UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MESTRADO ACADÊMICO EM MATEMÁTICA

LIA NOJOSA SENA

SOBRE ANÉIS DE VALORIZAÇÃO DISCRETA

FORTALEZA

2022

LIA NOJOSA SENA

SOBRE ANÉIS DE VALORIZAÇÃO DISCRETA

Dissertação apresentada ao Curso de Mestrado Acadêmico em Matemática do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Álgebra

Orientador: Prof. Dr. Antonio Caminha Muniz Neto

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S477s Sena, Lia Nojosa.
Sobre Anéis De Valorização Discreta / Lia Nojosa Sena. – 2022.
71 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2022.
Orientação: Prof. Dr. Antonio Caminha Muniz Neto.

1. Anéis de valorização discreta. 2. Curvas algébricas planas . I. Título.

CDD 510

LIA NOJOSA SENA

SOBRE ANÉIS DE VALORIZAÇÃO DISCRETA

Dissertação apresentada ao Curso de Mestrado Acadêmico em Matemática do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Álgebra

Aprovada em: 13/07/2022

BANCA EXAMINADORA

Prof. Dr. Antonio Caminha Muniz Neto (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Jonatan Floriano da Silva
Universidade Federal do Ceará (UFC)

Prof. Dr. Angelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Aos meus pais.

AGRADECIMENTOS

Agradeço à minha família e a todos que contribuíram direta ou indiretamente com a realização desse trabalho.

Agradeço ao professor Antonio Caminha pela orientação e paciência ao longo do mestrado. Aos professores Jonatan Floriano da Silva e Angelo Papa Neto, por aceitarem compor a banca de defesa.

À Andrea e à Jessyca, por seus auxílios e presteza.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Ao CNPq, pelo apoio financeiro.

"’Você deveria ser apenas um algebrista ou um geômetra?’ é como dizer ’Você prefere ser surdo ou cego?’

(ATIYAH, Michael)

RESUMO

Discorremos, de forma essencialmente autocontida, sobre alguns aspectos algébricos e geométricos de anéis de valorização discreta. Mais precisamente, do ponto de vista algébrico, caracterizamos tais anéis dentre os domínios noetherianos locais; do ponto de vista geométrico, mostramos que um ponto de uma curva algébrica plana é simples se, e só se, o correspondente anel local for de valorização discreta.

Palavras-chave: anel de valorização discreta; curva algébrica plana; ponto simples.

ABSTRACT

We survey, in a self-contained way, on some algebraic and geometric aspects of discrete valuation rings. More precisely, from an algebraic point of view, we characterize these rings among local Noetherian rings; from a geometric standpoint, we show that a point on a plane algebraic curve is simple if, and only if, its corresponding local ring is a discrete valuation ring.

Keywords: discrete valuation ring; plane algebraic curve; simple point.

SUMÁRIO

1 INTRODUÇÃO

A leitura deste trabalho pressupõe familiaridade com conceitos de álgebra comutativa, curvas algébricas e conhecimento de resultados básicos de álgebra. Indicamos como leitura complementar para os fundamentos de álgebra (LANG, 2002). Dividimos o texto em 5 capítulos: no segundo e terceiro capítulo damos algumas definições e alguns resultados que serão úteis para o desenvolvimento deste trabalho de modo a proporcionar um acompanhamento aos leitores com menos preparação nesta área e introduzir as notações e convensões escolhidas. No terceiro capítulo, damos a prova do teorema que caracteriza os anéis de valorização discreta 4.1.1, apresentada em (ASH, 2003) e por fim fazemos uma aplicação do que desenvolvemos sobre anéis de valorização discreta no estudo de curvas álgebricas planas simples, apresentada em (FULTON, 2008).

2 TÓPICOS DE ÁLGEBRA COMUTATIVA

Nesse trabalho estaremos sempre considerando R um anel comutativo com unidade.

Neste capítulo apresentaremos alguns resultados de álgebra comutativa que serão necessários para os resultados. Para uma leitura complementar indicamos (ASH, 2003) e (TENGAN; BORGES, 2015).

2.1 Radical de Jacobson, Anel Local, Radical de um anel, nilradical de R e Aniquilador de um R-módulo M

Definição 2.1.1 *O **Radical de Jacobson** de um anel R é definido como sendo a interseção de todos os ideais maximais de R. Denotamos por $J(R)$.*

Definição 2.1.2 *Um anel R é dito **local** se possui apenas um anel maximal.*

Definição 2.1.3 *Se I é ideal do anel R, **radical de I**, denotado por $\sqrt{I}$ ou RAD (I), é o conjunto*

$$\{a \in R;\ a^n \in I,\ \text{para algum } n \geq 1\}.$$

*É claro que $I \subset \sqrt{I}$. O ideal I é chamado **radical** se $I = \sqrt{I}$.*

Definição 2.1.4 *Um elemento a de um anel R é chamado **nilpotente** se existe algum número natural n tal que $a^n = 0$.*

Definição 2.1.5 *O **nilradical** de R é dado pelo conjunto*

$$\sqrt{(0)} = \{a \in R;\ a \text{ é nilpotente em } R\}.$$

Definição 2.1.6 *O **aniquilador** de um R-módulo M é o conjunto*

$$ann(M) = \{a \in R;\ a \cdot m = 0,\ \forall\ m \in M\}.$$

Proposição 2.1.1 *$\sqrt{I}$ é ideal de R.*

Prova: Se $a, b \in \sqrt{I},\ r \in R$, então

$$(ra)^n = r^n a^n \in I \text{ se } a^n \in I.$$
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k \in I,$$

para n suficientemente grande.

Se $a^{n-k} \in I$ ou $b^k \in I$, para todo $0 \leq k \leq n$, então tome $l,\ m \in \mathbb{N}$ tal que $a^l \in I,\ b^m \in I$.

Se $n-k \geq l$, então $a^{n-k} = a^{n-k-l} \cdot a^l \in I$.

Se $k \geq m$, então $b^k = b^m \cdot b^{k-m} \in I$.

Se $n-k \leq l-1$ e $k \leq m-1$, então $n = (n-k)+k \leq l+m-2$.

Logo, se considerarmos n maior ou igual a $l+m-1$, então isso garante que cada parcela do desenvolvimento binomial $(a+b)^n$ pertence a I, mais precisamente, temos:

$$\begin{aligned} n \geq l+m-1 &\Rightarrow n-k \geq l \text{ ou } k \geq m, \text{ para todo } 0 \leq k \leq n \\ &\Rightarrow a^{n-k} \in I \text{ ou } b^k \in I, \text{ para todo } 0 \leq k \leq n \\ &\Rightarrow \binom{n}{k} a^{n-k} b^k \in I, \text{ para todo } 0 \leq k \leq n \\ &\Rightarrow (a+b)^n \in I. \end{aligned}$$

Proposição 2.1.2 *Se P é um ideal primo de R, então* $\sqrt{P} = P$.

Prova: Se $a \in \sqrt{P}$, então existe $m \in P$ tal que $a^m \in P$. Como P é primo, temos que $a \in P$. Logo, $\sqrt{P} \subset P$. Como $P \subset \sqrt{P}$ sempre, então, $\sqrt{P} = P$.

Proposição 2.1.3 *Seja $J(R)$ um radical de Jacobson de um anel R. Então $a \in J(R)$ se, e somente se, $1+ax$ é uma unidade para todo $x \in R$.*

Prova: Assuma $a \in J(R)$. Se $1+ax$ não é unidade, então gera um ideal próprio, logo $1+ax$ pertence a algum ideal maximal $\mathscr{M}$. Mas então $a \in \mathscr{M}$, logo $ax \in \mathscr{M}$. Portanto, $1 \in \mathscr{M}$, o que é uma contradição. Por outro lado, se a não pertence a algum ideal maximal $\mathscr{M}$, então $\mathscr{M} + Ra = R$. Assim, para algum $b \in \mathscr{M}$ e $y \in R$ nós temos $b+ay = 1$. Se $x = -y$, então $1+ax = b \in \mathscr{M}$, logo $1+ax$ não pode ser uma unidade, caso contrário, teríamos $1 \in \mathscr{M}$.

Proposição 2.1.4 *Seja $\mathscr{M}$ um anel maximal de um anel R. Então R é um ideal local se, e somente se, todo elemento de $1+\mathscr{M}$ é uma unidade.*

Prova: Suponha R um anel local, e seja $a \in \mathscr{M}$. Se $1+a$ não é uma unidade, então deve pertencer a $\mathscr{M}$ que é o ideal das não unidades. Mas então $1 \in \mathscr{M}$, o que é uma contradição. Por outro lado, assuma que todo elemento de $1+\mathscr{M}$ é uma unidade.

Afirmação: $\mathscr{M} \subseteq J(R)$, logo, $\mathscr{M} = J(R)$.

Se $a \in \mathscr{M}$, então $ax \in \mathscr{M}$ para todo $x \in \mathscr{M}$, logo, $1+ax$ é uma unidade. Pela Proposição 2.1.3, $a \in J(R)$, provando a afirmação.

Se $\mathscr{N}$ é outro ideal maximal qualquer, então $\mathscr{M} = J(R) \subseteq \mathscr{M} \cap \mathscr{N}$. Assim, $\mathscr{M} \subseteq \mathscr{N}$ e como ambos são ideais maximais, logo são iguais. Portanto, R é um anel local.

2.2 Lema de Nakayama

Definição 2.2.1 *Seja M um R-módulo e I um ideal de R. Temos que IM é o conjunto das combinações lineares de elementos do R-módulo M.*

Lema 2.2.1 *1. Se M é um R-módulo finitamente gerado, I um ideal de R contido no radical de Jacobson $J(R)$ e $IM = M$, então $M = 0$.*

2. Se N é um submódulo finitamente gerado de um R-módulo M, I um ideal de R contido no radical de Jacobson $J(R)$ e $M = N + IM$, então $M = N$.

Prova:

1. Suponha por absurdo que $M \neq 0$ e considere um conjunto de geradores $x_1, \cdots, x_n$ de M, que podemos tornar minimal, ou seja, $x_j \notin \sum_{i \neq j} Rx_i$, para $j = 1, \cdots, n$. Podemos escrever:

$$\begin{aligned} x_1 \in M = IM \quad &\Rightarrow \quad x_1 = \sum_{i=1}^{n} y_i x_i;\ y_i \in I,\ \forall i \\ &\Rightarrow \quad (1 - y_1)x_1 = \sum_{i=2}^{n} y_i x_i. \end{aligned} \tag{2.1}$$

   Pela Proposição 2.1.3 temos que $J(R) = \{a \in R;\ 1 + ax \in R^*,\ \forall x \in R\}$.

   Assim,

$$\begin{aligned} y_1 \in I \subset J(R) \quad &\Rightarrow \quad 1 - xy_1 = 1 + (-x)y_1 \in R^* \subseteq R \\ &\Rightarrow \qquad 1 - y_1 \in R^*,\ com\ x = 1. \end{aligned}$$

   Seja $u = (1 - y_1)^{-1} \in R$. Então, multiplicando ambos os lados de (2.1) por u, obtemos:

$$x_1 = \sum_{i=2}^{n} u y_i x_i \Rightarrow x_1 \in \sum_{i=2}^{n} Rx_i,$$

   contradizendo a minimalidade de $\{x_1, \cdots, x_n\}$.

2. Por hipótese, $M = N + IM$. Logo, trabalhando no módulo quociente $\frac{M}{N}$, obtemos:

$$\begin{aligned} M = N + IM \quad &\Rightarrow \qquad \tfrac{M}{N} = I\tfrac{M}{N} \\ &\Rightarrow \quad \tfrac{M}{N} = 0,\ pelo\ item\ anterior \\ &\Rightarrow \qquad M = N. \end{aligned}$$

2.3 Anéis de Frações

Definição 2.3.1 *Seja R um anel. $S \subset R$ é um* ***sistema multiplicativo*** *ou* ***conjunto multiplicativo*** *se*

1. $1 \in S$ *e* $0 \notin S$.
2. $a,\ b \in S \Rightarrow ab \in S$.

Exemplo 2.3.1 *Se P é ideal primo de R, então $S = R \setminus P$ é um sistema multiplicativo. De fato,*

$$a,\ b \in S \Rightarrow a,\ b \notin P \Rightarrow ab \notin P \Rightarrow ab \in S.$$

Definição 2.3.2 *Seja R um anel e S um sistema multiplicativo de R. Em $R \times S$, defina*

$$(a,s) \sim (b,t) \Leftrightarrow u(ta - sb) = 0, \text{ para algum } u \in S.$$

Proposição 2.3.1 *A relação $\sim$ é uma relação de equivalência.*

Prova:

1. $(a,s) \sim (a,s) \Leftrightarrow u(sa - sa) = u(sa - sa) = 0$, para algum $u \in S$. Logo, $\sim$ é reflexiva.
2. Agora, temos que:
$$\begin{aligned}(a,s) \sim (b,t) &\Leftrightarrow u(ta - sb) = 0, \text{para algum } u \in S \\ &\Leftrightarrow 0 = u(ta - sb) = -u(ta - sb) = u(sb - ta),\ \text{para algum } u \in S \\ &\Leftrightarrow (b,t) \sim (a,s).\end{aligned}$$
Assim, $\sim$ é simétrica.
3. Sejam $(a,s) \sim (b,t) \Leftrightarrow u(ta - sb) = 0$, para algum $u \in S$ e $(b,t) \sim (c,x) \Leftrightarrow v(xb - tc) = 0$, para algum $v \in S$.

   Façamos as seguintes operações:
$$\begin{aligned}u(ta - sb) = 0 \ \times\ (vx) &\Leftrightarrow uv(xta - xsb) = 0 \\ v(xb - tc) = 0 \ \times\ u(-s) &\Leftrightarrow uv(-sxb + stc) = 0.\end{aligned}$$
   Logo,
$$\begin{aligned}uv(xta - xsb) - uv(-sxb + stc) &= 0 \\ uv(xta - xsb + sxb - stc) = 0,\ \text{pois}\ -xsb + sxb &= 0.\end{aligned}$$
   Assim, $uvt(xa - sc) = 0$ e $uvt \in S$ já que $u,v,t \in S$. Portanto, $\sim$ é transitiva.

Definição 2.3.3 *Defina* $\frac{a}{s} = \overline{(a,s)}$ *e* $S^{-1}R = R_S = R \times S/\sim = \left\{\frac{a}{s};\ a \in R,\ s \in S\right\}$.

$S^{-1}R$ é um anel, quando munido com as operações:

$$\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}.$$
$$\frac{a}{s}+\frac{b}{t}=\frac{ta+sb}{st}.$$

O anel $S^{-1}R$ é chamado **anel de frações** ou **anel de localização** de R com respeito a S.

O "zero"é $\frac{0}{1}=0_{S^{-1}R}$ e o "um"é $\frac{1}{1}=1_{S^{-1}R}$.

Definição 2.3.4 *Se P é um ideal primo de R e $S=R\setminus P$, denotamos por R_P ao invés de $S^{-1}P$. Assim, temos:*

$$S^{-1}P=R_P=\left\{\frac{a}{s};\ a\in P,\ s\in S\right\}.$$

*R_P é a **localização** de R em P.*

Proposição 2.3.2 *A função dada por*

$$\begin{array}{rcl} f:R & \to & S^{-1}R \\ a & \mapsto & \frac{a}{1} \end{array}$$

é homomorfismo de anéis, o qual é injetor se R for um domínio.

Prova: Temos que

$$f(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=f(a)+f(b)$$
$$f(a\cdot b)=\frac{a\cdot b}{1}=\frac{a}{1}\cdot\frac{b}{1}$$
$$f(1)=\frac{1}{1}=1_{S^{-1}R}.$$

Suponha R domínio. Como f é homomorfismo de anéis, temos que f é injetor se, e somente se, $Ker(f)=\{0\}$. Tome $a\in ker(f)$. Então $\frac{a}{1}=f(a)=0_{S^{-1}R}$. Logo, existe $u\in S$ tal que $u(1\cdot a-1\cdot 0)=0$, isto é, $ua=0$.

Como R é domínio e $u\neq 0$, já que $0\notin S$, temos que $a=0$.

Proposição 2.3.3 *Os ideais de $S^{-1}R$ são da forma $S^{-1}I$, com I ideal de R, onde $S^{-1}R=\left\{\frac{a}{s};\ a\in I,\ s\in S\right\}$.*

Além disso, $S^{-1}I=S^{-1}R$, se e somente se, $I\cap S\neq\emptyset$.

Prova: Sejam I um ideal de R e $S^{-1}R$ dado como no enunciado. Para $a,\ b \in I,\ s,\ t,\ u \in S,\ r \in R$, temos $\frac{a}{s} - \frac{b}{t} = \frac{ta-sb}{st} \in S^{-1}I$, onde $ta - sb \in I$ e $st \in S$.

Logo, $(S^{-1}I,\ +)$ é subgrupo de $(S^{-1}R, +)$.

Tome J ideal de $S^{-1}R$ e pela Proposição 2.3.2

$$\begin{array}{ccc} f : R & \to & S^{-1}R \\ a & \mapsto & \frac{a}{1} \end{array}$$

é homomorfismo de anéis.

Se $I = f^{-1}(J)$, então sabemos que I é ideal de R.

Afirmação: $J = S^{-1}R$.

De $I = f^{-1}(J)$, temos que $f(a) \in J$, ou seja $\frac{a}{1} \in J$. Logo, $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in J$, uma vez que J é ideal de $S^{-1}R$. Segue que $S^{-1}I \subset J$.

Tome, agora, $\frac{a}{s} \in J$. Como J é ideal, temos que $\frac{as}{s} = \frac{a}{s} \cdot \frac{s}{1} \in J$. Agora, $\frac{as}{s} = \frac{a}{1}$. Temos $a \in f^{-1}(J) = I$. Então, $\frac{a}{s} \in S^{-1}I$. Segue que $J \subset S^{-1}I$.

Agora suponha que $S^{-1}I = S^{-1}R$. Então, $\frac{1}{1} \in S^{-1}I$, logo, existem $a \in I,\ s \in S$ tais que $\frac{1}{1} = \frac{a}{s}$, ou seja, $u(1 \cdot s - 1 \cdot a) = 0$, para algum $u \in S$. Logo, $us - ua = 0$. Assim,

$\underbrace{us}_{\in S} = \underbrace{ua}_{\in I} \in S \cap I$. Logo, $S \cap I \neq \emptyset$.

Reciprocamente, suponha que $S \cap I \neq \emptyset$ e tome $r \in S \cap I$. Então, $\frac{1}{1} = \frac{r}{r} \in S^{-1}I$, logo, $S^{-1}I = S^{-1}R$.

Proposição 2.3.4 *Em $S^{-1}R$, o ideal $S^{-1}I$ é primo se, e somente se, I é um ideal primo de R tal que $I \cap S = \emptyset$.*

Prova: Já sabemos que $S^{-1}I \neq S^{-1}R$ se, e somente se, $I \cap S = \emptyset$. Tome, pois, I ideal de R tal que $I \cap S = \emptyset$. Temos de mostrar que I é primo em R se, e somente se, $S^{-1}I$ é primo em $S^{-1}R$. Isso é o mesmo que mostrar que $\frac{R}{I}$ é domínio se, e somente se, $\frac{S^{-1}R}{S^{-1}I}$ é domínio.

Seja $\overline{S} = \{S + I \in \frac{R}{I};\ s \in S\}$. Como $1 + I \in \overline{S}$ e, para $t, s \in S$, temos

$$(s+I)(t+I) = \underbrace{st}_{\in S} + I \in \overline{S},$$

então $\overline{S}$ é sistema multiplicativo em $\frac{R}{I}$.

Afirmação: $\frac{S^{-1}R}{S^{-1}I} \simeq \overline{S}^{-1}(\frac{R}{I})$.

Uma vez provada a afirmação, veja que:

1. $\frac{R}{I}$ domínio implica que $S^{-1}(\frac{R}{I})$ é domínio e subanel do corpo de frações de $\frac{R}{I}$. Logo, $\frac{S^{-1}R}{S^{-1}I}$ é domínio.

2. $\frac{S^{-1}R}{S^{-1}I}$ domínio implica que $\overline{S}^{-1}(\frac{R}{I})$. Logo, $\frac{R}{I}$ é domínio.

Para provar a implicação $\overline{S}^{-1}(\frac{R}{I}) \Rightarrow \frac{R}{I}$ é domínio, basta mostrar que se $S^{-1}R$ é domínio, então R é domínio.

Tome $a,\ b \in R$ tal que $ab = 0$. Então, $\frac{ab}{1} = \frac{a}{1}\frac{b}{1} = \frac{0}{1} = 0_{S^{-1}R}$. Logo, como $S^{-1}R$ é domínio, $\frac{a}{1} = 0$ ou $\frac{b}{1} = 0$.

Suponha que $\frac{a}{1} = \frac{0}{1}$, então existe $u \in S$ tal que $u(a\cdot 1 - 0\cdot 1) = 0$. Logo, $ua = 0$.

Como S é sistema multiplicativo, então S não tem divisores de zero. Assim, $a = 0$. Então R não tem divisores de zero, logo, R é domínio.

