Universidade Federal do ABC

Centro de Matemática, Computação e Cognição - CMCC

Trabalho de Conclusão de Curso

Geometria Algébrica: Uma Introdução ao Estudo de Curvas e Variedades

por

Henrique Matsuoka Medeiros

Orientador: Prof. Dr. Nazar Arakelian

Santo André - SP

2021

Resumo

Com origens no estudo dos zeros de polinômios em multiplas variáveis, a geometria algébrica é uma área muito rica e vasta que conversa com diversas outras áreas da matemática como álgebra comutativa, topologia e até, em seus aspectos mais modernos, teoria de categorias e feixes. Propomos uma introdução à geometria algébrica através do estudo de curvas algébricas, visando criar uma base da teoria clássica mas com perspectivas para o estudo da teoria moderna, abordando propriedades de curvas afins e projetivas bem como um estudo geral sobre variedades afins e projetivas.

Sumário

Introdução

A geometria algébrica é uma área ampla que para além das suas aplicações se estende pela história. É possível ver desde a antiguidade como o desenvolvimento da geometria e da álgebra preparou o caminho aos estudos de variedades algébricas. Como exemplo na Grécia, a solução de Menaechmus para o problema de dobrar o cubo (também conhecido como Problema Deliano), os trabalhos de Arquimedes e Apollonius em seções conicas e os matemáticos do Oriente Médio, como Omar Khayyam, matemático persa que desenvolveu um método para resolução de equações cúbicas intersectando uma parábola com um círculo e o matemático iraniano Sharaf al-Din al-Tusi com seu trabalho "Tratado Sobre Equações"que é descrito como a inauguração do começo da geometria algébrica.

Com o passar dos séculos a geometria algébrica foi evoluindo, sofrendo mudanças e adquirindo tópicos. Desde o século XVI com a introdução da geometria coordenada e o estudo das curvas algébricas, seguido pelo início dos estudos da geometria projetiva, o estudo das transformações birracionais e a classificação de superfícies algébricas pela escola italiana de geometria algébrica, a introdução das Superfícies Riemmanianas, a formalização por meio da álgebra comutativa e por fim no século XX a refundação moderna através da teoria de feixes e esquemas.

A parte de toda essa linha evolutiva, classicamente a geometria algébrica tem como principal objeto de estudo as variedades algébricas, que são manifestações geométricas de soluções de sistemas de equações polinomiais. Alguns exemplos das classes mais estudadas de variedades algébricas são curvas algébricas planas, que incluem retas, círculos, parábolas, elipses, hipérboles, curvas cúbicas como curvas elípticas e curvas quárticas como lemniscatas e ovais de Cassini. Algumas questões mais imediatas envolvem o estudo de certos pontos da variedade, como pontos singulares, pontos de inflexão e pontos no infinito, enquanto algumas questões mais complexas envolvem a topologia de uma curva e relações entre curvas definidas por equações diferentes.

Para além de uma área matemática em si mesma, a geometria algébrica conversa com a topologia, geometria complexa e teoria dos números, sendo uma ferramenta muito útil para a demonstração de resultados muito importantes, vide como exemplo a prova do Último Teorema de Fermat que teve como base diversos resultados de geometria aritmética. Além da matemática, também há aplicações em diversas outras áreas como estatística, códigos corretores de erros, robóticas e entre outras.

Propomos nesse Trabalho de Conclusão de Curso um estudo sobre variedades algébricas e curvas algébricas, tendo uma abordagem clássica mas com perspectivas para o estudo da teoria moderna. Consideraremos resultados sobre curvas algébricas afins e projetivas, bem como variedades afins e projetivas no geral, abordando toda parte de álgebra comutativa necessária para o estudo de tais tópicos.

A principal referência utilizada será [1], seguindo sua estrutura de tópicos. Como bibliografia auxiliar para eventuais resultados de álgebra comutativa, será utilizado [2]. No Apêndice 6.2, se encontram os resultados de [1] utilizados no corpo principal do Trabalho bem como demonstrações para a maior parte deles.

Capítulo 1

Preliminares Algébricas

Este capítulo tem como objetivo estabelecer os conceitos e definições de álgebra comutativa que virão a ser utilizados ao longo do trabalho.

Durante todo o texto, ao se referir à um *anel*, estaremos sempre considerando um anel associativo, comutativo e com identidade multiplicativa. Além disso, um *homomorfismo* de anéis deve levar a identidade multiplicativa do primeiro anel na do segundo.

Definição 1.1. *Um anel R é um* ***domínio integral*** *se não possui divisores de zero, isto é*

$$xy = 0 \implies x = 0 \text{ ou } y = 0$$

para todos $x, y \in R$.

Definição 1.2. *Um* ***corpo*** *L é um anel em que todo elemento não nulo é uma unidade (isto é, possui inverso multiplicativo).*

Associado com todo domínio integral R, temos os seu corpo de quocientes K, que é um corpo contendo R como subanel, e todo elemento de K pode ser escrito (não de forma única necessariamente) como uma fração de dois elementos de K.

Para qualquer anel R, denotamos por $R[X]$ o anel de polinômios na variável X com coeficientes em X. O grau de um polinômio não nulo $\sum a_i X^i$ é o maior inteiro d tal que $a_d \neq 0$, o polinômio é dito mônico se $a_d = 1$.

O anel de polinômios em n variáveis e coeficentes em R é denotado por $R[X_1, \ldots, X_n]$. Escreveremos $R[X, Y]$ e $R[X, Y, Z]$ quando $n = 2$ ou $n = 3$. Os monômios em $R[X, Y, Z]$ são os polinômios $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, onde os i_j são inteiros não negativos, e o grau do monômio será $i_1 + \cdots + i_n$. Todo $F \in R[X, Y, Z]$ tem uma expressão única da forma $F = \sum a_{(i)} X^{(i)}$,

onde $X^{(i)}$ são monômios e $a_{(i)} \in R$. F é dito homogêneo ou uma forma de grau d se todos os coeficientes $a_{(i)}$ são zero exceto nos monômios de grau d. Todo polinômio F tem uma expressão única $F = F_0 + F_1 + \cdots + F_d$, onde F_i é uma forma de grau i, e o grau do polinômio é o maior i tal que $F_i \neq 0$. Temos também que R será um subanel de $R[X_1, \ldots, X_n]$ e $R[X_1, \ldots, X_n]$ é canônicamente isomorfo à $R[X_1, \ldots, X_{n-1}][X_n]$.

Definição 1.3. *Um elemento $a \in R$ é dito **irredutível** se não é zero e nem uma unidade e para qualquer fatorização $a = bc$, $b, c \in R$, b ou c é uma unidade. Um domínio integral no qual todos os elementos não nulos podem ser fatorados unicamente (a menos de multiplicação por unidade) num produto de irredutíveis é chamado de **domínio de fatoração única**, abreviado para **DFU**.*

Se R é um DFU com corpo de frações K, então todo elemento irredutível $F \in R[X]$ permanece irredutível quando considerado em $K[X]$. Disso segue que polinômios $F, G \in R[X]$ sem fatores em comum em $R[X]$ não possuem fatores em comum em $K[X]$.

Se R é DFU então $R[X]$ também é DFU. Assim por indução $k[X_1, \ldots, X_n]$ é DFU para qualquer corpo k. O corpo de frações de $k[X_1, \ldots, X_n]$ é denotado por $k(X_1, \ldots, X_n)$ e chamado de corpo de funções racionais em n variáveis sobre k.

Definição 1.4. *Um conjunto S de elementos de um anel R gera um ideal $I = \{\sum a_i s_i |\ s_i \in S,\ a_i \in R\}$. Um ideal I é finitamente gerado se é gerado por um conjunto finito $S = \{f_1, \ldots, f_n\}$, escrevemos então $I = (f_1, \ldots, f_n)$. Um ideal gerado por um único elemento é chamado de ideal principal, e um domínio em que todos seus ideais são principais é dito um **domínio de ideais principais**, abreviado para **DIP**.*

Temos que dado k um corpo, e portanto um DIP, temos que $k[X]$ será um DIP.

Definição 1.5. *Um corpo k é **algebricamente fechado** se qualquer polinômio não constante $F \in k[X]$ possui uma raíz em k.*

Segue da Definição 1.5 que $F = \mu \prod (X - \lambda_i)^{e_i}, \mu, \lambda_i \in k$, onde os λ_i são as raízes distintas de F e e_i a multiplicidade de λ_i. Um polinômio de grau d possui d raízes em k, contando as mutliplicidades.

Definição 1.6. *Seja R um anel. A **derivada** de um polinômio $F = \sum a_i X^i \in R[X]$ é definida como $\sum i a_i X^{i-1}$ e é descrito como $\dfrac{\partial F}{\partial X}$ ou F_X. Se $F \in R[X_1, \ldots, X_n]$, $\dfrac{\partial F}{\partial X_i} = F_{X_i}$ é definida considerando F como um polinômio em X_i e coeficientes em $R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.*

Capítulo 2

Conjuntos Algébricos Afins

2.1 Espaço Afim e Conjuntos Algébricos

Seja k um corpo qualquer. Por $\mathbb{A}^n(k)$ ou simplesmente $\mathbb{A}^n$, denotaremos o produto cartesiano de k consigo mesmo n vezes. $\mathbb{A}^n(k)$ é chamado de **espaço afim** n-dimensional sobre k e seus elementos serão chamados de **pontos**. Em particular, $\mathbb{A}^1(k)$ é a reta afim e $\mathbb{A}^2(k)$ o plano afim. Se $F \in k[X_1, \ldots, X_n]$, um ponto $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ é chamado de um zero de F se $F(P) = 0$. Se F é não constante, o conjunto dos zeros de F é chamado de hipersuperfície definida por F é denotado por $V(F)$. Uma hipersuperfície em $\mathbb{A}^2(k)$ é chamada um curva plana afim. Se F é um polinômio de grau um, $V(F)$ é chamado de hiperplano em $\mathbb{A}^n(k)$; se $n = 2$ é uma reta. A Figura 2.1 ilustra alguns exemplos do conjunto de zeros de alguns polinômios quando $k = \mathbb{R}$.

De modo mais geral, se S é um conjunto qualquer de polinômios em $k[X_1, \ldots, X_n]$, denotaremos $V(S) = \{P \in \mathbb{A}^n(k) | F(P) = 0 \text{ para todo } F \in S\}$: $V(S) = \bigcap_{F \in S} V(F)$. Se $S = \{F_1, \ldots, F_r\}$, escreveremos $V(F_1, \ldots, F_r)$ ao invés de $V(\{F_1, \ldots, F_r\})$. Um subconjunto $X \subset \mathbb{A}^n(k)$ é um **conjunto algébrico afim**, ou simplesmente um **conjunto algébrico**, se $X = V(S)$ para algum $S \subset k[X_1, \ldots, X_n]$.

Proposição 2.1. *Algumas propriedades sobre conjuntos algébricos são*

(i) Se I é um ideal de $k[X_1, \ldots, X_n]$ gerado por S, então $V(I) = V(S)$; assim todo conjunto algébrico é igual a $V(I)$ para algum ideal I.

(ii) Se $\{I_\alpha\}$ é uma coleção qualquer de ideais, então $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$; então a intersecção de qualquer coleção de conjuntos algébricos é um conjunto algébrico.

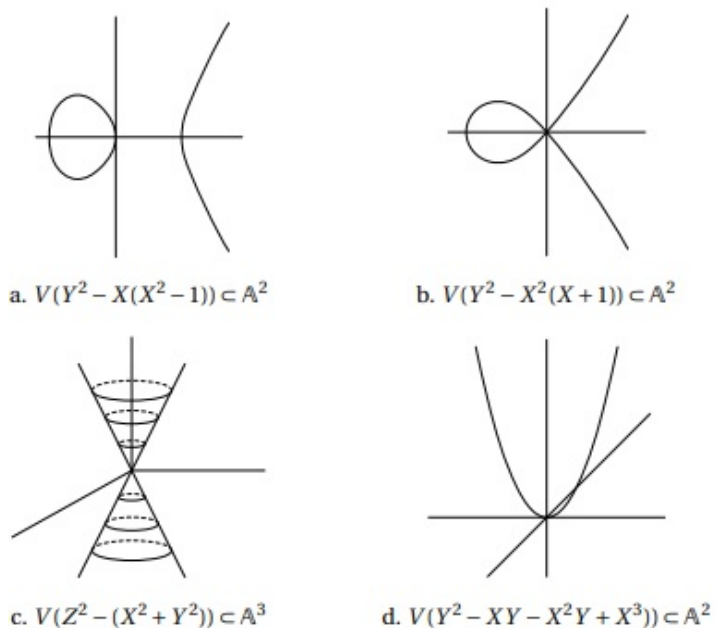

Figura 2.1: Exemplos de Zeros de Polinômios em $\mathbb{R}$ [1].

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

(iv) *$V(FG) = V(F) \cup V(G)$ para quaisquer polinômios F, G; $V(I) \cup V(J) = V(\{FG |\ F \in I, G \in J\})$; então qualquer união finita de conjuntos algébricos é um conjunto algébrico.*

(v) *$V(0) = \mathbb{A}^n(k)$; $V(1) = \emptyset$; $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$ para $a_i \in k$. Então qualquer conjunto finito de $\mathbb{A}^n(k)$ é um conjunto algébrico.*

Demonstração. **(i)** Dado $P \in V(S)$, temos que $F(P) = 0$ para todo $F \in S$.Agora dado $G \in I$ qualquer, como I é gerado por S, então todo polinômio de I é uma soma finita de polinômios de S com coeficientes em k. Logo $G = \sum_{i=0}^{n} a_i F_i$ com $a_i \in k$ e $F_i \in S$ para todo i. Então $G(P) = \sum_{i=0}^{n} a_i F_i(P) = 0$. Portanto $P \in V(I)$ e $V(S) \subset V(I)$. Agora dado $P \in V(I)$, temos que $F(P) = 0$ para todo $F \in I$ e como I é gerado por S, $S \subset I$ e assim $G(P) = 0$ para todo $G \in S$. Logo $P \in V(S)$ e concluindo temos $V(S) = V(I)$.

(ii) Dado $P \in V(\bigcup_\alpha I_\alpha)$ então P é um zero de todo polinômio em $\bigcup_\alpha I_\alpha$, em particular, será um zero de cada ideal I_α. Assim $P \in V(I_\alpha)$ para todo α e $P \in \bigcap_\alpha (I_\alpha)$. Agora dado $Q \in \bigcap_\alpha V(I_\alpha)$ então Q é um zero de todo polinômio em I_α para todo α, assim é um zero para todo polinômio em $\bigcup_\alpha I_\alpha$ e $Q \in V(\bigcup_\alpha I_\alpha)$.

(iii) Dado $P \in V(J)$, então $F(P) = 0$ para todo $F \in J$, em particular para todo $F \in I$. Logo $P \in V(I)$.

(iv) Dado $P \in V(FG)$, então $FG(P) = F(P)G(P) = 0$, logo $F(P) = 0$ ou $G(P) = 0$, o que implica que $P \in V(F)$ ou $P \in V(G)$ e assim $P \in V(F) \cup V(G)$. Agora dado $P \in V(F) \cup V(G)$, então $P \in V(F)$ ou $P \in V(G)$ e assim $FG(P) = F(P)G(P) = 0$, logo $P \in V(FG)$. Mais geralmente temos que se I e J são ideais de $k[X_1, \ldots, X_n]$ então $V(IJ) = V(\{FG |\ F \in I, G \in J\}) = V(I) \cup V(J)$ pois se $P \in V(I) \cup V(J)$, então $P \in V(I)$ ou $P \in V(J)$ e assim $FG(P) = 0$ para todo $F \in I$ e $G \in J$, logo $P \in V(IJ)$. E se $P \in V(IJ)$ necessariamente temos que $P \in V(I)$ ou $P \in V(J)$ pois caso contrário existem $H \in I$ e $B \in J$ tal que $H(P) \neq 0$ e $B(P) \neq 0$, logo $HB(P) \neq 0$ e como $HB \in IJ$, então $P \notin V(IJ)$.

(v) Como qualquer ponto P em $\mathbb{A}^n(k)$ é tal que $0(P) = 0$, então $V(0) = \mathbb{A}^n(k)$. De forma semelhante, todo ponto $P \in \mathbb{A}^n(k)$ é tal que $1(P) = 1 \neq 0$ e assim $V(1) = \emptyset$. Por fim $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$ dado que $(a_1, \ldots, a_n)$ claramente é um zero de $X_i - a_i$ para todo $i = 1, \ldots, n$ e se $P \in V(X_1 - a_1, \ldots, X_n - a_n)$ então cada coordenada i de P deve ser necessariamente igual a a_i e temos que $P = (a_1, \ldots, a_n)$.

□

2.2 O Ideal de um Conjunto de Pontos

Para qualquer subconjunto $X \subset \mathbb{A}^n(k)$, o conjunto dos polinômios que zeram em X formam um ideal de $k[X_1, \ldots, X_n]$. Isto é fácil de verificar, pois dados dois polinômios F, G tais que $F(P) = 0$ e $G(P) = 0$ e um polinômio qualquer $H \in k[X_1, \ldots, X_n]$

(i) $(F + G)(P) = F(P) + F(G) = 0$, para todo $P \in X$;

(ii) $(FG)(P) = F(P)G(P) = 0$, para todo $P \in X$;

(iii) $(HF)(P) = H(P)F(P) = H(P) \cdot 0 = 0$, para todo $P \in X$.

Esse ideal é chamado de **ideal de X** e é denotado por $I(X) = \{F \in k[X_1 \ldots, X_n] \mid F(P) = 0,\ \forall P \in X\}$.

Proposição 2.2. *As seguintes propriedades descrevem a relação entre ideais e conjuntos algébricos:*

(i) *Se $X \subset Y$, então $I(X) \supset I(Y)$;*

(ii) $I(\emptyset) = k[X_1, \ldots, X_n]$;

(iii) $I(\mathbb{A}^n(k)) = (0)$ *se k é um corpo infinito;*

(iv) $I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$ *para $a_1, \ldots, a_n \in k$;*

(v) $I(V(S)) \supset S$ *para qualquer conjunto de polinômios S; $V(I(X)) \supset X$ para qualquer conjunto de pontos X;*

(vi) $V(I(V(S))) = V(S)$ *para qualquer conjunto S de polinômios e $I(V(I(X))) = I(X)$ para qualquer conjunto X de pontos. Então se U é um conjunto algébrico $U = V(I(U))$ e se J é um ideal de um conjunto algébrico $J = I(V(J))$*

Demonstração. **(i)** Um elemento de $I(Y)$ será um polinômio $F \in k[X_1, \ldots, X_n]$ tal que $F(P) = 0$ para todo $P \in Y$. Mas se $F(P) = 0$ para todo $P \in Y$, então $F(A) = 0$ para todo $A \in X$, pois $X \subset Y$. Então $F \in I(X)$.

(ii) $I(\emptyset)$ é o conjunto

$$\{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots, a_n) \in \emptyset\}$$

e por vacuidade, todo $F \in k[X_1, \ldots, X_n]$ satisfaz a propriedade. Assim $I(\emptyset) = k[X_1, \ldots, X_n]$.

