} & Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n) \end{array} \tag{4.2}$$

Proposição 4.3. *Seja R um anel noetheriano e reduzido. Sejam $\mathfrak{p}_i,\ i = 1, \ldots, n$ primos minimais de R. Então $Q(R) \simeq \prod_{i=1}^{n} Q(R/\mathfrak{p}_i)$.*

Demonstração: Primeiro vale a pena lembrar que o corpo de frações de R é o conjunto

$$S^{-1}R = \left\{ \frac{r}{s}; r \in R \text{ e } s \in S \right\},$$

onde S é o conjunto de não divisores de zero de R e $r/s = r_1/s_1$ se e somente se existe $t \in S$ tal que $t(rs_1 - r_1s) = 0$ em R. Além disso, como $\mathfrak{p}_i$ é um ideal primo, $R/\mathfrak{p}_i$ é um domínio de integridade, para todo $i = 1, \ldots, n$. Nesse caso, o anel total de frações de $R/\mathfrak{p}_i$ é seu corpo de frações.

Afirmamos que $S^{-1}\mathfrak{p}_i$ são os únicos primos de $S^{-1}R$.

De fato, os ideais primos de $S^{-1}R$ são da forma $S^{-1}\mathfrak{p}$, onde $\mathfrak{p} \subset R$ é primo e $\mathfrak{p} \cap S = \emptyset$. Como $R\backslash S$ é o conjunto de divisores de zero de R , portanto é igual a $\bigcup_{i=1}^{n} \mathfrak{p}_i$ (ver [AM], pág.59) temos que:

$$\mathfrak{p} \cap S = \emptyset \Rightarrow \mathfrak{p} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}_i$$

para algum $i = 1, \ldots, n$. Como $\mathfrak{p}_i$ são primos minimais, $\mathfrak{p} = \mathfrak{p}_i$, para algum $i = 1, \ldots, n$. Assim, os ideais maximais de $S^{-1}R$ estão entre os ideais $S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_n$.

Para concluirmos a afirmação vamos mostrar que $S^{-1}\mathfrak{p}_i \subseteq S^{-1}\mathfrak{p}_j \Leftrightarrow \mathfrak{p}_i \subseteq \mathfrak{p}_j$.

Sejam $\frac{r_i}{s_i},\ \frac{r_j}{s_j} \in Q(R)$ tais que $\frac{r_i}{s_i} = \frac{r_j}{s_j}$, com $r_i \in \mathfrak{p}_i$ e $r_j \in \mathfrak{p}_j$. Então existe $t \in S$ (não divisor de zero) tal que $(r_i s_j - r_j s_i)t = 0$ em R. Logo,

$$(r_i s_j - r_j s_i) = 0 \Rightarrow r_i s_j = r_j s_i \in \mathfrak{p}_j.$$

Como $s_j \notin \mathfrak{p}_j$, $r_i \in \mathfrak{p}_j$ e, portanto, $\mathfrak{p}_i \subset \mathfrak{p}_j$. Sendo $\mathfrak{p}_i,\ \mathfrak{p}_j$ minimais, temos $\mathfrak{p}_i = \mathfrak{p}_j$.

Logo, pelo Teorema Chinês dos Restos, temos:

$$\frac{S^{-1}R}{\cap_{i=1}^{n} S^{-1}\mathfrak{p}_i} \simeq \frac{S^{-1}R}{S^{-1}\mathfrak{p}_1} \times \frac{S^{-1}R}{S^{-1}\mathfrak{p}_2} \times \cdots \times \frac{S^{-1}R}{S^{-1}\mathfrak{p}_n}.$$

Observe que $\bigcap_{i=1}^{n} S^{-1}\mathfrak{p}_i \subset S^{-1}(\bigcap_{i=1}^{n} \mathfrak{p}_i) = 0$ implica

$$Q(R) = S^{-1}R \simeq \frac{S^{-1}R}{S^{-1}\mathfrak{p}_1} \times \frac{S^{-1}R}{S^{-1}\mathfrak{p}_2} \times \cdots \times \frac{S^{-1}R}{S^{-1}\mathfrak{p}_n}.$$

Além disso, não é difícil ver que

$$\frac{S^{-1}R}{S^{-1}\mathfrak{p}_i} \simeq Q(R/\mathfrak{p}_i).$$

Portanto,

$$Q(R) \simeq Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n).$$

■

Proposição 4.4. *Seja R um anel noetheriano e reduzido e sejam $\mathfrak{p}_i$, para $i = 1, \ldots, n$, primos minimais de R. Então $\overline{R} \cong \overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n}$, onde $\overline{R}$ e $\overline{R/\mathfrak{p}_i}$, para $i = 1, \ldots, n$, representam o fecho inteiro dos respectivos anéis.*

Demonstração: Do diagrama a seguir, onde todos os homomorfismos são injetivos,

$$\begin{array}{ccc} R & \longrightarrow & R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n \\ \downarrow & & \downarrow \\ Q(R) & \xrightarrow{\simeq} & Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n) \end{array}$$

segue que $\overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n} \hookrightarrow Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n)$.