Prova da afirmação:

$$\begin{aligned} \phi : S^{-1}R \quad &\to \quad \overline{S}^{-1}(\tfrac{R}{I}) \\ \phi(\tfrac{a}{s}) &= \tfrac{a+I}{s+I}. \end{aligned}$$

Vamos provar que ϕ está bem definido:

$$\begin{aligned} \tfrac{a}{s} = \tfrac{b}{t} \quad &\Rightarrow \quad \exists\, u \in S,\ u(at - sb) = 0 \\ &\Rightarrow \quad uta = usb \\ &\Rightarrow \quad (u+I)(t+I)(a+I) = (u+I)(s+I)(b+I) \\ &\Rightarrow \quad \underbrace{u+I}_{\in S}((t+I)(a+I) - (s+I)(b+I)) = 0+I \\ &\Rightarrow \quad \tfrac{a+I}{s+I} = \tfrac{b+I}{t+I}. \end{aligned}$$

Agora vamos demonstrar que ϕ é homomorfismo:

$$\begin{aligned} \phi\left(\tfrac{a}{s} + \tfrac{a'}{s'}\right) &= \phi(\tfrac{as'+a's}{ss'}) \\ &= \tfrac{as'+a's+I}{ss'+I} \\ &= \tfrac{(a+I)(s'+I)+(a'+I)(s+I)}{(s+I)(s'+I)} \\ &= \tfrac{a+I}{s+I} + \tfrac{a'+I}{s'+I} \\ &= \phi(\tfrac{a}{s}) + \phi(\tfrac{a'}{s'}). \end{aligned}$$

e

$$\begin{aligned} \phi\left(\tfrac{a}{s}\cdot\tfrac{a'}{s'}\right) &= \phi(\tfrac{aa'}{ss'}) \\ &= \tfrac{aa'+I}{ss'+I} \\ &= \tfrac{(a+I)(a'+I)}{(s+I)(s'+I)} \\ &= \tfrac{(a+I)}{(s+I)}\cdot\tfrac{(a'+I)}{(s'+I)} \\ &= \phi(\tfrac{a}{s})\cdot\phi(\tfrac{a'}{s'}). \end{aligned}$$

Temos que $Ker\phi = S^{-1}I$.

De fato, temos $\phi(\frac{a}{s}) = \phi(\frac{0}{1}) \Rightarrow \frac{a+I}{s+I} = \frac{0+I}{1+I}$. Assim, existe $u \in S$ tal que

$$(u+I)((1+I)(a+I)-(s+I)(0+I))=0+I.$$

Logo,

$$ua \in I \Rightarrow \frac{a}{s}=\frac{ua}{us} \in S^{-1}I.$$

Portanto, $Ker \subseteq S^{-1}I$.

Mas, se $a \in I,\ s \in S$, então

$$\phi(\tfrac{a}{s})=\tfrac{a+I}{s+I}=\tfrac{0+I}{s+I}=\tfrac{0+I}{1+I}.$$

Logo, $S^{-1}R \subseteq Ker\phi$.

Como ϕ é sobrejetivo, temos pelo Teorema dos Homomorfismos que ϕ induz um isomorfismo $\overline{\phi}$.

$$\begin{array}{ccc} S^{-1}R & \xrightarrow{\phi} & \overline{S}^{-1}(\frac{R}{I}) \\ \downarrow \pi & \nearrow_{\overline{\phi}} & \\ \frac{S^{-1}R}{S^{-1}R} & & \end{array}$$

Logo, temos

$$\begin{array}{ccc} \overline{\phi} : \frac{S^{-1}R}{S^{-1}} & \Rightarrow & \overline{S}^{-1}(\frac{R}{I}) \\ \frac{a}{s}+S^{-1} & \mapsto & \frac{a+I}{s+J}. \end{array},$$

com isso encerramos a prova.

Definição 2.3.5 *Se I é ideal de R tal que $I \cap (R \setminus P)=\emptyset$, temos $I \subset P$. Nesse caso, denotamos $S^{-1}I$ por IR_P, de forma que:*

$$IR_P=\left\{\tfrac{a}{s};\ a \in I,\ s \notin P\right\}.$$

Se $I \subset J$, temos que $S^{-1}I \subseteq S^{-1}J$. Em particular, em R_P, temos $I \subset P \Rightarrow IR_P \subset PR_P$. Como todo ideal próprio de R_P é da forma IR_P, com I ideal de R tal que $I \subset P$, concluímos que todo ideal próprio de R_P está contido em PR_P. Logo, R_P é ideal, com ideal maximal PR_P. Uma vez que PR_P é ideal maximal de R_P, temos que $\frac{R_P}{PR_P}$ é um corpo.

2.4 Submódulos primários

Definição 2.4.1 *Sejam N um submódulo de um R-módulo M e $a \in R$. Seja*

$$\begin{array}{rcl} \lambda_a : \frac{M}{N} & \to & \frac{M}{N} \\ \frac{m}{n} & \mapsto & a\,\frac{m}{n}. \end{array}$$

*Dizemos que N é dito um **submódulo primário** de M se N é próprio e para todo a, tivermos que λ_a é injetiva ou nilpotente.*

A injetividade na definição acima significa que para todo $x \in M$, temos que

$$ax \in N \Rightarrow x \in N.$$

Por outro lado, nilpotência na definição acima significa que para algum inteiro positivo n, temos que

$$a^n M \subseteq N,$$

isto é, a^n pertence ao aniquilador de $\frac{M}{N}$, denotado por $ann(\frac{M}{N}) = \{a \in R;\ a^n M \subseteq N\}$. Equivalentemente, a pertence ao radical do aniquilador de $\frac{M}{N}$, denotado por $r_M(N)$.

Proposição 2.4.1 *λ_a não pode ser injetiva e nilpotente ao mesmo tempo.*

Prova: De fato, se λ_a é nilpotente, então $a^n M = a(a^{n-1})M \subseteq N$, para algum $n \in \mathbb{Z}$ positivo. E, se λ_a é injetiva, teríamos que $a^{n-1}M \subseteq N$. Indutivamente, $M \subseteq N$, então $M = N$, contradizendo o fato de N ser próprio.

Se N é submódulo primário de M, então $r_M(N)$ é o conjunto de todos os $a \in R$ tal que λ_a não é injetiva.

Definição 2.4.2 *Se $P = r_M(N)$, então dizemos que N é **P-primário**.*

Proposição 2.4.2 *Se I é um ideal qualquer de R, então $r_R(I) = \sqrt{I}$, pois $ann(\frac{R}{I}) = \sqrt{I}$.*

Prova: De fato, se $a \in ann(\frac{R}{I}) \Leftrightarrow aR \subseteq I \Leftrightarrow a = a1 \in I$.

Definição 2.4.3 *Agora, tome $M = R$ e $a = y$. Definimos **ideal primário** em um anel R um ideal próprio Q tal que se $xy \in Q$ então $x \in Q$ ou $y^n \in Q$ para algum $n \geq 1$. Equivalentemente, $\frac{R}{Q} \neq 0$ e todo divisor de zero em $\frac{R}{Q}$ é nilpotente.*

Proposição 2.4.3 *Se P é um ideal primo, então* $\sqrt{P^n} = P$ *para todo* $n \geq 1$.

Prova: O radical de P^n é a interseção de todos os ideais primos contendo P^n, um dos quais é P. Assim, $\sqrt{P^n} \subseteq P$. Reciprocamente, se $x \in P$, então $x^n \in P^n$. Logo, $x \in \sqrt{P^n}$.

Lema 2.4.1 *Se* $\sqrt{I}$ *é um ideal maximal* $\mathscr{M}$*, então I é* $\mathscr{M}$*-primário.*

Prova: Suponha que $ab \in I$ e b não pertence ao ideal $\sqrt{I} = M$. Então pela maximalidade de M, segue que $M + Rb = R$, ou seja, para algum $m \in M$ e $r \in R$ temos que $m + rb = 1$. Agora, $m \in M = \sqrt{I}$, consequentemente $m^k \in I$ para algum $k \geq 1$. Assim, $1 = 1^k = (m+rb)^k = m^k + sb$ para algum $s \in R$. Multiplicando por a temos que $a = am^k + sab \in I$.

Corolário 2.4.1 *Se* $\mathscr{M}$ *é um ideal maximal, então* $\mathscr{M}^n$ *é* $\mathscr{M}$*-primário.*

Prova: Pela Proposição 2.4.3 temos que $\sqrt{\mathscr{M}^n} = \mathscr{M}$, e o resultado segue do Lema 2.4.1.

2.5 Teorema da Base de Hilbert

Definição 2.5.1 *Um anel R é chamado* ***Noetheriano*** *se todo ideal de R é finitamente gerado.*

Essa propriedade é fundamental em álgebra comutativa e geometria algébrica. Trata-se de um divisor de águas nessas teorias. Hoje uma caracterização importante, devida a Emmy Noether, que envolve a noção de cadeia ascendente de ideais.

Teorema 2.5.1 ***(Da Base de Hilbert)*** *Se R é Noetheriano, então* $R[x]$ *é Noetheriano.*

Prova: Seja I ideal de $R[x]$. Se $I = (0)$, então o teorema é válido.

Se $I \neq (0)$, seja $J = \{a \in R;\ a\ é\ coeficiente\ líder\ de\ um\ polinomio\ em\ I\}$.

Afirmação: J é ideal de R.

De fato, $0 \in J$. Se $a,\ b \in J,\ r \in R$, digamos,

$ax^n + \cdots + a_0 \in I$ e $bx^m + \cdots + b_0 \in I$, então $r(ax^n + \cdots a_0) \in I$. Logo, $ra \in I$ e se $n \leq m$, então $(ax^n + \cdots)x^{m-n} + (bx^m + \cdots + b_0) \in I$. Logo, $a + b \in J$. Como R é Noetheriano, então J é finitamente gerado, digamos que seja $J = (a_1, \cdots, a_r)$.

Tome $F_j = a_j x^{n_j} + \cdots + a_0 \in I$.

Sejam $n = max\{n_1, \cdots, n_r\}$ e para $1 \leq m \leq n$, seja $J_m = \{a \in R$; a é coeficiente líder de um polinômio em I de grau $\leq m\} \cup \{0\}$. Como antes, J_m é ideal de R, logo é finitamente gerado, digamos $J_m = (b_{m1},\ b_{m2} \cdots,\ b_{ms_m})$. Seja $F_{mj} = b_{mj}x^j + \cdots \in I$ para $1 \leq m \leq n,\ 1 \leq j \leq s_m$.

Afirmação: $I = (F_1, \cdots, F_r, \{F_{mj};\ 1 \leq m \leq n,\ 1 \leq j \leq s_m\})$.

Seja I' o ideal do 2º membro. Como $F_j,\ F_{mj} \in I$, temos $I' \subset I$. Suponha que $I' \neq I$. Então, $I \setminus I \neq \emptyset$. Logo, podemos tomar $F \in I \setminus I'$ de grau o menor possível.

Escreva $F = ax^d + \cdots$

1º Caso: $d \geq n$: Seja $a = \sum_{j=1}^{r} c_j a_j$ e definamos $G = F - \sum_{j=1}^{r} c_j x^{d-n_j} F_j \in I$. Tome $H = \sum_{j=1}^{r} c_j x^{d-n_j} F_j \in I'$. Como $F = G + H$, encontramos que G não pertence a I'. Então, $G \in I \setminus I'$ e grau(G) < grau(F), temos um absurdo.

2º Caso: d < n. Então $a \in J_d$. Logo, existe $c_j \in R$ tal que $a = \sum_{j=1}^{sd} c_j b_{dj}$. Defina $G = F - \sum_{j=1}^{sd} c_j x^{d-grau(F_{dj})}.F_{dj} \in I \setminus I'$ e grau(G) < grau(F), assim encontramos um absurdo.

Corolário 2.5.1 *Se R Noetheriano, então $R[x_1, \cdots, x_n]$ é Noetheriano. Em particular, se K é corpo, então $K[x_1, \cdots, x_n]$ é Noetheriano.*

Prova:

$$\begin{aligned} R\ Noetheriano \quad &\Rightarrow \quad R[x_1]\ \text{é Noetheriano} \\ &\Rightarrow \quad R[x_1][x_2]\ \text{é Noetheriano} \\ &\simeq \quad R[x_1, x_2]\ \text{é Noetheriano}. \end{aligned}$$

Continuando com o processo, temos que $R[x_1, x_2, \cdots, x_n]$ é Noetheriano. Como todo corpo é Noetheriano, pois seus ideias são somente (0) e (1), então o resto segue.

Proposição 2.5.1 *Para um anel R, são equivalentes:*

1. *R é Noetheriano, ou seja, todo ideal $I \subset R$ é finitamente gerado, isto é, existem $x_1, \cdots, x_n \in I$, tais que $I = (x_1, \cdots, x_n)$.*
2. *Toda cadeia crescente de ideais de R estabiliza, isto é, se $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$, então existe $m \in \mathbb{N}$ tal que $I_n = I_m$, para todo $n \geq m$.*
3. *Toda família $\mathfrak{F}$ não vazia de ideais de R possui um elemento máximo, isto é, existe um ideal $M \in \mathfrak{F}$ tal que se $I \in \mathfrak{F}$ e $I \supset M$ então $I = M$.*

Prova: $(1) \Rightarrow (2)$

Seja $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ uma cadeia crescente de ideais de R. Seja $I = \bigcup_{n \in \mathbb{N}} I_n$. Como I é um ideal de R, existem $x_1,\ x_2, \cdots,\ x_k \in I$ tais que $I = (x_1,\ x_2, \cdots,\ x_k)$. Para cada x_i existe um inteiro $n_i \in \mathbb{N}$ tal que $x_i \in I_{n_i}$. Seja $m = max\{n_1,\ n_2,\ \cdots,\ n_k\}$. Logo,

$I = (x_1,\ x_2, \cdots,\ x_k) \subset I_m \subset I$, e portanto $I = I_m$. Segue que $I_n = I_m$, para todo $n \geq m$, e a cadeia crescente $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ de ideais de R estabiliza.

$(2) \Rightarrow (3)$

Seja $\mathfrak{F}$ uma família não vazia de ideais de R. Seja $I_1 \in \mathfrak{F}$. Se I_1 é um elemento máximo de $\mathfrak{F}$, nada temos a mostrar. Caso contrário, existe $I_2 \in \mathfrak{F}$ tal que $I_1 \subsetneqq I_2$. Se I_2 é um elemento máximo de $\mathfrak{F}$, terminamos a prova. Se não, existe $I_3 \in \mathfrak{F}$ tal que $I_2 \subsetneqq I_3$. Se I_3 é um elemento máximo de $\mathfrak{F}$, terminamos a prova. Proseguindo como acima, encontramos um elemento máximo de $\mathfrak{F}$ ou uma cadeia crescente de ideais $I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq \cdots$ que não estabiliza. Mas esta última possibilidade não pode ocorrer diante da nossa hipótese. Assim, a família $\mathfrak{F}$ tem um elemento máximo.

$(3) \Rightarrow (1)$

Se I é um ideal de R, seja $\mathfrak{F} = \{I';\ I' \textit{ é um ideal de } R,\ I' \subset I \textit{ e } I' \textit{é finitamente gerado}\}$. Temos que $\mathfrak{F} \neq \emptyset$, pois $(0) \in \mathfrak{F}$. Seja J um elemento máximo de $\mathfrak{F}$. Evidentemente, $J \subset I$. Se a inclusão fosse própria, teríamos um elemento $x \in I - J$. Assim, o ideal $(J,x) \in \mathfrak{F}$, contradizendo a maximalidade de J. Logo $I = J$ é finitamente gerado.

2.6 Elementos Inteiros

Definição 2.6.1 *Seja R um subanel de um anel S e seja $\alpha \in S$. Dizemos que α é um **inteiro sobre R** se α é a raiz de um polinômio mônico com coeficientes em R. Em outras palavras,*

$$\alpha^n + b_{n-1} \cdot \alpha^{n-1} + \cdots + b_0 = 0,\ \textit{com } b_i \in R.$$

Definição 2.6.2 *Se R é um corpo e S uma extensão de um corpo R, então α é inteiro sobre R se, e somente se, α é algébrico sobre R.*

Definição 2.6.3 *Se α é um número complexo inteiro sobre $\mathbb{Z}$, então α é dito um **inteiro algébrico**.*

Exemplo 2.6.1 *Seja $f(x) = x^2 - d$, para $d \in \mathbb{Z}$ qualquer. Temos $\sqrt{d}$ é um inteiro algébrico, pois é raiz do polinômio f.*

Definição 2.6.4 *Um R-módulo M é dito **fiel** se seu aniquilador é 0.*

Lema 2.6.1 *Sejam R, S e α como na Definição 2.6.1. Seja M um R-módulo finitamente gerado que é fiel quanto a $R[\alpha]$-módulo. Seja I um ideal de R tal que $\alpha M \subseteq IM$. Então α é uma raiz de um polinômio mônico com coeficientes em I.*

Prova: Sejam $x_1, \ldots, x_n$ geradores de M sobre R. Então $\alpha x_i \in \alpha M \subseteq$ IM, por hipotése. Logo, $\alpha x_i \in IM$. Portanto, podemos escrever escrever $\alpha x_i = \sum_{j=1}^{n} c_{ij} x_j$, com $c_{ij} \in I$. Assim,

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - c_{ij}) x_j = 0,\ 1 \leq i \leq n.$$

Como matriz, temos que Ax = 0, onde A é a matriz com entrada $\alpha - c_{ii}$ na sua diagonal, e $-c_{ij}$ nas demais entradas, ou seja, temos

$$A \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} (\star)$$

Sabemos que $adj(A) \cdot A = det(A) \cdot I$, onde I é a matriz identidade continua válida para matrizes A com coeficientes em anéis. Logo, multiplicando à esquerda em $(\star)$ pela matriz adjunta de A, obtemos que

$$(det\ A) \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Logo, $(det)x_i = 0$ para todo $1 \leq i \leq n$. Sendo $1 = b_1 x_1 + \cdots + b_n x_n,\ b_i \in R$, temos que $det\ A = b_1 \underbrace{(det\ A)x_1}_{=0} + \cdots + b_n \underbrace{(det\ A)x_n}_{=0} = 0$.

Entretanto,

$$A = \begin{bmatrix} \alpha - c_{11} & -c_{12} & -c_{13} - & \cdots & -c_{1n} \\ -c_{21} & \alpha - c_{22} & -c_{23} - & \cdots & -c_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{n1} & -c_{n2} & -c_{13} - & \cdots & -\alpha - c_{nn} \end{bmatrix}$$

Como $det\ A = 0$, então $\alpha^n + \underbrace{a_{n-1}}_{\in I}\alpha^{n-1} + \cdots + \underbrace{a_1}_{\in I}\alpha + \underbrace{a_0}_{\in I} = 0$, pois $c_{ij} \in I$ para todo $1 \leq i, j \leq n$. Logo, α é raiz de um polinômio mônico com coeficientes em I.

Observação: Se $\alpha M \subseteq IM$, então, em particular α estabiliza M, em outras palavras, $\alpha M \subseteq M$.

Teorema 2.6.1 *Sejam R um subanel de S, com $\alpha \in S$. As seguintes afirmações são equivalentes:*

1. *α é inteiro sobre R;*
2. *$R[\alpha]$ é um R-módulo finitamente gerado;*
3. *Existe um anel R' tal que $R[\alpha] \subset R' \subset S$ e R' é um R-módulo finitamente gerado;*
4. *Existe um $R[\alpha]$-módulo M fiel que é finitamente gerado como um R-módulo.*

Prova: $(1) \Rightarrow (2)$

Seja $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ tal que $f(\alpha) = 0$. Então,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

Logo,

$$\begin{aligned} \alpha^{n+1} &= -a_{n-1}\alpha^n - \cdots - a_1\alpha^2 - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-2} - \cdots - a_1\alpha^2 - a - 0\alpha \\ &= a'_{n-1} + a'_{n-2}\alpha^{n-2} + \cdots + a'_o \cdot 1, \end{aligned}$$

com $a'_i \in R$, para todo $0 \leq i \leq n-1$. Iterando esse argumento, obtemos

$$\alpha^m = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \cdot 1,$$

com $b_0,\ b_1, \cdots,\ b_{n-1} \in R$.

Logo,

$$a_m \in \underbrace{R\alpha^{n-1} + \cdots + R\alpha + R \cdot 1}_{\text{um } R-\text{módulo finitamente gerado}},\ \forall m \geq 0 \tag{2.2}$$

Tome $\beta \in R[\alpha]$. Temos

$$\begin{aligned} \beta &= c_l\alpha^l + \cdots + c_1\alpha + c_0 \cdot 1,\ \textit{com } c_0, \cdots, c_l \in R \\ &= c'_l\alpha^l + \cdots + c'_1\alpha + c'_0 \cdot 1,\ \textit{com } c'_0, \cdots, c'_l \in R,\ \textit{por } (2.2) \end{aligned}$$

Assim,

$$R[\alpha] \subset R\alpha^{n-1} + \cdots + R\alpha + R \cdot 1 \tag{2.3}$$

Como temos $\supset$, então (2.3) é uma igualdade. Logo, $R[\alpha]$ é R-módulo finitamente gerado.

$(2) \Rightarrow (3)$

Suponha 2 e tome R' = $R[\alpha]$.

$(3) \Rightarrow (4)$

Suponha 3 e tome $R' = M$. Seja $y \in R[\alpha]$ e $yM = 0$, então $y = y1 = 0$.

$(4) \Rightarrow (1)$

Suponha 4. Aplicando o Lema 2.6.1 com $I = R$, obtemos o desejado.

Definição 2.6.5 *Se R é um subanel de S, o* ***fecho inteiro*** *de R em S é o conjunto R_C dos elementos de S que são inteiros sobre S.*

Temos que $R \subseteq R_C$ já que para cada $a \in R$ é raiz do polinômio $x - a$.