(iii) $I(\mathbb{A}^n(k))$ é o conjunto

$$\{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0,\ \forall a_1, \ldots, a_n \in k\}$$

e pela Proposição 6.2, se $F \in I(\mathbb{A}^n(k))$, então $F = 0$.

(iv) $I(\{(a_1, \ldots, a_n)\}) = \{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0\}$. Pela Proposição 6.6 (b), se $F \in I(\{(a_1, \ldots, a_n)\})$, então $F = \sum_{i=1}^{n} (X_i - a_i)G_i$, assim $F \in (X_1 - a_1, \ldots, X_n - a_n)$. Um elemento $G \in (X_1 - a_1, \ldots, X_n - a_n)$ é da forma $G = \sum_{i=1}^{n} (X_i - a_i)H_i$, com $H_i \in k[X_1, \ldots, X_n]$ para todo i, assim $G(a_1, \ldots, a_n) = 0$, então $G \in I(\{(a_1, \ldots, a_n)\})$.

(v) Dado $F \in S$, temos que $\forall P \in V(S)$, $F(P) = 0$ e então $F \in I(V(S))$; dado $P \in X$, $\forall F \in I(X)$, $F(P) = 0$ e então $P \in V(I(X))$.

(vi) Pela propriedade anterior $V(I(V(S))) \supset V(S)$ e como $S \subset I(V(S))$ então $V(S) \supset V(I(V(S)))$. Analogamente, pela propriedade anterior $I(X) \subset I(V(I(X)))$ e como $X \subset V(I(X))$ então $I(X) \supset I(V(I(X)))$. □

Definição 2.1. *Se I é um ideal de um anel R, definimos o* ***radical*** *de I, descrito como $Rad(I)$, por*

$$Rad(I) = \{a \in R \mid a^n \in I \text{ para algum inteiro } n > 0\}$$

Lema 2.1. *Dado I um ideal de um anel R, então $Rad(I)$ também é um ideal.*

Demonstração. (i) Dado $a \in Rad(I)$ e $c \in R$, então $ac \in Rad(I)$, pois $a^n \in I$ para n inteiro positivo, então $(ac)^n = a^n c^n \in I$.

(ii) Dados $a, b \in Rad(I)$, com $a^n \in I$ e $b^m \in I$ para inteiros positivos n, m. Então $(a+b)^{n+m} \in I$, pois expandindo $(a+b)^{n+m}$, pela expansão binomial, cada termo será da forma $a^c b^d$ com $c + d = n + m$, então caso $c < n$, temos que $d > m$ e $a^c b^d = a^c b^{d-m} b^m \in I$ e caso $d < m$ temos que $c > n$ e $a^c b^d = a^n a^{c-n} b^d \in I$. Logo todo termo de $(a+b)^{n+m}$ pertence a I e $(a+b)^{n+m} \in I$. Isso implica que dados $a, b \in Rad(I)$ então $a + b \in Rad(I)$.

□

Definição 2.2. *Um ideal I de R é dito um* ***ideal radical*** *se $I = Rad(I)$.*

Proposição 2.3. *Dado um ideal I de um anel R e X um conjunto de pontos em $\mathbb{A}^n(k)$*

(i) $Rad(I)$ é um ideal radical;

(ii) $I(X)$ é um ideal radical;

(iii) Todo ideal primo é radical.

Demonstração. **(i)** Dado um elemento $a \in Rad(Rad(I))$, temos $a^n \in Rad(I)$ para algum inteiro positivo n. Como $a^n \in Rad(I)$, então $(a^n)^m \in I$ para algum inteiro positivo m. Logo $a^{nm} \in I$ e $a \in Rad(I)$. A inclusão $Rad(I) \subset Rad(Rad(I))$ é trivial.

(ii) Dado um elemento $F \in Rad(I(X))$, temos que para algum n inteiro positivo $F^n \in I(X)$, assim $F^n(P) = 0$ para todo $P \in X$. Mas $F^n(P) = \underbrace{F(P)F(P)\cdots F(P)}_{n \text{ vezes}} = 0$, então

$F(P) = 0$ pois todo corpo é um domínio integral. Assim $F \in I(X)$. A inclusão $I(X) \subset Rad(I(X))$ é trivial.

(iii) Seja P um ideal primo de um anel R e $a \in Rad(P)$. Logo $a^n \in P$ para algum n inteiro positivo. Mas como P é primo, então $a^n = a^{n-1}a$, implica que $a \in P$ ou a^{n-1} e repetindo o processo indutivamente para a^{n-1} temos que $a \in P$. A inclusão reciproca é trivial.

□

Proposição 2.4. *Dado um ideal I em $k[X_1, \ldots, X_n]$, $V(I) = V(Rad(I))$ e $Rad(I) \subset I(V(I))$.*

Demonstração. Temos que $I \subset Rad(I)$, logo $V(Rad(I)) \subset V(I)$. Reciprocamente, dado $P \in V(I)$, temos que $F(P) = 0$ para todo $F \in I$. Dado $G \in Rad(I)$ arbitrário, então $G^n \in I$ para algum inteiro positivo n. Então $G^n(P) = 0$, e assim, $G(P) \cdots G(P) = 0$ e como k é um corpo (logo, domínio integral), então $G(P) = 0$. Assim $P \in V(Rad(I))$.

Temos que $V(I) = V(Rad(I))$, logo $I(V(I)) = I(V(Rad(I)))$. Como $Rad(I) \subset I(V(Rad(I)))$ por definição, então $Rad(I) \subset I(V(I))$.

□

Proposição 2.5. *Dados $a_1, \ldots, a_n \in k$, o ideal $I = (X_1 - a_1, \ldots, X_n - a_n) \subset k[X_1, \ldots, X_n]$ é maximal e o homomorfismo natural de k para $k[X_1, \ldots, X_n]/I$ é um isomorfismo.*

Demonstração. Seja $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ e $I_a = (X_1 - a_1, \ldots, X_n - a_n)$. Considere o homomorfismo de evaluação $e_a : k[X_1, \ldots, X_n] \to k$, que leva $F \in k[X_1, \ldots, X_n]$ em $F(a)$.Temos que e_a é sobrejetor, pois para cada $b \in k$, $e_a(b) = b$. Então, pelo Teorema do Isomorfismo, $k[X_1, \ldots, X_n]/Ker\ e_a \cong k$ e $Ker\ e_a$ é um ideal maximal de $k[X_1, \ldots, X_n]$. Mostraremos que $I_a = Ker\ e_a$.

$I_a \subset Ker\ e_a$ trivialmente, pois se $F = \sum_{i=1}^n G_i(X_i - a_i)$ com $G_i \in k[X_1, \ldots, X_n]$, então $F(a) = 0$. Agora dado $F \in Ker\ e_a$, então $F(a) = 0$ e pela Proposição 6.6 (b), $F = \sum_{i=1}^n G_i(X_i - a_i)$, com $G_i \in k[X_1, \ldots, X_n]$ e $F \in I_a$. Portanto, $I_a = Ker\ e_a$.

O homomorfismo natural $\pi|_k : k \to k[X_1, \ldots, X_n]/I_a$ que leva $b \in k$ para $b + I_a$ será injetivo, pois se $\pi|_k(b) = 0$, então $b \in I_a$, mas I_a é ideal maximal, logo é ideal próprio, e $b = 0$ necessariamente. Agora dado $F \in k[X_1, \ldots, X_n]$, pela Proposição 6.6 (a), podemos escrever $F = \sum_i \lambda_i (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$ e assim $F + I_a = \sum_i \lambda_i (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n} + I_a$

e todos os termos $(X_j - a_j)^{i_j}$ com $i_j > 0$ serão iguais a 0 em $k[X_1, \ldots, X_n]/I_a$ e somente os termos constantes de F serão não triviais. Logo $F + I_a = b + I_a$ para algum $b \in k$ e $\pi|_k(b) = b + I_a = F + I_a$, e $\pi|_k$ será sobrejetor. Portanto $\pi|_k$ é um isomorfismo.

□

2.3 Teorema da Base de Hilbert

Definição 2.3. *Um anel R é dito* ***Noetheriano*** *se todo ideal em R é finitamente gerado.*

Como exemplos de anéis Noetherianos, temos os corpos (que só possuem os ideais gerados por 1 e 0) e os DIP's (como os inteiros). Um importante teorema envolvendo anéis Noetherianos é o Teorema de Base de Hilbert.

Teorema 2.1. ***(Teorema da Base de Hilbert)*** *Se R é um anel Noetheriano, então $R[X_1, \ldots, X_n]$ é também um anel Noetheriano.*

Demonstração. Como $R[X_1, \ldots, X_n]$ é isomorfo à $R[X_1, \ldots, X_{n-1}][X_n]$, o teorema seguirá por indução provando que $R[X]$ é Noetheriano se R for. Seja I um ideal de $R[X]$. Devemos encontrar um conjunto finito de geradores de I.

Se $F = a_0 + a_1X + \cdots + a_dX^d \in R[X]$, $a_d \neq 0$, chamamos a_d de coeficiente líder de F. Seja J o conjunto dos coeficientes líderes de todos polinômios em I. É fácil verificar que J é um ideal em R, então existem polinômios $F_1, \ldots, F_r \in I$ cujos coeficientes líderes geram J. Tome um inteiro N maior que o grau de cada F_i. Para cada $m \leq N$, seja J_m o ideal em R consistindo dos coeficientes líderes de todos os polinômios $F \in I$ tal que $deg(F) \leq m$. Seja $\{F_{mj}\}$ um conjunto finito de polinômios em I com grau $\leq m$ cujos coeficientes líderes geram J_m. Seja I' o ideal gerado pelos F_i's e todos os F_{mj}'s. É suficiente mostrar que $I = I'$.

Suponha que I' seja menor que I. Seja G o elemento de I de menor grau que não está em I'. Se $deg(G) > N$, podemos encontrar polinômios Q_i tais que $\sum Q_iF_i$ e G possuam o mesmo coeficiente líder. Mas assim $deg(G - \sum Q_iF_i) < deg(G)$, e então $G - \sum Q_iF_i \in I'$ e $G \in I'$. Similarmente, se $deg(G) = m \leq N$, podemos diminuir o grau subtraindo $\sum Q_jF_{mj}$ para algum Q_j, logo $deg(G - \sum Q_jF_{mj}) < deg(G)$ e $G - \sum Q_jF_{mj} \in I'$ o que implica que $G \in I'$.

□

Como consequência do Teorema da Base de Hilbert, temos que $k[X_1, \ldots, X_n]$ é um anel Noetheriano.

Apesar de termos permitido que um conjunto algébrico seja definido por um conjunto arbitrário de polinômios, na verdade um número finito de polinômios sempre será o bastante para definir qualquer conjunto algébrico.

Teorema 2.2. *Todo conjunto algébrico é uma interseção de um número finito de hipersuperfícies.*

Demonstração. Seja U um conjunto algébrico de $\mathbb{A}^n$. Então $U = V(I)$ para algum ideal I de $k[X_1, \ldots, X_n]$. Mas $k[X_1, \ldots, X_n]$ é um anel Noetheriano pelo Teorema da Base de Hilbert, então $I = (F_1, \ldots, F_r)$ e $U = V(F_1, \ldots, F_r) = V(F_1) \cap \cdots \cap V(F_r)$. □

2.4 Componentes Irredutíveis de um Conjunto Algébrico

Definição 2.4. *Um conjunto algébrico $V \subset \mathbb{A}^n(k)$ é **redutível** se $V = V_1 \cup V_2$, com V_1 e V_2 conjuntos algébricos em $\mathbb{A}^n(k)$, e $V_i \neq V$, $i = 1, 2$. Caso contrário, V é **irredutível**.*

Proposição 2.6. *Um conjunto algébrico V é irredutível se, e somente se, $I(V)$ é primo.*

Demonstração. Se $I(V)$ não é primo, suponha $F_1F_2 \in I(V)$, $F_i \notin I(V)$, $i = 1, 2$. Então $V = (V \cap V(F_1)) \cup (V \cap V(F_2)$, e $V \cap V(F_i) \subsetneq V$, então V é redutível.

Reciprocamente, se $V = V_1 \cup V_2$, $V_i \subsetneq V$, então $I(V_i) \supsetneq I(V)$. Seja $F_i \in I(V_i)$, $F_i \notin V$, então $F_1F_2 \in I(V)$ e $I(V)$ não é primo. □

Queremos mostrar que um conjunto algébrico é a união de um número finito de conjuntos algébricos irredutíveis. Se V é redutível, escrevemos $V = V_1 \cup V_2$, se V_2 é redutível, escrevemos $V_2 = V_3 \cup V_4$ e assim por diante. É preciso saber que esse processo acaba em algum momento.

Lema 2.2. *Seja $\mathfrak{I}$ uma coleção não vazia de ideais em um anel Noetheriano R. Então $\mathfrak{I}$ possui um membro maximal, isto é, existe um ideal I em $\mathfrak{I}$ que não está contido em nenhum outro ideal de $\mathfrak{I}$.*

Demonstração. Escolha (utilizando o Axioma da Escolha) um ideal de cada subconjunto de $\mathfrak{I}$. Seja I_0 o ideal escolhido para o próprio conjunto $\mathfrak{I}$. Seja $\mathfrak{I}_1 = \{I \in \mathfrak{I} \mid I \supsetneq I_0\}$ e I_1 o ideal escolhido de $\mathfrak{I}_1$. Seja $\mathfrak{I}_2 = \{I \in \mathfrak{I} \mid I \supsetneq I_1\}$ e assim por diante. É suficiente mostrar que algum $\mathfrak{I}_n$ é vazio. Se não, então seja $I = \bigcup_{n=0}^{\infty} I_n$, um ideal de R. Sejam $F_1, \ldots, F_r$ os polinômios que geram I, e para n suficientemente grande $F_i \in I_n$ para $i = 1, \ldots, r$. Mas então $I_n = I$ e $I_n = I_{n+1}$, uma contradição. □

Segue imediatamente do Lema 2.2 que qualquer coleção de conjuntos algébricos em $\mathbb{A}^n(k)$ possui um membro minimal. Pois se $\{V_\alpha\}$ é tal coleção, tome um membro maximal $I(V_{\alpha_0})$ de $\{I(V_\alpha)\}$. Então V_{α_0} é um membro minimal da coleção, pois se $I(V_{\alpha_0}) \not\subset I(U)$ para todo $U \in \{V_\alpha\}$, $U \neq V_{\alpha_0}$, então $U \not\subset V_{\alpha_0}$, pelo item (i) da Proposição 2.2.

Teorema 2.3. *Seja V um conjunto algébrico em $\mathbb{A}^n(k)$. Então existem conjuntos algébricos irredutíveis $V_1, \ldots, V_m$ únicos tal que $V = V_1 \cup \cdots \cup V_m$, e $V_i \not\subset V_j$ para $i \neq j$.*

Demonstração. Seja

$$\mathfrak{I} = \{\text{Conjuntos algébricos } V \subset \mathbb{A}^n(k) \mid V \text{ não é uma união finita de conjuntos algébricos irredutíveis}\}.$$

Queremos mostrar que $\mathfrak{I}$ é vazio. Se não, seja V o membro minimal de $\mathfrak{I}$. Como $V \in \mathfrak{I}$, V não é irredutível, então $V = V_1 \cup V_2$, $V_i \subsetneq V$. Pela minimalidade de V, então $V_i \notin \mathfrak{I}$, e assim $V_i = V_{i1} \cup \cdots \cup V_{im_i}$, com V_{ij} irredutível. Mas então $V = \bigcup_{i,j} V_{ij}$, uma contradição.

Então qualquer conjunto algébrico V pode ser escrito $V = V_1 \cup \cdots \cup V_m$, V_i irredutíveis. Para a segunda condição, basta descartar qualquer V_i tal que $V_i \subset V_j$ para $i \neq j$. Para mostrar a unicidade, seja $V = W_1 \cup \cdots \cup W_m$ outra decomposição em conjuntos irredutíveis. Então $V_i = \bigcup_j (W_j \cap V_i)$ e $V_i \subset W_{j(i)}$ para algum $j(i)$, pela irreducibilidade de V_i. Similarmente, $W_{j(i)} \subset V_l$ para algum l. Mas $V_i \subset V_l$ implica que $i = l$, então $V_i = W_{j(i)}$. Da mesma forma, W_j é igual a algum $V_{j(i)}$. □

Os V_i's são chamados de componentes irredutíveis de V e $V = V_1 \cup \cdots \cup V_m$ é a decomposição de V em componentes irredutíveis.

2.5 Subconjuntos Algébricos do Plano

Antes de progredir no desenvolvimento da teoria geral, daremos atenção ao plano afim $\mathbb{A}^2(k)$, encontrando todos seus subconjuntos algébricos. Pelo Teorema 2.3 é suficiente encontrar os conjuntos algébricos irredutíveis.

Proposição 2.7. *Sejam F e G polinômios em $k[X, Y]$ sem fatores em comum. Então $V(F, G) = V(F) \cap V(G)$ é um conjunto finito de pontos.*

Demonstração. F e G não possuem fatores em comum em $k[X, Y]$, então não possuem fatores comuns em $k(X)[Y]$ (onde $k(X)$ é o corpo de frações de $k[X]$). Como $k(X)[Y]$ é um

DIP, $(F,G) = (1) \in k(X)[Y]$, e assim $RF + SG = 1$ para algum $R, S \in k(X)[Y]$. Existe $D \in k[X]$ não nulo tal que $DR = A$, $DS = B$, $A, B \in k[X,Y]$, então $AF + BG = D$. Se $(a,b) \in V(F,G)$, então $D(a) = 0$. Mas D possui somente um número finito de zeros, o que mostra que somente um número finito de X-coordenadas aparece entre os pontos de $V(F,G)$. Dado que o mesmo procedimento se aplica para as Y-coordenadas, só pode existir um número finito de pontos em $V(F,G)$.

□

Corolário 2.1. *Se F é um polinômio irredutível em $k[X,Y]$, tal que $V(F)$ é infinito, então $I(V(F)) = (F)$, e $V(F)$ é irredutível.*

Demonstração. Se $G \in I(V(F))$, então $V(F) \subset V(G)$ e $V(F,G) = V(F) \cap V(G) = V(F)$ que é infinito. Pela contra-positiva da Proposição 2.7, F e G tem fator em comum, mas como F é irredutível, então F divide G, isto é, $G \in (F)$. Temos que $(F) \subset I(V(F))$ trivialmente, então $I(V(F)) = (F)$. Por fim, como (F) é ideal primo, $V(F)$ será irredutível pela Proposição 2.6.