Como $R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$ é um R-módulo finitamente gerado, temos que $R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$ é inteiro sobre R.

Além disso, $\overline{R/\mathfrak{p}_i}$ inteiro sobre $R/\mathfrak{p}_i$ implica que $\overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n}$ é inteiro sobre $R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$ e, consequentemente, inteiro sobre R.

Então, temos que $\overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n} \subseteq \overline{R} \subseteq Q(R)$. Agora devemos mostrar que $\overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n}$ é integralmente fechado em $Q(R) \simeq Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n)$.

Para isso, seja $(k_1, \ldots, k_n) \in Q(R) \simeq Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n)$ inteiro sobre R. Então, cada k_i é inteiro sobre R e portanto sobre $R/\mathfrak{p}_i$, ou seja, pertence a $\overline{R/\mathfrak{p}_i}$. ■

Agora, seguindo [BDF], veremos como associar a R o objeto chamado semigrupo de valores.

No que segue vamos supor que R é um anel **noetheriano, reduzido, unidimensional, local e tal que o fecho inteiro $\overline{R}$ no anel total de frações de R é um R-módulo finito.**

Uma importante classe de exemplos desses anéis são os anéis locais de uma curva algébrica.

Sejam $\mathfrak{p}_i$, para $i = 1, \ldots, n$, primos minimais de R. Então, pela Proposição 4.4, $\overline{R} = \overline{R/\mathfrak{p}_1} \times \cdots \times \overline{R/\mathfrak{p}_n}$, onde $\overline{R/\mathfrak{p}_i}$ é o fecho inteiro de $R/\mathfrak{p}_i$ em $Q(R/\mathfrak{p}_i)$. Desde que $\overline{R/\mathfrak{p}_i}$ é um domínio de integridade unidimensional, noetheriano e integralmente fechado, ele é a interseção de domínios de valorização discreta obtidos localizando-se $\overline{R/\mathfrak{p}_i}$ nos seus ideais maximais (ver [CDK], Teorema 2.10, pág. 407).

Observação 4.4. Que $\overline{R/\mathfrak{p}_i}$ é a interseção de anéis de valorização do seu corpo de frações segue do Corolário 2.5. Que tais anéis de valorizações são anéis de valorizações discretas segue de [AM], Proposição 9.2, pág. 105.

Então, para cada $i = 1, \ldots, n$ podemos escrever $\overline{R/\mathfrak{p}_i} = B_{i1} \cap B_{i2} \cap \ldots \cap B_{ih_i}$, onde B_{ij} são anéis de valorização discreta, para todo $1 \leq j \leq h_i$. Seja v_{ij} a valorização discreta associada a B_{ij}, para $1 \leq i \leq n$ e $1 \leq j \leq h_i$.

Definição 4.14. Para cada $r = (r_1, \ldots, r_n) \in Q(R) \simeq Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n)$ definimos:

$$v(r) := (v_{11}(r_1), \ldots, v_{1h_1}(r_1), v_{21}(r_2), \ldots, v_{2h_2}(r_2), \ldots, v_{n1}(r_n), \ldots, v_{nh_n}(r_n))$$

e

$$v(R) = \{v(r); r \in R \text{ é não divisor de zero}\}.$$

Observação 4.5. Observe que no isomorfismo $Q(R) \simeq Q(R/\mathfrak{p}_1) \times \cdots \times Q(R/\mathfrak{p}_n)$, um elemento $r \in R$ é da forma $r = (r_1, \ldots, r_n)$, onde $r_i = \overline{r}/1$ e $\overline{r}$ é a classe de r em $R/\mathfrak{p}_i$, para todo $i = 1, \ldots, n$. Nesse caso, por um abuso de notação escrevemos $r = (r, \ldots, r)$.

Definição 4.15. Seja $d = \sum_{i=1}^{n} h_i$. Então $v(R) \subset \mathbb{N}^d$ é um semigrupo chamado *semigrupo de valores de R.*

Observação 4.6. Sem perda de generalidade podemos supor que os domínios $\overline{R/\mathfrak{p}_i}$, $1 \leq i \leq n$, são domínios de valorização discreta e nesse caso, teremos que $n = d$ (ver [BDF]).