Definição 2.6.6 *Dizemos que R é* ***inteiramente fechado*** *em S se $R_C = R$. Dizemos que R é* ***inteiramente fechado sem referência a*** *S, quando assumimos que R é um domínio com corpo de frações K e R é inteiramente fechado em K.*

2.7 Sequências Exatas

Definição 2.7.1 *Uma* ***sequência (ou complexo) de R-módulos*** *e homomorfismos é da forma*

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

com $f_i \circ f_{i+1} = 0$, para todo i. Temos que a condição de composição é equivalente a $Im(f_{i+1}) \subseteq Ker(f_i)$. Se valer $Im(f_{i+1}) = Ker(f_i)$, para algum i, dizemos que a sequencia é ***exata na i-ésima etapa****. Se a igualdade ocorre para todo i, dizemos simplesmente que a sequência é* ***exata (ou que o complexo é acíclico)****.*

Definição 2.7.2 *Uma sequencia exata da forma*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

é chamada ***sequência exata curta****.*

Casos particulares fundamentais:

1. $0 \longrightarrow M \xrightarrow{f} N$ é exata se, e somente se, f é injetiva.
2. $N \xrightarrow{g} P \longrightarrow 0$ é exata se, e somente se, g é sobrejetiva.
3. $0 \longrightarrow M_1 \xrightarrow{h} M_2 \longrightarrow 0$ é exata se, e somente se, h é isomorfismo.
4. $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ é exata, se e somente, se g é sobrejetiva, f é injetiva e $Im(f) = Ker(f)$.
5. Se $J \subset I$ são ideais de um anel R, então existe uma sequência exata natural de R-módulos:
$$0 \longrightarrow \frac{I}{J} \longrightarrow \frac{R}{J} \longrightarrow \frac{R}{I} \longrightarrow 0 \tag{2.4}$$

De maneira geral, toda sequência exata "longa"

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

pode ser "quebrada"em várias sequencias exatas curtas:

$$0 \longrightarrow \underbrace{Im(f_i)}_{=Ker(f_i)} \xrightarrow{\psi} M_i \xrightarrow{\phi} \underbrace{Im(f_i)}_{=Ker(f_{i-1})} \longrightarrow 0$$

Proposição 2.7.1 *1. Seja*

$$0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\phi} V'' \longrightarrow 0$$

uma sequência exata de espaços vetorias de dimensões finitas sobre K. Então $dim\, V' + dim\, V'' = dim\, V$.

2. Seja

$$0 \longrightarrow V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} V_3 \xrightarrow{\phi_3} V_4 \longrightarrow 0$$

uma sequência exata de espaços vetorias de dimensões finitas sobre K. Então $dim\, V_4 = dim\, V_3 - dim\, V_2 + dim\, V_1$.

Prova:

1. Por hipótese, temos que $Im(\psi) = Ker(\phi)$, ϕ é sobrejetiva e ψ é injetiva. Logo, $Im(\phi) = V''$ e $Ker(\psi) = \{0\}$. Portanto, pelo Teorema do Núcleo e da Imagem, temos:

$$\begin{aligned} dim\,(V') &= dim\,(ker\ \psi) + dim(Im\ \psi) \\ &= 0 + dim(Ker\ \phi). \end{aligned}$$

Logo, $dim(V') = dim(Ker\ \phi)$. Novamente pelo Teorema do Núcleo e da Imagem, temos:

$$\begin{aligned} dim(V) &= dim(Ker\ \phi) + dim(Im\ \phi) \\ &= dim(V') + dim(V''). \end{aligned}$$

2. Seja $W = Im(\phi_2) = Ker(\phi_3)$. Temos que:

$$0 \longrightarrow V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} W \xrightarrow{\phi_3} 0$$

e

$$0 \longrightarrow W \xrightarrow{\psi} V_3 \xrightarrow{\phi_2} V_4 \xrightarrow{\phi_3} 0$$

são exatas e ψ é a inclusão. Pelo item anterior, temos:

$$dim(V_2) = dim(V_1) + dim(W)$$

e

$$dim(V_3) = dim(W) + dim(V_4)$$

Logo, $dim(V_4) = dim(V_3) - dim(V_2) + dim(V_1)$.

2.8 Comprimento de módulos

A noção de comprimento de um módulo estende a noção de dimensão de espaços vetoriais.

Definição 2.8.1 *Seja R um anel e seja M um R-módulo.*

1. *M é dito* ***simples*** *ou* ***irredutível*** *se $M \neq 0$ e seus únicos submódulos são 0 e M.*
2. *Uma* ***série de composição*** *de M de tamanho n é uma sequência de submódulos*

$$M = M_n \supsetneq M_{n-1} \supsetneq M_{n-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

   tais que os quocientes consecutivos $\frac{M_{i+1}}{M_i}$ são todos simples.
3. *O* ***comprimento*** *de M sobre R, denotado por $l_R(M)$, é o mínimo entre todos os tamanhos das séries de composição de M ou ∞ se M não admite série de composição finita.*

Da teoria de módulos temos o teorema:

Teorema 2.8.1 *(**Aditividade em Sequências Exatas**) Seja*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

uma sequência de R-módulos. Então

$$l_R(M) < \infty \Leftrightarrow l_R(M') < \infty \; e \; l_R(M'') < \infty.$$

Nesse caso,

$$l_R(M) = l_R(M') + l_R(M'').$$

2.9 Anéis de Valorização

Os resultados desta seção são extremamente relevantes quando se analisa o comportamento de uma aplicação definida na vizinhança de um ponto em uma curva algébrica.

Da teoria de corpos temos o seguinte teorema:

Teorema 2.9.1 *Seja R um subanel de um corpo K e $h : R \to C$ um homomorfismo de anéis de R em um corpo algebricamente fechado C. Se α é um elemento não nulo de K, então h pode ser estendido para um homomorfismo de anéis $\overline{h} : R[\alpha] \to C$ ou para um homomorfismo de anéis $\overline{h} : R[\alpha^{-1}] \to C$.*

É natural tentar estender h para um domínio maior, é com isso que entra em cena o conceito de anéis de valorização.

Definição 2.9.1 *Um subanel R de um corpo K é dito um **anel de valorização** de K se para todo $\alpha \in K$ não nulo, temos que α ou α^{-1} são elementos de R.*

Exemplo 2.9.1

1. *O corpo K é um anel de valorização de K.*
2. *Seja $K = \mathbb{Q}$, com p primo fixado. Tome R sendo o conjunto de todos os números racionais da forma $\frac{p^r m}{n}$, com $r \geq 0$ e p não divide nem m e nem n. Então R é um anel de valorização de K.*
3. *Seja K = K(x) e seja R o conjunto de todas as funções racionais $\frac{f}{g} \in K(x)$ tais que grau(f) < grau(g). Então R é um anel de valorização de $K(x)$.*

Da teoria de corpos temos o seguinte teorema:

Teorema 2.9.2 *Seja R um subanel de um corpo K e $h : R \to C$ um homomorfismo de anéis de R para um corpo algebricamente fechado C. Então h possui um elemento maximal $(V, \overline{h})$. Em outras palavras, V é um subanel de K contendo R, $\overline{h}$ é uma extensão de h e não existe uma extensão para um subanel estritamente maior. Em adição, para qualquer extensão maximal, V é um anel de valorização de K.*

2.9.1 Propriedades de Anéis de Valorização

Seja V um anel de valorização de um corpo K.

1. O corpo de frações de V é K.
   De fato, todo elemento não nulo α de K pode ser escrito como $\frac{\alpha}{1}$ ou $\frac{1}{\alpha^{-1}}$.
2. Todo subanel de K contendo V é um anel de valorização de K.
   Seja U um subanel qualquer de K tal que $V \subset U$. Nesse caso, segue da definição de anel de valorização que U é um anel de valorização de K, já que para todo $\alpha \in K$ não nulo, temos que $\alpha \in V \subset U$ ou $\alpha^{-1} \in V \subset U$.

3. V é um anel local.

   Pela Proposição 2.1.4, basta mostrarmos que o conjunto M dos elementos que não são unidades de V é um ideal.

   Se a e b são elementos não nulos e não são unidades, então $\frac{a}{b}$ ou $\frac{b}{a}$ pertencem a V.

   $$\frac{a}{b} \in V \Rightarrow a+b = b\left(1+\frac{a}{b}\right) \in M,$$

   pois se $b\left(1+\frac{a}{b}\right)$ fosse unidade, então b seria unidade.

   Similarmente,

   $$\frac{b}{a} \in V \Rightarrow a+b = a\left(1+\frac{b}{a}\right) \in M,$$

   pois se $a\left(1+\frac{b}{a}\right)$ fosse unidade, então a também seria uma unidade.

   Logo, M é um ideal.

4. V é integralmente fechado.

   Seja α um elemento não nulo de K, com α inteiro sobre V. Então existe uma equação da forma

   $$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \ com\ c_i \in V. \tag{2.5}$$

   Vamos mostrar que $\alpha \in V$ ou $\alpha^{-1} \in V$. Multiplique a equação (2.5) por $\alpha^{-(n-1)}$, logo temos que $\alpha = -c_{n-1} - c_{n-2}\alpha^{-1} - \cdots - c_1\alpha^{n-2} - c_0\alpha^{n-1} \in V$.

5. Se I e J são ideais de V, então $I \subseteq J$ ou $J \subseteq I$. Assim, os ideais de V são totalmente ordenados pela inclusão.

   De fato, suponha que I não está condido em J e tome $a \in I \setminus J$, com $a \neq 0$.

   Seja $b \in J$, vamos provar que $b \in I$.

   Se $b = 0$, então $b \in I$. Assuma que $b \neq 0$, então $\frac{b}{a} \in V$, já que se $\frac{a}{b} \in V$, então $a = \left(\frac{a}{b}\right) b \in J$, o que é uma contradição, Portanto, $b = \left(\frac{b}{a}\right) a \in J$.

6. Por outro lado, seja V um domínio com corpo de fração K. Se os ideias de V são parcialmente ordenados pela inclusão, então V é um anel de valorização de K.

   Se α é um elemento não nulo de K, então $\alpha = \frac{a}{b}$ com a e b elementos não nulos de V. Por hipótese, $(a) \subseteq (b)$, o que implica que, $\frac{a}{b} \in V$. Ou $(b) \subseteq (a)$, o que implica que, $\frac{b}{a} \in V$.

7. Se P é um ideal primo de um anel de valorização V, então V_p, ou seja, localização de V em P, e $\frac{V}{P}$ são aneis de valorizações.

   Primeiro note que se K é o corpo de frações de V, então também será de V_p. Temos que $\frac{V}{P}$ é um domínio, portanto possui corpo de frações. Por 5, os ideias de V são totalmente

ordenados pela inclusão, e o mesmo acontece para os ideias de V_P e $\frac{V}{P}$. Assim, o resultado segue por 6.

8. Se V é um anel de valorização Noetheriano, então V é um domínio de ideais principais. Além disso, para algum primo $p \in V$, todo ideal é da forma $(p^m),\ m \geq 0$. Para cada p, temos $\bigcap_{m=1}^{\infty} (p^m) = 0$.

   Como V é Noetheriano, um ideal I de V é finitamente gerado, digamos por $a_1, \cdots, a_n$. Por 5, podemos renumerar os a_i tais que $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n)$. Mas $I \subseteq (a_n) \subseteq I$, então $I = (a_n)$.

   Em particular, o ideal maximal M de V é (p) para algum p, e p é primo pois M é um ideal primo. Se (a) é um ideal arbitrário, então $(a) = V$ se a é uma unidade. Então, assuma que a não é unidade, isto é, $a \in M$. Mas então p divide a, logo $a = pb$. Se b não é unidade, então p divide b, logo $a = p^2c$. Continuando indutivamente e usando o fato de que V é domínio de ideias principais, logo também é domínio de fatoração única, temos $a = p^m u$, para algum inteiro m e unidade u. Assim, $(a) = (p^m)$. Finalmente, se a pertence a (p^m) para todo $m \geq 1$, então p^m divide a para todo $m \geq 1$. Usando novamente a fatoração única, temos que $a = 0$. Note que se a é uma unidade, então p também é, o que é uma contradição.

9. Seja R um subanel de um corpo K. O fecho inteiro $\bar{R}$ de R em K é a interseção de todos os anéis de valorizações V de K tal que $V \supseteq R$.

   Se $a \in \bar{R}$, então a é inteiro sobre R. Portanto, sobre qualquer anel de valorização já que $V \supseteq R$. Mas V é integralmente fechado por 4, logo $a \in V$. Por outro lado, assuma que $a \notin \bar{R}$. Então a não pertence ao anel $R' = R[a^{-1}]$ (se a é um polinômio em a^{-1}, multiplicando por uma potência suficientemente grande de a para obter um polinômio mônico satisfeito por a). Assim, a^{-1} não pode ser uma unidade em R' (se ba^{-1}, com $b \in R'$, então $a = a1 = aa^{-1}b \in R'$, o que é uma contradição).

   Segue que a^{-1} pertence ao ideal maximal M' de R'. Seja C o fecho algébrico do corpo $K = \frac{R'}{M'}$ e seja h a composição da aplicação canônica $R' \longrightarrow \frac{R'}{M'} = k$ com a inclusão $k \longrightarrow C$. Pelo Teorema 2.9.2, h possui uma extensão maximal dada por $\bar{h} : V \longrightarrow C$ para algum anel de valorização V de K contendo $R' \supseteq R$.

   Agora, $\bar{h}(a^{-1}) = h(a^{-1}) = 0$, por definição de h. Consequentemente, $a \notin V$, pois se $a \in V$, então $1 = \bar{h}(1) = \bar{h}(aa^{-1}) = \bar{h}(a)\bar{h}(a^{-1}) = 0$, que é uma contradição. O resultado segue.

10. Seja R um domínio com corpo de frações de K. Então R é integralmente fechado se,

e somente se, $R = \bigcap_{\alpha} V_\alpha$, a interseção para alguns (não necessariamente todos) anéis de valorização de K.

A implicação " $\Longrightarrow$ " segue por 9.

Para cada V_α é integralmente fechado por 4, logo R também é. Se a é inteiro sobre R, então a é inteiro sobre cada V_α, consequentemente a pertence a cada V_α, o que implica que $a \in R$.

Definição 2.9.2 *Um **valor absoluto** em um corpo K é uma aplicação*

$$|\cdot| : K \to \mathbb{R}$$

tal que para todo $x,\ y \in K$:

$$1.\ |x| \geq 0 \text{ e } |x| = 0 \Leftrightarrow x = 0;$$
$$2.\ |xy| = |x||y|;$$
$$3.\ |x+y| \leq |x| + |y|.$$

*O valor absoluto é dito **não arquimediano** se no lugar da condição 3. tivermos a condição mais forte:*

$$3'.\ |x+y| \leq max(|x|, |y|).$$

Os familiares valores absolutos dos números reais e complexos são arquimedianos.

Definição 2.9.3 *Uma **valorização discreta** em K é uma aplicação sobrejetiva*

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

tal que para todo $x,\ y \in K$, temos que

$$a)\ v(x) = \infty \Leftrightarrow x = 0;$$
$$b)\ v(xy) = v(x) + v(y);$$
$$c)\ v(x+y) \geq min(v(x), v(y)).$$

Exemplo 2.9.2 *Tome os corpos dos exemplo 2.9.1. No exemplo 1. e 2. tome $v\left(\frac{p^r m}{n}\right) = r$. No exemplo 3. tome $v\left(\frac{f}{g}\right) = grau(g) - grau(f)$.*

Lema 2.9.1 *Seja $v : K \to \mathbb{Z} \cup \{\infty\}$ uma valorização discreta. Então*

1. $v(\pm 1) = 0$ *e* $v(-a) = a$ *para todo* $a \in K$.
2. $v\left(\frac{a}{b}\right) = v(a) - v(b)$ *e* $v(b^{-1}) = -v(b)$ *para todo* $a,\ b \in K$ *com* $b \neq 0$.
3. $v(a+b) = v(b)$ *se* $v(a) > v(b)$.
4. *se* $a_1 + \cdots + a_n = 0$ *com* $n \geq 2$ *então existem* $i \neq j$ *tais que* $v(a_i) = v(a_j)$.

Prova:

1. Segue de

$$v(1) = v(1 \cdot 1) = v(1) + v(1)$$

$$v(1) = v((-1)(-1)) = v(-1) + v(-1)$$

e

$$v(-a) = v((-1) \cdot a) = v(-1) + v(a).$$

2. Segue de $v(b) + v(b^{-1}) = v(b \cdot b^{-1}) = v(1)$ e $v\left(\frac{a}{b}\right) = v(a) + v(b^{-1})$.
3. Temos $v(a+b) \geq min\{v(a),\ v(b)\} = v(b)$. Para mostrar a desigualdade oposta, observe que

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

Como $v(-a) = v(a) > v(b)$, temos $min\{v(a+b), v(-a)\} = v(a+b)$ obrigatoriamente, logo $v(b) \geq v(a+b)$ também.

4. Segue do item anterior, já que se $v(a_i) \neq v(a_j)$ para todo $i \neq j$. Em particular, haveria no máximo um termo $a_i = 0$. Logo, teríamos que a valorização do lado esquerdo da igualdade seria igual a $min\{v(a_i)\} \in \mathbb{Z}$, pois há algum termo não nulo enquanto que a valorização do lado direito seria ∞.

Proposição 2.9.1 *Se v é uma valorização discreta em um corpo K, então* $V = \{a \in K;\ v(a) \geq 0\}$ *é um anel de valorização com ideal maximal* $M = \{a \in K; v(a) \geq 1\}$.

Prova: Temos que V é um subanel de K, pois $v(a) \geq 0$ e $v(b) \geq 0$ implica que $v(a \pm b) \geq min\{v(a), v(b)\} \geq 0$ e $v(ab) = v(a) + v(b) \geq 0$.

Se $a \notin V$, então $v(a) < 0$, logo $v(a^{-1}) = v(1) - v(a) = 0 - v(a) > 0$. Assim, $a^{-1} \in V$. Portanto, V é um anel de valorização.

Além disso, como a é uma unidade de V se, e somente, se a e $a^{-1} \in V$ se, e somente se, v(a) = 0. Portanto, M é o ideal dos elementos que não são unidades e logo é ideal maximal do anel de valorização.

(V, M) é um anel local. As valorizações discretas não determinam todos os anéis de valorizações.

Definição 2.9.4 *Um anel de valorização V com valorização discreta v como na Proposição 2.9.1 é dito um* ***anel de valorização discreta****. Um elemento $t \in V$ com $v(t) = 1$ é chamado* ***uniformizador*** *ou* ***elemento primo*** *(de V).*

Proposição 2.9.2 *Seja t um uniformizador de um anel de valorização discreta V. Então t gera o ideal maximal M de V. Em particular, M é principal. Por outro lado, se t' é qualquer gerador de M, então t' é um uniformizador.*

Prova: Como M é o único ideal maximal, então $(t) \subseteq M$. Se $a \in M$, então $v(a) > 0$. Logo $v(at^{-1}) = v(a) - v(t) \geq 1 - 1 = 0$. Assim, $at^{-1} \in V$, ou seja, $a \in (t)$.

Agora, suponha que $M = (t')$. Como $t \in M$, temos que $t = ct'$ para algum $c \in V$. Assim, $1 = v(t) = v(ct') = v(c) + v(t') \geq 0 + 1 = 1$, o que implica que, v(t) = 1.

Proposição 2.9.3 *Se t é um uniformizador, então todo elemento não nulo $a \in K$ pode ser expresso unicamente por $a = ut^n$, com u unidade de V e $n \in \mathbb{Z}$. Também $K = V_t$, isto é, $K = S^{-1}V$, com $S = \{1, t, t^2, \cdots\}$.*

Prova: Seja $n = v(a)$, de modo que $v(at^{-n}) = 0$. Logo, at^{-1} é uma unidade u. De fato, temos que $v(at^{-n}) = v(a) - v(t^n) = v(a) - nv(t) = n - n = 0$.

Para provar a unicidade, note que se $a = ut^n$, então $v(a) = v(ut^n) = v(u) + nv(t) = 0 + n = n$, de modo que n, e portanto u, é determinado por a. A última afirmação segue da propriedade 1, da Seção 2.9.1 e do fato de que todos os elementos de V são aqueles com valorização $n \geq 0$.

Proposição 2.9.4 *Todo ideal não nulo I de um anel de valorização discreta V é da forma M^n, com M sendo um ideal maximal de V e n é o único inteiro não negativo. Escrevemos $v(I) = n$. Por convenção, temos $M^0 = V$.*

Prova: Escolha $a \in I$ tal que $n = v(a)$ é o menor possível. Pela Proposição 2.9.3 temos que $a = ut^n$, implica que, $t^n = u^{-1}a \in I$. Pela Proposição 2.9.2, temos que $M = (t)$, e portanto, $M^n \subseteq I$. Por outro lado, seja $b \in I$, com $v(b) = K \geq n$, pela minimalidade de n. Logo, pela prova da Proposição 2.9.3 temos que bt^{-k} é uma unidade u'. Assim, $b = u'k^k$ é uma unidade u'. Assim, $b = u't^k$. Como $k \geq n$ então $b \in (t^n) = M^n$. Portanto, $I \subseteq M^n$. Assim, $I = M^n$.

A unicidade de n é consequência do Lema de Nakayama:

Se $M^r = M^s$, com $r < s$, então $M^r = M^{r+1} = MM^r$. Assim, M^r, consequentemente, M, é 0, contradizendo o fato de que I é não nulo.

Interpretamos $v(I)$ como sendo o comprimento de uma série de composição.

Proposição 2.9.5 *Seja I um ideal não nulo do anel de valorização discreta R. Então* $v(I) = l_R(\frac{R}{I})$*, o comprimento do R-módulo* $\frac{R}{I}$.

Prova: Pela Proposição 2.9.4, temos

$$R \supset M \supset M^2 \supset \cdots \supset M^n = I.$$

Logo,

$$\tfrac{R}{I} \supset \tfrac{M}{I} \supset \tfrac{M^2}{I} \supset \cdots \supset \tfrac{M^n}{I} = 0.$$

Pela Proposição 2.8.1, tomando $l = l_R$, temos:

$$\begin{aligned} l\left(\tfrac{R}{I}\right) &= l\left(\tfrac{\frac{R}{I}}{\frac{M}{I}}\right) + l\left(\tfrac{M}{I}\right) \\ &= l\left(\tfrac{R}{M}\right) + l\left(\tfrac{\frac{M}{I}}{\frac{M^2}{I}}\right) + l\left(\tfrac{M^2}{I}\right). \end{aligned}$$

Prosseguindo, obtemos que $l\left(\frac{R}{I}\right) = \sum_{i=0}^{n-1} l\left(\frac{M^i}{M^{i+1}}\right)$.