□

Corolário 2.2. *Suponha k infinito. Então os conjuntos algébricos irredutíveis de $\mathbb{A}^2(k)$ são: $\mathbb{A}^2(k)$, $\emptyset$, pontos, e curvas planas irredutíveis $V(F)$, onde F é um polinômio irredutível e $V(F)$ é infinito.*

Demonstração. Seja V um conjunto algébrico irredutível em $\mathbb{A}^2(k)$. Se V é finito ou $I(V) = (0)$, então V é do tipo requerido. Caso contrário, $I(V)$ contém um polinômio não constante F. Como $I(V)$ é primo, então algum fator polinomial irredutível de F pertence a $I(V)$, então podemos assumir que F é irredutível. Afirmamos então que $I(V) = (F)$. Temos que $(F) \subset I(V)$ trivialmente. Se existe $G \in I(V)$, tal que $G \notin (F)$, então F e G não possuem fatores em comum visto que F é irredutível, mas $V \subset V(F)$, $V \subset V(G)$ e então $V \subset V(F,G)$ que é finito pela Proposição 2.7, uma contradição. □

Corolário 2.3. *Assuma k algebricamente fechado, F um polinômio não constante em $k[X,Y]$. Seja $F = F_1^{n_1} \cdots F_r^{n_r}$ a decomposição de F em fatores irredutíveis. Então $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ é a decomposição de $V(F)$ em componentes irredutíveis e $I(V(F)) = (F_1 \cdots F_r)$.*

Demonstração. $V(F) = V(F_1^{n_1}) \cup \cdots \cup V(F_r^{n_r}) = V(F_1) \cup \cdots \cup V(F_r)$ e nenhum F_i divide nenhum F_j para $j \neq i$, então não há relações de inclusão entre os $V(F_i)$.

Para a segunda afirmação, $I(\bigcup_i V(F_i)) = \bigcap_i I(V(F_i)) = \bigcap_i (F_i)$ pelo Corolário 2.2, pois cada $V(F_i)$ será infinito dado que k é algebricamente fechado (Proposição 6.8). Como qualquer polinômio divisível por cada F_i será divisível por $F_1 \cdots F_r$, $\bigcap_i (F_i) = (F_1 \cdots F_r)$. □

2.6 Módulos e Condições de Finitude

Definição 2.5. *Seja R um anel. Um R-módulo é um grupo comutativo M (a operação do grupo é escrita $+$ e sua identidade 0 ou 0_M) junto com uma multiplicação escalar, isto é, um mapa de $R \times M$ para M (denote a imagem de (a, m) por am ou $a \cdot m$) satisfazendo:*

(i) $(a + b)m = am + bm$ *para* $a, b \in R$, $m \in M$;

(ii) $a \cdot (m + n) = am + an$ *para* $a \in R$, $m, n \in M$;

(iii) $(ab) \cdot m = a \cdot (bm)$ *para* $a, b \in R$, $m \in M$;

(iv) $1_R \cdot m = m$ *para* $m \in M$, *onde* 1_R *é a unidade multiplicativa de* R.

Definição 2.6. *Um subgrupo N de um R-módulo M é chamado de submódulo de M se $am \in N$ para todo $a \in R$ e $m \in N$. N então possui uma estrutura R-módulo com as operações restritas a N, e será chamado de um* ***submódulo*** *de M.*

Definição 2.7. *Se S é um conjunto de elementos de um R-módulo M, o submódulo gerado por S é definido como $\{\sum_{i=1}^{n} r_i s_i \mid r_i \in R, s_i \in S\}$. É o menor submódulo de M que contém S. Se $S = \{s_1, \ldots, s_n\}$ é finito, o submódulo gerado por S é denotado por $\sum Rs_i$. O R-módulo M é dito finitamente gerado se $M = \sum Rs_i$ para $s_1, \ldots, s_n \in M$.*

Definição 2.8. *Seja R um subanel de um anel S. Existem vários tipos de condições de finitude para S sobre R, dependendo se considerarmos S como um R-módulo, um anel, ou (possivelmente) um corpo.*

(i) *S é dito módulo-finito sobre R, se S é* ***finitamente gerado*** *como um R-módulo. Se R e S são corpos, e S é módulo-finito sobre R, denotamos a dimensão de S sobre R por $[S : R]$.*

(ii) *Sejam $v_1, \ldots, v_n \in S$. Seja $\phi : R[X_1, \ldots, x_n] \to S$ o homomorfismo de anéis que leva X_i para v_i. A imagem de ϕ é escrita como $R[v_1, \ldots, v_n]$. É o menor subanel de S contendo R e $v_1, \ldots, v_n$. O anel S é* ***anel-finito*** *sobre R se $S = R[v_1, \ldots, v_n]$ para algum conjunto de $v_1, \ldots, v_n \in S$.*

(iii) Suponha que $R = K$, $S = L$ são corpos. Se $v_1, \ldots, v_n \in L$, seja $K(v_1, \ldots, v_n)$ o corpo de frações de $K[v_1, \ldots, v_n]$. Consideramos $K(v_1, \ldots, v_n)$ um subcorpo de L, e é o menor subcorpo que contém K e $v_1, \ldots, v_n$. O corpo L é dito uma ***extensão finitamente gerada*** *de K se $L = K(v_1, \ldots, v_n)$ para algum conjunto de $v_1, \ldots, v_n \in L$.*

2.7 Elementos Integrais

Definição 2.9. *Seja R um subanel de S. Um elemento $v \in S$ é dito* ***integral*** *sobre R se existe um polinômio mônico $F = X^n + a_1X^{n-1} + \cdots + a_n \in R[X]$ tal que $F(v) = 0$. Se R e S são corpos, é dito que v é algébrico sobre R se v é integral sobre R.*

Proposição 2.8. *Seja R um subanel de um domínio S, $v \in S$. Então são equivalentes:*

(i) v é integral sobre R.

(ii) $R[v]$ é módulo-finito sobre R.

(iii) Existe um subanel R' de S contendo $R[v]$ que é módulo-finito sobre R.

Demonstração. $((i) \Rightarrow (ii))$: Se $v^n + a_1v^{n-1} + \cdots + a_n = 0$, então $v^n \in \sum_{i=0}^{n-1} Rv_i$. Segue disso que $v^m \in \sum_{i=0}^{n-1} Rv_i$ para todo m, então $R[v] = \sum_{i=0}^{n-1} Rv_i$.

$((ii) \Rightarrow (iii))$ Tome $R' = R[v]$.

$((iii) \Rightarrow (i))$ Se $R' = \sum_{i=1}^{n} Rw_i$, então $vw_i = \sum_{i=1}^{n} a_{ij}w_j$ para $a_{ij} \in R$. Então $\sum_{j=1}^{n}(\delta_{ij}v - a_{ij})w_j = 0$ para todo i, onde $\delta_{ij} = 0$ se $i \neq j$ e $\delta_{ii} = 1$. Considerando essas equações no corpo de frações de S, vemos que $(w_1, \ldots, w_n)$ é uma solução não trivial do sistema de equações determinado pela matriz $(\delta_{ij}v - a_{ij})$, e assim $det(\delta_{ij}v - a_{ij}) = 0$. Como v só aparece na diagonal da matriz, esse determinante tem a forma $v^n + a_1v^{n-1} + \cdots + a_n$, $a_i \in R$, então v é integral sobre R.

□

Corolário 2.4. *O conjunto de elementos de S que são integrais sobre R é um subanel de S que contém R.*

Demonstração. Se a, b são integrais sobre R, então $R[a]$ e $R[b]$ são módulo-finito pela Proposição 2.8. Como b é integral sobre R, então é integral sobre $R[a] \supset R$. Pela Proposição 2.8

então $R[a, b]$ é módulo finito sobre $R[a]$ e, pela Proposição 6.14 e por $R[a]$ ser módulo-finito sobre R, $R[a, b]$ é módulo-finito sobre R. Como $a \pm b, ab \in R[a, b]$, então serão integrais sobre R pela Proposição 2.8, pois $R[a \pm b]$, $R[ab] \subset R[a, b]$ que é módulo-finito sobre R. □

S é dito integral sobre R se todo elemento de S é integral sobre R. Se R e S são corpos, S é dito uma extensão algébrica sobre R se S é integral sobre R.

Lema 2.3. *Seja R um subanel de S e $a_1, \ldots, a_n \in S$, tal que a_i é integral sobre $R[a_1, \ldots, a_{i-1}]$ para $i = 2, \ldots, n$ (com a_1 integral sobre R). Então $R[a_1, \ldots, a_n]$ é módulo-finito sobre R.*

Demonstração. O caso $n = 1$ é satisfeito pela Proposição 2.8. Para o passo indutivo, seja $a_1, \ldots, a_{n-1}$ como no enunciado e a_n integral sobre $R[a_1, \ldots, a_{n-1}]$. Pela Proposição 2.8, $R[a_1, \ldots, a_{n-1}, a_n]$ é módulo-finito sobre $R[a_1, \ldots, a_{n-1}]$, e pela transitividade da condição de módulo-finito da Proposição 6.14 (a) como $R[a_1, \ldots, a_{n-1}]$ é módulo-finito sobre R, então $R[a_1, \ldots, a_n]$ é módulo-finito sobre R.

□

2.8 Extensões de Corpos

Suponha que K é um subcorpo de um corpo L, e $L = K(v)$ para algum $v \in L$. Seja $\phi : K[X] \to L$ o homomorfismo que leva X a v. Seja $Ker(\phi) = (F)$, $F \in K[X]$ (dado que $K[X]$ é DIP). Então $K[X]/(F)$ é isomorfo à $K[v]$ pelo Teorema do Isomorfismo, e (F) é primo. Dois casos podem ocorrer:

(i) $F = 0$. Então $K[v]$ é isomorfo à $K[X]$, e assim $K(v) = L$ é isomorfo à $K(X)$. Nesse caso L não é anel-finito (ou módulo-finito) sobre K pelo Exemplo 6.2.

(ii) $F \neq 0$. Podemos assumir que F é mônico. Então (F) é primo, logo F é irredutível e (F) é maximal pela Proposição 6.5. Portanto $K[v]$ é um corpo, e $K[v] = K(v)$. Além disso, $F(v) = 0$, pois $Ker(\phi) = (F)$, então v é algébrico sobre K e $L = K[v]$ é módulo-finito sobre K.

Assim a discussão acima mostra que uma extensão anel-finita L de um corpo K é módulo-finita sobre K .

Proposição 2.9. *Se um corpo L é anel-finito sobre um subcorpo K, então L é módulo-finito (e assim, algébrico) sobre K.*

Demonstração. Seja $L = K[v_1, \ldots, v_n]$. Suponha $n = 1$, e seja $\phi : K[X] \to L$ o homomorfismo que leva X a v_1 e $Ker(\phi) = (F)$, $F \in K[X]$ (dado que $K[X]$ é DIP). Pelo Teorema do Isomorfismo $K[X]/(F) \cong K[v_1]$. Mas então (F) não pode ser igual a (0) pois se fosse $K[v_1]$ seria isomorfo a $K[X]$ e $K[v_1] \cong K(v_1) \cong K(X)$ que não é anel finito pelo Exemplo 6.2. Assim $F \neq 0$ e $F(v_1) = 0$, logo v_1 é algébrico sobre K e $L = K[v_1]$ é módulo-finito sobre K pela Proposição 2.8.

Seguiremos por indução, assumindo que o resultado é válido para uma extensão anel-finita gerada por $n-1$ elementos. Seja $K_1 = K(v_1)$. Por indução, $L = K_1[v_2, \ldots, v_n]$ é módulo-finito sobre K_1. Podemos assumir que v_1 não é algébrico sobre K, pois caso contrário a Proposição 6.14 (a) finalizaria a demonstração.

Cada v_i satisfaz uma equação $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots = 0$, $a_{ij} \in K_1$. Tomando $a \in K[v_1]$ que é um múltiplo de todos os denominadores dos a_{ij}, temos equações $(av_i)^{n_i} + aa_{i1}(av_1)^{n-1} + \cdots = 0$. Segue do Corolário 2.4 que para qualquer $z \in L = K[v_1, \ldots, v_n]$ existe um N inteiro positivo tal que $a^N z$ é integral sobre $K[v_1]$. Em particular isso deve valer para $z \in K(v_1)$. Mas como $K(v_1)$ é isomorfo ao corpo de funções racionais em uma variável sobre K, isso é impossível (pela Proposição 6.18). □

2.9 Teorema dos Zeros de Hilbert

Dado um conjunto algébrico V a Proposição 2.6 nos dá um critério para averiguar se V é irredutível ou não. O que nos falta é uma forma de descrever V em termos de um dado conjunto de polinômios que definem V. Isso será feito a partir do Teorema dos Zeros de Hilbert que diz exatamente qual a relação entre ideais e conjuntos algébricos. Começaremos provando uma versão mais fraca do teorema que será utilizada na demonstração do principal.

Lema 2.4. *Se um corpo algebricamente fechado k é subcorpo de um corpo L e existe um homomorfismo de anéis sobrejetivo de $k[X_1, \ldots, X_n]$ para L (que é a identidade restrito a k), então $k = L$.*

Demonstração. L será anel finito sobre k, pois o homomorfismo de $k[X_1, \ldots, X_n]$ para L é sobrejetivo e é uma extensão da inclusão de k em L. Assim existem $v_1, \ldots, v_n \in L$ tal que $L = k[v_1, \ldots, v_n]$. Temos que pela Proposição 2.9, L será módulo-finito sobre k, mas como k é algebricamente fechado, então pela Proposição 6.17, $k = L$. □

Durante toda essa seção assumiremos que k é um corpo algebricamente fechado.

Teorema 2.4. ***(Teorema dos Zeros Fraco)*** *Se I é um ideal próprio de $k[X_1, \ldots, X_n]$, então $V(I) \neq \emptyset$.*

Demonstração. Podemos assumir que I é um maximal ideal, pois existe um ideal maximal J contendo I pelo Corolário 6.6, e $V(J) \subset V(I)$. Então $L = k[X_1, \ldots, X_n]/I$ é um corpo, e k pode ser visto como um subcorpo de L. Como o homomorfismo passagem ao quociente de $k[X_1, \ldots, X_n]$ para L é um homomorfismo de anéis sobrejetivo e é a identidade quando restrito a k, pelo Lema 2.4 $k = L$.

Então para cada X_i, temos um a_i tal que a_i é o resíduo de X_i, isto é, $X_i - a_i \in I$. Mas $(X_1 - a_1, \ldots, X_n - a_n)$ é um ideal maximal de $k[X_1, \ldots, X_n]$ (Proposição 2.5), então $I = (X_1 - a_1, \ldots, X_n - a_n)$ e $V(I) = \{(a_1, \ldots, a_n)\} \neq \emptyset$. □

Teorema 2.5. ***(Teorema dos Zeros de Hilbert)*** *Seja I um ideal em $k[X_1, \ldots, X_n]$. Então $I(V(I)) = Rad(I)$.*

Em termos concretos, o teorema diz o seguinte: se $F_1, \ldots, F_r$ e G pertencem à $k[X_1, \ldots, X_n]$, e G se anula em todos os pontos que $F_1, \ldots, F_r$ se anulam, então existe uma equação $G^N = A_1F_1 + A_2F_2 + \cdots + A_rF_r$, para algum $N > 0$ e alguns $A_i \in k[X_1, \ldots, X_n]$.

Demonstração. Temos que $Rad(I) \subset I(V(I))$ pela Proposição 2.4. Suponha $G \in I(V(F_1, \ldots, F_r))$, $F_i \in k[X_1, \ldots, X_n]$ para todo i. Seja $J = (F_1, \ldots, F_r, X_{n+1}G - 1) \subset k[X_1, \ldots, X_n, X_{n+1}]$. Então $V(J) \subset \mathbb{A}^{n+1}(k)$ é vazio, dado que G se anula em todos os pontos em que os F_i's são zero. Aplicando o Teorema dos Zeros Fraco à J, temos que J não é ideal próprio e assim $1 \in J$, logo existe uma equação $1 = \sum A_i(X_1, \ldots, X_n, X_{n+1})F_i + B(X_1, \ldots, X_n, X_{n+1})(X_{n+1}G - 1)$. Seja $Y = \dfrac{1}{X_{n+1}}$, e multiplique a equação por uma potência de Y grande o suficiente para que resulte $Y^N = \sum C_i(X_1, \ldots, X_n, Y)F_i + D(X_1, \ldots, X_n, Y)(G - Y) \in k[X_1, \ldots, X_n, Y]$. Substituindo G por Y, temos a equação desejada. □

Corolário 2.5. *Se I é um ideal radical em $k[X_1, \ldots, X_n]$, então $I(V(I)) = I$. Assim existe uma correspondência um para um entre ideais radicais e conjuntos algébricos.*

Corolário 2.6. *Se I é um ideal primo, então $V(I)$ é um conjunto algébrico irredutível. Existe uma correspondência um para um entre conjuntos algébricos irredutíveis e ideais primos. Ideais maximais correspondem a pontos.*

Corolário 2.7. *Seja F um polinômio não constante em $k[X_1, \ldots, X_n]$, $F = F_1^{n_1} \cdots F_r^{n_r}$ sua decomposição em fatores irredutíveis. Então $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ é a decomposição*

de $V(F)$ em componentes irredutíveis, e $I(V(F)) = (F_1 \cdots F_r)$. Existe uma correspondência entre polinômios irredutíveis $F \in k[X_1, \ldots, X_n]$ (até multiplicação por um elemento não nulo de k) e hipersuperfícies irredutíveis em $\mathbb{A}^n(k)$.

Os três Corolários 2.5, 2.6 e 2.7 são consequência imediata do Teorema dos Zeros de Hilbert.

Corolário 2.8. *Seja I um ideal em $k[X_1, \ldots, X_n]$. Então $V(I)$ é um conjunto finito se, e somente se, $k[X_1, \ldots, X_n]/I$ é um espaço vetorial sobre k de dimensão finita. Se isso ocorre, então o número de pontos em $V(I)$ é no máximo $dim_k(k[X_1, \ldots, X_n]/I)$.*

Demonstração. Assuma que $k[X_1, \ldots, X_n]/I$ é espaço vetorial sobre k de dimensão finita e sejam $P_1, \ldots, P_r \in V(I)$. Escolha $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ tal que $F_i(P_j) = 0$ se $i \neq j$ e $F_i(P_i) = 1$ (que é possível pela Proposição 6.10 (ii)). Seja $\overline{F}_i$ o I-resíduo de cada F_i. Se $\sum \lambda_i \overline{F}_i = 0$, $\lambda_i \in k$, então $\sum \lambda_i F_i \in I$. Logo $\lambda_j = \sum \lambda_i F_i(P_j) = 0$, para todo j. Assim os $\overline{F}_i$'s são linearmente independentes e $r \leq dim_k(k[X_1])$. Assim $\#V(I) \leq dim_k(k[X_1])$.

Reciprocamente, se $V(I) = \{P_1, \ldots, P_r\}$ é finito, seja $P_i = (a_{i1}, \ldots, a_{in})$, e defina F_j por $F_j = \prod_{i=1}^{r}(X_j - a_{ij})$, $j = 1, \ldots, n$. Então $F_j \in I(V(I)) = Rad(I)$ e para algum $N > 0$ $F_j^N \in I$ (tome N grande o bastante para que funcione para todo F_j). Tomando I-resíduos, $\overline{F}_j^N = 0$, e $\overline{X}_j^{Nr}$ é uma combinação k-linear de $\overline{1}, \overline{X}_j, \ldots, \overline{X}_j^{rN-1}$. Segue por indução que $\overline{X}_j^s$ é uma combinação k-linear de $\overline{1}, \overline{X}_j, \ldots, \overline{X}_j^{rN-1}$ para todo s, e então o conjunto $\{\overline{X}_1^{m_1}, \ldots, \overline{X}_n^{m_n} \mid m_i < rN\}$ gera $k[X_1, \ldots, X_n]/I$ como um espaço vetorial sobre k. □

Capítulo 3

Variedades Afins

A partir de agora, k será um corpo algebricamente fechado. Conjuntos algébricos afins estarão em $\mathbb{A} = \mathbb{A}^n(k)$ para algum n. Um conjunto algébrico irredutível é chamado de **variedade afim**.