Afim de simplificar as notações e os argumentos é possível supor R completo. De fato, os semigrupos de R e $\hat{R}$, o completamento de R com respeito ao ideal de Jacobson de R, são iguais como pode ser visto em [BDF]. Vamos também supor que R é residualmente racional, isto é, para todo ideal maximal $\mathfrak{m}_{ij}$ de $\overline{R/\mathfrak{p}_i}$ temos $R/\mathfrak{m} \simeq (\overline{R/\mathfrak{p}_i})/\mathfrak{m}_{ij}$, onde $\mathfrak{m}$ é o maximal de R.

Proposição 4.5. *Seja $S = v(R) \subset \mathbb{N}^d$. Então,*

i) Se $a, b \in S$, então $a + b \in S$.

(ii) Se $a = (a_1, \ldots, a_d), b = (b_1, \ldots, b_d) \in S$, então

$$min(a, b) := (min(a_1, b_1), \ldots, min(a_d, b_d)) \in S.$$

(iii) Se $a, b \in S$, $a \neq b$ e $a_i = b_i$, para algum $i \in \{1, \ldots, d\}$, então existe $\varepsilon \in S$ tal que $\varepsilon_i > a_i = b_i$ e $\epsilon_j \geq min(a_j, b_j)$, para cada $j \neq i$, e a igualdade acontece se $a_j \neq b_j$.

(iv) $(0, \ldots, 0)$ é o único elemento em S com uma componente nula.

Demonstração: Dados, $a, b \in S$ sejam $x, y \in R$ tais que $a = v(x)$ e $b = v(y)$.

i) Temos $a = v(x) = (v_1(x), \ldots, v_d(x))$ e $b = v(y) = (v_1(y), \ldots, v_d(y))$, onde $v_i : Q(R/\mathfrak{p}_i) \to \mathbb{Z} \cup \{\infty\}$, para $i = 1, \ldots, d$, são valorizações. Então,

$$a + b = ((v_1(x) + v_1(y), \ldots, v_d(x) + v_d(y)) = (v_1(xy), \ldots, v_d(xy)) = v(xy) \in S.$$

ii) Se $v_i(x) \neq v_i(y)$, para todo $i \in \{1, \ldots, d\}$, então $v_i(x + y) = \min\{v_i(x), v_i(y)\}$ (ver Proposição 2.9). Assim, nesse caso,

$$min(a, b) = (v_1(x + y), \ldots, v_d(x + y)) = v(x + y) \in S.$$

Se $v_i(x) = v_i(y)$ para algum $i \in \{1, \ldots, d\}$, podemos assumir (reordenando se necessário) que $v_i(x) = v_i(y), \ldots, v_d(x) = v_d(y)$ (para algum $i > 1$). Então, consideremos os elementos $x = u_j t_j^{a_j}$ e $y = v_j t_j^{b_j} \in \overline{R/\mathfrak{p}_j}$ onde t_j é o parâmetro de uniformização em $\overline{R/\mathfrak{p}_j}$ e $u_j, v_j \in \overline{R/\mathfrak{p}_j}$ são invertíveis. Como estamos supondo $(\overline{R/\mathfrak{p}_j})/\mathfrak{m}_j \simeq R/\mathfrak{m}$, podemos assumir que u_j, v_j são invertíveis em $R/\mathfrak{m}$. Supondo que a cardinalidade de

$R/\mathfrak{m}$ é maior que d, existe $c \in R/\mathfrak{m}$ tal que $cu_j - v_j \neq 0$, para todo $j = \{i, \ldots, d\}$. Ou seja, existe $c \in \overline{R/\mathfrak{p}_i}$ invertível tal que $v_j(cx_j - y_j) = a_j = b_j$, para todo $j = \{i, \ldots, d\}$. Observe ainda que, para $1 \leq j \leq i$, temos $v_j(x) \neq v_j(y)$, por hipótese, o que implica $v_j(cx_j - y_j) = \min\{a_j, b_j\}$. Logo, $v(cx - y) = min(a, b)$.

(iii) Suponhamos $a_i = b_i$. Então $v_i(x) = v_i(y)$, o que implica $v_i(x/y) = 0$ e, portanto, $x/y \notin \mathfrak{m}_i$ (o ideal maximal de $\overline{R/\mathfrak{p}_i}$). Por assumirmos que R é residualmente racional, existe $u \in R$ invertível tal que $x/y - u \in \langle t_i \rangle = \mathfrak{m}_i$. Portanto,

$$v_i\left(\frac{x - yu}{y}\right) > 0 \Rightarrow v_i(x - yu) - v_i(y) > 0 \Rightarrow v_i(x - yu) > v_i(y) = a_i = b_i.$$

Além disso,

$$v_j(x - yu) \geq min\{v_j(x), v_j(y) + v_j(u)\} = min\{v_j(x), v_j(y)\} = min(a_j, b_j).$$

E, se $a_j \neq b_j$, então

$$v_j(x - yu) = min\{v_j(x), v_j(y) + v_j(u)\} = min\{v_j(x), v_j(y)\} = min(a_j, b_j).$$

Então, tome $\varepsilon = v(x - yu)$.