Como M é gerado pelo uniformizador t, segue que $t^i + M^{i+1}$ gera $\frac{M^i}{M^{i+1}}$. Como $\frac{M^i}{M^{i+1}}$ é aniquilado por M, isto é, é um $\frac{R}{M}$-módulo, ou seja, um espaço vetorial sobre o corpo $\frac{R}{M}$. O espaço vetorial tem dimensão 1, pois segue da prova de 2.9.4 que M^i, com $i \in \{0, 1, \cdots, n\}$ são distintos. Portanto, $l(\frac{R}{I}) = n$.

Proposição 2.9.6 *Seja I um ideal de um anel Noetheriano R. Então, para algum inteiro positivo m temos que* $(\sqrt{I})^m \subseteq I$*. Em particular (tome* $I = 0$*), o nilradical de R é nilpotente.*

Prova: Como R é Noetheriano, $\sqrt{I}$ é finitamente gerado, digamos por $a_1, \cdots, a_t$ com $a_i^{n_i} \in I$. Então $(\sqrt{I})^m$ é gerado por todos os produtos $a_1^{r_1} \cdots a_t^{r_t}$, com $\sum_{i=1}^{t} r_i = m$.

Podemos escolher m da forma $m = 1 + \sum_{i=1}^{t} (n_i - 1)$. Ou seja, $r_i \geq n_i$ para algum i. Caso contrário, $r_i \leq n_i - 1$ para todo i e $m = \sum_{i=1}^{t} r_i < 1 + \sum_{i=1}^{t} (n_i - 1) = m$, uma contradição. Mas cada produto $a_1^{r_1} \cdots a_t^{r_t}$ está em I, logo, $(\sqrt{I})^m \subseteq I$.

Proposição 2.9.7 *Seja M um ideal maximal de um anel Noetheriano R e seja Q um ideal qualquer de R. As seguintes condições são equivalentes:*

1. *Q é M-primário;*
2. *$\sqrt{Q} = M$;*
3. *Para algum inteiro positivo n, temos que $M^n \subseteq Q \subseteq M$.*

Prova: 1. $\Rightarrow$ 2.

Como Q é M-primário, então Q é próprio e $xy \in Q \Rightarrow x \in Q$ ou $y^n \in Q$, para algum $n \geq 1$, isto é, $\sqrt{Q} = M$.

2. $\Rightarrow$ 1. Como $\sqrt{Q} = M$ é um ideal maximal, pelo Lema 2.4.1 Q é M-primário.

2. $\Rightarrow$ 3

Seja $I = Q$, pela Proposição 2.9.6, temos para algum inteiro n, tal que

$$(\sqrt{I})^n = M^n \subseteq Q \subseteq \sqrt{Q} = M,$$

o que implica que, $M^n \subseteq Q \subseteq M$.

3. $\Rightarrow$ 2

Pela Proposição 2.4.3, temos $M = \sqrt{M^n} \subseteq \sqrt{Q} \subseteq \sqrt{M} = M$.

3 TÓPICOS DE CURVAS ALGÉBRICAS

Nesse trabalho iremos considerar o corpo K sendo algebricamente fechado. Lembrando que um corpo K é algebricamente fechado quando todo $F \in K[x_1, \cdots, x_n]$ não constante se anula para um certo $(a_1, \cdots, a_n) \in K^n$.

Nesse capítulo apresentaremos alguns resultados de curvas algébricas que serão necessários para os resultados. Para uma leitura complemenar indicamos (FULTON, 2008).

3.1 Espaços Afins e Conjuntos Algébricos

Definição 3.1.1 *Temos que* $A^n(K) = K^n = \{p = (a_1, \cdots, a_n);\ a_i \in K,\ \forall\ 1 \leq i \leq n\}$ *é o conjunto de n-uplas de elementos de K. Chamamos* $A^n(K)$ *de* ***n-espaço afim****. Temos que* $A^1(K)$ *é a* ***reta afim*** *e* $A^2(K)$ *é o dito* ***plano afim****.*

Temos que A^n é o conjunto $K^n = \underbrace{K \times \cdots \times K}_{n\ vezes}$, ou seja, é o produto cartesiano considerando sem estrutura de espaço vetorial.

Definição 3.1.2 *Se* $p = (a_1, \cdots, a_n)$ *e* $F \in K[x_1, \cdots, x_n]$*, dizemos que p é* ***zero de F*** *ou* ***F anula p*** *se* $F(a_1, \cdots, a_n) = 0$*.*

Definição 3.1.3 *Dado F não constante, denotamos* $V(F) = \{p \in A^n(K);\ p\ é\ zero\ de\ F\}$ *e dizemos que* $V(F)$ *é a* ***hipersuperfície*** *determinada por F.*

Definição 3.1.4 *Se grau(F) = 1, dizemos que* $V(F)$ *é* ***hiperplano****, tipicamente,* $F = \sum_{i=1}^{n} \alpha_i x_i + \alpha_0$ *e* $V(F) = \{(a_1, \cdots, a_n);\ \sum_{i=1}^{n} \alpha_i a_i + a_0 = 0\}$.

Definição 3.1.5 *Em* $A^2(K)$*, dizemos que* $V(F)$*, para F não necessariamente de grau 1, é uma* ***curva plana afim*** *para* $S \subset K[x_1, \cdots, x_n]$*. Definimos* $V(S) = \{p \in A^n(K);\ F(p) = 0,\ para\ todo\ F \in S\} = \bigcap_{F \in S} V(F)$*. Dizemos que* $V(S)$ *é um* ***conjunto algébrico afim****.*

Notação: Se $S = \{F_1, \cdots, F_n\}$, então denotamos $V(S)$ por $V(F_1, \cdots, F_n)$.

3.2 Propriedades de Conjuntos Algébricos

1. $\emptyset$ e $A^n(K)$ são conjuntos algébricos afins
2. Seja $p \in A^n(K)$. Então $\{p\}$ é um conjunto algébrico afim;

3. Se $I =< S >$ é o ideal gerado por S, então $V(S) = V(I)$. Em particular, todo conjunto algébrico afim é da forma $V(I)$, para algum ideal I de $K[x_1, \cdots, x_n]$;
4. Se $\{I_\lambda;\ \lambda \in \Lambda\}$ é uma coleção de ideais de $K[x_1, \cdots, x_n]$, então $\bigcap\limits_{\lambda\in\Lambda} V(I_\lambda) = V\left(\bigcup\limits_{\lambda\in\Lambda} I_\lambda\right)$. Em particular, a interseção de conjuntos algébricos afins é um conjunto algébrico afim;
5. Se $I \subset J$, então $V(I) \supset V(J)$;
6. $V(I) \cup V(J) = V(IJ)$, onde $IJ = \{\sum\limits_{i=1}^{r} F_i G_i;\ r \in \mathbb{N},\ F_i \in I,\ G_i \in J\}$.

Prova:

1. De fato, temos que $V(\emptyset) = A^n(K)$ e $V(A^n(K)) = \emptyset$.
2. Seja $p = (a_1, a_2, \cdots, a_n)$. Então, temos que $\{p\} = \{(a_1, a_2, \cdots, a_n)\} = V(x_1 - a_1,\ x_2 - a_2, \cdots,\ x_n - a_n)$.
3. Como I é gerado por S, então $S \subset I$. Tome $p \in V(I)$, logo, $F(p) = 0,\ \forall\ F \in I$ e como, $S \subset I$, então $V(S) \supset V(I)$.

   Agora, tome $p \in V(S)$. Se $F \in I$, existem $F_1, \cdots,\ F_r \in S,\ G_1, \cdots,\ G_r \in K[x_1, \cdots, x_n]$ tal que

   $$F = G_1F_1 + \cdots + G_rF_r.$$

   Logo,

   $$F(p) = \sum_{i=1}^{r} G_i(p)\underbrace{F_i(p)}_{=0} = 0.$$

   Temos que $p \in V(I)$. Portanto, $V(S) \subset V(I)$.
4. Seja $p \in \bigcap\limits_{\lambda} V(I_\lambda)$, então p é zero de todo $F_\lambda \in I_\lambda,\ \forall\ \lambda$. Assim, p é zero de todo $F \in \bigcup\limits_{\lambda} I_\lambda$, o que implica que, $\bigcap\limits_{\lambda\in\Lambda} V(I_\lambda) \subset V\left(\bigcup\limits_{\lambda\in\Lambda} I_\lambda\right)$.
   Por outro lado, se $I_\lambda \subset \bigcup I_\alpha$, então $p \in V(\bigcup\limits_{\lambda\in\Lambda} I_\lambda)$. Assim, $p \in V(I_\lambda)$ e como λ é arbitrário, temos $p \in \bigcap_\lambda V(I_\lambda)$. Logo, $\bigcap\limits_{\lambda\in\Lambda} V(I_\lambda) \supset V\left(\bigcup\limits_{\lambda\in\Lambda} I_\lambda\right)$.
5. Tome $p \in V(J)$, logo, $F(p) = 0,\ \forall\ F \in J$ e como, $I \subset J$, então $V(I) \supset V(J)$.
6. Temos que

   $$\begin{aligned} IJ \subset I,\ J &\Rightarrow V(IJ) \supset V(I),\ V(J) \\ &\Rightarrow V(IJ) \supset V(I) \cup V(J). \end{aligned}$$

   Tome, agora, $p \in V(IJ) \setminus V(I)$. Então, $\exists\ F \in I$ tal que $F(p) \neq 0$. Se $G \in J$, temos $FG \in IJ$, logo, $(FG)(p) = 0$. Então, $\underbrace{F(p)}_{\neq 0} G_(p) = 0$. Logo, $G(p) = 0$.

   Como G foi escolhido arbitrariamente, temos $p \in V(J)$.

3.3 O ideal de um conjunto de pontos

Para $X \subset A^n(K)$, definimos $I(X) = \{F \in K[x_1, \cdots, x_n];\ F(p) = 0,\ \textit{para todo } p \in X\}$. Se $F, G \in I(X),\ H \in K[x_1, \cdots, x_n], p \in X$, então

$$(F-G)(p) = F(p) - G(p) = 0 - 0 = 0,$$
$$(F \cdot H)(p) = \underbrace{F(p)}_{=0} \cdot H(p) = 0 \cdot H(p) = 0.$$

Logo, $F - G,\ F \cdot H \in I(X)$. Portanto, I(X) é um ideal de X.

3.4 Propriedades do ideal de um conjunto de pontos

1. Se $X \subset Y$, então $I(X) \supset I(Y)$.
2. $I(\emptyset) = K[x_1, \cdots, x_n]$.
3. $I(\{(a_1, \cdots, a_n)\}) = (x_1 - a_1, \cdots, x_n - a_n)$.
4. $I(A^n(K)) = (0)$ se K for infinito.
5. $I(V(S)) \supset S$, para todo $S \subset K[x_1, \cdots, x_n]$ e $V(I(X)) \supset X$, para todo $X \subset A^n(K)$.
6. Se $W \subset A^n(K)$ é conjunto algébrico afim, então $V(I(W)) = W$. Se $J \subset K[x_1, \cdots, x_n]$ é ideal de um conjunto de pontos, então $I(V(J)) = J$.
7. $I(X)$ é ideal radical, para todo $X \subset A^n(K)$.

Prova 3.4.1 *1. Seja $F \in I(Y)$, então $F(p) = 0$, para todo $p \in Y$ e como $X \subset Y$, então $F(p) = 0$, para todo $p \in X$. Assim, $I(X) \supset I(Y)$.*

2. Seja o conjunto dos polinômios que não satisfazem nenhuma propriedade, então temos que $I(\emptyset) = K[x_1, \cdots, x_n]$.

3. Temos que $x_i - a_i$ anula $(a_1, \cdots, a_n)$ para todo $1 \leq i \leq n$. Logo, $x_i - a_i \in I(\{(a_1, \cdots, a_n)\})$, para todo i. Assim, temos que vale $I(\{(a_1, \cdots, a_n)\}) \supset (x_1 - a_1, \cdots, x_n - a_n)$.

Agora, tome $F \in K[x_1, \cdots, x_n]$ tal que $F(a_1, \cdots, a_n) = 0$. Logo,

$$\begin{aligned} F &= \sum_{i=1} a(i) x_1^{i_1} \cdots x_n^{i_n} \\ &= \sum_{i=1} (x_i - a_i + a_i)^{i_1} \cdots (x_n - a_n + a_n)^{i_n}. \end{aligned}$$

Como para $i_k > 0$, temos

$$\begin{aligned} (x_k - a_k + a_k)^{i_k} &= \sum_{j=0}^{i_k - 1} \binom{i_k}{j} (x_k - a_k)^{i_k - j} a_k^j + a_K^{i_k} \\ &= (x_k - a_k) G(x_1, \cdots, x_n) + a_K^{i_k}. \end{aligned}$$

Temos que

$$(x_1 - a_1 + a_1)^{i_1} \cdots (x_n - a_n + a_n)^{i_n} = \sum_{i=1}^{n} (x_j - a_j) H_j(x_1, \cdots, x_n) + a_i^{i_1} \cdots a_n^{i_n}.$$

Logo,

$$F = \sum_{i=1}^{n} (x_i - a_i) L_i(x_1, \cdots, x_n) + c.$$

Como $F(a_1, \cdots, a_n) = 0$*, temos* $c = 0$*. Logo,* $F \in (x_1 - a_1, \cdots, x_n - a_n)$.

4. *Usaremos indução sobre* $n \geq 1$.

   Tome $n = 1$*. Seja* $F \in K[x]$ *é tal que* $F(a) = 0$*, para todo* $a \in K$*. Como* K *é infinito, devemos ter* $F = 0$ *(No nosso caso,* K *sempre será infinito já que admitimos no início que* K *é algebricamente fechado).*

   Suponha a propriedade válida para $n < m$*, com* $m > 1$.

   Tome $F \in K[x_1, \cdots, x_n]$ *tal que* $F(a_1, \cdots, a_m) = 0$*, para todo* $a_1, \cdots, a_m \in K$.

   Seja

   $$F = F_0(x_1, \cdots, x_{m-1}) + F_1(x_1, \cdots, x_{m-1}) x_m + \cdots + F_k(x_1, \cdots, x_{m-1}) x_m^k \tag{3.1}$$

   e escolha $a_1, \cdots, a_{m-1} \in K$*. Se* $G(X_m) = F(a_1, \cdots, a_{m-1}, X_m)$*, temos por hipótese que* $G(a_m) = 0$*, para todo* $a_m \in K$*. Pelo caso inicial,* $G = 0$*. Logo,*

   $$\begin{aligned} 0 = G(X_m) &= \sum_{j=0}^{n} F_j(a_1, \cdots, a_{m-1} x_m^j \\ &\Rightarrow F_j(a_1, \cdots, a_{m-1}) = 0, \end{aligned}$$

   para todo $0 \leq j \leq k$.

   Como $a_1, \cdots, a_{m-1} \in K$ *foram escolhidos arbitrariamente, temos, por hipótese de indução,* $F_j = 0$*, para todo* $0 \leq j \leq K$*. Por* (3.1)*, temos* $F = 0$.

5. *Mostraremos que* $S \subset I(V(S))$*, para todo* $S \subset K[x_1, \cdots, x_n]$*. Tome* $F \in I(V(S))$*. Então,* $F(p) = 0$*, para todo* $p \in V(S)$*. Mas*

   $p \in V(S) \Leftrightarrow G(p) = 0, \ \forall \ G \in S.$ (3.2)

   Tome $G \in S$*. Para que* $G \in I(V(S))$*, devemos ter* $G(p) = 0, \forall \ p \in V(S)$*, que vem de* (3.2)*.*

   Agora, vamos mostrar que $X \subset V(I(X))$*. Tome* $p \in V(I(X))$*, então* $F(p) = 0$*, para todo* $F \in I(X)$*. Entretanto,*

   $F \in I(X) \Leftrightarrow F(p) = 0, \ \forall p \in X.$ (3.3)

   Tome $q \in X$*. Para que* $q \in V(I(X))$*, devemos ter* $F(q) = 0, \ \forall F \in I(X)$*, que vem de* (3.3)*.* .

6. *Já sabemos que* $V(I(W)) \supset W$ *e* $I(V(J)) \supset J$. *Agora, existe* $S \subset K[x_1, \cdots, x_n]$ *tal que* $W = V(S)$. *Logo,*

$$I(W) = I(V(S)) \supset S \Rightarrow V(I(W)) \subset V(S) = W.$$

A outra igualdade é provada do mesmo modo: $I(V(J)) \supset J$ *sempre e, se* $J = I(X)$, *então* $I(V(J)) = I(V(I(X))) \subset I(X) = J$.

7. *Temos de mostrar que* $\sqrt{I(X)} \subset I(X)$. *Se* $F \in \sqrt{I(X)}$, *digamos* $F^n \in I(X)$. *Então,* $F^n(p) = (F(p))^n = 0$, *para todo* $p \in X$. *Logo,* $F(p) = 0$, *para todo* $p \in X$, *isto é,* $F \in I(X)$.

3.5 Número finito de hipersuperficies

Teorema 3.5.1 *Todo conjunto algebricamente afim é a interseção de um número finito de hipersuperfícies.*

Prova: Se $W \subset A^n(K)$ é algébrico, sabemos que existe ideal I de $K[x_1, \ldots, x_n]$ tal que $W = V(I)$.

Como K é corpo, então por 2.5.1, temos que $K[x_1, \cdots, x_n]$ é Noetheriano. Logo, todo ideal de $K[x_1, \cdots, x_n]$ é finitamente gerado.

Seja $I = (F_1, \cdots, F_r)$, para certos $F_1, \cdots, F_r \in K[x_1, \cdots, x_n]$, então $W = V(I) = V(\{F_1, \cdots, F_r\}) = \bigcap_{j=1}^{r} V(F_j)$.

3.6 Componentes Irredutíveis de conjuntos algébricos

Definição 3.6.1 *Um conjunto algébrico* $V \in A^n(K)$ *é chamado* ***redutível*** *se tivermos* $V = V_1 \cup V_2$, *com* $V_1, V_2 \neq V$ *algébricos. Caso contrário, V é dito* ***irredutível****.*

Proposição 3.6.1 *Um conjunto algébrico* $V \subset A^n(K)$ *é irredutível se, e somente se,* $I(V)$ *é um ideal primo de* $K[x_1, \cdots, x_n]$.

Prova: Mostraremos que $V \subset A^n(K)$ é redutível se, e somente se, $I(V)$ não é um ideal primo de $K[x_1, \cdots, x_n]$.

Suponha que V é redutível, ou seja, $V = V_1 \cup V_2$, com $V_1,\ V_2 \neq V$ algébricos. Então $I(V) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$. Logo, $I(V) \subset I(V_1),\ I(V_2)$. Se tivessemos $I(V) = I(V_1)$, teríamos $V = V(I(V)) = V(I(V_1)) = V_1$, o que é um absurdo. Logo, $I(V) \subset I(V_1)$ e $I(V) \neq I(V_1)$. Analogamente, temos $I(V) \subset I(V_2)$ e $I(V) \neq I(V_2)$.

Tome $E_i \in I(V_i) \setminus I(V),\ i = 1,2$. Então, $E_1, E_2 \in I(V_1) \cap I(V_2) = I(V)$, com $E_1, E_2 \notin I(V)$. Segue que $I(V)$ não é primo.

Agora, suponha que $I(V)$ não é primo. Então, existem $F_1, F_2 \in K[x_1, \cdots, x_n] \setminus I(V)$ tais que $F_1, F_2 \in I(V)$. Logo, $(F_1F_2) \subset I(V)$. Portanto, $V = V(I(V)) \subset V(F_1F_2) = V(F_1) \cup V(F_2)$ de forma que: $V = V \cap (V(F_1) \cup V(F_2)) = (V \cap V(F_1)) \cup (V \cap V(F_2))$, com $V \cap V(F_1)$ e $V \cap V(F_2)$ algébricos.

Se tivessemos, $V = V \cap V(F_1)$, teríamos $V \subset V(F_1)$, logo $F_1 \in I(V(F_1)) \subset I(V)$. Mas isso contradiz a escolha de F_1. Assim, $V \neq V \cap V(E_1)$. Analogamente, $V \neq V \cap V(F_2)$. Então, V é redutível.

Proposição 3.6.2 *Se K é um corpo infinito (nosso caso pela hipótese de K ser algebricamente fechado), então $A^n(K)$ é irredutível.*

Prova: De fato, se K é infinito, temos $I(A^n(K)) = (0)$. Como $K[x_1, \cdots, x_n]$ é domínio, temos (0) primo. Logo, $A^n(K)$ é irredutível.

Em breve, vamos demonstrar que $I(V(J)) = \sqrt{J}$, para todo ideal J em $K[x_1, \cdots, x_n]$, onde K é algebricamente fechado. Esse resultado é conhecido como Teorema de Nullstellensatz.

Assumindo o Teorema de Nullstelensatz temos a seguinte propriedade:

Proposição 3.6.3 *Se K é um corpo algebricamente fechado e $F \in K[x_1, \cdots, x_n]$ é irredutível, então a hipersuperfície V(F) é um conjunto algebricamente irredutível.*

Prova: Como K é algebricamente fechado, o Nullstellensatz, garante que $I(V(F)) = \sqrt{(F)}$.

Por outro lado, como $K[x_1, \cdots, x_n]$ é domínio de fatoração única e F é irredutível, temos F primo, isto é, (F) é ideal primo. Assim, V(F) é um conjunto algébrico irredutível.

Pela Proposição 2.1.2 e pelo Teorema de Nullstellensatz, temos que $I(V(F)) = \sqrt{(F)} = (F)$ é um ideal primo, seque da Proposição 2.1.2. Logo, pela Proposição 3.6.1 temos que V(F) é irredutível.