Todos os anéis e corpos terão k como subanel. Por um homomorfismo $\phi : R \to S$ de anéis, queremos dizer um homomorfismo de anéis tal que $\phi(\lambda) = \lambda$ para todo $\lambda \in k$.

Nesse capítulo trataremos apenas de variedades afins, portanto as chamaremos apenas de variedades.

3.1 Anéis Coordenados

Definição 3.1. *Seja $V \subset \mathbb{A}^n$ uma variedade não vazia. Então $I(V)$ é um ideal primo em $k[X_1, \ldots, X_n]$, e $k[X_1, \ldots, X_n]/I(V)$ é um domínio integral. Definimos $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$, e o chamaremos de **anel coordenado** de V.*

Para qualquer conjunto não vazio V, denotamos por $\mathfrak{F}(V, k)$ o conjunto de todas as funções de V para k. Tornamos $\mathfrak{F}(V, k)$ um anel de forma usual: se $f, g \in \mathfrak{F}(V, k)$, $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$, para todo $x \in V$. É usual identificar k com o subanel de $\mathfrak{F}(V, k)$ consistindo de todas as funções constantes.

Definição 3.2. *Se $V \subset \mathbb{A}^n$ é uma variedade, uma função $f \in \mathfrak{F}(V, k)$ é chamada de uma **função polinomial** se existe um polinômio $F \in k[X_1, \ldots, X_n]$ tal que $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ para todo $(a_1, \ldots, a_n) \in V$*

As funções polinomiais formam um subanel de $\mathfrak{F}(V,k)$ que contém k. Dois polinômios F, G determinam a mesma função se, e somente se, $(F-G)(a_1,\ldots,a_n) = 0$ para todo $(a_1,\ldots,a_n) \in V$, isto é, $F - G \in I(V)$. Podemos então identificar $\Gamma(V)$ como o subanel de $\mathfrak{F}(V,k)$ consistindo de todas as funções polinomiais em V. Assim temos duas maneiras de enxergar um elemento de $\Gamma(V)$: como uma função em V, ou uma classe de equivalência de polinômios.

Definição 3.3. *Seja $V \subset \mathbb{A}^n$ uma variedade. Uma **subvariedade** de V é uma variedade $W \subset \mathbb{A}^n$ contida em V.*

3.2 Mapas Polinomiais

Definição 3.4. *Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades. Um mapa $\phi : V \to W$ é chamado de um **mapa polinomial** se existem polinômio $T_1,\ldots,T_m \in k[X_1,\ldots,X_n]$ tal que $\phi(a_1,\ldots,a_n) = (T_1(a_1,\ldots,a_n),\ldots,T_m(a_1,\ldots,a_n))$, para todo $(a_1,\ldots,a_n) \in V$.*

Qualquer mapa $\phi : V \to W$ induz um homomorfismo $\widetilde{\phi} : \mathfrak{F}(W,k) \to \mathfrak{F}(V,k)$, definindo $\widetilde{\phi}(f) = f \circ \phi$. Se ϕ é um mapa polinomial, então $\widetilde{\phi}(\Gamma(W)) \subset \Gamma(V)$, assim $\widetilde{\phi}$ se restringe a um homomorfismo (também denotado por $\widetilde{\phi}$) de $\Gamma(W)$ para $\Gamma(V)$; pois se $f \in \Gamma(W)$ é o $I(W)$-resíduo de um polinômio $F \in k[X_1,\ldots,X_m]$, então $\widetilde{\phi}(f) = f \circ \phi$ será o $I(V)$-resíduo do polinômio $F(T_1,\ldots,T_m) \in k[X_1,\ldots,X_n]$.

Se $V = \mathbb{A}^n$, $W = \mathbb{A}^m$ e $T_1,\ldots,T_m \in k[X_1,\ldots,X_n]$ determinam um mapa polinomial $T : \mathbb{A}^n \to \mathbb{A}^m$, os T_i's são unicamente determinados por T, então escreveremos $T = (T_1,\ldots,T_m)$.

Proposição 3.1. *Sejam $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades afins. Existe uma correspondência um para um natural entre mapas polinomiais $\phi : V \to W$ e homomorfismos $\widetilde{\phi} : \Gamma(W) \to \Gamma(V)$. Qualquer mapa polinomial ϕ será uma restrição de um mapa polinomial de $\mathbb{A}^n$ para $\mathbb{A}^m$.*

Demonstração. Assuma que $\alpha : \Gamma(W) \to \Gamma(V)$ seja um homomorfismo. Para cada $X_i \in k[X_1,\ldots,X_m]$ escolha $T_i \in k[X_1,\ldots,X_n]$ tal que $\alpha(X_i + I(W)) = T_i + I(V)$, assim $\alpha(F + I(W)) = F(T_1,\ldots,T_m) + I(V)$ para todo $F \in k[X_1,\ldots,X_m]$. Temos que $T = (T_1,\ldots,T_m)$ é um mapa polinomial de $\mathbb{A}^n$ para $\mathbb{A}^m$, que induzirá o homomorfismo $\widetilde{T} : \Gamma(\mathbb{A}^m) = k[X_1,\ldots,X_m] \to \Gamma(\mathbb{A}^n) = k[X_1,\ldots,X_n]$. Dado $F \in I(W)$, $\widetilde{T}(F) = F(T_1,\ldots,T_m)$, porém $\alpha(I(W)) = \alpha(F + I(W)) = F(T_1,\ldots,T_m) + I(V) = I(V)$. Portanto $\widetilde{T}(F) \in I(V)$ e assim $\widetilde{T}(I(W)) \subset I(V)$. Logo para todo $p \in V$, $(T_1(p),\ldots,T_m(p)) \in W$ o

que implica que $T(V) \subset W$, e T se restringe a um mapa polinomial $\phi : V \to W$. É simples ver que $\widetilde{\phi} = \alpha$, pois $\widetilde{\phi}(F + I(W)) = F(T_1, \ldots, T_m) + I(V)$, para todo $F \in k[X_1, \ldots, X_m]$. Como sabemos construir $\widetilde{\phi}$ a partir de um mapa polinomial $\phi : V \to W$, isso completa a prova. □

Um mapa polinomial $\phi : V \to W$ é um isomorfismo se existe um mapa polinomial $\psi : W \to V$ tal que $\psi \circ \phi$ é a identidade em V e $\phi \circ \psi$ é a identidade em W. A Proposição 3.1 mostra que duas variedades afins são isomorfas se, e somente se, seus anéis coordenados são isomorfos (sobre k).

3.3 Mudança de Coordenadas

Se $T = (T_1, \ldots, T_m)$ é um mapa polinomial de $\mathbb{A}^n$ para $\mathbb{A}^m$, e F é um polinômio em $k[X_1, \ldots, X_m]$, definimos $F^T = \widetilde{T}(F) = F(T_1, \ldots, T_m)$. Para ideais I e conjuntos algébricos V em $\mathbb{A}^m$, I^Tdenotará o ideal em $k[X_1, \ldots, X_n]$ gerado por $\{F^T | \ F \in I\}$ e V^T o conjunto algébrico $T^{-1}(V) = V(I^T)$, onde $I = I(V)$. Se V é a hipersuperfície de F, V^T é a hipersuperfície de F^T (se F^T é não constante).

Definição 3.5. *Uma **mudança afim de coordenadas** em $\mathbb{A}^n$ é um mapa polinomial $T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n$ tal que cada T_i é um polinômio de grau 1 e T é uma bijeção.*

Se $T_i = \sum a_{ij}X_j + a_{i0}$, então $T = T'' \circ T'$, onde T' é um mapa linear ($T'_i = \sum a_{ij}X_j$) e T'' é uma translação ($T''_i = X_i + a_{i0}$). Como toda translação possui uma inversa (que também será uma translação), segue que T será uma bijeção se, e somente se, T' é inversível. Se T e U são mudanças de coordenadas em $\mathbb{A}^n$ então $T \circ U$ também o será.

Definição 3.6. *Um conjunto $V \subset \mathbb{A}^n(k)$ é uma **subvariedade linear** de $\mathbb{A}^n(k)$ se $V = V(F_1, \ldots, F_r)$ para polinômios F_i de grau 1.*

Definição 3.7. *Sejam $P = (a_1, \ldots, a_n)$ e $Q = (b_1, \ldots, b_n)$ pontos distintos de $\mathbb{A}^n$. A **reta que passa por** P e Q é definida como o conjunto $\{(a_1+t(b_1-a_1), \ldots, a_n+t(b_n-a_n)) \mid t \in k\}$.*

3.4 Funções Racionais e Anéis Locais

Definição 3.8. *Dada uma variedade $V \subset \mathbb{A}^n$ e $\Gamma(V)$ seu anel coordenado, como $\Gamma(V)$ é um domínio, podemos formar seu corpo de frações. Ele será denominado o **corpo de funções racionais** em V, e denotado por $k(V)$. Um elemento de $k(V)$ é uma função racional em V.*

Se f é uma função racional em V, e $P \in V$, dizemos que f está definida em P se para alguns $a, b \in \Gamma(V)$, $f = \dfrac{a}{b}$ e $b(P) \neq 0$. Note que existem muitas formas de se escrever f como uma fração de funções polinomiais, assim f está definida em P se é possível encontrar um "denominador"que não se anula em P. No entanto se $\Gamma(V)$ é um DFU, existe uma única representação $f = \dfrac{a}{b}$, onde a e b não possuem fatores em comum, assim f está definida em P se, e somente se $b(P) \neq 0$.

Definição 3.9. *Se f é uma função racional em V, e $P \in V$, dizemos que f está definida em P se para alguns $a, b \in \Gamma(V)$, $f = \dfrac{a}{b}$ e $b(P) \neq 0$. Note que existem muitas formas de se escrever f como uma fração de funções polinomiais, assim f está definida em P se é possível encontrar um "denominador"que não se anula em P. Definimos $\mathcal{O}_P(V)$ o conjunto de funções racionais em V definidas em P. O conjunto $\mathcal{O}_P(V)$ será um anel que contém $\Gamma(V)$, e será denominado o* ***anel local*** *de V em P.*

Definição 3.10. *O conjunto de pontos de V tal que uma função racional em V não está definida é chamado de o* ***conjunto de polos*** *de f.*

Proposição 3.2. *(i) O conjunto de polos de uma função racional em V é um conjunto algébrico de V.*

(ii) $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$.

Demonstração. **(i)** Suponha $V \subset \mathbb{A}^n$. Para $G \in k[X_1, \ldots, X_n]$, denote o resíduo de G em $\Gamma(V)$ por $\overline{G}$. Seja $f \in k(V)$ e defina $J_f = \{G \in k[X_1, \ldots, X_n] \mid \overline{G}f \in \Gamma(V)\}$. Assim dados $G, F \in J_f$, existem $a, b \in \Gamma(V)$ tais que $f = \dfrac{a}{\overline{G}} = \dfrac{b}{\overline{F}}$. Logo $\overline{FG}f = \overline{FG}\dfrac{a}{\overline{G}} = \overline{F}a \in \Gamma(V)$, $\overline{G-F}f = \overline{G}f - \overline{F}f = a - b \in \Gamma(V)$ e dado $H \in k[X_1, \ldots, X_n]$, $\overline{HG}f = \overline{H}a \in \Gamma(V)$ e temos que $GF,\ (G-F),\ HG \in J_f$. Portanto J_f será um ideal de $k[X_1, \ldots, X_n]$ e que contém $I(V)$ (dado $F \in I(V)$, $\overline{F}f = \overline{0}f = \overline{0} \in \Gamma(V)$). Os pontos de $V(J_f)$ serão justamente os pontos onde f não está definida, pois dado $P \in V(J_f)$ então $G(P) = 0$ para todo $G \in k[X_1, \ldots, X_n]$ tal que $f = \dfrac{a}{\overline{G}}$ (com $a \in \Gamma(V)$) e assim todo "denominador"de f se anula em P. Portanto $V(J_f)$ é o conjunto de polos de f.

(ii) Se $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$ então f está definida em todo $P \in V$ e $V(J_f) = \emptyset$. Pela versão fraca do Teorema dos Zeros de Hilbert, $1 \in J_f$, e assim $1 \cdot f \in \Gamma(V)$. Assim $\bigcap_{P \in V} \mathcal{O}_P(V) \subset \Gamma(V)$. A inclusão $\Gamma(V) \subset \bigcap_{P \in V} \mathcal{O}_P(V)$ é trivial, e assim $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$. □

Suponha $f \in \mathfrak{O}_P(V)$. Podemos definir o valor de f em P, escrito como $f(P)$, da seguinte maneira: escreva $f = \frac{a}{b}$, com $a, b \in \Gamma(V)$, $b(P) \neq 0$, e seja $f(P) = \frac{a(P)}{b(P)}$ (nota-se que o valor de f em P não depende da escolha de a e b). O ideal $\mathfrak{m}_P(V) = \{f \in \mathfrak{O}_P(V) \mid f(P) = 0\}$ é chamado de ideal maximal de V em P. Ele é o núcleo do homomorfismo de evaluação $f \mapsto f(P)$ de $\mathfrak{O}_P(V)$ sobre k, assim $\mathfrak{O}_P(V)/\mathfrak{m}_P(V)$ é isomorfo à k. um elemento $f \in \mathfrak{O}_P(V)$ é uma unidade em $\mathfrak{O}_P(V)$ se, e somente se, $f(P) \neq 0$, então $\mathfrak{m}_P(V) = \{\text{Não-unidades de } \mathfrak{O}_P(V)\}$. Assim $\mathfrak{O}_P(V)$ é um anel local pelo Lema 3.1.

Lema 3.1. *As seguintes condições em um anel R são equivalentes:*

(i) O conjunto das não-unidades em R forma um ideal.

(ii) R possui um único ideal maximal que contém todos os ideais próprios de R.

Demonstração. Seja $\mathfrak{m} = R/U(R)$, onde $U(R) = \{\text{Unidades de } R\}$. Temos que todo ideal próprio de R está em $\mathfrak{m}$. Assim todo ideal maximal de R está em $\mathfrak{m}$ e se $\mathfrak{m}$ é um ideal, então ele será um ideal maximal pois contém todo ideal próprio de R e será único. Reciprocamente se R possui um unico ideal maximal I que contém todos os ideais próprios de R, então I contém todas as não-unidades de R e $\mathfrak{m} \subset I$. Porém I é um ideal próprio de R, logo $I \subset \mathfrak{m}$ e assim $\mathfrak{m}$ é um ideal.

□

Definição 3.11. *Um anel R que possui um único ideal maximal, e portanto contém todo ideal próprio de R (consequentemente satisfazendo as condições do Lema 3.1) é dito um* ***anel local****. As unidades de R são os elementos que não pertencem ao ideal maximal.*

Vimos que $\mathfrak{O}_P(V)$ é um anel local e $\mathfrak{m}_P$ é seu ideal maximal. Anéis locais tem um papel proeminente no estudo moderno de variedades algébricas, pois todas propriedade de uma variedade V que só dependem de uma "vizinhança"de P são refletidas em $\mathfrak{O}_P(V)$.

Proposição 3.3. *$\mathfrak{O}_P(V)$ é um domínio local Noetheriano.*

Demonstração. É preciso mostrar que qualquer ideal I de $\mathfrak{O}_P(V)$ é finitamente gerado. Como $\Gamma(V)$ é Noetheriano (pela Proposição 6.11), escolha geradores $f_1, \ldots, f_r$ para o ideal $I \cap \Gamma(V)$ de $\Gamma(V)$. Afirmamos que $f_1, \ldots, f_r$ geram I como um ideal em $\mathfrak{O}_P(V)$. Pois se $f \in I \subset \mathfrak{O}_P(V)$, existe $b \in \Gamma(V)$ com $b(P) \neq 0$ tal que $bf \in \Gamma(V)$. Então $bf = \sum a_i f_i,\ a_i \in \Gamma(V)$ e portanto $f = \sum(\frac{a_i}{b})f_i$, como desejado.

□

3.5 Anéis de Avaliação Discretos

Proposição 3.4. *Seja R um domínio que não é um corpo. Então as seguintes afirmações são equivalentes:*

(i) R é Noetheriano e local, e seu ideal maximal é principal.

(ii) Existe um elemento irredutível $t \in R$ tal que todo $z \in R$ não nulo pode ser escrito unicamente como $z = ut^n$, u uma unidade de R e n um inteiro não negativo.

Demonstração. $(i) \Rightarrow (ii)$: Seja $\mathfrak{m}$ o ideal maximal de R, t um gerador de $\mathfrak{m}$. Suponha $ut^n = vt^m$, com u, v unidades e $n \geq m$. Então $ut^{n-m} = v$, uma unidade, o que implica que $n = m$ e $u = v$. Assim a expressão de qualquer $z = ut^n$ é única. Para mostrar que todo z não nulo possui tal expressão, assumiremos que z não é uma unidade, assim $z = z_1 t$ para algum $z_1 \in R$, pois $z \in \mathfrak{m}$. Se z_1 é uma unidade está provado, então assuma $z_1 = z_2 t$. Continuando esse processo, temos uma sequência infinita de $z_1,\ z_2, \ldots$ com $z_i = z_{i+1} t$. Como R é Noetheriano, a cadeia de ideais $(z_1) \subset (z_2) \subset \cdots$ deve ter um membro maximal (pelo Lema 2.2), então $(z_n) = (z_{n+1})$ para algum n. Então $z_{n+1} = vz_n$ para algum $v \in R$. Mas então $z_{n+1} = vtz_{n+1}$ e $1 = vt$, uma contradição pois t não é unidade. Portanto o processo deve parar para algum z_m que será uma unidade, e assim $z = z_m t^m$.

$(ii) \Rightarrow (i)$ O conjunto $\mathfrak{m} = (t)$ será o conjunto de todas as não unidades, assim R é local. Além disso, todos os ideais em R serão os ideais principais da forma (t^n), onde n é um inteiro não negativo. Portanto R é DIP.

□

Definição 3.12. *Um anel R satisfazendo as condições da Proposição 3.4 é chamado de* ***anel de avaliação discreto****, abreviado como AAD. Um elemento t como na afirmação* (2) *é dito um parâmetro uniformizante para R.*

Qualquer outro parâmetro uniformizante para R é da forma ut, com u uma unidade em R. Seja K o corpo de frações de R. Então (com t fixado) qualquer elemento não nulo $z \in K$ possuí uma única expressão $z = ut^n$, u uma unidade em R e $n \in \mathbb{Z}$. O expoente de n é chamado de ordem de z, e é escrito como $n = ord(z)$; definimos $ord(0) = \infty$. Note que $R = \{z \in K \mid ord(z) \geq 0\}$, e $\mathfrak{m} = \{z \in K \mid ord(z) > 0\}$ é o ideal maximal em R.