(iv) Seja $a = v(x) \in S$, tal que $v(x) = (v_1(x), \ldots, v_d(x))$ e $v_i(x) = 0$, para algum $i \in \{1, \ldots, d\}$. Como, $v_i(x) = 0$ implica que x é invertível em $\overline{R/\mathfrak{p}_i}$, isto é, $x \notin \mathfrak{m}_i$ (o ideal maximal de $\overline{R/\mathfrak{p}_i}$) temos que $\overline{x} \neq \overline{0}$ em $\dfrac{\overline{R/\mathfrak{p}_i}}{\mathfrak{m}_i} \simeq \dfrac{R}{\mathfrak{m}}$. Como $x \notin \mathfrak{m}$, então x é invertível em R. Daí segue que, existe $y \in R$ tal que $xy = 1$, o que implica x invertível em $\overline{R/\mathfrak{p}_j}$, para todo $j = 1, \ldots, d$, e $v_j(x) = 0$, para todo $j = 1, \ldots, d$.

Logo, $a = v(x) = (0, \ldots, 0)$.

■

Proposição 4.6. *Seja $S = v(R) \subset \mathbb{N}^d$. Então, existe $c \in \mathbb{N}^d$, chamado condutor de R, tal que $S \supset c + \mathbb{N}^d$.*

Demonstração: Ver [D], Proposição 1.3, pág. 2943. ■

Exemplo 4.9. Sejam C a curva plana $(Y - X^2)Y = 0$ e $p = (0, 0)$ o único ponto singular de C. Seja R o anel local de C em p. Então R satisfaz as condições assumidas para a definição de $v(R)$ e, trocando R pelo seu completamento, podemos supor $\overline{R} = k[[t]] \times k[[u]]$. De fato, observe que:

$$\Gamma(C) = \frac{k[X, Y]}{\langle (Y - X^2)Y \rangle} = k[x, y],$$

onde x e y são as classes de X e Y em $k[X, Y]/\langle (Y - X^2)Y \rangle$. Portanto $(y - x^2)y = 0$.

Como $\langle 0\rangle = \langle y-x^2\rangle\langle y\rangle = \langle y-x^2\rangle \cap \langle y\rangle \subset k[x,y]$ e $\langle y-x^2\rangle$, $\langle y\rangle$ são ideais primos de $k[x,y]$ temos que $\mathfrak{q}_1 = \langle y-x^2\rangle$ e $\mathfrak{q}_2 = \langle y\rangle$ são os primos minimais de $k[x,y]$.

Mas $R = \mathcal{O}_p(C) = k[x,y]_{\langle x,y\rangle}$ e portanto, segue do homomorfismo canônico $k[x,y] \to k[x,y]_{\langle x,y\rangle}$, que os primos minimais de R são $\mathfrak{p}_1$ e $\mathfrak{p}_2$, as localizações de $\mathfrak{q}_1$ e $\mathfrak{q}_2$ em $\langle x,y\rangle$, respectivamente.

Logo, pelo diagrama 4.2, temos a sequência exata

$$0 \to \underbrace{k[x,y]_{\langle x,y\rangle}}_{R} \to \frac{k[x,y]_{\langle x,y\rangle}}{\mathfrak{p}_1} \times \frac{k[x,y]_{\langle x,y\rangle}}{\mathfrak{p}_2} \simeq \left(\frac{k[x,y]}{\langle y-x^2\rangle}\right)_{\langle x,y\rangle} \times \left(\frac{k[x,y]}{\langle y\rangle}\right)_{\langle x,y\rangle}$$

ou, equivalentemente,

$$0 \to R \to \left(\frac{k[x,y]}{\langle y-x^2\rangle}\right)_{\langle x,y\rangle} \times \left(\frac{k[x,y]}{\langle y\rangle}\right)_{\langle x,y\rangle} = k[x,x^2]_{\langle x,x^2\rangle} \times k[x]_{\langle x\rangle} = k[t]_{\langle t\rangle} \times k[u]_{\langle u\rangle}.$$

Fizemos $x = t$ e $x = u$ nos anéis, $k[x,x^2]_{\langle x,x^2\rangle}$ e $k[x]_{\langle x\rangle}$, respectivamente, para evitar confusão.