Lema 3.6.1 *Se $\mathscr{V}$ é uma família não vazia de conjuntos algébricos de $A^n(K)$, então $\mathscr{V}$ tem pelo menos um elemento maximal (em relação à inclusão).*

Prova Seja $\mathscr{F} = \{I(V); V \in \mathscr{V}\}$ uma família não vazia de ideais do anel Noetheriano $K[x_1, \cdots, x_n]$. Então, sabemos que existe $V \in \mathscr{V}$ tal que $I(V)$ é maximal em $\mathscr{F}$.

Se $W \in \mathscr{V}$ fosse tal que $W \subset V$, então $I(W) \supset I(V)$ e a maximalidade de $I(V)$ garante que $I(W) = I(V)$. Logo, $W = V(I(W) = V(I(V)) = V$.

Teorema 3.6.1 *Todo $V \subset A^n(K)$ conjunto algébrico pode ser escrito, de modo único, como união finita de conjunto algébricos irredutíveis dois a dois incomparáveis em relação à inclusão.*

Prova: Existência: Suponha que exista um conjunto algébrico V_0 em $A^n(K)$ que não pode ser ecrtito como uma união finita de conjuntos algébricos irredutíveis.

Então, a família ν dos conjuntos algébricos de $A^n(K)$ que tem a mesma propriedade de V_0 é não vazia.

Pelo Lema 3.6.1, podemos tomar $V \in \mathscr{V}$ minimal. Em particular, V é redutível. Logo, temos $V = V_1 \cap V_2$, com $V_1, V_2 \neq V$ e algébricos. Pela minimalidade de V, temos $V_1, V_2 \notin \mathscr{V}$ algébricos. Logo, $V_1 = U_1 \cup \cdots \cup U_n$ e $V_2 = W_1 \cup \cdots \cup W_m$, com $U_i,\ W_j$ conjuntos algébricos irredutíveis. Segue que $V = V_1 \cup V_2 = \left(\bigcup_{i=1}^{n} U_i\right) \cup \left(\bigcup_{1=1}^{m} W_j\right)$ é uma união finita de conjuntos algébricos irredutível, o que é um absurdo.

Logo, $\mathscr{V} = \emptyset$, e assim, todo $V \subset A^n(K)$ algébrico pode ser escrito como

$$V = V_1 \cup \cdots \cup V_r, \ com\ V_1, \cdots, V_r, \tag{3.4}$$

conjuntos algébricos irredutíveis.

Agora, se $V_i \subset V_j$, para $i \neq j$ podemos retirar V_i de (3.4). Fazendo assim, podemos supor que, em (3.4), $V_1, \cdots, V_r$ são dois a dois incomparáveis em relação à inclusão.

Unicidade: Sejam

$$V = V_1 \cup \cdots \cup V_n \ \text{ e}$$
$$V = W_1 \cup \cdots \cup V_m,$$

com V_i, W_j irredutíveis e $V_i \not\subset V_j,\ W_i \not\subset W_j$, para todo $i \neq j$.

Para $1 \leq i \leq m$, temos

$$V_i = V_i \cap V = V_i \cap (W_1 \cup \cdots \cup W_m) = \bigcup_{j=1}^{m} (V_i \cap W_j).$$

Como V_i é irredutível e $V_i \cap W_j$ é algébrico, para todo $1 \leq j \leq m$, temos que existe $1 \leq j \leq m$ tal que $V_i = V_i \cap W_j$. Logo, existe $1 \leq j \leq m$ tal que $V_i \subset W_j$.

Da mesma forma, existe $1 \leq l \leq n$ tal que $W_j \subset V_l$. Logo, $V_i \subset W_j \subset V_l$, e para não termos um absurdo, deve ser i = l. Assim, $V_i = W_j$, isto é, para todo $1 \leq i \leq n$, existe $1 \leq j \leq m$ tal que

$$V_i = W_j \tag{3.5}$$

Se $V_i = W_{ji}$ e $V_i = W_{j2}$, teríamos $W_{j1} = W_{j2}$, logo, $j_1 = j_2$. Assim, (3.5) define uma função:

$$\phi : \{1, \cdots, n\} \longrightarrow \{1, \cdots, m\}.$$

Se $i_i,\ i_j$ são tais que $V_{i1} = W_j \Leftrightarrow \phi(i_1) = j$ e $V_{i2} = W_j \Leftrightarrow \phi(i_2) = j$, então $V_{i1} = V_{i2}$. Logo, $i1 = i2$. Assim, ϕ é injetiva, o que implica que $n \leq m$. Trocando os papeis dos $V_i's$ e $W_i's$, concluímos, de modo similar, que $m \leq n$. Logo, n = m, ϕ é bijetiva e $\{V_1, \cdots, V_n\} = \{W_1, \cdots, W_m\}$.

Definição 3.6.2 *Os V_i são chamados de **componentes irredutíveis** de V tais que $V = V_1 \cup \cdots \cup V_n$ é uma decomposição de V em componentes irredutíveis.*

3.7 Subconjunto Algébrico do Plano Afim

Proposição 3.7.1 *Se $F, G \in K[x,y]$ não tem fatores em comum, então $V(F,G) = V(F) \cap V(G)$ é finito.*

Prova: $mdc(F,\ G) = 1$ em $K[x,y] \simeq K[x][y]$. De fato, como $K[x]$ é domínio de ideais principais, então também é domínio de fatoração única, logo, o Lema de Gauss garante que $MDC(F,G) = 1$ em $K[x][y]$. E temos também que F e G não tem fatores em comum em $K(x)[y]$.

Como $K(x)[y]$ é domínio de ideais principais, então existem $U,\ V \in K(x)[y]$ tais que

$$F \cdot U + G \cdot V = 1. \tag{3.6}$$

Escreva U como $\frac{D(x,y)}{H(x)}$ e V como $\frac{E(x,y)}{H(x)}$. Substitua em (3.6), obtemos

$$F(x,y) \cdot D(x,y) + G(x,y) \cdot E(x,y) = H(x). \tag{3.7}$$

Se $P = (a,b) \in V(F,G)$, então, fazendo as substituições $x \mapsto a,\ y \mapsto b$ em (3.7), obtemos $H(a) = 0$. Logo, há no máximo um número finito de valores para a.

Trocando o papel de x e y, concluímos que só há um número finito de possibilidades para b. Logo, $V(F,G) = V(F) \cap V(G)$ é finito.

Corolário 3.7.1 *Se $F \in K[x,y]$ é irredutível e tal que $V(F)$ é infinito (automático se K for albebricamente fechado). Então $V(F)$ é irredudível e $I(V(F)) = (F)$.*

Prova: Se K é algebricamente fechado, então K é infinito. Logo, V(F) é infinito. Tome $x = a \in K$ (temos infinitas possibilidades). Assim, $F(a,y) = 0$ tem pelo menos uma solução, pois K é algebricamente fechado.

Como F é irredutível, então F é primo. Se mostrarmos que I(V(F)) = (F) teremos I(V(F)) ideal primo, logo, V(F) é irredutível.

Para o que falta, já sabemos que $I(V(F)) \supset (F)$. Suponha que $I(V(F)) \not\subset (F)$ e tome $G \in I(V(F)) \setminus (F)$.

Então, F não divide G, e como F é irredutível, F e G não tem fatores comuns. Pela Proposição 3.7.1, temos que $V(F) \cup V(G)$ é finito. Mas $G \in I(V(F))$, implica que $(G) \subset I(V(F))$, ou seja, $V(G) \supset V(I(V(F))) = V(F)$. Logo, temos $V(F) \cap V(G) = V(F)$, que é infinito por hipótese. Contradiçao.

Logo, $I(V(F)) \subset (F)$.

Corolário 3.7.2 *Seja K um corpo infinito. Os conjuntos algébricos irredutíveis de $A^2(K)$ são $\emptyset$, $A^2(K)$, $\{p\}$, curvas V(F), com $F \in K[x,y]$ irredutíveis tais que V(F) é infinito.*

Prova: Pela Proposição 3.6.2 temos que $A^2(K)$ é irredutível. Já pela Proposição 3.6.3 temos que $V(F)$ é irredutível quando $F \in K[x,\ y]$ é irredutível. Como seguirá da Proposição 3.7.1 que $I(\{p\}) = I(a_1,\ a_2) = (x - a_1,\ y - a_2)$ é maximal, logo primo, então $\{p\}$ é irredutível.

Reciprocamente, seja $V \in A^2(K)$ conjunto algébrico irredutível. Temos as seguintes possibilidades:

1. Se $V \neq \emptyset$ e finito, então V é um ponto.
2. Se $I(V) = (1)$, então $V = V(I(V)) = V(1) = \emptyset$.
3. Se $I(V) = (0)$, então $V = V(I(V)) = V(0) = A^2(K)$.
4. V é infinito e tal que $I(V)$ contém um polinômio não constante $F \in K[x,y]$. Seja $F = F_1 \cdots F_r$ a fatoração de F em irredutível. Como $F_1, \cdots, F_r \in I(V)$ e $I(V)$ é primo, então existe $1 \leq i \leq r$ tal que $F_i \in I(V)$.

   Assim, mudando a notação, podemos tomar $F \in I(V)$ irredutível.

   Afirmação: $I(V) = (F)$.

   De fato, já temos $(F) \subset I(V)$. Se a inclusão for estrita, podemos tomar $G \in I(V) \setminus (F)$. Logo, $G \notin (F)$, o que implica que G e F não tem fatores em comuns. Logo, $V(F) \cap V(G)$ é finito.

   Como $(F) \subset I(V)$ e $G \subset I(V)$, já que $G \in I(V)$, então $V(F),\ V(G) \supset V(I(V)) = V$. Assim, $V \subset V(F) \cap V(G)$, logo V seria finito, o que é um absurdo. Portanto, $I(V) = (F)$, logo, $V = V(I(V)) = V(F)$.

Corolário 3.7.3 *Sejam K corpo algébrico fechado e $F \in K[x_1, \cdots, x_n] \setminus K$. Se $F = F_1^{n_1} \cdots F_r^{n_r}$ é a decomposição de F em irredutíveis, com $F_1, \cdots, F_r$ dois a dois não associados, então:*

1. *a decomposição de V(F) em irredutíveis é $V(F) = V(F_1) \cup \cdots \cup V(F_r)$;*

2. $I(V(F)) = (F_1 \cdots F_r) = \sqrt{(F)}$.

Prova:

1. $V(F) = V(F_1^{n_1} \cdots F_r^{n_r}) = V(F_1) \cup \cdots \cup V(F_r)$.

   Agora, como K é algebricamente fechado, então $V(F_i)$ é infinito, para todo $1 \leq i \leq r$. Pelo corlário 3.7.1, $V(F_i)$ é irredutível e $I(V(F_i)) = (F_i)$, para todo $1 \leq i \leq r$.

   Se $i \neq j$ tais que $V(F_i) \subset V(F_j)$, então $(F_i) = I(V(F_i)) \supset I(V(F_j)) = (F_j)$, logo, $F_i | F_j$, o que é um absurdo. Então $i \neq j$, implica que $V(F_i) \not\subset V(F_j)$.

2. Temos que

$$\begin{aligned} I(V(F)) &= I(V(F_1) \cup \cdots \cup V(F_r)) \\ &= I(V(F_1)) \cap \cdots \cap I(V(F_r)) \\ &= (F_1) \cap \cdots \cap (F_r) \\ &= (F_1 \cdots F_r). \end{aligned}$$

   Por fim, temos

$$\begin{aligned} G \in \sqrt{(F)} &\Leftrightarrow \exists\, m \in \mathbb{N},\ G^m \in (F) \\ &\Leftrightarrow \exists\, m \in \mathbb{N},\ F \mid G^m \\ &\Leftrightarrow F_1, F_2, \cdots, F_r \mid G \\ &\Leftrightarrow F_1 \cdots F_r \mid G \\ &\Leftrightarrow G \in (F_1 \cdots F_r). \end{aligned}$$

Teorema 3.7.1 *Os ideais maximais de* $K[x_1, \cdots, x_n]$ *são da forma* $(x_1 - a_1, \cdots, x_n - a_n)$*, com* $a_1, \cdots, a_n \in K$.

Prova: Se $I = (x_1 - a_1, \cdots, x_n - a_n)$, então I é maximal. Temos que

$$F(x_1, \cdots, x_n) = \sum_{i=1}^{n} (x_i - a_i) F_i(x_1, \cdots, x_n) + F(a_1, \cdots, a_n), \tag{3.8}$$

onde $F \in K[x_1, \cdots, x_n]$. Agora, temos que

$$\begin{aligned} \psi : K[x_1, \cdots, x_n] &\to K \\ F &\mapsto F(a_1, \cdots, a_n) \end{aligned}$$

é claramente um homomorfismo sobrejetor. Se mostrarmos que $I = Ker\,\psi$, teremos, pelo Teorema dos homomorfismos que,

$$\frac{K[x_1, \cdots, x_n]}{I} \simeq K.$$

Como K é corpo, I deve ser maximal. Para o que falta, se $F \in I$, digamos

$$F = \sum_{i=1}^{n} (x_i - a_i)F_i, \tag{3.9}$$

temos que $\psi(F) = F(a_1, \cdots, a_n) = 0$. Assim, $F \in Ker\ \psi$.

Reciprocamente, se $F \in Ker\ \psi$, então $F(a_1, \cdots, a_n) = 0$ e (3.8) garante que F é da forma (3.9), isto é, $F \in I$.

Tome, agora, M ideal maximal de $K[x_1, \cdots, x_n]$. Se $L = \frac{K[x_1, \cdots, x_n]}{M}$, então L é corpo. Também temos que a composição

$$\begin{array}{ccccc} K & \to & K[x_1, \cdots, x_n] & \to & \frac{K[x_1, \cdots, x_n]}{M} \\ a & \mapsto & a & \mapsto & a + M \end{array}$$

é injetiva. Logo, sendo $\overline{K}$ sua imagem, temos que $\overline{K} = K$ e $\overline{K} \subset L$. Logo, é um corpo.

Como L é um corpo e uma K-álgebra finitamente gerada, temos que $\overline{L} = K$. Então, $x_1 + M, \cdots, x_n + M \in \overline{K}$, digamos

$$\begin{array}{rcl} \exists\, a_1 \in K,\ x_1 + M & = & a_1 + M \\ & \vdots & \\ \exists\, a_n \in K,\ x_n + M & = & a_n + M. \end{array}$$

Logo, $x_i - a_i \in M$, para todo $1 \leq i \leq n$ e, assim, $(x_1 - a_1, \cdots, x_n - a_n) \subset M$. Como ambos são maximais, então são iguais.

3.8 Nullstellensatz de Hilbert

Corolário 3.8.1 ***(Nullstellensatz Fraco)***

Se I é ideal próprio de $K[x_1, \cdots, x_n]$, então $V(I) \supset V(M)$, onde $M = (x_1 - a_1, \cdots, x_n - a_n)$.

Prova: Seja I ideal próprio, então existe ideal maximal M de $K[x_1, \cdots, x_n]$ tal que $I \subset M$. Logo, $V(I) \supset V(M)$.

Como $M = (x_1 - a_1, \cdots, x_n - a_n)$, então $V(M) = \{(a_1, \cdots, a_n)\}$. Assim, $(a_1, \cdots, a_n) \in V(I)$.

A existência de um ideal maximal contendo um ideal de um anel é conhecida como Teorema de Krull e é equivalente ao axioma da escolha.

Teorema 3.8.1 ***(Nullstellensatz de Hilbert)***

Se I é ideal de $K[x_1,\cdots,x_n]$, então $I(V(I)) = \sqrt{I}$.

Prova: Já temos que $I \subset I(V(I))$ e que $I(V(I))$, sendo o ideal do conjunto algébrico $V(I)$, é radical.

Logo, $\sqrt{I} \subset \sqrt{I(V(I))} = I(V(I))$.

Resta provarmos que $I(V(I)) \subset \sqrt{I}$.

Tome $G \in I(V(I))$. Seja $J = (F_1,\cdots,\ F_r,\ x_{n+1}G-1)$ ideal de $K[x_1,\cdots,\ x_n,\ x_{n+1}]$. Tome $H = x_{n+1}G-1$.

Vejamos quem é $V(J) \subset A^{n+1}(K)$.

Se $Q = (a_1,\cdots,\ a_n,\ a_{n+1}) \in V(J)$, então $P = (a_1,\cdots,\ a_n)$ anula $F_1,\cdots,\ F_r$. Como $G \in I(V(I))$ e $I = (F_1,\cdots,F_r)$, temos que G(P) = 0.

Logo, $0 = H(Q) = a_{n+1}G(P) - 1 = -1 \neq 0$, pois $G(P) = 0$, o que é um absurdo. Assim, $V(J) = \emptyset$ e pelo Nullstellensatz Fraco, temos $J = K[x_1,\cdots,x_{n+1}]$. Em particular, existem $A_1,\cdots,\ A_r,\ B \in K[x_1,\cdots,x_{n+1}]$ tais que

$$\sum_{i=1}^{r} A_i(x_1,\cdots,x_n,\ x_{n+1})F_i(x_1,\cdots,\ x_n) + B(x_1,\cdots,\ x_{n+1})(x_{n+1}G(x_1,\cdots,\ x_n)-1) = 1. \qquad (3.10)$$

A igualdade acima vale em $K[x_1,\cdots,x_{n+1}]$ logo, vale em $K(x_1,\cdots,x_{n+1})$.

Seja

$$\begin{aligned} \phi : K(x_1,\cdots,\ x_{n+1}) &\rightarrow K[x_1,\cdots,\ x_n] \\ H(x_1,\cdots,\ x_n,\ x_{n+1}) &\mapsto H\left(x_1,\cdots,\ x_n,\ \tfrac{1}{x_{n+1}}\right). \end{aligned}$$

Temos que ϕ é um homomorfismo e $\phi \circ \phi = Id$, logo, ϕ é um automorfismo de $K(x_1,\cdots,x_{n+1})$.

Aplicando ϕ a (3.10), obtemos

$$\sum_{i=1}^{r} A_i\left(x_1,\cdots,x_n,\frac{1}{x_{n+1}}\right)F_i(x_1,\cdots,x_n) + B\left(x_1,\cdots,x_n,\ \frac{1}{x_{n+1}}\right)\left(\frac{1}{x_{n+1}}G(x_1,\cdots,x_n)-1\right) = 1. \qquad (3.11)$$

Multiplique ambos os membros de (3.11) por x_{n+1}^m, com m suficientemente grande, logo

$$\sum_{i=1}^{r} \bar{A}\,(x_1,\cdots,x_n,x_{n+1})\,F_i(x_1,\cdots,x_n) + \bar{B}\,(x_1,\cdots,x_n,x_{n+1})\,(G(x_1,\cdots,x_n)-x_{n+1}) = x_{n+1}^m,$$

com $\bar{A},\ \bar{B} \in K[x_1,\ x_2, \cdots,\ x_{n+1}]$.

Aplique, por fim, o homormofismo de substituição:

$$\begin{array}{rcl} K[x_1, \cdots, x_n,\ x_{n+1}] & \rightarrow & K[x_1, \cdots,\ x_n] \\ x_i & \mapsto & x_i,\ \textit{para todo}\ 1 \leq i \leq n \\ x_{n+1} & \mapsto & G(x_1, \cdots,\ x_n). \end{array}$$

Obtemos

$$\sum_{i=1}^{r} \bar{A}_i(x_1, \cdots,\ x_n,\ G(x_1, \cdots, x_n))F_i(x_1, \cdots,\ x_n) = G(x_1, \cdots,\ x_n)^m,$$

onde $\bar{A}_i(x_1, \cdots,\ x_n,\ G(x_1, \cdots, x_n))F_i(x_1, \cdots,\ x_n) \in K[x_1, \cdots, x_n]$. Logo, $I(V(I)) \subset \sqrt{I}$.

O Corolário 3.8.1 recebe o nome de "Fraco"pois "formalmente", ele é uma consequência do Nullstellensatz.

De fato, se J é ideal primo de R, então $\sqrt{J}$ é ideal próprio de R, realmente, temos $1 \in \sqrt{J} \Rightarrow 1 \in J$, isto é, $\sqrt{J} = (1) \Rightarrow J = (1)$.

Em particular, se I é ideal próprio de $K[x_1, \cdots, x_n]$, temos $I(V(I)) = \sqrt{I}$, que é próprio. Logo, $V(I) \neq \emptyset$, pois do contrário teríamos $I(V(I)) = I(\emptyset) = K[x_1, \cdots, x_n] = (1)$.

Sendo $I = (F_1, \cdots, F_r)$, sabemos que $P = (a_1, \cdots, a_n) \in V(I)$ se e só se $(a_1, \cdots, a_n)$ é solução do sitema de equações:

$$\begin{array}{rcl} F_1 & = & 0 \\ F_2 & = & 0 \\ \cdots & & \\ F_r & = & 0. \end{array}$$

Agora, $G \in I(V(I)) \Leftrightarrow G$ se anula em todas as n-uplas $(a_1, \cdots, a_n)$ soluções do sistema de equações anterior. O Nullstellensatz diz que, nesse caso, existe $m \in \mathbb{N}$ tal que $G \in (F_1, \cdots,\ F_r)$, isto é, G^m é combinação linear de $F_1, \cdots, F_r$, com coeficiente em $K[x_1, \cdots,\ x_n]$.

Corolário 3.8.2 *Se $I \subset K[x_1, \cdots,\ x_n]$ é ideal radical, então $I(V(I)) = I$. Ademais, existem correspondências biunívocas, inversas uma da outra.*

1. *Ideais Radicais de $K[x_1, \cdots, x_n] \longleftrightarrow$ conjuntos algébricos afins em $A^n(K)$;*
2. *Ideais primos $\longleftrightarrow$ conjuntos algébricos irredutíveis;*
3. *Ideais maximais $\longleftrightarrow$ pontos.*

Prova: A primeira parte segue por Nullstellensatz.