Definição 3.13. *Uma função de ordem em um corpo K é uma função sobrejetora $\phi : K \to \mathbb{Z} \cup \{\infty\}$, satisfazendo:*

(i) $\phi(a) = \infty$ *se, e somente se,* $a = 0$.

(ii) $\phi(ab) = \phi(a) + \phi(b)$.

(iii) $\phi(a + b) \geq min(\phi(a), \phi(b))$.

3.6 Formas

Seja R um domínio. Se $F \in R[X_1, \ldots, X_{n+1}]$ é uma forma, definimos $F_* \in R[X_1, \ldots, X_n]$ por $F_* = F(X_1, \ldots, X_n, 1)$. Reciprocamente, para qualquer polinômio $f \in R[X_1, \ldots, X_n]$ de grau d, escrevendo $f = f_0 + f_1 + \cdots + f_d$, onde f_i é uma forma de grau i, e defina $f^* \in R[X_1, \ldots, X_{n+1}]$ por

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + f_d = X_{n+1}^d f(X_1/X_{n+1}, \ldots, X_n/X_{n+1});$$

f^* é uma forma de grau d. Esse processo é comumente chamado de "homogenizar"e "dehomogenizar"polinômios com respeito a X_{n+1}.

Corolário 3.1. *Se* $F \in k[X, Y]$ *é uma forma,* k *algebricamente fechado, então* F *fatora em um produto de fatores lineares.*

Demonstração. A primeira afirmação segue diretamente dos itens (1) e (2) da Proposição 6.44. Para o segundo, escreva $F = Y^r G$, tal que Y não divida G. Então $F_* = G_* = \epsilon \prod(X - \lambda_i)$ dado que k é algebricamente fechado, então $F = \epsilon Y^r \prod(X - \lambda_i Y)$.

□

3.7 Operações com Ideais

Sejam I, J ideais de um anel R. O ideal gerado por $\{ab \mid a \in I, b \in J\}$ é denotado por IJ. Similarmente, se $I_1, \ldots, I_n$ são ideais, $I_1 \cdots I_n$ é o ideal gerado por $\{a_1 a_2 \cdots a_n \mid a_i \in I_i\}$. Definimos I^n como $II \cdots I$ (n vezes). Note que enquanto I^n contém todas as enésimas potências de elementos de I, ele pode não ser gerado por eles. Se I é gerado por $a_1, \ldots, a_r$, então I^n é gerado por $\{a_1^{i_1} \cdots a_r^{i_r} \mid \sum i_j = n\}$.

Exemplo 3.1. $R = k[X_1, \ldots, X_r],\ I = (X_1, \ldots, X_r)$. *Então* I^n *é gerado por monomios de grau menor que* n*, e* I^n *consiste dos polinômios sem termos de grau menor que* n*. Segue que*

os residuos dos monomios de grau meno que n formam uma base de $k[X_1, \ldots, X_r]/I^n$ *sobre* k.

Se R é um subanel de um anel S, IS denota o ideal de S gerado pelos elementos de I.

Definição 3.14. *Sejam* I, J *ideais de um anel* R. *Definimos* $I + J = \{a + b \mid a \in I,\ b \in J\}$. *Assim* $I + J$ *é um ideal, e na verdade é o menor ideal em* R *que contém* I *e* J

Dois ideais I, J de R são ditos ser comaximais se $I + J = R$, isto é, se $1 = a + b$ para $a \in I$ e $b \in J$. Como exemplo, dois ideais maximais distintos são comaximais.

Lema 3.2. *(1)* $IJ \subset I \cap J$, *para quaisquer ideais* I *e* J.

(2) Se I *e* J *são comaximais,* $IJ = I \cap J$.

Demonstração. A afirmação (1) é trivial pois para todo $a \in I$ e $b \in J$, $ab \in I$ e $ab \in J$, logo $ab \in I \cap J$.

Para (2), se $I + J = R$, então $I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subset JI + IJ = IJ$.

□

3.8 Ideais com Finitos Zeros

A proposição dessa seção será utilizada para relacionar questões locais (em termos dos anéis locais $\mathfrak{O}_P(V)$) com questões globais (em termos do aneis coordenados).

Proposição 3.5. *Seja* I *um ideal em* $k[X_1, \ldots, X_n]$ *(*k *algebricamente fechado), e suponha que* $V(I) = \{P_1, \ldots, P_n\}$ *é finito. Sendo* $\mathfrak{O}_i = \mathfrak{O}_{P_i}(\mathbb{A}^n)$. *Então existe um isomorfismo natural de* $k[X_1, \ldots, X_n]/I$ *com* $\prod_{i=1}^N \mathfrak{O}_i/I\mathfrak{O}_i$

Demonstração. Seja $I_i = I(\{P_i\}) \subset k[X_1, \ldots, X_n]$ os ideais maximais distintos que contém I. Seja $R = k[X_1, \ldots, X_n]/I$, $R_i = \mathfrak{O}_i/I\mathfrak{O}_i$. Os homomorfismos naturais (Proposição 6.48 (b)) ϕ_i, de R para R_i induzem um homomorfismo ϕ de R para $\prod_{i=1}^N R_i$.

Pelo Teorema dos Zeros, $Rad(I) = I(\{P_1, \ldots, P_N\}) = \cap_{i=1}^N I_i$, então $(\cap I_i)^d \subset I$ para algum d (Proposição 6.46). Como $\cap_{i \neq j} I_j$ e I_i são comaximais (Proposição 6.51) segue que (da Proposição 6.47) $\cap I_j^d = (I_1 \cdots I_N)^d = (\cap I_j)^d \subset I$.

Agora, escolha $F_i \in k[X_1, \ldots, X_n]$ tal que $F_i(P_j) = 0$ se $i \neq j$ e $F_i(P_i) = 1$ (Proposição 6.10). Seja $E_i = 1 - (1 - F_i^d)^d$. Note que $E_i = F_i^d D_i$ para algum $D_i \in k[X_1, \ldots, X_n]$, então

$E_i \in I_j$ se $i \neq j$ e $1-\sum_i E_i = (1-E_j)-\sum_{i\neq j} E_i \in \cap I_j^d \subset I$. Além disso, $E_i - E_i^2 = E_i(1-F_i^d)^d$ pertence a $\cap_{i\neq j} I_j^d \cdot I_i^d \subset I$. Tomando e_i como o resíduo de E_i em R/I, temos que $e_i^2 = e_i$, $e_i e_j = 0$ se $i \neq j$ e $\sum e_i = 1$.

Afirmação: Se $G \in k[X_1, \ldots, X_n]$ e $G(P_i) \neq 0$, então existe um $t \in R$ tal que $tg = e_i$, onde g é o I-resíduo de G.

Assumindo a afirmação por um momento, mostraremos que ϕ é um isomorfismo:

(i) ϕ é injetiva: Se $\phi(f) = 0$ (com f sendo I-resíduo de $F \in k[X_1, \ldots, X_n]$), então para cada i, existe G_i, com $G_i(P_i) \neq 0$ e $G_i F \in I$. Seja $t_i g_i = e_i$ (t_i existe pela afirmação). Então $f = f(\sum_i e_i) = \sum_i f e_i = \sum_i t_i f g_i = 0$.

(ii) ϕ é sobrejetiva: Como $E_i(P_i) = 1$, $\phi_i(e_i)$ é uma unidade em R_i. Como $\phi_i(e_i)\phi_i(e_j) = \phi_i(e_i e_j) = 0$ se $i \neq j$, $\phi_i(e_j) = 0$ para $i \neq j$. Assim, $\phi_i(e_i) = \phi_i(\sum e_j) = \phi_i(1) = 1$. Agora suponha $z = (a_1/s_1, \ldots, a_N/s_N) \in \prod R_i$. Pela afirmação, podemos encontrar t_i's tais que $t_i s_i = e_i$ em R_i, então $\phi_i(\sum t_j a_j e_j) = \phi_i(a_i t_i) = a_i/s_i$, logo $\phi(\sum t_j a_j e_j) = z$.

Para provar a afirmação, podemos assumir que $G(P_i) = 1$. Seja $H = 1 - G$. Segue que

$$(1-H)(E_i + HE_i + \cdots + H^{d-1}E_i) = E_i - H^d E_i,$$

e como $H \in I_i$, $H^d E_i \in I$. Portanto $g(e_i + he_i + \cdots + h^{d-1}e_i) = e_i$, como desejado. □

Corolário 3.2. *$dim_k\ (k[X_1, \ldots, X_n]/I) = \sum_{i=1}^N\ dim_k\ (\mathfrak{O}_i/I\mathfrak{O}_i)$*

Corolário 3.3. *Se $V(I) = \{P\}$, então $k[X_1, \ldots, X_n]/I$ é isomorfo a $\mathfrak{O}_P(\mathbb{A}^n)/I\mathfrak{O}_P(\mathbb{A}^n)$.*

3.9 Módulo Quociente e Sequências Exatas

Seja R um anel, M e M' R-módulos. Um homomorfismo $\phi : M \to M'$ de grupos abelianos é dito um homomorfismo de R-módulos se $\phi(am) = a\phi(m)$ para todo $a \in R$ e $m \in M$. Um homomorfismo de R-módulos é dito um isomorfismo de R-módulos se é bijetivo.

Definição 3.15. *Se N é um submódulo de um R-módulo M, o grupo quociente M/N de cosets de N em M é transformado em um R-módulo da seguinte maneira: Se $\overline{m}$ é um coset (ou classe de equivalência) conténdo m, e $a \in R$, defina $a\overline{m} = \overline{am}$. Definida a multplicação por elementos de R, temos que M/N é um R-módulo, chamado de módulo quociente de M por N. Além disso o mapa natural de M para M/N será um homomorfismo de R-módulos.*

Definição 3.16. *Sejam $\phi : M' \to M$, $\psi : M \to M''$ homomorfismos de R-módulo. Dizemos que a sequência (de R-módulos e homomorfismos)*

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

é exata se (ou exata em M) se $Im(\phi) = Ker(\psi)$. Como existe somente um homomorfismo de R-módulos do módulo 0 para qualquer R-módulo M e de M para 0. Assim $M \xrightarrow{\psi} M'' \to 0$ é exata se, e somente se, ψ é sobrejetiva e $0 \xrightarrow{\phi} M' \to M$ é exata se, e somente se, ϕ é injetiva.

Se $\phi_i : M_i \to M_{i+1}$ são homomorfismos de R-módulo, dizemos que a sequência

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_n} M_{n+1}$$

é exata se $Im(\phi_i) = Ker(\phi_{i+1})$, para cada $i = 1, \ldots, n$. Assim

$$0 \to M' \xrightarrow{\psi} M \xrightarrow{\phi} M'' \to 0$$

é exata se, e somente se, ϕ é sobrejetiva e ψ mapeia M' isomorficamente ao núcleo de ϕ.

Proposição 3.6. *(i) Seja $0 \to V' \xrightarrow{\psi} V \xrightarrow{\phi} V'' \to 0$ uma sequência exata de espaços vetoriais sobre um corpo k, com dimensão finita. Então $dim\ V' + dim\ V'' = dim\ V$.*

(ii) Seja

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

uma sequência exata de espaços vetoriais de dimensão finita. Então

$$dim\ V_4 = dim\ V_3 - dim\ V_2 + dim\ V_1$$

Demonstração. **(i)** Pelo Teorema do Núcleo-Imagem, temos que

$$dim\ V = dim\ Ker(\phi) + dim\ Im(\phi)$$

Como ϕ é sobrejetiva (dado que a sequência é exata), então $Im(\phi) = V''$, logo $dim\ Im(\phi) = dim\ V''$. Como a sequência é exata, então $Ker(\phi) = Im(\psi)$, mas como ψ é injetiva (pela

sequência ser exata), e pelo Teorema Núcleo-Imagem $dim\ V' = dim\ Ker(\psi) + dim\ Im(\psi) = dim\ Im(\psi)$, então $dim\ Im(\psi) = dim\ V'$ e temos

$$dim\ V = dim\ V' + dim\ V''$$

(ii) Segue de (1) tomando $W = Im(\phi_2) = Ker(\phi_3)$. Pois então $0 \to V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} W \to 0$ e $0 \to W \xrightarrow{\psi} V_3 \xrightarrow{\phi_3} V_4 \to 0$ são exatas, onde ψ é a inclusão, e o resultado segue dado que

$$dim\ V_2 = dim\ V_1 + dim\ W \Rightarrow dim\ W = dim\ V_2 - dim\ V_1$$

E

$$dim\ V_3 = dim\ W + dim\ V_4 \Rightarrow dim\ W = dim\ V_3 - dim\ V_4$$

Logo

$$dim\ V_3 - dim\ V_4 = dim\ V_2 - dim\ V_1 \Rightarrow dim\ V_4 = dim\ V_3 - dim\ V_2 + dim\ V_1.$$

□

Capítulo 4

Propriedades Locais de Curvas Planas

4.1 Pontos Múltiplos e Retas Tangentes

Vimos que curvas planas afins correspondem a polinômios não constantes $F \in k[X,Y]$ sem fatores múltiplos, onde F é determinado a menos de multiplicação por uma constante não nula (Capítulo 2, Seção 2.5). Para algumas finalidades é útil permitir que F tenha múltiplos fatores, e para isso mudaremos a definição levemente:

Definição 4.1. *Dois polinômios $F, G \in k[X,Y]$ são ditos ser equivalentes se $F = \lambda G$ para algum $\lambda \in k$ não nulo. Uma **curva plana afim** será uma classe de equivalência de polinômios não constantes sobre essa relação de equivalência.*

O grau de uma curva é o grau dos polinômios que definem a curva.

Uma curva de grau 1 é uma reta, dizemos então "a reta $aX + bY + c$", ou "a reta $aX + bY + c = 0$".

Se $F = \prod F_i^{e_i}$, onde os F_i's são os fatores irredutíveis de F, dizemos que os F_i's são as componentes de F e e_i a multiplicidade do componente F_i. F_i é uma componente simples se $e_i = 1$ e múltipla caso contrário. Observe que as componentes F_i de F podem ser recuperadas (até uma equivalência de polinômios) de $V(F)$ (Corolário 2.3), mas as multiplicidades das componentes não podem ser recuperadas.

Se F é um polinômio irredutível, então $V(F)$ é uma variedade em $\mathbb{A}^2$. Denotaremos $\Gamma(F)$, $k(F)$ e $\mathfrak{O}_P(F)$ ao invés de $\Gamma(V(F))$, $k(V(F))$ e $\mathfrak{O}_P(V(F))$.

Definição 4.2. *Seja F uma curva, $P = (a, b) \in V(F)$. O ponto P é chamado de um* ***ponto simples*** *de F se $F_X(P) \neq 0$ ou $F_Y(P) \neq 0$. Neste caso, a reta $F_X(P)(X - a) + F_Y(P)(Y - b) = 0$ é chamada de* ***reta tangente*** *de F em P. Um ponto que não é simples é chamado de múltiplo (ou singular). Uma curva apenas com pontos simples é dita uma curva não singular.*

Exemplo 4.1. *A seguir alguns exemplos gráficos de curvas. Se F é uma curva em $\mathbb{A}^2(\mathbb{C})$, podemos apenas visualizar a parte real de F, isto é $V(F) \cap \mathbb{A}^2(\mathbb{R})$.*

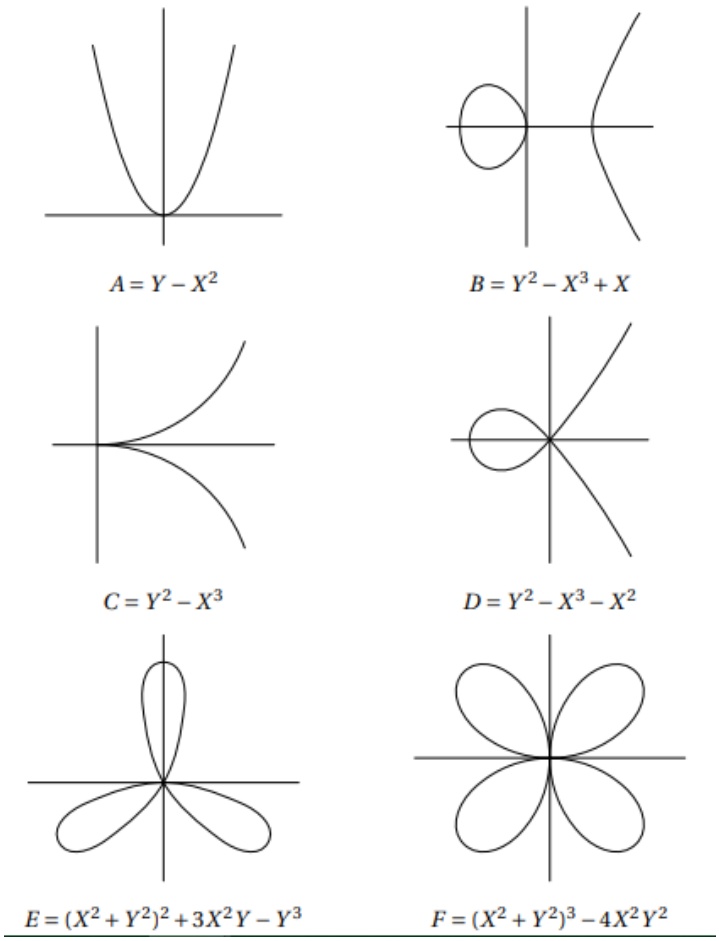

Figura 4.1: Exemplos de Curvas em $\mathbb{A}^2(\mathbb{R})$ [1].

Temos que $A_Y = 1$, logo A é não singular pois todo ponto $P \in V(F)$ não é um zero de $A_Y = 1$. De forma semelhante $B_X = -3X^2 + 1$ o que implica que as raízes de B_X são $X = \pm(\frac{1}{\sqrt{3}})$ e como $B_Y = 2Y$, então a única raíz é $Y = 0$, mas os pontos $P_1 = (\frac{1}{\sqrt{3}}, 0)$ e $P_2 = (-\frac{1}{\sqrt{3}}, 0)$ não são raízes de B e assim B não possui pontos singulares. Um cálculo

semelhante com derivadas mostra que $P = (0,0)$ é o único ponto múltiplo das curvas C, D, E e F.

Nos primeiros dois exemplos temos que os termos lineares Y e X são as retas tangentes no ponto $(0,0)$ de A e B, respectivamente, pois $A_X(0,0)X + A_Y(0,0)Y = Y$ e $B_X(0,0)X + B_Y(0,0)Y = X$. Os termos de menor grau de C, D, E e F são, respectivamente, Y^2, $Y^2 - X^2 = (X+Y)(X-Y)$, $3X^2Y - Y^3 = Y(\sqrt{3}X - Y)(\sqrt{3}X + Y)$ e $-4X^2Y^2$. Em cada caso, a forma de menor ordem traduz as retas que melhor poderiam ser chamadas de tangentes à curva em $(0,0)$.