Sejam $\widehat{R}$ o completamento de R com respeito ao seu ideal maximal $\mathfrak{m} = \langle x,y\rangle k[x,y]_{\langle x,y\rangle}$ e $\widehat{R_1}$, $\widehat{R_2}$ os completamentos de $k[t]_{\langle t\rangle}$ e $k[u]_{\langle u\rangle}$, com respeitos aos ideais $\mathfrak{m}_1 = \langle t\rangle k[t]_{\langle t\rangle}$ e $\mathfrak{m}_2 = \langle u\rangle k[u]_{\langle u\rangle}$, respectivamente. Observe que esses dois últimos ideais são as imagens de $\mathfrak{m}$ em $k[t]_{\langle t\rangle}$ e $k[u]_{\langle u\rangle}$, respectivamente.

Então, pelo item i) do Teorema 4.2, temos que

$$0 \to \widehat{R} \to \widehat{R_1} \times \widehat{R_2}.$$

Mas, $\widehat{R} \simeq k[[x,y]]$, $\widehat{R_1} \simeq k[[t]]$ e $\widehat{R_2} \simeq k[[u]]$.

Logo,

$$0 \to \widehat{R} = k[[x,y]] \xrightarrow{\psi} \widehat{R_1} = k[[t]] \times \widehat{R_2} = k[[u]],$$

onde

$$\begin{array}{rccc} \psi: & k[[x,y]] & \longrightarrow & k[[t]] \times k[[u]] \\ & 1 & \longmapsto & (1,1) \\ & x & \longmapsto & (t,u) \\ & y & \longmapsto & (t^2,0). \end{array}$$

Finalmente, como $k[[t]] \times k[[u]]$ é inteiro sobre $k[[x,y]]$ e integralmente fechado em $k((t)) \times k((u))$, temos que o fecho inteiro de $\widehat{R}$ no seu anel total de frações é $k[[t]] \times k[[u]]$.

Para efeito do cálculo do semigrupo de valores de R, $S = v(R)$, observamos que $k[[t]]$ é um anel local, cujo ideal maximal é $\mathfrak{m}_1 = \langle t\rangle$. Portanto é um anel de valorização discreta, cuja valorização associada é $v_1 : k((t)) \to \mathbb{Z} \cup \{\infty\}$ tal que $v_1(t) = 1$. Analogamente, $k[[u]]$

é um anel de valorização discreta e a valorização associada é $v_2 : k((u)) \to \mathbb{Z} \cup \{\infty\}$ com $v_2(u) = 1$. Então,

$$S = v(R) = \{v(f(x,y)); f(x,y) \text{ é não divisor de zero em } k[[x,y]]\} \text{ e}$$

$$v(f(x,y)) = (v_1(\psi(f(x,y))), v_2(\psi(f(x,y)))) = (v_1(f(t,t^2)), v_2(f(u,0))).$$

Agora, note que:

i) $v(1) = (v_1(1), v_2(1)) = (0,0) \in S$;

ii) $v(x) = (v_1(t), v_2(u)) = (1,1) \in S$ implica que $v(x^n) = (v_1(t^n), v_2(u^n)) = (n,n) \in S$, para todo $n \in \mathbb{N}$;

iii) y é um divisor de zero em $k[[x,y]]$, portanto $v(y)$ não está definido;

iv) $v(x^3 + y) = (v_1(t^3 + t^2), v_2(u^3 + 0)) = (v_1(t^3 + t^2), v_2(u^3)) = (2,3) \in S$.;

v) Como $(2,3)$ e $(2,2) \in S$, então pela propriedade (iii) da Proposição 4.5, temos que existe $\epsilon = (\epsilon_1, \epsilon_2) \in S$ tal que $\epsilon_1 > 2$ e $\epsilon_2 = 2$. Ou seja, $(\epsilon_1, 2) \in S$, com $\epsilon_1 > 2$. Afirmamos que para todo $n \in \mathbb{N}$, tal que $2 < n < \epsilon_1$, $(n,2) \in S$. De fato, pela propriedade (ii) da Proposição 4.5,

$$(n,2) = \min\{(n,n), (\epsilon_1, 2)\} \in S.$$

Aplicando novamente a propriedade (iii) da Proposição 4.5 aos pares $(\epsilon_1, 2), (\epsilon_1, \epsilon_1)$ de S temos que existe $\delta \in S$ tal que $\delta_1 > \epsilon_1$ e $\delta_2 = 2$. Ou seja, $(\delta_1, 2) \in S$, com $\epsilon_1 < \delta_1$. Novamente, para todo $m \in \mathbb{N}$, tal que $\epsilon_1 < m < \delta_1$, temos

$$(m,2) = \min\{(m,m), (\delta_1, 2)\} \in S.$$

Continuando o processo, concluímos que $(a,2) \in S$, para todo $a \in \mathbb{N}$ e $a \geq 2$.