1. se $J \in K[x_1, \cdots, x_n]$ é radical, então $I(V(J)) = J = \sqrt{J}$. Para $W \subset A^n(K)$ algébrico, já sabemos que $V(I(W)) = W$. Logo, I e V são bijeções, inversas uma da outra, entre os conjuntos em (1).
2. Já sabemos que se J é primo, então $I(V(J)) = J$, já que ideal primo implica ideal radical. Logo, V(J) é irredutível. Também, se $W \subset A^n(K)$ é irredutível, então já sabemos que I(W) é primo e V(I(W)) = W.
3. Por fim, para (3), já vimos que M maximal $\Leftrightarrow$ existem $a_1, \cdots, a_n \in K$ tais que $M = (x_1 - a_1, \cdots, x_n - a_n)$. Logo, $V(M) = \{(a_1, \cdots, a_n)\}$.
   Também já vimos que $F(a_1, \cdots, a_n) = 0$, o que implica que, $F \in (x_1 - a_1, \cdots, x_n - a_n)$, que é maximal.

3.9 Variedades Afins

Os conjuntos algébricos sob considerações serão os subconjuntos de $A^n(K)$, para algum $n \in \mathbb{N}$.

Definição 3.9.1 *Uma **variedade afim** em $A^n(K)$ é um conjunto algébrico afim irredutível $V \subseteq A^n(K)$.*

Vamos considerar apenas variedades afins, então vamos simplesmente chamá-las de variedades.

Definição 3.9.2 *Seja $V \subseteq A^n(K)$ uma variedade não vazia. Então $I(V)$ é um ideal primo em $K[x_1, \cdots, x_n]$. Logo $\frac{K[x_1, \cdots, x_n]}{I(V)}$ é um domínio Noetheriano. Chamamos o **anel de coordenadas** de V, o anel Noetheriano $\Gamma(V) = \frac{K[x_1, \cdots, x_n]}{I(V)}$.*

Definição 3.9.3 *Para qualquer conjunto não vazio V, seja $\mathscr{F}(V,K)$ o **conjunto de todas as funções de V para K**. Se $f, g \in \mathscr{F}(V,K)$, então $(f+g)(x) = f(x) + g(x)$ e $(fg)(x) = f(x)g(x)$, para todo $x \in V$.*

Definição 3.9.4 *Se $V \subset A^n$ é uma variedade, uma função $f \in \mathscr{F}(V,K)$ é chamada de **função polinomial** se existe um polinômio $F \in K[x_1, \cdots, x_n]$ tal que $f(a_1, \cdots, a_n) = F(a_1, \cdots, a_n)$ para todo $(a_1, \cdots, a_n) \in V$.*

Proposição 3.9.1 *Se $V \subseteq A^n(K)$ é uma variedade afim, então a aplicação*

$$\begin{array}{rcl} \phi : K[x_1,\cdots,x_n] & \to & \mathscr{F}(V,K) \\ F & \mapsto & f, \end{array}$$

onde $f : V \to K$ *é dada por* $f(a_1,\cdots,a_n) = F(a_1,\cdots,a_n)$ *é um homomorfismo de anéis com núcleo* $I(V)$. *Em particular,* ϕ *induz um homomorfismo injetor* $\overline{\phi} : \Gamma(V) \to \mathscr{F}(V,K)$ *que torna comutativo o diagrama:*

$$\begin{array}{ccc} K[x_1,\cdots,x_n] & \xrightarrow{\phi} & \mathscr{F}(V,K) \\ \downarrow & \nearrow_{\overline{\phi}} & \\ \Gamma(V) & & \end{array}$$

A imagem de $\Gamma(V)$ *por* $\overline{\phi}$ *é o subanel de* $\mathscr{F}(V,K)$ *formado pelas funções polinomais de V em K.*

Prova: Se $F \in K[x_1,\cdots,x_n]$, então F induz uma função

$$\overline{F} : V \to K,$$

dada por

$$\overline{F}(a_1,\cdots,a_n) = F(a_1,\cdots,a_n).$$

Assim, temos a aplicação:

$$\begin{array}{rcl} \phi : K[x_1,\cdots,x_n] & \to & \mathscr{F}(V,K) \\ F & \mapsto & \bar{F}, \end{array}$$

que é um homomorfismo de anéis, pois

$$\overline{F+G} = \overline{F} + \overline{G},$$

já que

$$\begin{array}{rcl} \overline{F+G}(a_1,\cdots,a_n) & = & (F+G)(a_1,\cdots,a_n) \\ & = & F(a_1,\cdots,a_n) + G(a_1,\cdots,a_n) \\ & = & \overline{F}(a_1,\cdots,a_n) + \overline{G}(a_1,\cdots,a_n) \\ & = & (\overline{F}+\overline{G})(a_1,\cdots,a_n). \end{array}$$

Da mesma forma, temos $\overline{FG} = \overline{F}\,\overline{G}$.

Veja que

$$\begin{aligned}
\overline{F} = 0 &\Leftrightarrow \overline{F}(a_1,\cdots,a_n) = 0,\ \forall\ (a_1,\cdots,a_n) \in V \\
&\Leftrightarrow F(a_1,\cdots,a_n) = 0,\ \forall\ (a_1,\cdots,a_n) \in V \\
&\Leftrightarrow \qquad\qquad F \in I(V).
\end{aligned}$$

Pelo Teorema dos Homomorfismos:

$$\begin{array}{ccc}
K[x_1,\cdots,x_n] & \xrightarrow{\ \phi\ } & \mathscr{F}(V,K) \\
\Big\downarrow \pi & \nearrow_{\overline{\phi}} & \\
\Gamma(V) = \frac{K[x_1,\cdots,x_n]}{I(V)} & &
\end{array}$$

com

$$\begin{aligned}
\Gamma(V) &\to \mathscr{F}(V,K) \\
F + I(V) &\mapsto \overline{F}
\end{aligned}$$

injetivo. Assim, podemos ver $\Gamma(V)$ como subanel de $\mathscr{F}(V,K)$. Quando vemos $\Gamma(V)$ como conjunto de funções, dizemos que seus elementos são as funções polinomiais de V em K.

3.10 Aplicações Polinomiais

Definição 3.10.1 *Sejam $V \subset A^n(K)$ e $W \subset A^m(K)$ variedades afins. Uma aplicação $\phi : V \to W$ é chamada **aplicação polinomial** se existem polinômios $T_1,\cdots,T_m \in K[x_1,\cdots x_n]$ tais que $\phi(a_1,\cdots,a_n) = (T_1(a_1,\cdots,a_n),\cdots,T_m(a_1,\cdots,a_n))$ para todo $(a_1,\cdots,a_n) \in V$.*

Se $V = A^n$, $W = A^m$ e $T_1,\cdots,\ T_m \in K[x_1,\cdots,x_n]$ determinam uma aplicação polinomial $T : A^n \to A^m$, então T_i são unicamente determinados por T. Assim, podemos escrever $T = (T_1,\cdots,\ T_m)$.

Proposição 3.10.1 *Sejam $V \subset A^n(K)$ e $W \subset A^m(K)$ variedades afins e $\phi : V \to W$ aplicação polinomial. Então ϕ induz um homomorfismo $\phi^* : \Gamma(W) \to \Gamma(V)$ (o pullback de ϕ), por $\phi^*(f) = f \circ \phi : V \to K$, ou seja, $\phi^*(T + I(W)) = F \circ \phi + I(V)$, onde $f : W \to K$ e $T \in K[x_1,\cdots,x_n]$.*

Prova: Seja $\phi = (T_1,\cdots,T_m)$, com $T_1,\cdots,T_m \in K[x_1,\cdots,x_n]$. Se $T \in K[x_1,\cdots,x_n]$, então $T \circ \phi = T(T_1(x_1,\cdots,x_n),\cdots,T_m(x_1,\cdots,x_n))$ é um polinômio em $K[x_1,\cdots,x_n]$.

Se $T,\ U \in K[x_1,\cdots,x_n]$ são tais que $T + I(W) = U + I(W)$, então $T - U \in I(W)$, logo, $(T-U)(Q) = 0,\ \forall\ Q \in W$.

Em particular, $(T-U)(\phi(P)) = 0,\ \forall\ P \in V$, isto é, $(T \circ \phi - U \circ \phi)(P) = 0, \forall\ P \in V$.

Assim, $T \circ \phi - U \circ \phi \in I(V)$, logo, $T \circ \phi + I(V) = U \circ \phi + I(V)$.

Por fim, para $\overline{T},\overline{U} \in K[x_1,\cdots,x_m]$, temos

$$\begin{aligned}
\phi^*(\overline{T}+\overline{U}) &= \phi^*(\overline{T+U}) \\
&= (\overline{T+U})\circ\phi \\
&= (\overline{T}+\overline{U})\circ\phi \\
&= \overline{T}\circ\phi+\overline{U}\circ\phi \\
&= \phi^*(\overline{T})+\phi^*(\overline{U}).
\end{aligned}$$

Veja que se $Id : V \to V$, então $Id^* = Id : \Gamma(V) \to \Gamma(V)$.

Se $\phi : V \to W$ e $\psi : W \to Z$ são polinomiais, então $\psi\circ\phi : V \to Z$ é polinomial. De fato, se $\phi = (T_1,\cdots,T_m), \psi = (U_1,\cdots,U_p)$, então $\psi\circ\phi = (U_1(T_1,\cdots,T_m),\cdots U_p(T_1,\cdots,T_m)))$ e $(\psi\circ\phi)^* = \phi^*\circ\psi^*$.

Proposição 3.10.2 *Se $\alpha : \Gamma(W) \to \Gamma(V)$ é um K-homomorfismo de anéis, então existe uma aplicação polinomial $\phi^* : V \to W$ tal que $\alpha = \phi^*$. Além disso, a correspondência*

$$\begin{array}{ccccc}
\Phi : \{\phi : V \to W; \phi \text{ é polinomial}\} & \to & \{\alpha : \Gamma(w) \to \Gamma(V); \alpha \text{ é homomorfismo}\} \\
\phi & \mapsto & \phi^*
\end{array}$$

é uma bijeção.

Prova: Já vimos que Φ está bem definida.

Dada $\alpha : \Gamma(W) \to \Gamma(V)$ homomorfismo, se mostrarmos que existe $\phi : V \to W$ polinomial, tal que $\alpha = \phi^*$, então $\alpha = \Phi(\phi)$ e Φ será sobrejetiva.

Para $1 \leq i \leq m$, temos

$$\alpha(y_i + I(W)) = T_i + I(V),$$

por definição e com $T_i = (T_1,\cdots,T_n)$.

Defina $\phi = (T_1,\cdots,T_m) : A^n(K) \to A^m(K)$ polinomial para mostrar que $\phi(V) \subset W$, tome $G = G(y_1,\ldots,y_m) \in K[y_1,\cdots,y_m]$, digamos, $G = \sum_I a_I y_1^{i_1}\cdots y_m^{i_m}$. Então,

$$\begin{aligned}
\alpha(G+I(W)) &= \alpha\left(\sum_I a_I y_1^{i_1}\cdots y_m^{i_m} + I(W)\right) \\
&= \alpha\left(\sum_I (a_I + I(W))\cdot(y_1+I(W))^{i_1}\cdots(y_m+I(W))^{i_m}\right) \\
&= \sum_I \alpha(a_I+I(W))\cdot\alpha(y_1+I(W))^{i_1}\cdots\alpha(y_m+I(V))^{i_m} \\
&= \sum_I a_I + I(V))(T_1+I(V))^{i_1}\cdots(T_m+I(V))^{i_m} \\
&= \sum_I T_1^{i_1}\cdots T_m^{i_m} + I(V) \\
&= G\circ\phi + I(V).
\end{aligned}$$

Em resumo, $\alpha(G+I(W)) = G\circ\phi + I(V)$.

Portanto,

$$\begin{aligned} G\in I(W) \Rightarrow G\circ\phi + I(V) &= \alpha(G+I(W)) \\ &= \alpha(0+I(W)) \\ &= 0+I(V). \end{aligned}$$

Logo, $G\circ\phi \in I(V)$, o que implica que $G\in I(\phi(V))$.

Para $P\in V$, temos que:

$$\begin{aligned} G\in I(\phi(V)) &\Leftrightarrow G(\phi(P)) = 0 \\ &\Leftrightarrow (G\circ\phi)(P) = 0 \\ &\Leftrightarrow G\circ\phi \in I(V). \end{aligned}$$

Logo, $I(W)\subset I(\phi(V))$, de modo que $W = V(I(W)) \supset V(I(\phi(V)) \supset \phi(V)$, já que W é algébrico. Assim, $\phi : V\to W$ é polinomial, de sorte que induz $\phi^* : \Gamma(W)\to\Gamma(V)$. Mas,

$$\begin{aligned} \alpha(G+I(W)) &= G\circ\alpha + I(V) \\ &= \phi^*(G+I(W)). \end{aligned}$$

Portanto, $\alpha = \phi^*$. Resta mostrar que Φ é injetiva.

Para tanto, tome $\phi,\ \psi : V\to W$ polinomiais tais que $\phi^* = \psi^* : \Gamma(W)\to\Gamma(V)$. Então,

$$\underbrace{\phi^*(y_i+I(W))}_{T_i+I(V)} = \underbrace{\psi^*(y_i+I(W))}_{G_i+I(V)},$$

para todo $1\le i\le m$.

De modo que, $T_i - G_i \in I(V)$, para todo $1\le i\le m$. Assim, para $P\in V$, temos $\phi(P) = (T_1(P),\cdots,T_m(P)) = (G_1(P),\cdots G_m(P)) = \psi(P)$.

Definição 3.10.2 *Uma aplicação polinomial $\phi : V\to W$ é um **isomorfismo** se existe uma aplicação polinomial $\psi : W\to V$ tal que $\psi\circ\phi = identidade\ em\ V$ e $\phi\circ\psi = identidade\ em\ W$. Nesse caso, denotamos $V\simeq W$.*

Proposição 3.10.3 *V é isomorfo a W se, e somente se, $\Gamma(V)$ é isomorfo a $\Gamma(W)$.*

Prova: Sejam $\phi : V\to W,\ \psi : V\to W$ aplicações polinomiais bijetivas, com $\psi\circ\phi = Id_V,\ \phi\circ\psi = Id_W$. Então,

$$Id_{\Gamma(V)} = (Id_V)^* = (\psi\circ\phi)^* = \phi^*\circ\psi^*.$$

E, analogamente, $Id_{\Gamma(W)} = \psi^* \circ \phi^*$.

Assim, $\phi^* : \Gamma(W) \to \Gamma(V)$ e $\psi^* : \Gamma(V) \to \Gamma(W)$ são isomorfismos inversos um do outro.

Agora, sejam $\phi : \Gamma(V) \to \Gamma(W)$ e $\beta : \Gamma(W) \to \Gamma(V)$ inversos um do outro. Pela proposição anterior, existe $\phi : V \to W$ e $\psi : W \to V$ tais que $\alpha = \psi^*$, $\beta = \phi^*$. Então, $(Id_W)^* = Id_{\Gamma(W)} = \alpha \circ \beta = \psi^* \circ \phi^* = (\phi \circ \psi)^*$. Logo, $\phi \circ \psi = Id_W$, pela proposição anterior. Analogamente. $\psi \circ \phi = Id_V$. Logo, $V \simeq W$.

Definição 3.10.3 *Um conjunto $V \subset A^n(K)$ é chamado de **subvariedade linear** de $A^n(K)$ se $V = V(F_1, \cdots, F_r)$ para alguns polinômios F_i de grau 1.*

3.11 Mudança de Coordenadas

Definição 3.11.1 *Se $T = (T_1, \cdots, T_m)$ é uma aplicação polinomial de A^n para A^m e $F \in K[x_1, \cdots, x_m]$, temos que $F^T = \widetilde{T}(F) = F(T_1, \cdots, T_m)$, onde $\widetilde{T} : \Gamma(A^m) \to \Gamma(A^n)$. Para ideais I e conjuntos algébricos V em A^m, denotamos I^T o ideal em $K[x_1, \cdots, x_n]$ gerado por $\{F^T;\ F \in I\}$ e V^T o conjunto algébrico $T^{-1}(V) = V(I^T)$, com $I = I(V)$. Temos:*

$$\begin{array}{rccc} \widetilde{T} : K[x_1, \cdots, x_m] & \to & K[x_1, \cdots, x_n] \\ T & \mapsto & I^T \\ F & \mapsto & F^T, \end{array}$$

e também que

$$\begin{array}{rcl} P \in T^{-1} & \Leftrightarrow & V \in T(P) \\ & \Leftrightarrow & F(T(P)) = 0,\ \forall F \in I(V) \\ & \Leftrightarrow & F^T(P) = 0,\ \forall F \in I(V) = I \\ & \Leftrightarrow & P \in V(I^T). \end{array}$$

Definição 3.11.2 *Uma **mudança de coordenadas afim** em A^n é uma aplicação polinomial $T = (T_1, \cdots, T_n) : A^n \to A^n$ tal que cada T_i é um polinômio de grau 1 e de tal modo que T é injetiva e sobrejetiva. Se $T_i = \sum a_{ij}x_j + a_{i0}$, então $T = T'' \circ T'$, com T' uma aplicação linear $T_i' = \sum a_{ij}x_j$ e T'' uma translação $T_i'' = x_i + a_{i0}$. Como qualquer tranlação possui inversa e esta também é uma translação, segue que T também é injetiva (e sobrejetiva) se, e somente se, T' é invertível, ou seja, $Det(a_{ij}) \neq 0$. Se T e U são mudanças de coordenadas em A^n, então $T \circ U$ e T^{-1} também são.*

Proposição 3.11.1 *Seja $P=(a_1,\cdots,a_n)$, $Q=(b_1,\cdots,b_n)$ pontos distintos de A^n. A reta que passa pelos pontos P e Q é definida por $\{a_1+t(b_1-a_1),\cdots,a_n+t(b_n-a_n));\ t\in K\}$. Então: Sejam P, $P'\in A^2$, L_1, L_2 duas retas distintas que passam por P, então L_1', L_2' retas distintas que passam por P'. Logo, existe uma mudança de coordenadas T de A^2 tal que $T(P)=P'$ e $T(L_i)=L_i',\ i=1,\ 2$.*

Prova: Como uma translação leva P em $(0,\ 0)$, podemos supor que $L_1,\ L_2$ passam por $(0,\ 0)$. Por composição, basta provarmos a existência de T, uma mudança afim de coordenadas, que leva L_1 no eixo x e L_2 no eixo y. Seja $L_1=V(ax+by),\ L_2=V(cx+dy)$. De $L_1\neq L_2$ temos $ad-bc\neq 0$. Logo, se

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix}$$

tome $T^{-1}=(T_1,\ T_2)$, com

$$T_1(x,\ y)=t_{11}x+t_{12}y,\ T_2(x,\ y)=t_{21}x+t_{22}y.$$

3.12 Funções Racionais

Seja V uma variedade não vazia e $\Gamma(V)$ seu anel de coordenadas.

Definição 3.12.1 *O corpo de frações de $\Gamma(V)$, denotado por $K(V)$, é **corpo de funções racionais** de V. Um elemento $\alpha\in K(V)$ é uma **função racional** em V.*

*Dada $\alpha\in K(V)$, dizemos que α **está bem definida** em $P\in V$ se tivermos $\alpha=\frac{f}{g}$, com $f=\overline{F},\ g=\overline{G}$ e $G(P)\neq 0$.*

*Portanto, se α não estiver bem definida em $P\in V$, teremos $G(P)=0$ para toda representação fracionária $\frac{\overline{F}}{\overline{G}}$. Dizemos que P é um **pólo** de α. O conjunto dos pólos de α é $P(\alpha)$.*

Proposição 3.12.1 *Sejam $V\subset A^n(K)$ variedade e $\alpha\in K(V)$. Então $P(\alpha)$ é um conjunto algébrico de V. Mais precisamente,*

$$P(\alpha)=V(J_\alpha), \tag{3.12}$$

onde J_α é o ideal $J_\alpha=\{G\in K[x_1,\cdots,x_n];\ \overline{G}\alpha\in\Gamma(V)\}$.

Prova: Se $G_1,G_2\in K[x_1,\cdots,x_n]$ são tais que $\overline{G_1}\alpha,\ \overline{G_2}\alpha\in\Gamma(V)$, então $(\overline{G_1-G_2})\alpha=\overline{G_1}\alpha-\overline{G_2}\alpha\in\Gamma(V)$. Logo, $G_1-G_2\in J_\alpha$.

Se $G \in J_\alpha,\ H \in K[x_1,\cdots,x_n]$, então $\overline{HG}\alpha = \overline{H}\ \overline{G}\alpha \in \Gamma(V)$. Logo, $HG \in J_\alpha$.

Note que $J_\alpha \neq \emptyset$, pois, se $\alpha = \frac{\overline{F}}{\overline{G}}$ é uma representação fracionária de α, então $\overline{G}\alpha = \overline{G}\frac{\overline{F}}{\overline{G}} = \overline{F} \in \Gamma(V)$, logo, $G \in J_\alpha$. Para (3.12), vamos mostrar que $P(\alpha) \subset V(J_\alpha)$ e $V(J_\alpha) \subset P(\alpha)$.

$P(\alpha) \subset V(J_\alpha)$: Tome $P \in P(\alpha)$ e $G \in J_\alpha$. Então, $\overline{G}\alpha \in \Gamma(V)$, digamos $\overline{G}\alpha = \overline{F}$, com $F \in K[x_1,\cdots,x_n]$. Logo, $\alpha = \frac{\overline{F}}{\overline{G}}$ e, como, $P \in P(\alpha)$, temos $G(P) = 0$. Assim, $P \in V(J_\alpha)$.