Definição 4.3. *Seja F uma curva qualquer e $P = (0,0)$. Escreva $F = F_m + F_{m+1} + \cdots + F_n$, onde F_i é uma forma em $k[X,Y]$ de grau i, com $F_m \neq 0$. Definimos m como a multiplicidade de F em $P = (0,0)$ e escrevemos $m = m_P(F)$. Se $m = 2$, P é chamado de um ponto duplo, se $m = 3$ um ponto triplo, e assim por diante. Note que $P \in V(F)$ se, e somente se, $m_P(F) > 0$.*

Temos também que P será um ponto simples de F se, e somente se, $m_P(F) = 1$, pois se $P \in V(F)$ é simples, temos que $m_P(F) > 0$ e $F_X(P) \neq 0$ ou $F_Y(P) \neq 0$, logo $m_P(F_X) = 0$ ou $m_P(F_Y) = 0$ e assim $m_P(F) = 1$. Reciprocamente, se $m_P(F) = 1$, então $m_P(F_X) = 0$ ou $m_P(F_Y) = 0$ e com $(F_X)_0 \neq 0$ ou $(F_Y)_0 \neq 0$ respectivamente. Assim $F_X(P) = (F_X)_0 \neq 0$ ou $F_Y(P) = (F_Y)_0 \neq 0$ e P é simples. Nesses casos F_1 é exatamente a reta tangente de F em P, pois $F_X(P)X + F_Y(P)Y = (F_X)_0X + (F_Y)_0Y = F_1$.

Definição 4.4. *Como F_m é uma forma em duas variáveis, podemos escrever $F_m = \prod L_i^{r_i}$ onde os L_i's são retas distintas (Corolário 3.1). As L_i's são chamadas de* ***retas tangentes de F em $P = (0,0)$****, e os r_i's são as multiplicidades de cada reta. A reta L_i é uma tangente simples (respec. dupla, etc) se $r_i = 1$ (resp. 2, etc). Se F possui m tangentes distintas (simples), dizemos que P é um* ***ponto múltiplo ordinário*** *de F. Um ponto ordinário duplo é chamado de nódulo. Por conveniência, chamaremos uma reta por P uma tangente de mutiplicidade zero se F não é tangente a P.*

Seja $F = \prod F_i^{e_i}$ a fatorização de F em componentes irredutíveis. Então $m_P(F) = \sum e_i m_P(F_i)$. Se L é uma reta tangente de F_i com multiplicidade r_i, então L é tangente à F com multiplicidade $\sum e_i r_i$. Isso é consequência direta do fato de que os termos de menor grau de F são o produto dos termos de menor grau dos fatores de F.

Em particular, um ponto P é um ponto simples de F se, e somente se, P pertence a

somente uma componente F_i de F, F_i é uma componente simples de F e P é um ponto simples de F_i.

Para estender essas definições para um ponto $P = (a, b) \neq (0, 0)$, seja T a translação que leva $(0, 0)$ em (a, b), isto é $T(X, Y) = (X + a, Y + b)$. Então $F^T = F(X + a, Y + b)$. Defina $m_P(F)$ como $m_{(0,0)}(F^T)$, isto é, escreva $F^T = G_m + G_{m+1} + \cdots + G_n$, onde G_i são formas de grau i e $G_m \neq 0$ e tome $m = m_P(F)$. Se $G_m = \prod L_i^{r_i}$, $L_i = \alpha_i X + \beta_i Y$, as retas $\alpha_i(X - a) + \beta_i(Y - b)$ são definidas como as retas tangentes de F em P, com r_i a multiplicidade da tangente.

4.2 Multiplicidades e Anéis Locais

Seja F uma curva plana irredutível, $P \in F$. Nessa seção encontraremos a multiplicidade de P em F, em termos do anel local $\mathfrak{O}_P(F)$. A seguinte notação se mostrará útil: para qualquer polinômio $G \in k[X, Y]$ denote sua imagem (resíduo) em $\Gamma(F) = k[X, Y]/(F)$ por g.

Teorema 4.1. *P é ponto simples de F se, e somente se, $\mathfrak{O}_P(F)$ é um anel de avaliação discreto. Nesse caso, se $L = aX + bY + c$ é uma reta qualquer que passa por P, que não é tangente à F em P, então a imagem l de L em $\mathfrak{O}_P(F)$ é um parametro uniformizante para $\mathfrak{O}_P(F)$.*

Demonstração. Suponha que P é um ponto simples de F, e L é uma reta que passa por P, que não é tangente à F em P. Tomando uma mudança afim de coordenadas, podemos assumir que $P = (0, 0)$, que Y é a reta tangente e $L = X$ (pelas Proposições 3.12 (d) e 6.37). Pela Proposição 3.4 é suficiente mostrar que $\mathfrak{m}_P(F)$ é gerado por x.

Note primeiro que $\mathfrak{m}_P(F) = (x, y)$, sendo P simples ou não (pelas Proposições 6.49 e 6.50).

Agora com essas hipóteses, temos que $F = Y +$ termos de maior grau. Agrupando esses termos de maior grau com Y, podemos escrever $F = YG - X^2H$, onde $G = 1 +$ termos de maior grau e $H \in k[X]$.

Então $yg = x^2h \in \Gamma(F)$, logo $y = x^2hg^{-1} \in (x)$, dado que $g(P) \neq 0$. Assim $\mathfrak{m}_P(F) = (x, y) = (x)$, como desejado.

A volta será demonstrada a partir do Teorema 4.2.

□

Seja P é um ponto simples em uma curva irredutível F. Definimos ord_P^F como a ordem da função de ordem em $k(F)$, definida pelo AAD $\mathfrak{O}_P(F)$. Quando F é fixo, podemos simplesmente escrever ord_P. Se $G \in k[X,Y]$, e g é a imagem de G em $\Gamma(F)$, escreveremos $ord_P^F(G)$ ao invés de $ord_P^F(g)$.

Se P é um ponto simples de uma curva redutível F, escrevemos ord_P^F ao invés de $ord_P^{F_i}$, onde F_i é a componente de F contendo P.

Suponha que P é um ponto simples em F, e L uma reta qualquer que passa por P. Então $ord_P^F(L) = 1$ se L não é tangente à F em P e $ord_P^F(L) > 1$ se L é tangente à F em P. Isso se deve, pois podemos assumir as condições do Teorema 4.1 e então a tangente Y é tal que $y = x^2hg^{-1}$, então $ord_P(y) = ord_P(x^2) + ord_P(hg^{-1}) \geq 2$.

A demonstração do próximo teorema nos permite calcular a dimensão de certos espaços vetoriais do tipo $\mathfrak{O}_P(V)/I$, onde I é um ideal de $\mathfrak{O}_P(V)$.

Teorema 4.2. *Seja P um ponto em uma curva irredutível F. Então para todo n suficientemente grande,*

$$m_P(F) = dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}).$$

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

Demonstração. Escreva $\mathfrak{O}_P(F)$, $\mathfrak{m}_P(F)$ como $\mathfrak{O}$ e $\mathfrak{m}$ respectivamente. Da sequência exata

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathfrak{O}/\mathfrak{m}^{n+1} \to \mathfrak{O}/\mathfrak{m}^n \to 0$$

segue que basta provar que $dim_k(\mathfrak{O}/\mathfrak{m}^n) = nm_P(F) + s$, para alguma constante s e para todo $n \geq m_P(F)$ (pelas Proposições 3.6 e 6.53 (e)). Podemos assumir que $P = (0,0)$, então $\mathfrak{m}^n = I^n\mathfrak{O}$, onde $I = (X,Y) \subset k[X,Y]$ (Proposição 6.49). Como $V(I^n) = \{P\}$, $k[X,Y]/(I^n,F) \cong \mathfrak{O}_P(\mathbb{A}^2)/(I^n,F)\mathfrak{O}_P(\mathbb{A}^2 \cong \mathfrak{O}_P(F)/I^n\mathfrak{O}_P(F) = \mathfrak{O}/\mathfrak{m}^n$ (Corolário 3.3 e Proposição 6.50).

Então basta calcular a dimensão de $k[X,Y]/(I^n,F)$. Seja $m = m_P(F)$. Então $FG \in I^n$ sempre que $G \in I^{n-m}$. Existe um homomorfismo natural de anéis ϕ de $k[X,Y]/I^n$ para $k[X,Y]/(I^n,F)$ e uma aplicação k-linear ψ de $k[X,Y]/I^{n-m}$ para $k[X,Y]/I^n$ definida por $\psi(\overline{G}) = \overline{FG}$ (as barras denotam os resíduos dos quociente). É fácil ver que ψ será injetiva e ψ sobrejetiva, e então temos a sequência exata

$$0 \to k[X,Y]/I^{n-m} \to k[X,Y]/I^n \to k[X,Y]/(I^n,F) \to 0.$$

Aplicando a Proposição 6.52 e a Proposição 3.6 novamente, temos que

$$dim_k(k[X,Y]/(I^n,F)) = nm - \frac{m(m-1)}{2},$$

para todo $n \geq m$, como desejado. Note que se $\mathfrak{D}_P(F)$ é um AAD, então $m_P(F) = 1$ (Proposição 6.54 (a)) então P é simples, o que garante a volta do Teorema 4.1.

□

4.3 Números de Interseção

Sejam F e G curvas planas e $P \in \mathbb{A}^2$. Queremos definir o número de interseção de F e G em P, denotado por $I(P, F \cap G)$. Dada a intuitividade única da definição, descreveremos sete propriedades que esse número de interseção deve possuir e um teorema demonstrará que só existe uma definição possível.

Definição 4.5. *Dizemos que F e G se **intersectam propriamente** em P se F e G não possuem componentes comuns que passam por P.*

(1) $I(P, F \cap G)$ é um inteiro não negativo para quaisquers F e G e P tais que F e G se intersectam propriamente em P. Se F e G não se intersectam propriamente em P então $I(P, F \cap G) = \infty$.

(2) $I(P, F \cap G) = 0$ se, e somente se, $P \notin F \cap G$. $I(P, F \cap G)$ depende somente das componentes de F e G que passam por P. Se F ou G é uma constante não nula, então $I(P, F \cap G) = 0$.

(3) Se T é uma mudança afim de coordenadas em $\mathbb{A}^2$, e $T(Q) = P$, então $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

(4) $I(P, F \cap G) = I(P, G \cap F)$.

Definição 4.6. *Dizemos que duas curvas F e G se **intersectam transversalmente** em um ponto P se P é um ponto simples de ambas F e G, e se a reta tangente de F em P é diferente da reta tangente de G em P.*

Desejamos que o número de interseção seja exatamente um quando F e G se intersectam transversalmente em P. De forma mais geral, queremos que:

(5) $I(P, F \cap G) \geq m_P(F)m_P(G)$, com a igualdade ocorrendo se, e somente se, F e G não possuem retas tangentes em P em comum.

Os números de interseção devem ser adicionados quando tomamos uniões de curvas:

(6) Se $F = \prod F_i^{r_i}$, e $G = \prod G_j^{s_j}$, então $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.

A última propriedade é provavelmente a menos intuitiva. Se F é irredutível, então $I(P, F \cap G)$ deve depender somente da imagem de G em $\Gamma(F)$. Ou para F arbitrário:

(7) $I(P, F \cap G) = I(P, F \cap (G + AF))$ para qualquer $A \in k[X, Y]$.

Teorema 4.3. *Existe um único $I(P, F \cap G)$ definido para todas as curvas planas F, G e todos os pontos $P \in \mathbb{A}^2$, satisfazendo as propriedades $(1) - (7)$. Ele é dado pela fórmula:*

$$I(P, F \cap G) = dim_k(\mathfrak{O}_P(\mathbb{A}^2)/(F, G)).$$

Demonstração. Unicidade: Assuma que exista um número $I(P, F \cap G)$ definido para todos F, G e P e que satisfaça as condições $(1) - (7)$. Mostraremos um procedimento para calcular $I(P, F \cap G)$ usando somente as sete propriedades, e que é mais forte que a unicidade requerida. Podemos assumir que $P = (0, 0)$ (por (3)) e que $I(P, F \cap G)$ é finito (por (1)). O caso em que $I(P, F \cap G) = 0$ é garantido por (2), então podemos seguir por indução. Assuma que $I(P, F \cap G) = n > 0$, e $I(P, A \cap B)$ pode ser calculado sempre que $I(P, A \cap B) < n$. Sejam $F(X, 0)$, $G(X, 0) \in k[X]$ de grau r e s respectivamente, onde r e s são iguais a zero se o polinômio se anula. Podemos supor $r \leq s$ (por (4)).

Caso 1: $r = 0$. Então Y divide F, logo $F = YH$ e

$$I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G)$$

(por (6)). Se $G(X, 0) = X^m(a_0 + a_1X + \cdots)$, com $a_0 \neq 0$, então $I(P, Y \cap G) = I(P, Y \cap G(X, 0)$ (por (7)), $I(P, Y \cap G(X, 0)) = I(P, Y \cap X^m) + I(P, Y \cap (a_0 + a_1X + \cdots))$ (por (6)) e como $P = (0, 0) \notin a_0 + a_1X + \cdots$, então $P \notin Y \cap (a_0 + a_1X + \cdots)$ e por (2), $I(P, Y \cap (a_0 + a_1X + \cdots)) = 0$, logo $I(P, Y \cap G) = I(P, Y \cap X^m) = m$ por (5). Como $P \in G$, $m > 0$, logo $I(P, H \cap G) < n$ e temos o resultado pelo argumento indutivo.

Caso 2: $r > 0$. Podemos multiplicar F e G por constantes para fazer $F(X,0)$ e $G(X,0)$ serem mônicos. Seja $H = G - X^{s-r}F$. Então $I(P, F \cap G) = I(P, F \cap H)$ (por (7)), e $deg(H(X,0)) = t < s$. Repetindo esse processo (trocando a ordem de F e H se $t < r$) um número finito de vezes, eventualmente chegaremos a um par de curvas A, B que entram no Caso 1 e com $I(P, F \cap G) = I(P, A \cap B)$. Isso conclui a prova.

Existência: Defina $I(P, F \cap G)$ como $dim_k(\mathfrak{O}_P(\mathbb{A}^2)/(F,G))$. Considere $\mathfrak{O} = \mathfrak{O}_P(\mathbb{A}^2)$ Mostraremos que as propriedades $(1)-(7)$ são satisfeitas. Como $I(P, F \cap G)$ depende apenas do ideal em $\mathfrak{O}_P$ gerado por F e G, as propriedades $(2), (4)$ e (7) são válidas diretamente, pois:

- Se $P \notin F \cap G$, então para toda fração $\frac{a}{b} \in \mathfrak{O}_P$, temos que $\frac{Fa}{Fb} \in \mathfrak{O}_P$ ou $\frac{Ga}{Gb} \in \mathfrak{O}_P$ (pois $Gb(P) \neq 0$ ou $Fb(P) \neq 0$). Assuma S.P.G que $\frac{Fa}{Fb} \in \mathfrak{O}_P$. Então $\frac{a}{b} + (F,G) = \frac{Fa}{Fb} + (F,G) = F\frac{a}{Fb} + (F,G) = 0 + (F,G)$. Portanto $\mathfrak{O}_P/(F,G) = \{0\}$ e temos que $dim_k(\mathfrak{O}_P/(F,G)) = 0$.

  Reciprocamente, se $I(P, F \cap G) = 0$, então $dim_k(\mathfrak{O}_P/(F,G)) = 0$ e $\mathfrak{O}_P/(F,G) = \{0\}$. Como $(F,G) \subset \mathfrak{O}_P$, então $(F,G) = \mathfrak{O}_P$. Assim $P \notin F \cap G$, pois dada qualquer constante não nula $a \in \mathfrak{O}_P$, $a(P) = a \neq 0$ e como $(F,G) = \mathfrak{O}_P$, então $a = AF + BG$, com $A, B \in \mathfrak{O}_P$ e $AF(P) + BG(P) = a(P) \neq 0$.

- $(F,G) = (G,F)$ e assim vale (4).

- $(F,G) = (F, G + AF)$, para todo $A \in k[X,Y]$, logo temos (7).

Como uma mudança afim de coordenadas induz um isomorfismo de anéis locais (Proposição 6.37), a propriedade (3) também será satisfeita pois teremos um isomorfismo entre $\mathfrak{O}_P/(F,G)$ e $\mathfrak{O}_Q/(F^T, G^T)$ e ambos terão a mesma dimensão enquanto espaços vetoriais, logo $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

Podemos assumir então que $P = (0,0)$ e que todas as componentes de F e G passam por P.

Se F e G não possuem componentes em comum, então $I(P, F \cap G)$ é finito pelo Corolário 3.2. Se F e G possuem uma componente em comum H, então $(F,G) \subset (H)$, assim existe um homomorfismo sobrejetor de $\mathfrak{O}/(F,G)$ para $\mathfrak{O}/(H)$ (Proposição 6.48), e $I(P, F \cap G) \geq dim_k(\mathfrak{O}/(H))$. No entanto, $\mathfrak{O}/(H)$ é isomorfo a $\mathfrak{O}_P(H)$ (Proposição 6.50) e $\Gamma(H) \subset \mathfrak{O}_P(H)$,

com $\Gamma(H)$ de dimensão infinita pelo Corolário 2.8 do Teorema dos Zeros de Hilbert. Isso prova a propriedade (1).

Para provar (6) é suficiente mostrar que $I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$ para quaisquer $F, G, H \in k[X, Y]$. Podemos assumir que F e GH não possuem componentes em comum, dado que o resultado é direto caso contrário. Seja $\phi : \mathfrak{O}/(F, GH) \to \mathfrak{O}/(F, G)$ o homomorfismo natural (Proposição 6.48), e defina um mapa k-linear $\phi : \mathfrak{O}/(F, G) \to \mathfrak{O}/(F, GH)$ como $\psi(\overline{z}) = \overline{Gz}$, $z \in \mathfrak{O}$ (onde a barra denota os resíduos). Pela Proposição 3.6, é suficiente mostrar que a sequência

$$0 \to \mathfrak{O}/(F, H) \xrightarrow{\psi} \mathfrak{O}/(F, GH) \xrightarrow{\phi} \mathfrak{O}/(F, G) \to 0$$

é exata.

Temos que ϕ é sobrejetora como resultado da Proposição 6.48, logo basta verificar que ψ é injetiva. Se $\psi(\overline{z}) = 0$, então $Gz = uF + vGH$, com $u, v \in \mathfrak{O}$. Tome $S \in k[X, Y]$ com $S(P) \neq 0$ e $Su = A$, $Sv = B$ e $Sz = C \in k[X, Y]$. Então $G(C - BH) = AF \in k[X, Y]$. Como F e G não possuem fatores em comum, F deve dividir $C - BH$, assim $C - BH = DF$, logo $\overline{z} = (B/S)H + (D/S)F$ e então $\overline{z} = 0$. Logo a sequência é exata e $dim_k(\mathfrak{O}/(F, GH)) = dim_k(\mathfrak{O}/(F, G)) + dim_k(\mathfrak{O}/(F, H))$.

Finalizaremos mostrando a propriedade (5). Seja $m = m_P(F)$, $n = m_P(G)$. Seja I um ideal em $k[X, Y]$ gerado por X e Y. Considere o seguinte diagrama de espaços vetoriais e transformações lineares:

$$\begin{array}{ccccccc} k[X,Y]/I^n \times k[X,Y]/I^m & \xrightarrow{\psi} & k[X,Y]/I^{m+n} & \xrightarrow{\phi} & k[X,Y]/(I^{m+n}, F, G) & \longrightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & \mathfrak{O}/(F,G) & \xrightarrow{\pi} & \mathfrak{O}/(I^{m+n}, F, G) & \longrightarrow & 0 \end{array}$$

onde ϕ, π e α são os homomorfismos naturais e ψ é definido como $\psi(\overline{A}, \overline{B}) = \overline{AF + BG}$.