vi) Do item anterior temos que $(3,2) \in S$. Como $(2,2)$ também está em S temos, pela propriedade (iii) da Proposição 4.5, que existe $\epsilon = (\epsilon_1, \epsilon_2) \in S$ tal que $\epsilon_1 = 2$ e $\epsilon_2 > 2$. Ou seja, $(2, \epsilon_2) \in S$, com $\epsilon_2 > 2$. Afirmamos que dado $n \in \mathbb{N}$ tal que $2 < n < \epsilon_2$, $(2,n) \in S$. De fato, pela propriedade (ii) da Proposição 4.5,

$$(2,n) = \min\{(n,n), (2, \epsilon_2)\} \in S.$$

Novamente, aplicando sucessivamente as propriedades (ii) e (iii) da Proposição 4.5 concluímos que $(2,b) \in S$, para todo $b \in \mathbb{N}$ e $b \geq 2$.

vii) Finalmente, dado $(a,b) \in \mathbb{N}^2$ tal que $a, b \geq 2$ e $a \neq b$, temos que

$$(a,b) = (a - 2 + 2, b - 2 + 2) = (a-2, 2) + (2, b-2) \in S,$$

pelos itens v) e vi), se $a-2, b-2 \geq 2$. Caso, $0 \leq a-2, b-2 < 2$, isto é, $2 \leq a, b < 4$, teremos (a, b) pertencente ao conjunto

$$\{(2,3),(2,4),(3,2),(3,4) = (2,3)+(1,1),(4,2),(4,3) = (3,2)+(1,1)\} \subset S.$$

Logo, $\{(0,0),(1,1)\} \cup \{(2,2)+\mathbb{N}^2\} \subset S$.

Para mostrar a inclusão contrária considere $f(x,y) \in k[[x,y]]$ um não divisor de zero. Então,

$$\begin{aligned} f(x,y) &= \sum_{i+j=0}^{\infty} a_{ij}x^i y^j = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}^2y^2 + \ldots \\ f(t,t^2) &= a_{00} + a_{10}t + a_{01}t^2 + a_{20}t^2 + a_{11}t^3 + a_{02}^2t^4 + \ldots \\ f(u,0) &= a_{00} + a_{10}u + a_{20}u^2 + \ldots \end{aligned}$$

Assim,

$$v(f(x,y)) = (v_1(f(t,t^2)), v_2(f(u,0))) = \begin{cases} (0,0), & \text{se } a_{00} \neq 0; \\ (1,1), & \text{se } a_{00} = 0 \text{ e } a_{10} \neq 0; \\ (a,b), & \text{com } a \geq 2 \text{ e } b \geq 2, \text{ se } a_{00} = a_{10} = 0, \end{cases}$$

ou seja, $S \subset \{(0,0),(1,1)\} \cup \{(2,2)+\mathbb{N}^2\}$.

Veremos em dois exemplos, como usar os semigrupos de valores para calcular as classes de isomorfismos de R-módulos livres de torção e posto 1.

Para isso, assumimos R um anel local, noetheriano, reduzido e unidimensional tal que seu fecho inteiro, $\overline{R}$, é finito como R-módulo. Então, todo R-módulo M finitamente gerado, livre de torção e posto 1 é isomorfo a um R-módulo M' tal que $R \subset M' \subset \overline{R}$ (ver [ARM]).

Analogamente ao que fizemos para R, definimos o semigrupo de valores de qualquer subconjunto de $\overline{R}$.

Definição 4.16. Para qualquer subconjunto $T \subset \overline{R}$, definimos:

$$v(T) = \left\{ v(f);\ f \in T \text{ é um não divisor de zero em } \overline{R} \right\}.$$

Proposição 4.7. *Sejam M um R-módulo finitamente gerado tal que $R \subset M \subset \overline{R}$ e $S = v(R) \subset \mathbb{N}^d$. Então, $E := v(M) \subset \mathbb{N}^d$ satisfaz as seguintes condições:*

(i) Dados $a \in S$ e $b \in E$, então $a + b \in E$.

(ii) Se $a, b \in E$, então $min(a, b) \in E$.