$V(J_\alpha) \subset P(\alpha)$: Tome $P \in V(J_\alpha)$. Se $\alpha = \frac{\overline{F}}{\overline{G}}$, com $F, G \in K[x_1,\cdots,x_n]$, então $\overline{G}\alpha = \overline{F} \in \Gamma(V)$, logo, $G \in J_\alpha$. Assim, $G(P) = 0$, de modo que α não está definida em P, isto é, $P \in P(\alpha)$.

Proposição 3.12.2 *Se $\alpha \in K(V)$, então α define uma função*

$$\begin{array}{rcl} \alpha : V \setminus P(\alpha) & \to & K \\ P & \mapsto & \frac{F(P)}{G(P)}. \end{array}$$

Seja $\alpha = \frac{\overline{F}}{\overline{G}}$ é representação de α tal que $G(p) \neq 0$. Uma tal representação existe, pois $P \notin P(\alpha)$. Além disso, se $\beta \in K(V)$ é tal que $P(\alpha) = P(\beta) = W$ e $\alpha = \beta$ em funções de $V \setminus W$ em K, então $\alpha = \beta$ em $K(V)$.

Prova: Fixada α e $P \notin P(\alpha)$, seja $\alpha = \frac{\overline{F_1}}{\overline{G_1}} = \frac{\overline{F_2}}{\overline{G_2}}$, com $\overline{G_1(P)},\ \overline{G_2(P)} \neq 0$. Então, $\overline{F_1}\ \overline{G_2} = \overline{F_2}\ \overline{G_1}$, ou ainda, $\overline{F_1 G_2} = \overline{F_2 G_1}$. Assim, $F_1G_2 - F_2G_1 \in I(V)$. Portanto, para $P \in V \setminus P(\alpha)$ temos $(F_1G_2 - F_2G_1)(P) = 0$, isto é, $F_1(P)G_2(P) = F_2(P)G_1(P)$. Como $G_1(P),\ G_2(P) \neq 0$, segue que, $\frac{F_1(P)}{G_1(P)} = \frac{F_2(P)}{G_2(P)}$. Tome $\alpha,\ \beta \in K(V)$ tais que $P(\alpha) = P(\beta) = W$ e $\alpha = \beta$ como funções de $V \setminus W$ em K.

Se $\alpha = \frac{\overline{F}}{\overline{G}}$ e $\beta = \frac{\overline{H}}{\overline{L}}$, temos que mostrar que $\frac{\overline{F}}{\overline{G}} = \frac{\overline{H}}{\overline{L}}$ isto é, $FL - GH \in I(V)$. Para tanto, tome $P \in V$.

Há dois casos:

1. $P \in W$. Como $W = P(\alpha) = P(\beta)$, temos que α e β não estão definidas em P. Logo, $\overline{G}(P) = \overline{L}(P) = 0$. Assim, $(FL - GH)(P) = F(P)L(P) - G(P)H(P) = 0$, já que $G(P) = L(P) = 0$.
2. $P \in V \setminus W$. Tome representação fracionárias $\frac{\overline{F_1}}{\overline{G_1}} = \frac{\overline{H_1}}{\overline{L_1}}$ tais que $G_1(p) \neq 0,\ L_1(P) \neq 0$. Então, $\alpha(P) = \beta(P)$, implica que $\frac{F_1(P)}{G_1(P)} = \frac{H_1(P)}{L_1(P)}$, ou seja, $(F_1L_1 - G_1H_1)(P) = 0$. Mas $\frac{\overline{F}}{\overline{G}} = \frac{\overline{F_1}}{\overline{G_1}}$ e $\frac{\overline{H}}{\overline{L}} = \frac{\overline{H_1}}{\overline{L_1}}$, implicam que $FG_1 - F_1G_1$ *e* $HL_1 - H_1L \in I(V)$.
   Avaliando a identidade:

$$\underbrace{(FG_1 - F_1G)LL_1}_{\in I(V)} - \underbrace{(HL_1 - H_1L)GG_1}_{\in I(V)} = (FL - HG)G_1L_1 - \underbrace{(F_1L_1 - G_1H_1)}_{0 \text{ em } P}GL,$$

em P, obtemos $(FL-GH)(P)\underbrace{G_1(P)L_1(P)}_{\neq 0} = 0$. Logo, $(FL-GH)(P) = 0$. Assim, $(FL-HG)(P) = 0$, $\forall P \in V$, isto é, $FL - GH \in I(V)$.

Definição 3.12.2 *Fixados uma variedade afim $V \subset A^n(K)$ e um ponto $P \in V$, seja $\mathcal{O}_P(V) = \{\alpha \in K(V); \alpha \text{ está bem definida em } P\}$. Definimos $\mathcal{O}_P(V)$ o* ***conjunto das funções racionais em V tal que P está bem definida****.*

Se $P = (a_1, \cdots, a_n)$, então α está bem definida em P se, e somente se, existem $F,\ G \in K[x_1, \cdots, x_n]$ tais que $\alpha = \frac{\overline{F}}{\overline{G}}$, com $G(P) \neq 0$. A condição $G(P) \neq 0$ equivale a $G \notin I(P) = (x_1 - a_1, \cdots, x_n - a_n)$ um ideal maximal de $K[x_1, \cdots, x_n]$, logo, também é um ideal primo.

Portanto, $\alpha \in \mathcal{O}_P \Leftrightarrow \alpha = \frac{\overline{F}}{\overline{G}}$, com $\overline{F} \in \Gamma(V)$ e $\overline{G} \in \Gamma(V) \setminus \overline{I(P)}$.

Veja que $P \in V$ implica que $I(P) \supset I(V)$. Logo, $\frac{I(P)}{I(V)} = \overline{I(P)}$ é um ideal primo de $\Gamma(V) = \frac{K[x_1, \cdots, x_n]}{I(V)}$. Aqui estamos usando o fato de que se $\pi : R \to \frac{R}{I}$ é homomorfismo de anéis, então os ideais de $\frac{R}{I}$ são da forma $\frac{J}{I}$ onde J é ideal de R contendo I. Além disso, $\frac{J}{I}$ é primo, se, e somente se, J é primo.

Assim, $\mathcal{O}_P$ é a localização tal que $\mathcal{O}_P(V) = \Gamma(V)_{\overline{I(P)}}$.

Vimos que, se Q é ideal primo do anel R, então a localização R_Q é um anel local, com um único ideal maximal $Q_{R_Q} = \{\frac{a}{b};\ a,\ b \in R,\ a \in Q,\ b \notin Q\}$.

Temos que R Notheriano implica que R_Q é Noetheriano, então temos que $\mathcal{O}_P(V)$ é um anel Noetheriano local, com ideal maximal:

$$\begin{aligned} M_P(V) &= \overline{I(P)}\Gamma(V)_{\overline{I(P)}} \\ &= \left\{\frac{\overline{F}}{\overline{G}};\ F(P) = 0,\ G(P) \neq 0\right\}. \end{aligned}$$

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

Proposição 3.12.3 *Seja $T : A^n \to A^n$ uma mudança de coordenadas afim tal que $T(P) = Q$. Então $\widetilde{T} : \mathcal{O}_Q(A^n) \to \mathcal{O}_P(A^n)$ é um isomorfismo e $\widetilde{T}$ induz um isomorfismo de $\mathcal{O}_Q(V)$ para $\mathcal{O}_P(V^T)$ se $P \in V^T$, onde V é uma subvariedade de A^n.*

Prova: Temos que $\widetilde{T}$ é um homomorfismo. Seja agora $f \in \mathscr{O}_Q(A^n)$ tal que $\widetilde{T}(f) = 0$. Então, se $f = \frac{\overline{F}}{\overline{G}}$, com $G(Q) \neq 0$, temos que $0 = \widetilde{T}(f) = \frac{\overline{F \circ T}}{\overline{G \circ T}}$, onde $F \circ T = 0$. Assim, $F = F \circ T \circ T^{-1} = 0$ e $f = 0$. Segue que $\widetilde{T}$ é injetora.

Seja, agora, $g \in \mathscr{O}_P(A^n)$, digamos $g = \frac{\overline{T}}{\overline{G}}$, com $G(P) \neq 0$. Então, $g = \widetilde{F}(f)$ onde $f = \frac{\overline{F \circ T^{-1}}}{\overline{G \circ T^{-1}}}$, e $\widetilde{T}$ é sobrejetiva. De fato, veja que $(G \circ T^{-1}(Q)) = G(P) \neq 0$, de modo que tem-se realmente que $f \in \mathscr{O}_Q(A^n)$.

Agora, seja V uma subvariedade afim de A^n e $P \in V$. Repetindo o processo acima, concluímos que $\widetilde{T}_{|\mathscr{O}_Q(T(V))} : \mathscr{O}_Q(T(V)) \to \mathscr{O}_P(V)$ é um isomorfismo, onde $Q = T(P)$.

Proposição 3.12.4 *Seja $P = (0, \cdots, 0) \in A^n$, $\mathscr{O} = \mathscr{O}_P(A^n)$, $M = M_P(A^n)$, onde $M = M_P(A^n)$ é o conjunto das não unidades de $\mathscr{O}_P(A^n)$. Se $I \subset K[x_1, \cdots, x_n]$ é um ideal gerado por $x_1, \cdots, x_n$. Então $I\mathscr{O} = M$ e $I^r\mathscr{O} = M^r$ para todo r.*

Prova: Sejam $\frac{\overline{G_1}}{\overline{H_1}}, \cdots, \frac{\overline{G_k}}{\overline{H_k}} \in \mathscr{O}$ e $F_1, \cdots, F_k \in I$. Então,

$$\sum_{i=1}^{k} \frac{\overline{F_i G_i}}{\overline{H_i}} = \sum_{i=1}^{k} \overline{F_i} \frac{\overline{G_i}}{\overline{H_i}} = 0,$$

desde que $F_i(P) = 0$. Logo, $I\mathscr{O} \subseteq M$.

Agora, se $\frac{\overline{F}}{\overline{G}} \in M$, então $F(P) = 0$, o que implica que, $F \in I$. Assim, $\frac{\overline{F}}{\overline{G}} = \overline{F}\frac{1}{\overline{G}} \in I\mathscr{O}$.

Para o que falta, temos que $I^r\mathscr{O} = (I\mathscr{O})^r$, donde $I^r\mathscr{O} = (I\mathscr{O})^r = M^r$.

Proposição 3.12.5 *Seja V uma variedade em A^n, $I = I(V) \subset K[x_1, \cdots, x_n]$, $P \in V$, J um ideal de $K[x_1, \cdots, x_n]$ que contém I e J' a imagem de J em $\Gamma(V)$. Então, existe um homomorfismo natural ϕ de $\frac{\mathscr{O}_P(A^n)}{J\mathscr{O}_P(A^n)}$ para $\frac{V}{J'\mathscr{O}_P(V)}$ e ϕ é um isomorfismo. Em particular, $\frac{\mathscr{O}_P(A^n)}{I\mathscr{O}_P(A^n)}$ é isomorfo a $\mathscr{O}_P(V)$.*

Prova: Seja $\phi : \frac{\mathscr{O}_P(A^n)}{J\mathscr{O}_P(A^n)} \to \frac{\mathscr{O}_P(V)}{J'\mathscr{O}_P(V)}$ do seguinte modo: dados $F,\ G \in \Gamma(A^n) = K[x_1, \cdots, x_n]$, com $G(P) \neq 0$, defina:

$$\phi\left(\frac{F}{G} + J\mathscr{O}_P(A^n)\right) = \frac{\overline{F}}{\overline{G}} + J'\mathscr{O}_P(V),$$

onde $\overline{F}$ e $\overline{G}$ denotam as imagens de F e G em $\Gamma = \frac{K[x_1, \cdots, x_n]}{I(V)}$.

Se ϕ estiver bem definida, será claramente um homomorfismo sobrejetor de aneis.

Vamos para a prova de que ϕ está bem definida: se $\frac{F}{G} \in J\mathscr{O}_P(A^n)$, então existem $F_1 \in J,\ G_1 \in \Gamma(A^n)$ tais que $G_1(P) \neq 0$ e $\frac{F}{G} = \frac{F_1}{G_1}$. Logo, $\frac{\overline{F}}{\overline{G}} = \frac{\overline{F_1}}{\overline{G_1}} \in J'\mathscr{O}_P(V)$.

ϕ é injetiva: sejam $F,\ G \in \Gamma(A^n)$, com $G(P) \neq 0$ tais que $\frac{\overline{F}}{\overline{G}} \in J'\mathscr{O}_P(V)$. Então, existem $F_1 \in J,\ G_1 \in \Gamma(A^n)$, com $G_1(P) \neq 0$ tais que $\frac{\overline{F}}{\overline{G}} = \frac{\overline{F_1}}{\overline{G_1}}$, de modo que $FG_1 - F_1G \in I(V) = I \subset J$. Portanto, $\frac{F}{G} = \frac{F_1}{G_1} + \frac{1}{GG_1}(FG_1 - F_1G)$ pertence a $J\mathscr{O}_P(A^n)$.

Segue do que fizemos acima que ϕ é um isomorfismo. Em particular, se $J = I$, então $J' = (0)$ e

$$\frac{\mathscr{O}_P(A^n)}{I\mathscr{O}_P(A^n)} \simeq \frac{\mathscr{O}_P(V)}{(0)} \simeq \mathscr{O}_P(V).$$

Proposição 3.12.6 *Seja $I = (x,\ y) \subset K[x,\ y]$. Então $dim_k(\frac{K[x,\ y]}{I^n}) = 1+2+\cdots+n = \frac{n(n+1)}{2}$.*

Prova: Temos que $\frac{K[x,\ y]}{I^n}$ é gerado pelos resíduos dos monômios x^iy^j, com $i+j<n$ e estes são linearmente independentes sobre K. Como há $k+1$ monômios com $i+j=k$, segue que $dim_k(\frac{K[x,\ y]}{I^n}) = \sum_{k=0}^{n-1}(k+1) = \binom{n+1}{2} = 1+2+\cdots+n = \frac{n(n+1)}{2}$.

3.13 Formas

Seja R um domínio. Se $F \in R[x_1,\cdots,x_{n+1}]$ é uma forma, definimos F_* sendo $F_* = F(x_1,\cdots,\ x_n,\ 1)$. Por outro lado, para qualquer polinômio $f \in R[x_1,\cdots,x_n]$ de grau d, escrevemos $f = f_0+f_1+\cdots+f_d$, onde f é uma forma de grau i e definimos $f^* \in R[x_1,\cdots,x_{n+1}]$ sendo

$$f^* \ = \ x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + f_d \ = \ x_{n+1}^d \left(\frac{x_1}{x_{n+1}},\cdots,\frac{x_n}{x_{n+1}}\right),$$

tal que f^* é uma forma de grau d.

Proposição 3.13.1 *Se $F \in K[x,\ y]$ é uma forma, K algebricamente fechado, então F é o produto de fatores lineares.*

Prova: Seja $F = Y^rG$, onde Y não divide G. Então, temos que $F_* = G_* = \varepsilon\prod(X-\lambda_i)$ já que temos que K é algebricamente fechado, então $F = \varepsilon Y^r\prod(X-\lambda_i)$.

3.14 Ideais com um número finito de zeros

Proposição 3.14.1 *Seja I um ideal em $K[x_1,\cdots,x_n]$ e suponha que $V(I) = \{P_1,\cdots,P_n\}$ é finito. Seja $\mathscr{O}_i = \mathscr{O}_{P_i}(A^n)$. Então existe um isormofismo natural de $\frac{K[x_1,\cdots,x_n]}{I}$ em $\prod_{i=1}^{n}\frac{\mathscr{O}_i}{I\mathscr{O}_i}$.*

Prova: Seja $I_i = I(\{P_i\}) \subset K[x_1, \cdots, x_n]$ ideais maximais distintos que contém I. Seja $R = \frac{K[x_1,\cdots,x_n]}{I}$ e $R_i = \frac{\mathscr{O}_i}{I\mathscr{O}}$. O homomorfismo natural $\mathscr{O}_i$ de R para R_i induz um homorfismo ϕ de R para $\prod_{i=1}^{n} R_i$.

Por Nullstellensatz, $\sqrt{I} = I(\{P_1, \cdots, P_n\}) = \bigcap_{i=1}^{n} I_i$. Logo, $((\bigcap_{i=1}^{n} I_i)^d \subset I$ para algum d.

Como $\bigcap_{j\neq i}^{n} I_j$ e I_i são comaximais, segue $\cap I_j^d = (I_1 \cdots I_n)^d = (\cap I_j)^d \subset I$.

Agora, escolha $F_i \in K[x_1, \cdots, x_n]$ tal que $F_i(P_j) = 0$ se $i \neq j$ e $F_i(P_i) = 1$.

Seja $E_i = 1 - (1 - F_i^d)^d$. Note que $E_i = F_i^d D_i$ para algum D_i, então $E_i \in I_j^d$ se $i \neq j$ e $1 - \sum_i E_i = (1 - E_j) - \sum_{i\neq j} E_i \in \bigcap I_j^d \subset I$.

Em adição, $E_i - E_i^2 = E_i(1 - F_i)^d$ e $\bigcap_{j\neq i} I_j^d \cdot I_i^d \subset I$. Se e_i é o resíduo de E_i em R, temos $e_i^2 = e_i,\ e_i e_j = 0$ se $i \neq j$ e $\sum e_i = 1$.

Afirmação: Se $G \in K[x_1, \cdots,\ x_n]$ e $G(P_i) \neq 0$, então existe $t \in R$ tal que $tg = e_i$, onde g é um I-resíduo de G.

Assuma a afirmação por um momento e vamos concluir que ϕ é um isomorfismo:

1. ϕ é injetiva: Se $\phi(f) = 0$, então para cada i existe um G_i com $G_i(P_i) \neq 0$ e $G_i F \in I$, onde f é I-resídulo de F. Seja $t_i g_i = e_i$. Então $f = \sum e_i f = \sum t_i g_i f = 0$.
2. ϕ é sobrejetiva: Como $E_i(P_i) = 1$, então $\phi_i(e_i)$ é uma unidade em R_i, desde que $\phi_i(e_i)\phi_i(e_j)\phi_i(e_i e_j) = 0$. Se $i \neq j,$ então $\phi_i(e_i) = 0$. Portanto, $\phi_i(e_i) = \phi_i(\sum e_j) = \phi_i(1) = 1$. Agora, suponha que $z = \left(\frac{a_1}{s_1}, \cdots, \frac{a_n}{s_n}\right) \in \prod R_i$. Pela afirmação, encontramos t_i tal que $t_i s_i = e_i$. Então $\frac{a_i}{s_i} = a_i t_i$ em R_i. Logo, $\phi_i(\sum t_j a_j e_j) = \phi_i(t_i a_i) = \frac{a_i}{s_i}$ e $\phi_i(\sum t_j a_j e_j) = z$.

Prova da afirmação: Assuma que $G_(P_i) = 1$. Seja $H = 1 - G$. Segue que $(1-H)(E_i + HE_i + \cdots + H^{d-1}E_i = E_i - H^d E_i$. Então $H \in I_i$ e $H^d E_i \in I$. Portanto, $g(e_i + he_i + \cdots + h^{d-1}e_i) = e_i$, como desejado.

Proposição 3.14.2 *Se $V(I) = \{P\}$, então $\frac{K[x_1,\cdots,\ x_n]}{I}$ é isomorfo a $\frac{\mathscr{O}_P(A^n)}{I\mathscr{O}_P(A^n)}$*

Prova: Como $V(I) = \{P\}$ é finito, então pelo Teorema 3.14.1 temos o isomorfismo desejado.

3.15 Pontos Múltiplos e retas tangentes

Já sabemos que as curvas planas afim correspondem a polinômios não constantes $F \in K[x,y]$ sem múltiplos fatores, onde F é determinado pela multiplicação por uma constante

não nula. Será útil permitir que F tenha múltiplos fatores, por exemplo, vamos fazer distinção entre as curvas "$X = 0$" e "$X^2 = 0$". Para isso vamos introduzir a seguinte definição:

Definição 3.15.1 *Sejam $F, G \in K[x,y]$ polinômios. Dizemos que F é equivalente a G se, e somente se, $F = \lambda G$ para algum $\lambda \in K$ não nulo.*

Proposição 3.15.1 *A relação definida em 3.15.1 é uma relação de equivalência.*

Prova: De fato, F é equivalente a F, pois $F = 1 \cdot F$ e tome $\lambda = 1$.

Seja F equivalente G, então

$$F = \lambda G \Leftrightarrow G = \tfrac{1}{\lambda} F,$$

pois λ é um elemento de um corpo K não nulo. Assim, G é equivalente a F.

Agora, seja F equivalente a G e G equivalente a H. Então

$$F = \lambda G \text{ e } G = \lambda' H.$$

Logo,

$$F = \lambda G = \lambda \lambda' H.$$

Portanto, F é equivalente a H.

Definição 3.15.2 *Definimos uma **curva plana afim** como sendo uma classe de equivalência de polinômios constantes não nulos com a relação de equivalência definida em 3.15.1.*

Definição 3.15.3 *O **grau de uma curva** é o grau do polinômio que define a curva e não muda com o representante. Curvas de grau 1 são retas do tipo "$ax + by + c$", onde $a \neq 0,\ b \neq 0$. Se $F = \prod F_i^{e_i}$, onde F_i são fatores irredutíveis de F, então dizemos que F_i são componentes de F e e_i é a multiplicidade da componente F_i. Dizemos que F_i é uma compontente simples se $e_i = 1$ e uma componente múltipla caso contrário.*

Se F é irredutível, $V(F)$ é uma variedade em A^2. Usualmente escrevemos $\Gamma(F)$, $K(F)$ e $\mathcal{O}_P(F)$ ao invéns de $\Gamma(V(F)), K(V(F))$ e $\mathcal{O}_P(V(F))$.