Temos que ϕ e π são sobrejetivos, e como $V(I^{m+n}, F, G) \subset \{P\}$, α é um isomorfismo pelo Corolário 3.3. Dados $(\overline{A}, \overline{B}) \in k[X, Y]/I^n \times k[X, Y]/I^m$, temos que $\phi(\psi(\overline{A}, \overline{B})) = \phi(\overline{AF + GB}) = AF + BG + (Im + n, F, G) = (Im + n, F, G)$. E como ϕ é sobrejetiva, a linha de cima do diagrama é exata. Disso segue que

$$dim(k[X, Y]/I^n) + dim(k[X, Y]/I^m) \geq dim(Ker(\phi)),$$

com igualdade se, e somente se, ψ é injetiva, e assim

$$dim(k[X,Y]/(I^{m+n},F,G)) = dim(k[X,Y]/I^{m+n}) - dim(Ker(\phi)).$$

Juntando tudo, temos a seguinte cadeia de desigualdades:

$$\begin{aligned} I(P,F\cap G) &= dim(\mathfrak{O}/(F,G)) \geq dim(\mathfrak{O}/(I^{m+n},F,G)) \\ &= dim(k[X,Y]/(I^{m+n},F,G)) \\ &\geq dim(k[X,Y]/I^{m+n}) - dim(k[X,Y]/I^{n}) - dim(k[X,Y]/I^{m}) \\ &= mn \end{aligned}$$

(pela Proposição 6.52 e aritmética).

Isso mostra que $I(P,F\cap G)\geq mn$, e que $I(P,F\cap G)=mn$ se, e somente se, as duas desigualdades são igualdades. A primeira desigualdade é uma é uma igualdade se π é um isomorfismo, isto é, se $I^{m+n}\subset (F,G)\mathfrak{O}$. A segunda é uma igualdade se, e somente se, ψ é injetiva. A propriedade (5) é portanto uma consequência da seguinte afirmação

Afirmação 4.1. *(i) Se F e G não possuem tangentes em comum em P, então $I^t\subset (F,G)\mathfrak{O}$ para $t\geq m+n-1$.*

(ii) ψ é injetiva se, e somente se, F e G possuem tangentes distintas em P.

Demonstração de (a): Sejam $L_1,\ldots,L_m$ as tangentes de F em P, $M_1,\ldots,M_n$ as tangentes para G. Defin $L_i=L_m$ se $i>m$, $M_j=M_n$, se $j>n$, e seja $A_{ij}=L_1\cdots L_iM_1\cdots M_j$ para todos $i,j\geq 0$ ($A_{00}=1$). O conjunto $\{A_{ij}\mid i+j=t\}$ forma uma base do espaço vetorial de todas as formas de grau t em $k[X,Y]$ (Proposição 6.45 (c)).

Para provar (a), é suficiente mostrar que $A_{ij}\in(F,G)\mathfrak{O}$ para todos $i+j\geq m+n-1$. Mas $i+j\geq m+n-1$ implica que $i\geq m$ ou $j\geq n$. Seja $i\geq m$, então $A_{ij}=A_{m0}B$ onde B é uma forma de grau $t=i+j-m$. Escreva $F=A_{m0}+F'$, onde os termos de F' são de grau maior ou igual a $m+1$. Então $A_{ij}=BF-BF'$, onde cada termo de BF' possui grau maior ou igual $i+j+1$. Está provado então se mostrarmos que $I^t\subset(F,G))\mathfrak{O}$ para todo t suficientemente grande.

Esse fato é uma consequência do Teorema dos Zeros: Seja $V(F,G)=\{P,Q_1,\ldots,Q_s\}$, e escolha um polinômio H, tal que $H(Q_i)=0$, $H(P)\neq 0$ (Proposição 6.10). Então HX e HY

pertencem a $I(V(F,G))$, logo $(HX)^N$, $(HY)^N \in (F,G) \subset k[X,Y]$ para algum N. Como H^N é uma unidade em $\mathfrak{O}$, X^N e Y^N pertencem a $(F,G)\mathfrak{O}$ e portanto $I^{2N} \subset (F,G)\mathfrak{O}$, como desejado.

Demonstração de (b): Suponha que as tangentes são distintas e que

$$\psi(\overline{A},\overline{B}) = \overline{AF+BG} = 0,$$

isto é, $AF+BG$ consiste de termos de grau maior ou igual a $m+n$. Suponha que $r<m$ ou $s<n$. Escreva $A = A_r +$ termos de maior grau, $B = B_s + \cdots$, assim $AF+BG = A_rF_m + B_sG_n + \cdots$. Então devemos ter que $r+m = s+n$ e $A_rF_m = -B_sG_n$. Mas F_m e G_n não possuem fatores em comum, então F_m divide B_s e G_n divide A_r. Portanto $s \geq m$, $r \geq n$, logo $(\overline{A},\overline{B}) = 0$.

Reciprocamente, se L é uma tangente comum a F e G em P, escreva $F_m = LF'_{m-1}$ e $G_n = LG'_{n-1}$. Então $\psi(\overline{G'_{n-1}},\overline{F'_{m-1}}) = 0$, logo ψ não é injetiva. Isso completa a demonstração da Afirmação e também o Teorema 4.3. □

Exemplo 4.2. *Calcularemos $I(P,E\cap F)$, onde $E = (X^2+Y^2)^2+3X^2Y-Y^3$, $F = (X^2+Y^2)^3-4X^2Y^2$ e $P=(0,0)$. Podemos simplificar os termos de F tomando $F-(X^2+Y^2)E = Y((X^2+Y^2)(Y^2-3X^2)-4X^2Y) = YG$, no lugar de F (pela propriedade (7)). Aplicaremos o processo de unicidade para remover os termos com X: No lugar de G, tome $G+3E = Y(5X^2-3Y^2+4Y^3+4X^2Y) = YH$. Então $I(P,E\cap F) = 2I(P,E\cap Y)+I(P,E\cap H)$. Mas $I(P,E\cap Y) = I(P,X^4\cap Y) = 4$ (por (7) e (6)), e $I(P,E\cap H) = m_P(E)m_P(H) = 6$ (por (5)). Então $I(P,E\cap F) = 14$.*

Mais duas propriedades do número de interseção serão úteis posteriormente. A primeira delas pode também ser utilizada para facilitar os cálculos.

(8) Se P é um ponto simples de F, então $I(P,F\cap G) = ord_P^F(G)$

Demonstração: Podemos assumir que F é irredutível. Se g é a imagem de G em $\mathfrak{O}_P(F)$, então $ord_P^F(G) = dim_k(\mathfrak{O}_P/(g))$ (Proposição 6.54 (c)). Como $\mathfrak{O}_P(F)/(g)$ é isomorfo a $\mathfrak{O}_P(\mathbb{A}^2)/(F,G)$ (Proposição 6.50), sua dimensão é $I(P,F\cap G)$.

(9) Se F e G não possuem componentes em comum, então

$$\sum_P I(P,F\cap G) = dim_k(k[X,Y]/(F,G))$$

A propriedade (9) será uma consequência do Corolário 3.2.

Proposição 4.1. *A reta L é tangente à curva F no ponto P se, e somente se, $I(P, F \cap L) > m_P(F)$.*

Demonstração. Podemos assumir que $P = (0, 0)$ com uma mudança de coordenadas afim adequada e que $P \in F \cap L$. Como L é uma reta, então $m_P(L) = 1$. Pela Propriedade (5) do número de interseção, temos que $I(P, F \cap L) \geq m_P(F)m_P(L) = m_P(F)$, com igualdade se, e somente se, F e L não possuem retas tangentes em P em comum, como L é uma reta, sua única tangente em P é a própria L, logo se F e L não possuem tangentes em comum em P então L não é tangente a F em P e temos a proposição. □

Capítulo 5

Variedades Projetivas

5.1 Espaço Projetivo

Suponha que desejamos estudar todos os pontos de interseção de duas curvas, considere por exemplo a curva $Y^2 = X^2 + 1$ e a reta $Y = \alpha X$, $\alpha \in k$. Se $\alpha \neq \pm 1$, elas se intersectam em dois pontos. No caso em que $\alpha = \pm 1$ elas não se intersectam, mas a curva é assintótica à reta. Queremos expandir o plano de forma que duas curvas desse tipo se intersectem "no infinito".

Uma forma de conseguir isso é identificar cada ponto $(x, y) \in \mathbb{A}^2$ com o ponto $(x, y, 1) \in \mathbb{A}^3$. Todo ponto $(x, y, 1)$ define uma reta em $\mathbb{A}^3$ que passa por $(0, 0, 0)$ e $(x, y, 1)$. As retas que passam por $(0, 0, 0)$, exceto as no plano $z = 0$, correspondem a exatamente um desses pontos. As retas que passam por $(0, 0, 0)$ no plano $z = 0$ podem ser pensadas como "pontos no infinito". Isso nos direciona para a seguinte definição:

Definição 5.1. *Seja k um corpo qualquer. O n-Espaço Projetivo sobre k, escrito $\mathbb{P}^n(k)$, ou simplesmente $\mathbb{P}^n$, é definido como o conjunto de todas as retas que passam por $(0, 0, \ldots, 0)$ em $\mathbb{A}^{n+1}(k)$. Qualquer ponto $(x) = (x_1, \ldots, x_{n+1}) \neq (0, 0, \ldots, 0)$ define uma única reta, no caso $\{\lambda x_1, \ldots, \lambda x_{n+1} \mid \lambda \in k\}$. Dois pontos (x) e (y) determinam a mesma reta se, e somente se, existe um $\lambda \in k$ não nulo tal que $y_i = \lambda x_i$ para $i = 1, \ldots, n + 1$, e diremos que (x) e (y) são equivalentes se esse é o caso. Então $\mathbb{P}^n$ pode ser identificado como o conjunto das classes de equivalência em $\mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\}$.*

Elementos de $\mathbb{P}^n$ serão chamados de pontos. Se um ponto $P \in \mathbb{P}^n$ é determinado por algum $(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}$, dizemos que $(x_1, \ldots, x_{n+1})$ são as coordenadas homogêneas de P. Denotaremos $P = [x_1 : \cdots : x_{n+1}]$ para indicar que $(x_1, \ldots, x_{n+1})$ são coordenadas homogeneas de P.

Definição 5.2. *Definimos* $U_i = \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n \mid x_i \neq 0\}$. *Cada* $P \in U_i$ *pode ser escrito unicamente na forma*

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

As coordenadas $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1})$ *são chamadas de coordenadas não homogêneas de* P *com respeito a* U_i *(ou* X_i*, ou simplesmente* i*). Se definirmos* $\phi_i : \mathbb{A}^n \to U_i$ *como* $\phi_i(a_1, \ldots, a_n) = [a_1 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n]$*, então* ϕ_i *é uma correspondência um para um entre os pontos de* $\mathbb{A}^n$ *e os pontos de* U_i*. Note que* $\mathbb{P}^n = \cup_{i=1}^{n+1} U_i$*, então* $\mathbb{P}^n$ *é coberto por* $n+1$ *conjuntos que se parecem com o* n*-espaço afim.*

Por conveniência, nos concentraremos em U_{n+1}.

Definição 5.3. *Defina*

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

H_∞ *é chamado de hiperplano no infinito. A correspondência* $[x_1 : \cdots : x_n : 0] \iff [x_1 : \cdots : x_n]$ *mostra que* H_∞ *pode ser identificado com* $\mathbb{P}^{n-1}$*. Logo* $\mathbb{P}^n = U_{n+1} \cup H_\infty$ *é a união de um* n*-espaço afim e um conjunto que dá todas as direções no* n*-espaço afim.*

Exemplo 5.1. *(i)* $\mathbb{P}^0(k)$ *é um ponto.*

(ii) $\mathbb{P}^1(k) = \{[x : 1] \mid x \in k\} \cup \{[1 : 0]\}$. $\mathbb{P}^1(k)$ *é a reta afim mais um ponto no infinito.* $\mathbb{P}^1(k)$ *é a reta projetiva sobre* k*.*

(iii) $\mathbb{P}^2(k) = \{[x : y : 1] \mid (x, y) \in \mathbb{A}^2\} \cup \{[x : y : 0] \mid [x : y] \in \mathbb{P}^1\}$. *Aqui* H_∞ *é chamada de reta no infinito.* $\mathbb{P}^2(k)$ *é o plano projetivo sobre* k*.*

(iv) Considere a reta $Y = mX + b$ em $\mathbb{A}^2$. Se identificarmos $\mathbb{A}^2$ com $U_3 \subset \mathbb{P}^2$, os pontos da reta correspondem aos pontos $[x : y : z] \in \mathbb{P}^2$ com $y = mx + bz$ e $z \neq 0$ (devemos tornar a equação homogenea para que as soluções sejam invariantes sobre a relação de equivalência). O conjunto $\{[x : y : z] \in \mathbb{P}^2 \mid y = mx + bz\} \cap H_\infty = [1 : m : 0]$. Então todas as retas com o mesmo coeficiente angular, quando estendidas dessa maneira, passam pelo mesmo ponto no infinito.

(v) Considere novamente a curva $Y^2 = X^2 + 1$. O conjunto correspondente em $\mathbb{P}^2$ é dado pela equações homogenea $Y^2 = X^2 + Z^2$, $Z \neq 0$. O conjunto $\{[x : y : z] \in \mathbb{P}^2 \mid y^2 = x^2 + z^2\}$ intersecta H_∞ nos pontos $[1 : 1 : 0]$ e $[1 : -1 : 0]$. Esses são os pontos onde as retas $Y = X$ e $Y = -X$ intersectam a curva.

5.2 Conjuntos Algébricos Projetivos

Nessa seção desenvolveremos o conceito de conjuntos algébricos em $\mathbb{P}^n = \mathbb{P}^n(k)$.

Um ponto $P \in \mathbb{P}^n$ é dito um zero de um polinômio $F \in k[X_1, \ldots, X_{n+1}]$ se

$$F(x_1, \ldots, x_{n+1}) = 0$$

para toda escolha de coordenadas homogêneas $(x_1, \ldots, x_{n+1})$ de P, escrevemos então $F(P) = 0$. Se F é uma forma, e F se anula em uma escolha de coordenadas de P, então F se anula em qualquer escolha de coordenadas de P.

Se escrevermos F como uma soma de formas, então cada forma se anula em qualquer conjunto de coordenadas homogêneas de P (Proposição 6.55).

Para qualquer conjunto S de polinômios em $k[X_1, \ldots, X_{n+1}]$, definimos

$$V(S) = \{P \in \mathbb{P}^n \mid P \text{ é um zero de cada } F \in S\}$$

Se I é o ideal gerado por S, $V(I) = V(S)$. Se $I = (F^{(1)}, \ldots, F^{(r)})$, onde $F^{(i)} = \sum F_j^{(i)}$, $F_j^{(i)}$ uma forma de grau j, então $V(I) = V(\{F_j^{(i)}\})$, então $V(S) = V(\{F_j^{(i)}\})$ é o conjunto de zeros de um número finito de formas. Um conjunto desse tipo é denominado um **conjunto algébrico** de $\mathbb{P}^n$, ou um **conjunto algébrico projetivo**.

Para qualquer conjunto $X \subset \mathbb{P}^n$, definimos $I(X) = \{F \in k[X_1, \ldots, X_{n+1}] \mid \forall P \in X,\ F(P) = 0\}$, e $I(X)$ será um ideal de $k[X_1, \ldots, X_{n+1}]$, $I(X)$ é denominado o **ideal de** X.

Um ideal $I \subset k[X_1, \ldots, X_{n+1}]$ é chamado de um **ideal homogêneo** se para todo $F = \sum_{i=0}^{m} F_i \in I$, F_i uma forma de grau i, temos também que $F_i \in I$ para todo i. Para qualquer conjunto $X \subset \mathbb{P}^n$, $I(X)$ é um ideal homogêneo.

Proposição 5.1. *Um ideal $I \subset k[X_1, \ldots, X_{n+1}]$ é homogêneo se, e somente se, é gerado por um conjunto (finito) de formas.*

Demonstração. Se $I = (F^{(1)}, \ldots, F^{(r)})$ é homogêneo, então I é gerado por $\{F_j^{(i)}\}$. Reciprocamente, seja $S = \{F^\alpha\}$ um conjunto de formas gerando o ideal I, com $deg(F^\alpha) = d_\alpha$, e suponha $F = F_m + \cdots + F_r \in I$, $deg(F_i) = i$. É suficiente mostrar que $F_m \in I$, pois então $F - F_m \in I$ e um argumento indutivo finaliza a demonstração. Escreva $F = \sum A^{(\alpha)} F^{(\alpha)}$. Comparando os termos com mesmo grau, concluímos que $F_m = \sum A^{(\alpha)}_{m-d_\alpha} F^{(\alpha)}$, então $F_m \in I$. □

Um conjunto algébrico $V \subset \mathbb{P}^n$ é **irredutível** se não é a união de dois conjuntos algébricos distintos e não vazios (i.e $V \neq A \cup B$, com $A, B \neq \emptyset$ conjuntos algébricos e $A \neq B$).

Seguindo a mesma demonstração para o caso afim, temos que V é irredutível se, e somente se, $I(V)$ é primo. Um conjunto irredutível de $\mathbb{P}^n$ é chamado de uma **Variedade Projetiva**. Todo conjunto algébrico projetivo pode ser escrito unicamente como uma união de variedades projetivas, suas componentes irredutíveis.

As operações

$$V : \{\text{Ideais Homogêneos de } k[X_1, \ldots, X_{n+1}]\} \to \{\text{Conjuntos Algébricos em } \mathbb{P}^n(k)\}$$

$$I : \{\text{Conjuntos Algébricos em } \mathbb{P}^n(k)\} \to \{\text{Ideais Homogêneos de } k[X_1, \ldots, X_{n+1}]\}$$

satisfazem as propriedades das Proposições 2.1 e 2.2 para o caso afim, e utilizamos a mesma notação para as operações no caso afim e projetivo. No geral, será claro qual das operações estaremos utilizando (o caso afim ou projetivo), caso haja espaço para confusão, escreveremos V_p, I_p para as operações projetivas e V_a, I_a para as afim.

Definição 5.4. *Se V é um conjunto algébrico em $\mathbb{P}^n$, definimos*

$$C(V) = \{(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1} \mid [x_1 : \cdots : x_{n+1}] \in V \text{ } ou \text{ } (x_1, \ldots, x_{n+1}) = (0, \ldots, 0)\}$$

como o ***cone*** *sobre* V.