(iii) Se $a, b \in E$ e $a_i = b_i$, então existe $\varepsilon \in E$ tal que $\varepsilon_i > a_i = b_i$ e $\epsilon_j \geq min(a_j, b_j)$ onde a igualdade acontece se $a_j \neq b_j$.

(iv) Existe $c \in S$ tal que $a + E \subset S$.

Demonstração: Ver [D], pág. 2946. ■

Definição 4.17. Um ideal satisfazendo as propriedades da Proposição 4.7 é chamado *ideal relativo* de S.

Exemplo 4.10. Seja R o anel local da curva plana $Y^2 = X^n$ na origem, onde $n = 2l + 1$. Vimos no Exemplo 4.5 que

$$S = v(R) = \{0, 2, 4. \ldots, n-3, n-1, \longrightarrow\} = \langle 2, n\rangle.$$

Seja E um ideal relativo de S tal que $S \subsetneq E \subsetneq \mathbb{N}$.

Note que, se $a \in E$, então $a + 2 \in E$, pois $2 \in S$. Afirmamos que

$$E = \{0\} \cup \{a + \mathbb{N}\},$$

onde a é um número ímpar tal que $2 \leq a \leq n - 3$.

Observe que, pela definição de ideal relativo de S, temos que $S \subset E$. Logo, todos os inteiros positivos pares e menores que n estão em E, bem como todo inteiro positivo maior que n. Como $E \neq S$, existe c inteiro ímpar, $0 < c < n$, tal que $c \in E$. Seja a o menor inteiro ímpar que pertence a E. Então,

$$\{a, a+2, (a+2)+2, \ldots, a+2k;\ k\ \in \mathbb{N} \text{ e } a + 2k = n\} \subset E$$

e a afirmação segue.

Trocando R por seu completamento e usando a descrição de E veremos que o conjunto das classes de isomorfismos de R-módulos livres de torção de posto 1, denotado por $TF(R)$, pode ser representado por:

$$TF(R) := \{R, R + t^{n-2}R, R + t^{n-4}R, \ldots, R + t^5R, R + t^3R, \overline{R}\}.$$

De fato, vimos no Exemplo 4.5 que $R = k[t^2, t^n]_{\langle t^2, t^n\rangle}$, $\overline{R} = k[t]_{\langle t\rangle}$ e $k(C) = k(t)$. Logo, $\widehat{R} \simeq k[[t^2, t^n]]$.

Supondo R completo, isto é, $R = \widehat{R}$ temos então que $\overline{R} = k[[t]]$. Seja M um R-módulo tal que $R \subset M \subset \overline{R}$. Então, dado $m \in M$ temos que

$$m = \sum_{i=0}^{\infty} a_i t^i = \sum_{k=0}^{\infty} a_{2k} t^{2k} + \sum_{j=0}^{\infty} a_{2j+1} t^{2j+1} = \underbrace{\sum_{k=0}^{\infty} a_{2k} t^{2k}}_{\in R} + t^a \underbrace{(\sum_{j=0}^{\infty} a_{2j+1} t^{2j+1-a})}_{\in R}.$$

Observe que sendo a ímpar, $2j + 1 - a$ é sempre par. Logo, $M = R + t^a R$, com $2 \leq a \leq n - 3$.

Note que, embora tenhamos substituído R por seu completamento para simplificar a computação, os módulos acima são precisamente aqueles que representam as classes de isomorfismos, tomando $R = k[t^2, t^n]_{\langle t^2, t^n \rangle}$.

Exemplo 4.11. Seja R o anel local da curva plana $(Y - X^2)Y = 0$ na origem. Vimos no Exemplo 4.9 que

$$S = v(R) = \{(0,0), (1,1)\} \cup \{(2,2) + \mathbb{N}^2\}.$$

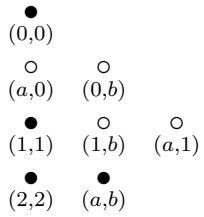


Figura 6 – Bolinhas pretas indicam que o elemento está em $S \subset E$

Agora, seja E um ideal relativo de S tal que $S \subsetneq E \subsetneq \mathbb{N}^2$.

(i) Se $(a, 0) \in E$ para algum $a > 0$, afirmamos que $(0, b) \in E$ para qualquer $b > 0$.

De fato, aplicando o item (iii) da Proposição 4.7 aos pares $(a, 0), (0, 0) \in E$, temos que existe $(\epsilon_1, \epsilon_2) \in E$ tal que $\epsilon_1 = 0$ e $\epsilon_2 > 0$. Seja a um número inteiro tal que $0 < a < \epsilon_2$. Então, pelo item (ii) da Proposição 4.7, segue que

$$(0, a) = \min\{(a, a), (0, \epsilon_2)\} \in E.$$

Usando sucessivamente (ii) e (iii) da Proposição 4.7, concluímos que $(0, b) \in E$, para qualquer $b > 0$.