Definição 3.15.4 *Seja F uma curva, $P=(a,\ b)\in F$. O ponto P é chamado* ***simples*** *de F se a derivada $F_X(P)\neq 0$ ou $F_Y(P)\neq 0$. Nesse caso, a reta $F_X(P)(x-a)+F_Y(y-a)=0$ é chamada* ***reta tangente para*** *F* ***em*** *P. Um ponto que não é simples é chamado* ***múltiplo*** *ou* ***singular****. Uma curva onde todos seus pontos são simples é chamada de* ***curva não singular****.*

Definição 3.15.5 *Seja F uma curva qualquer e $P=(0,\ 0)$. Escrevemos $F=F_m+F_{m+1}+\cdots+F_n$, onde F_i é uma forma em $K[x,\ y]$ de grau i, com $F_m\neq 0$. Definimos M sendo a* ***multiplicidade*** *de F em $P=(0,\ 0)$ e escrevemos $M=M_P(F)$. Note que $P\in F$ se, e somente se, $M_P(F)>0$ e que P é um ponto simples em F se, e somente se, $M_P(F)=1$, e que nesse caso, F_1 é exatamente a reta tangente para F em P. Se $M=2$, o ponto P é chamado de* ***ponto duplo****. Se $M=3$, o ponto P é chamado de* ***ponto triplo****, etc.*

Como F_m é uma forma em duas variáveis, podemos escrever $F_m=\prod L_i^{r_i}$, onde L_i são retas distintas, isso segue da Proposição em 3.13.1. Temos que L_i são chamadas de ***retas tangentes*** *para F em $P=(0,\ 0)$ e r_i é a* ***multiplicidade da reta tangente****. A reta L_i é* ***simples*** *se $r_i=1$. Se F possui m retas tangentes distintas em P, dizemos que P é um* ***ponto ordinário*** *de F. Um ponto ordinário duplo é chamado de* ***nó****. Por conveniência, chamamos a reta que passa através de P uma* ***reta tangente de multiplicidade zero*** *se não é tangente para F em P.*

Seja $F=\prod F_i^{e_i}$ uma fatorização em F em componentes irredutíveis. Então $M_P(F)=\sum e_i M_P(F_i)$; e se L é uma reta tangente para F_i com multiplicidade r_i, então L é tangente a F com multiplicidade $\sum e_i r_i$.

Em particular, um ponto P é um ponto simples se, e somente se, P pertence unicamente a uma componente F_i de F, F_i é uma componente simples de F, e P é um ponto simples de F_i.

A extensão dessas definições ao ponto $P=(a,\ b)\neq(0,\ 0)$: seja T uma translação de $(0,\ 0)$ para P, isto é, $T(x,\ y)=(x+a,\ y+b)$. Então, $F^T=F(x+a,\ y+b)$. Defina $m_P(F)$ sendo $M_{(0,0)}(F^T)$, isto é, escreva $F^T=G_m+G_{m+1}+\cdots$, onde G_i são formas, $G_m\neq 0$ e seja $M=M_P(F)$. Se $G_m=\prod L_i r_i$, $L_i=\alpha_i x+\beta_i y$, a reta $\alpha_i(x-a)+\beta_i(y-a)$ são definidas como sendo ***retas tangentes*** *de F para P e r_i sendo a* ***multiplicidade*** *da reta tangente. Note que T leva os pontos de F^T para os pontos de F e as retas tangentes para F^T em $(0,\ 0)$ para as retas tangentes para F em P. Como $F_X(P)=F_X^T(0,\ 0)$ e $F_Y(P)=F_X^T(0,\ 0)$, então P é um ponto simples em F se, e somente se, $M_P(F)=1$, portanto as duas definições de reta tangente em um ponto simples coincidem.*

4 RESULTADOS

4.1 Anéis de Valorização Discreta

Teorema 4.1.1 *Seja R um domínio local Noetheriano com corpo de frações K e o único ideal maximal $M \neq 0$. (Assim, R não é um corpo). As seguintes condições são equivalentes:*

1. *R é um anel de valorização discreta;*
2. *R é um domínio de ideais principais;*
3. *M é um ideal principal;*
4. *R é integralmente fechado e todo ideal primo não nulo é maximal;*
5. *Todo ideal não nulo é uma potência de M;*
6. *A dimensão de $\frac{M}{M^2}$ como espaço vetorial sobre $\frac{R}{M}$ é 1.*

Prova: $(1) \Rightarrow (2)$

Suponha que R é um anel de valorização discreta, ou seja, v é uma valorização discreta de K e $R = \{a \in K;\ v(a) \geq 0\}$. Então $M = \{a \in K;\ v(a) \geq 1\}$ é seu ideal maximal.

Pela Proposição 2.9.2, temos que M é um ideal principal, t gera M e pela Proposição 2.9.4, todo ideal não nulo I de R é da forma M^n. Logo, R é domínio de ideais principais.

$(2) \Rightarrow (4)$

Temos que todo domínio de ideais principais é integralmente fechado e também domínio de fatoração única. Assim, todo ideal primo não nulo é maximal.

$(4) \Rightarrow (3)$

Seja t um elemento não nulo de M. Por hipótese, M é o único ideal primo não nulo, então o radical de (t) que é a interseção de todos os ideais primos contendo t, coincide com M. Pela Proposição 2.9.7, para algum $n \geq 1$ temos $M^n \subseteq (t) \subseteq M$. Assuma que $(t) \subset M$, caso contrário estaria terminado. Assim, para algum $n \geq 2$, temos que $M^n \subseteq (t)$ mas $M^{n-1} \not\subseteq (t)$. Escolha $a \in M^{n-1}$ com $a \notin (t)$ e seja $\beta = \frac{t}{a} \in K$. Se $\beta^{-1} = \frac{a}{t} \in R$, então $a \in R_t = (t)$, o que é uma contradição pela escolha de a. Portanto, $\beta^{-1} \notin R$. Como R é integralmente fechado, β^{-1} não é inteiro sobre R. Mas então $\beta^{-1}M \not\subseteq M$. Se tivessemos $\beta^{-1}M \subseteq M$, então β^{-1} estabiliza um R-módulo finitamente gerado e pela implicação de $(4) \Rightarrow (1)$ no Teorema 2.6.1 temos que β^{-1} é um inteiro sobre R, o que é uma contradição.

Agora, $\beta^{-1}M \subseteq R$, pois

$$\beta^{-1}M = \left(\tfrac{a}{t}\right) \subseteq \left(\tfrac{1}{t}\right) M^n \subseteq R.$$

Note que $a \in M^n$ e $M^n \subseteq (t)$. Assim, $\beta^{-1}M$ é um ideal de R, e se for próprio, está contido em M, contradizendo $\beta^{-1}M \not\subseteq M$. Consequentemente, $\beta^{-1}M = R$ e M é um ideal principal (β).

$(3) \Rightarrow (2)$

Por hipótese, M é um ideal principal (t) e $\bigcap_{n=0}^{\infty} M^n = 0$.

Suponha que a pertence a M^n para todo n, com $a = b_n t^n$ para algum $b_n \in R$. Então $b_n t^n = b_{n+1} t^{n+1}$, logo $b_n = b_{n+1} t$. Assim, $(b_n) \subseteq (b_{n+1})$ para todo n e de fato $(b_n) = (b^{n+1})$ para n suficientemente grande pois R é Noetheriano. Portanto, $b_n = b_{n+1} t = ctb_n$ para algum $c \in R$, então $(1-ct)b_n = 0$. Mas $t \in M$, então t não é uma unidade, consequentemente, $ct \neq 1$. Assim, $b_n = 0$, ou seja, $a = b_n t^n = 0$. Portanto, $\bigcap_{n=0}^{\infty} M^n = 0$.

Agora, seja I um ideal não nulo qualquer de R. Então $I \subseteq M$. Mas como $\bigcap_{n=0}^{\infty} M^n = 0$, então $I \not\subseteq \bigcap_{n=0}^{\infty} M^n$. Assim, existe $n \geq 0$ tal que $I \subseteq M^n$ e $I \not\subseteq M^{n+1}$. Escolha $a \in I \setminus M^{n+1}$. Como $M^n = (t)^n = (t^n)$, temos que $a = ut^n$ com $u \notin M$, pois $a \notin M^{n+1}$. Mas então u é unidade, logo $t^n = u^{-1}a \in I$. Portanto, $I \subseteq M^n = (t^n) \subseteq I$. Logo, I é principal.

$(2) \Rightarrow (1)$

Por hipótese, M é um ideal principal (t) e pela prova de $(3) \Rightarrow (2)$ temos $\bigcap_{n=0}^{\infty} M^n = 0$. Seja a um elemento não nulo qualquer de R. Então, $(a) \subseteq M$ e como $\bigcap_{n=0}^{\infty} M^n = 0$, queremos que $a \in (t^n)$. Mas $a \notin (t^{n+1})$ para algum n. Assim, $a = ut^n$, com $u \notin M$. Em outras palavaras, u é uma unidade. Para a fixado, u e n são únicos (pois t, um elemento de M, não é uma unidade). Seque que se β é um elemento não nulo de um corpo de frações K, então $\beta = ut^n$ unicamente determinado, sendo u uma unidade de R e m um inteiro, possivelmente negativo. Então definimos $v(\beta) = m$, então m é uma valorização discreta em K com anel de valorização R.

$(1) \Rightarrow (5)$

Segue imediatamente da Proposição 2.9.4.

$(5) \Rightarrow (3)$

Segue da prova da Proposição 2.9.4 que $M \neq M^2$ (pela unicidade de n em M^n). Escolha $t \in M \setminus M^2$. Por hipótese, $(t) = M^n$, para algum $n \geq 0$. Logo, não podemos ter $n = 0$ já que $(t) \subseteq M \subset R$, e não podemos ter para $n \geq 2$ pela escolha de t. Portanto, a única possibilidade é $n = 1$. Assim, $M = (t)$.

$(1) \Rightarrow (6)$ Como R é um anel de valorização, por hipótese, segue pela prova da Proposição 2.9.5 que $dim\left(\frac{M}{M^2}\right)$ é 1, olhando $\frac{M}{M^2}$ como espaço vetorial sobre $\frac{R}{M}$.

$(6) \Rightarrow (3)$

Por hipótese, $M \neq M^2$. Seja $t \in M \setminus M^2$. Mas $t + M^2$ é um gerador do espaço vetorial $\frac{M}{M^2}$ sobre o corpo $\frac{R}{M}$. Assim, $\frac{R(t+M^2)}{M^2} = \frac{M}{M^2}$. Pelo Teorema de Correspondência, temos $t + M^2 = M$. Agora, $M\left(\frac{M}{(t)}\right) = \frac{M^2+(t)}{(t)} = \frac{M}{(t)}$, então pelo Lema de Nakayama em 2.2.1, temos $\frac{M}{(t)} = 0$, isto é, $M = (t)$.

Agora vamos excluir a valorização trivial $v(a) = 0$ para todo $a \neq 0$.

Corolário 4.1.1 *O anel R é um anel de valorização discreta se, e somente se, R é um anel local, domínio de ideais principais que não é um corpo.*

Prova: Seja R um anel de valorização discreta. Temos que R é domínio de ideais principais por $(1) \Rightarrow (2)$ no Teorema 4.1.1. Nesta implicação não é usado que R é Noetheriano no Teorema 4.1.1. Além disso, pela propriedade 3 da Seção 2.9.1, R é um anel local. Se R é um corpo, então todo elemento não nulo $a \in R$ é uma unidade, logo $v(a) = 0$. Assim, a valorização v é a trivial, contradizendo a convenção anterior.

A recíproca do corolário segue diretamente da implicação $(1) \Rightarrow (2)$ do Teorema 4.1.1.

4.2 Multiplicidades e Anéis Locais

Seja F uma curva plana irredutível e $P \in F$. Nessa seção vamos relacionar multiplicidade com anel local, ou seja, vamos encontrar a multiplicidade de P em F em termos no anel local $\mathcal{O}_P(F)$.

Usaremos a notação: para um polinômio qualquer $G \in K[X, Y]$ denotamos a imagem (resíduo) em $\Gamma(F) = \frac{K[X, Y]}{(F)}$ por g.

Teorema 4.2.1 *P é um ponto simples de F se, e somente se, $\mathcal{O}_P(F)$ é anel de valorização discreta. Nesse caso, se $L = aX + bY + c$ é uma reta qualquer que passa por P que não é tangente a F em P, então a imagem l de L em $\mathcal{O}_P(F)$ é o uniformizador para $\mathcal{O}_P(F)$.*

Prova: Suponha que P é um ponto simples em F e L uma reta que passa por P, que não é tangente a F em P. Seja M a reta tangente de F em P.

Afirmação 1: Por mundanças de coordenadas, podemos assumir que $P = (0, 0)$ e Y é uma reta tangente a F em P e que $L = X$.

De fato, pela Proposição 3.11.1, como temos L e M duas retas distintas que passam por P, então existe uma mudança de coordenadas T tal que $T(P) = (0,\ 0)$, $T(M) = Y$, isto é, Y é a reta tangente a F em P e $T(L) = X$.

Afirmação 2: Com a mudança de coordendas $P = (0,\ 0)$ ainda é um ponto simples.

Como F é uma curva irredutível, então F^T também é uma curva irredutível já que é a composisão de F com T. Pela Proposição 3.12.3 temos que : $\widetilde{T} : \mathscr{O}_{(0,\ 0)}(A^2) \to \mathscr{O}_P(A^2)$ é um isomorfimo e que $\widetilde{T}$ induz um isomorfismo nos anéis locais $\mathscr{O}_{(0,\ 0)}(F)$ para $\mathscr{O}_P(F^T)$ já que $(0,0) \in F^T$.

Afirmação 3: É suficiente mostrar que $M_P(F)$ é gerado por x.

Se $\mathscr{O}_P(F)$ satisfizer o Teorema 4.1.1 então pela Proposição 2.9.3 qualquer elemento de $M(F)$ pode ser escrito como ux^n, onde u é unidade de $\mathscr{O}_P(F)$, com $n \in \mathbb{Z}$.

Note que $M_P(F) = (x,\ y)$, onde P pode ser ou não simples.

De fato, pela Proposição 3.12.4 temos que $I\mathscr{O}_P(A^2) = M_P(F)$ e pela Proposição 3.12.5 temos que $\frac{\mathscr{O}_P(A^2)}{I\mathscr{O}_P(A^2)}$ é isomorfo a $\mathscr{O}_P(F)$.

Agora com as suposições acima, temos $F = Y+$ termos de graus altos. Agrupando esses termos com Y, podemos escrever $F = YG - X^2H$, onde $G = 1+$ termos de graus altos e $H \in K[X]$.

Então, módulo F temos o seguinte $yg = x^2h \in \Gamma(F)$, logo, $y = x^2hy^{-1} \in (x)$, pois g é unidade em $\mathscr{O}_P(F)$ já que $g(P) \neq 0$. Assim, $M_P(F) = (x,\ y) = (x)$, como desejado.

Portanto, pelo Teorema 4.1.1, temos que $\mathscr{O}_P F$ é um anel de valorização discreta.

A recíproca segue do seguinte teorema:

Teorema 4.2.2 *Seja P um ponto em uma curva irredutível F. Então para n suficientemente grande, temos*

$$M_P(F) = dim_K \left(\frac{M_P(F)^n}{M_P(F)^{n+1}} \right).$$

Em particular, a multiplicidade de F em P depende unicamente do anel local $\mathscr{O}_P(F)$.

Prova: Escreva $\mathscr{O}$, M ao invés de $\mathscr{O}_P(F)$, $M_P(F)$, respectivamente. Pelo item 5 dos casos particulares fundamentais de (2.4) temos a seguinte sequência exata:

$$0 \longrightarrow \frac{M}{M^{n+1}} \longrightarrow \frac{\mathscr{O}}{M^{n+1}} \longrightarrow \frac{\mathscr{O}}{M^n} \longrightarrow 0$$

Tome $I = M^n$, $J = M^{n+1}$ e $R = \mathscr{O}$ no item 5 de (2.4) da Seção 2.7.

Pela Proposição 2.7.1 temos que

$$dim_K\left(\frac{\mathscr{O}}{M^{n+1}}\right) = dim_K\left(\frac{M^n}{M^{n+1}}\right) + dim_K\left(\frac{\mathscr{O}}{M^n}\right).$$

Afirmação 1: $dim_K\left(\frac{\mathscr{O}}{M^n}\right) = n \cdot m_P(F) + s$, onde s é uma constante e todo $n \geq M_P(F)$.

Já vimos que podemos assumir $P = (0,\ 0)$, então pela Proposição 3.12.4 temos $M^n = I^n\mathscr{O}$, onde $I = (X,\ Y) \subset K[X,\ Y]$. Como $V(I^n) = \{P\}$, então pelas Proposições 3.14.2 e 3.12.5 temos que:

$$\frac{K[X,\ Y]}{(I^n,\ F)} \cong \frac{\mathscr{O}_P(A^2)}{(I^n,\ F)\mathscr{O}_P(A^2)} \cong \frac{\mathscr{O}_P(F)}{I^n\mathscr{O}_P(F)} = \frac{\mathscr{O}}{M^n}.$$

Agora, fomos reduzidos ao cálculo da dimensão de $\frac{K[X,\ Y]}{(I^n,\ F)}$. Seja $M = M_P(F)$. Então $FG \in I^n$, desde que $G \in I^{n-m}$. Temos que existe um homomorfismo ϕ natural de anéis de $\frac{K[X,\ Y]}{I^n}$ para $\frac{K[X,\ Y]}{(I^n,\ F)}$ e uma aplicação ψ K-linear de $\frac{K[X,\ Y]}{I^{n-m}}$ para $\frac{K[X,\ Y]}{I^n}$ definida por $\psi(\overline{G}) = \overline{FG}$.

Afirmação 2: A seguencia é exata:

$$0 \longrightarrow \frac{K[X,\ Y]}{I^{n-m}} \xrightarrow{\psi} \frac{K[X,\ Y]}{I^n} \xrightarrow{\phi} \frac{K[X,\ Y]}{(I^n,\ F)} \longrightarrow 0$$

De fato, temos que:

1. ψ é injetiva

   Suponha que $\overline{FG} = 0$. Como I^n são os polinômios que quando expressos em termo de formas então a forma de menor grau é pelo menos n. Assim, o polinômio FG quando expresso como forma tem grau pelo menos n. Logo, $\overline{G} = 0$.

2. ϕ é sobrejetiva

   Nesse caso, como $I^n \subset (I^n,\ F)$ e a aplicação ϕ leva classes em resíduos em classes de resíduos, a aplicação ϕ é sobrejetiva por construção.

3. $Ker(\phi) = Im(\psi)$.

   Seja $\overline{G} \in Im(\psi)$. Logo, $\overline{G} = \overline{FG} = 0$ em $\frac{K[X,\ Y]}{(I^n,\ F)}$. Assim, $\phi(\overline{G}) = 0$ e $\overline{G} \in Ker(\phi)$. Logo, $Im(\psi) \subset Ker(\phi)$.

   Reciprocamente, seja $\overline{G} \in Ker(\phi)$ então $G \in (I^n,\ F)$. Logo G quando é expresso em formas a forma de menor grau tem pelo menos grau n. Digamos que: $G = AF +$ forma de grau n. Assim, temos $\overline{G} = \overline{AF} \in Im(\psi)$. Daí, $Ker(\phi) \subset Im(\psi)$.

   Portanto, podemos aplicar novamente as Proposições 2.7.1 e 3.12.6:

$$\begin{aligned} dim_K\left(\frac{K[X,Y]}{(I^n,\ F)}\right) &= dim_K\left(\frac{K[X,\ Y]}{I^n}\right) - dim_K\left(\frac{K[X,\ Y]}{I^{n-m}}\right) = \\ &= \frac{n(n+1)}{2} - \left(\frac{(m-n)(m-n+1)}{2}\right) \\ &= mn - \frac{m(m-1)}{2}, \end{aligned}$$

para todo $n \geq m$, como desejado. Tome $s = \frac{m(m-1)}{2}$.

Para finalizar o Teorema 4.2.1 temos que pela prova da Proposição 2.9.5 e como $\mathcal{O}_P(F)$ é um anel de valorização,

$$M_P(F) = dim_K \left(\frac{M_P(F)^n}{M_P(F)^{n+1}} \right) = 1.$$

Portanto, P é um ponto simples.

5 CONCLUSÃO

A construção deste trabalho nos permitiu entender alguns conceitos clássicos a partir de anéis de valorização, com ênfase em anéis de valorização discreta. Além disso, nos permitiu concluir que podemos estudar propriedades geométricas a partir do ponto de vista algébrico.

Uma extensão dos anéis de valorização discreta são os estudos dos domínios de Dedekind. De fato, temos o teorema que caracteriza os domínios de Dedekind:

Teorema 5.0.1 *Seja A um domínio Noetheriano de dimensão* 1. *As propriedades são equivalentes:*

1. *A é integralmente fechado;*
2. *Todo ideal primário é a potência de algum primo;*
3. *Todo anel local A_P é um anel de valorização discreta.*

Além disso, outras aplicações são demonstrar que os anéis $\mathbb{Z}_p$ de inteiros p-ádicos e as séries de potências formais $R = K[[T]]$ em uma variável T sobre o corpo K são anéis de valorização discreta. Para mais detalhes consulte (ATIYAH, 2018).

REFERÊNCIAS

ASH, R. B. **A course in commutative algebra**. [*S. l.*]: Department of Mathematics, University of Illiois at Urbana-Champaign, 2003.

ATIYAH, M. **Introduction to commutative algebra**. [*S. l.*]: CRC Press, 2018.

FULTON, W. **Algebraic curves**: an introduction to algebraic geometry. [*S. l.*]: Addison-Wesley, 2008.

LANG, S. **Algebra**. [*S. l.*]: Springer, 2002. Graduate Texts in Mathematics.

TENGAN, E.; BORGES, H. M. F. **Álgebra comutativa em quatro movimentos**. [*S. l.*: *s. n.*], 2015.