(ii) Analogamente, mostramos que se $(0, b) \in E$, para algum $b > 0$, então $(a, 0) \in E$ para qualquer $a > 0$.

(iii) Se $(a, 1) \in E$ para algum $a > 1$, então $(1, b) \in E$ para qualquer $b > 1$.

De fato, aplicando o item (iii) da Proposição 4.7 aos pares $(a, 1), (1, 1) \in E$, temos que existe $(\epsilon_1, \epsilon_2) \in E$ tal que $\epsilon_1 = 1$ e $\epsilon_2 > 1$. Seja b um número inteiro tal que $1 < b < \epsilon_2$. Então, pelo item (ii) da Proposição 4.7, segue que

$$(1, b) = \min\{(b, b), (1, \epsilon_2)\} \in E.$$

Usando sucessivamente (ii) e (iii) da Proposição 4.7, concluímos que $(1, b) \in E$, para qualquer $b > 1$.

Além disso, se $(1, b) \in E$, para algum $b > 1$, mostra-se que $(a, 1) \in E$ para qualquer $a > 1$.

(iv) Finalmente, se $(a,0) \in E$ para algum $a > 0$, então $(a+1,1) \in E$ desde que $S + E \subset E$.

Usando todas as afirmações feitas nos itens anteriores temos que se $(a,0) \in E$ para algum $a > 0$, então $(m,n) \in E$, para todo $m, n \in \mathbb{N}$, ou seja, $E = \mathbb{N}^2$.

E se não existir um elemento em E de $(a,0) \in E$ para algum $a > 0$ e $S \subsetneq E$, então $(a,1) \in E$ para algum $a > 1$.

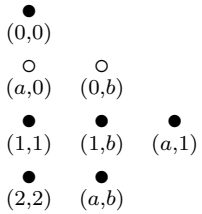


Figura 7 – Bolinhas pretas indicam que o elemento está em E

Assim E deve ser da forma $E = \{(0,0)\} \cup ((1,1) + \mathbb{N}^2)$.

Nesse caso, ordenando E pela relação $(a_1, b_1) \geq (a_2, b_2)$ se $a_i \geq b_i$, para $i = 1, 2$, temos que $(1,2) = v(t, u^2)$ é o menor elemento de $E = v(M)$ que não está em $S = v(R)$.

Logo, podemos escrever

$$TF(R) = \{R, R + (t, u^2)R, \overline{R}\}$$

ou, em termos de ideais,

$$TF(R) = \{R, \mathfrak{m}, F\},$$

onde $F = (R : \overline{R})$.

REFERÊNCIAS

[AM] Atiyah, M. F., Macdonald, I. G. *Introducción al Álgebra Conmutativa*. Universidad de Oxford: Addison-Wesley Publishing Company, Inc., Massachusetts, 1989.

[ALR] Avritzer, D., Lange, H., Ribeiro, F. A. *Torsion-free Sheaves on Nodal Curves and Triples*. Bull. Braz. Math. Soc., New Series 41(3) (2010), 421-447.

[ARM] Avritzer, D., Ribeiro, F. R., Martins, R. V. *Torsion Free Sheaves on Cuspidal Curves*. arXiv:1203.5329 [math.AG].

[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, A., Delgado, F.,Kiyek, K. *Gorenstein property and symmetry for one-dimensional local Coehn-Macaulay ring*. Manuscripta Math. 83 (1994) 405-423.

[D] D'Anna, M. *The canonical module of a one-dimensional reduced ring*. Comm. Algebra 25(1997) 2939-2965.

[EO] Endler, O. *Valuation Theory*. New York: Springer-Verlag, 1972.

[HR] Hartshorne, R. *Algebraic Geometry*. New York: Springer-Verlag, 1977.

[MR] Matsumura, H., Reid, M. *Commutative Ring Theory*. Cambridge: Cambridge University Press, 1989.

[R] Reid, Miles. *Undergraduate Commutative Algebra*. Cambridge: Cambridge University Press, London Mathematical Society Texts 29, 1995.

[RG] J.C.Rosales, P.A.García-Sánchez. *Numerical Semigroups*. Developments in Mathematics, 20. Springer, New York, 2009.

[S] Seshadri, C.S. *Fibrés Vectoriels sur les Courbes Algébriques*. Astérisque 96 (1982).

[WF] Fulton, W. *Algebraic Curves. An Introduction To Algebraic Geometry*. W.A.Benjamin, Inc., New York, 1969.