Se $V \neq \emptyset$, então $I_a(C(V)) = I_p(V)$; e se I é um ideal homogêneo em $k[X_1, \ldots, X_{n+1}]$ tal que $V_p(I) \neq \emptyset$, então $C(V_p(I)) = V_a(I)$. Isso reduz muitas questões sobre $\mathbb{P}^n$ para questões sobre $\mathbb{A}^{n+1}$

Teorema 5.1. *(**Teorema dos Zeros Projetivo**) Seja I um ideal homogêneo em $k[X_1, \ldots, X_{n+1}]$. Então*

(1) $V_p(I) = \emptyset$ se, e somente se, existe um inteiro N tal que I contém todas as formas de grau maior que N.

(2) Se $V_p(I) \neq \emptyset$, então $I_p(V_p(I)) = Rad(I)$.

Demonstração. **(1)** Temos as seguintes equivalências:

(i) $V_p(I) = \emptyset$;

(ii) $V_a(I) \subset \{(0, \ldots, 0)\}$;

(iii) $Rad(I) = I_a(V_a(I)) \supset (X_1, \ldots, X_{n+1})$ (Pelo Teorema dos Zeros Afim);

(iv) $(X_1, \ldots, X_{n+1})^N \subset I$

$(i) \Rightarrow (ii)$: Como $\mathbb{P}^n = \mathbb{A}^{n+1}/\{(0, \ldots, 0)\}$, temos que se $V_p(I) = \emptyset$ então $V_a(I) = \{(0, \ldots, 0)\}$ ou $V_a(I) = \emptyset$ e $V_a(I) \subset \{(0, \ldots, 0)\}$ em ambos os casos.

$(ii) \Rightarrow (iii)$: Se $V_a(I) \subset \{(0, \ldots, 0)\}$, então $V_a(I) = \emptyset$ ou $V_a(I) = (0, \ldots, 0)$. Se $V_a(I) = (0, \ldots, 0)$, pelo Teorema dos Zeros, $I_a(V_a(I)) = Rad(I)$ e assim $Rad(I) = I_a(\{(0, \ldots, 0)\}) = (X_1, \ldots, X_{n+1})$ e se $V_a(I) = \emptyset$, então $I = k[X_1, \ldots, X_{n+1}]$ e $(X_1, \ldots, X_{n+1}) \subset Rad(I)$.

$(iii) \Rightarrow (iv)$: Se $(X_1, \ldots, X_{n+1}) \subset Rad(I)$, então existe $m \in \mathbb{N}$ tal que $X_i \in I$ para todo $i = 1, \ldots, n+1$. Assim para qualquer produto $X_1^{i_1} \cdots X_{n+1}^{i_{n+1}}$ tal que $\sum_{j=1}^{n+1} i_j = m(n+1)$, deve existir ao menos um j tal que $i_j > m$ e assim $X_j^{i_j} \in I$ e assim $X_1^{i_1} \cdots X_{n+1}^{i_{n+1}} \in I$. Portanto $(X_1, \ldots, X_{n+1})^{m(n+1)} \subset I$.

$(iv) \Rightarrow (i)$ Se $(X_1, \ldots, X_{n+1})^N \subset I$, então se $P \in V_p(I)$ temos que $X_i^N \in I$ para todo $i = 1, \ldots, n+1$. Mas o único ponto afim que anula X_i^N para todo i é $P = (0, \ldots, 0)$. Assim $V_a(I) \subset \{(0, \ldots, 0)\}$, logo $V_a(I) = \{(0, \ldots, 0)\}$ e então $C(V_p(I)) = \{(0, \ldots, 0)\}$ o que implica que $V_p(I) = \emptyset$ e o mesmo vale para o caso $V_a(I) = \emptyset$ (note que essa afirmação é explicitamente $(ii) \Rightarrow (i)$).

Provadas as equivalências, temos o resultado desejado.

(2) $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = Rad(I)$.

□

Os corolário usuais do Teorema dos Zeros também se mantém, exceto que sempre devemos manter uma exceção com o ideal $(X_1, \ldots, X_{n+1})$. Em particular, temos uma correspondência um para um entre hipersuperfícies projetivas $V = V(F)$ e as formas (não constantes) F que definem V, considerando que F não possui multiplos fatores (F é determinado até multiplicação por um $\lambda \in k$ não nulo). Hipersuperfícies irredutíveis correspondem a formas irredutíveis. Um hiperplano é uma hipersuperfície definida por uma forma de grau 1. Os hiperplanos $V(X_i)$, $i = 1, \ldots, n+1$, são chamados de hiperplanos coordenados, ou hiperplanos no infinito com respeito a U_i. Se $n = 2$, os três $V(X_i)$ são os três eixos de coordenadas.

Definição 5.5. *Seja V uma variedade projetiva não vazia em $\mathbb{P}^n$. Então $I(V)$ é um ideal primo e o anel de resíduos $\Gamma_h(V) = k[X_1, \ldots, X_{n+1}]/I(V)$ é um domínio, e é denominado o* ***anel coordenado homogêneo*** *de V.*

De forma mais geral, seja I um ideal homogêneo qualquer em $k[X_1, \ldots, X_{n+1}]$ e seja $\Gamma = k[X_1, \ldots, X_{n+1}]/I$. Um elemento $f \in \Gamma$ será denominado uma forma de grau d se existe uma forma $F \in k[X_1, \ldots, X_{n+1}]$ de grau d cujo resíduo é f.

Proposição 5.2. *Todo elemento $f \in \Gamma$ pode ser escrito unicamente como $f = f_0 + \cdots + f_m$, com f_i uma forma de grau i.*

Demonstração. Se f é o resíduo de $F \in k[X_1, \ldots, X_{n+1}]$, escreva $F = \sum F_i$, onde cada F_i é uma forma de grau i, e então $f = \sum f_i$. Para mostrar a unicidade, suponha que $f = \sum g_i$, com g_i resíduo de G_i para todo i. Então $F - \sum G_i = \sum (F_i - G_i) \in I$, e como I é homogêneo, cada $F_i - G_i \in I$, logo $f_i = g_i$ para todo i.

□

Seja $k_h(V)$ o corpo de frações de $\Gamma_h(V)$, o qual denominaremos o corpo de frações homogêneas de V. Em contraste com as variedades afins, apenas as constantes de $k_h(V)$ determinam funções em V, e a maioria dos elementos de $k_h(V)$ não podem ser considerados funções. No entanto se f e g são ambas formas de grau d em $\Gamma(V)$, então $\dfrac{f}{g}$ define uma função, ao menos nos pontos onde g não se anula, pois $\dfrac{f(\lambda x)}{g(\lambda x)} = \dfrac{\lambda^d f(x)}{\lambda^d g(x)} = \dfrac{f(x)}{g(x)}$, assim o valor de $\dfrac{f}{g}$ independe da escolha de coordenadas homogêneas.

O corpo de funções de V, escrito $k(V)$ é definido como $\{z \in k_h(V) \mid z = \dfrac{f}{g},\ f,g \in \Gamma_h(V), \text{com f,g formas de mesmo grau}\}$. Elementos de $k(V)$ são chamados de funções racionais em V.

Seja $P \in V$, $z \in k(V)$. Dizemos que z está definido em P se z pode ser escrito como $z = \dfrac{f}{g}$, f, g formas de mesmo grau, e $g(P) \neq 0$. Definimos

$$\mathfrak{O}_P(V) = \{z \in k(V) \mid z \text{ está definido em } P\};$$

$\mathfrak{O}_P(V)$ é um subanel de $k(V)$, e é um anel local com ideal maximal

$$\mathfrak{m}_P(V) = \{z \mid z = \frac{f}{g},\ g(P) \neq 0,\ f(P) = 0\}.$$

$\mathfrak{O}_P(V)$ é chamado de **anel local** de V em P. O valor $z(P)$ de uma função $z \in \mathfrak{O}$ é bem definido.

Se $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ é uma mudança linear de coordenadas, então T leva retas que passam pela origem para retas que passam pela origem (Proposição 6.35). Assim T define uma função de $\mathbb{P}^n$ para $\mathbb{P}^n$, chamada de **mudança de coordenadas projetivas**.

Se V é um conjunto algébrico em $\mathbb{P}^n$, então $T^{-1}(V)$ também é um conjunto algébrico em$\mathbb{P}^n$. Escreveremos V^T para $T^{-1}(V)$. Se $V = V(F_1, \ldots, F_r)$, e $T = (T_1, \ldots, T_{n+1})$, com T_i's formas de grau 1, então $V^T = V(F_1^T, \ldots, F_r^T)$, onde $F_i^T = F_i(T_1, \ldots, T_{n+1})$. Então V é uma variedade se, e somente se, V^T é uma variedade, e T induz isomorfismos $\tilde{T} : \Gamma_h(V) \to \Gamma_h(V^T)$, $k(V) \to k(V^T)$ e $\mathfrak{O}_P(V) \to \mathfrak{O}_P(V^T)$ se $T(Q) = P$.

5.3 Variedades Afins e Projetivas

Consideramos $\mathbb{A}^n$ como um subconjunto de $\mathbb{P}^n$, pelo mapa $\phi_{n+1} : \mathbb{A}^n \to U_{n+1} \subset \mathbb{P}^n$. Nesta seção estudaremos as relações entre os conjuntos algébricos em $\mathbb{A}^n$ e os em $\mathbb{P}^n$.

Seja V um conjunto algébrico em $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$. Seja I^* o ideal em $k[X_1, \ldots, X_{n+1}]$ gerado por $\{F^* \mid F \in I\}$ (com a notação da seção 3.6). Esse ideal I^* é homogêneo. Definimos V^* como $V(I^*) \subset \mathbb{A}^n$.

Reciprocamente, seja V um conjunto algébrico em $\mathbb{P}^n$, $I = I(V) \subset k[X_1, \ldots, X_{n+1}]$. Seja I_* o ideal em $k[X_1, \ldots, X_n]$ gerado por $\{F_* \mid F \in I\}$. Definimos V_* como $V(I_*) \subset \mathbb{A}^n$.

Proposição 5.3. *(1) Se $V \subset \mathbb{A}^n$, então $\phi_{n+1}(V) = V^* \cap U_{n+1}$, e $(V^*)_* = V$.*

(2) Se $V \subset W \subset \mathbb{A}^n$, então $V^* \subset W^* \subset \mathbb{P}^n$.

(3) Se V é irredutível em $\mathbb{A}^n$,então V^* é irredutível em $\mathbb{P}^n$.

(4) Se $V = \cup_i V_i$ é a decomposição em irredutíveis de V em $\mathbb{A}^n$, então $V^* = \cup_i V_i^*$ é a decomposição em irredutíveis de V^* em $\mathbb{P}^n$.

(5) Se $V \subset \mathbb{A}^n$, então V^* é o menor conjunto algébrico em $\mathbb{P}^n$ que contém $\phi_{n+1}(V)$.

(6) Se $V \subsetneq \mathbb{A}^n$ é não vazio, então nenhuma componente de V^* está contida ou contém $H_\infty = \mathbb{P}^n/U_{n+1}$.

(7) Se $V \subset \mathbb{P}^n$, e nenhuma componente de V está contida ou contém H_∞, então $V_* \subsetneq \mathbb{A}^n$ e $(V_*)^* = V$.

Demonstração. O item (1) segue da Proposição 6.44, pois dado $P = (a_1, \ldots, a_n) \in V$, $\phi_{n+1}(P) = [a_1 : \cdots : a_n : 1]$, e para todo gerador $F^* \in I^*$, $F^*([a_1 : \cdots : a_n : 1]) = F(a_1, \ldots, a_n) = 0$, logo $\phi_{n+1}(P) \in V^* \cap U_{n+1}$ e temos que $\phi_{n+1}(V) \subset V^* \cap U_{n+1}$. Reciprocamente, dado $P \in V^* \cap U_{n+1}$, então $P \in V^*$ o que implica que para todo gerador $F^* \in I^*$, $F^*(P) = 0$, e $P \in U_{n+1}$, então $P = [a_1 : \cdots : a_n : 1]$. Assim $F(a_1, \ldots, a_n) = F^*([a_1 : \cdots : a_n : 1]) = F(a_1, \ldots, a_n) = 0$ para todo $F \in I$. Logo $P \in \phi_{n+1}(V)$.

A outra afirmação do item (1) é resultado da Proposição 6.44, especificamente $F = (F^*)_*$.

O item (2) é direta, dado como $V \subset W$, então $I(V) \supset I(W)$, assim $I^*(V) \supset I^*(W)$ e portanto $V^* = V(I^*(V)) \subset V(I^*(W)) = W^*$.

Se $V \subset \mathbb{A}^n$, $I = I(V)$, então uma forma F pertence a I^* se, e somente se, $F_* \in I$. Se I é primo, segue prontamente que I^* é primo, o que prova o item (3).

Para provar (5), suponha que W é um conjunto algébrico de $\mathbb{P}^n$ que contém $\phi_{n+1}(V)$. Se $F \in I(W)$, então $F_* \in I(V)$, assim $F = X_{n+1}^r (F_*)^* \in I(V)^*$. Portanto, $I(W) \subset I(V)^*$, então $W \supset V^*$, como desejado.

O item (4) vem dos itens (2), (3) e (5), pois se $V = \cup_i V_i$, então

Para provar (6) podemos assumir que V é irredutível. $V^* \subset \not H_\infty$ por (1). Se $V^* \supset H_\infty$, então $I(V)^* \subset I(V^*) \subset I(H_\infty) = (X_{n+1})$. Mas se $0 \neq F \in I(V)$, então $F^* \in I(V^*)$, com $F^* \notin (X_{n+1})$. Logo $V^* \supset \not H_\infty$.

Para o item (7), novamente, podemos assumir que $V \subset \mathbb{P}^n$ é irredutível. Dado que $\phi_{n+1}(V_*) \subset V$, é suficiente mostrar que $V \subset (V_*)^*$, ou que $I(V_*)^* \subset I(V)$. Seja $F \in I(V_*)$. Então $F^N \in I(V)_*$ para algum N (pelo Teorema dos Zeros), assim $X_{n+1}^t (F^N)^* \in I(V)$ para

algum t (pela Proposição 6.44). Mas $I(V)$ é primo, e $X_{n+1} \notin I(V)$ dado que $V \not\subset H_\infty$, então $F^* \in I(V)$, como desejado.

□

Se V é um conjunto algébrico em $\mathbb{A}^n$, $V^* \subset \mathbb{P}^n$ é chamado de fecho projetivo de V. Se $V = V(F)$ é uma hipersuperfície afim, então $V^* = V(F^*)$ (pela Proposiçãp 6.64). Exceto para variedades contidas em H_∞, existe uma correspondência um para um natural entre variedades afim não vazias e variedades projetivas (pela Proposição 6.65).

Seja V uma variedade afim, $V^* \subset \mathbb{P}^n$ seu fecho projetivo. Se $f \in \Gamma_h(V^*)$ é uma forma de grau d, podemos definir $f_* \in \Gamma(V)$ da seguinte maneira: Tome uma forma $F \in k[X_1, \ldots, X_{n+1}]$ cujo $I_p(V^*)$-resíduo é f, e seja f_* o $I(V)$-resíduo de F_* (essa identificação é independente da escolha de F). Definimos então um isomorfismo natural $\alpha : k(V^*) \to k(V)$ da seguinte maneira: $\alpha(\frac{f}{g}) = \frac{f_*}{g_*}$, onde f, g são formas de mesmo grau em V^*. Se $P \in V$, podemos considerar $P \in V^*$ (por meio de ϕ_{n+1}) e então α induz um isomorfismo de $\mathfrak{O}_P(V^*)$ para $\mathfrak{O}_P(V)$. Utilizaremos α para identificar $k(V)$ com $k(V^*)$ e $\mathfrak{O}_P(V)$ com $\mathfrak{O}_P(V^*)$.

Qualquer variedade projetiva $V \subset \mathbb{P}^n$ é coberta pelos $n+1$ conjuntos $V \cap U_i$. Se formarmos V_* com respeito aos U_i (assim como U_{n+1}) os pontos em $V \cap U_i$ correspondem aos pontos em V_*, e os anéis locais são isomorfos. Assim questões sobre V perto de um ponto P podem ser reduzidas a questões sobre uma variedade afim V_* (ao menos se a questão pode ser respondinda ao olharmos para $\mathfrak{O}_P(V)$).

Capítulo 6

Curvas Planas Projetivas

Definição 6.1. *Uma **curva plana projetiva** é uma hipersuperfície em $\mathbb{P}^2$, exceto que, assim como curvas planas afins, desejamos permitir múltiplas componentes: Dizemos que duas formas não constantes $F, G \in k[X, Y, Z]$ são equivalentes se existe um $\lambda \in k$ tal que $G = \lambda F$. Uma curva plana projetiva é uma classe de equivalência de formas.O grau de uma curva é o grau de uma forma que define a curva.*

Curvas de grau $1, 2, 3$ e 4 são chamadas retas, conicas, cubicas e quarticas respectivamente.

Utilizaremos as mesmas notações e convenções de curvas afins: assim falaremos sobre componentes simples e múltiplas, e escreveremos $\mathfrak{O}_P(F)$ ao invés de $\mathfrak{O}_P(V(F))$ para um F irredutível. Note que quando $P = [x : y : 1]$, então $\mathfrak{O}_P$ é canonicamente isomorfo a $\mathfrak{O}_{(x,y)}(F_*)$, onde $F_* = F(X, Y, 1)$, é a curva afim correspondente.

Os resultados de curvas afins nos garantem que a multiplicidade de um ponto em uma curva depende apenas do anel local da curva naquele ponto. Então se F é uma curva plana projetiva, $P \in U_i$ ($i = 1, 2$ ou 3), podemos dehomogenizar F com respeito a X_i e definir a multiplicidade de F em P, $m_P(F)$, como $m_P(F_*)$. A multiplicidade é independente da escolha de U_i, e invariante sobre mudanças de coordenadas projetivas.

A seguinte notação será útil. Se consideramos um conjunto finito de pontos $P_1, \ldots, P_n \in \mathbb{P}^2$, podemos sempre encontrar uma reta L que não passa por nenhum dos pontos (6.67). Se F é uma curva de grau d, definimos $F_* = F/L^d \in k(\mathbb{P}^2)$. Essa F_* depende de L, mas se L' é outra reta na mesmas condições de L, então $F/(L')^d = (L/L')^d F_*$ e (L/L') é uma unidade em cada um dos $\mathfrak{O}_{P_i}(\mathbb{P}^2)$. Note também que sempre podemos encontrar uma mudança de coordenadas projetiva tal que a reta L se torne a reta Z no infinito: então, sobre a

identificação de $k(\mathbb{A}^2)$ com $k(\mathbb{P}^2)$, esta F_* é a mesma que $F_* = F(X, Y, 1)$.

Se P é um ponto simples de F (i.e., $m_P(F) = 1$), e F é irredutível, então $\mathfrak{O}_P(F)$ é um AAD. Denotaremos a correspondente função de ordem em $k(F)$ por ord_P^F. Se G é uma forma em $k[X, Y, Z]$, $G_* \in \mathfrak{O}_P(\mathbb{P}^2)$ definido como no parágrafo anterior, e $\overline{G}_*$ é o resíduo de G_* em $\mathfrak{O}_P(F)$, definimos $ord_P^F(G)$ como $ord_P^F(\overline{G}_*)$. Equivalentemente, $ord_P^F(G)$ é a ordem de G/H em P, onde H é qualquer forma de mesmo grau que G e $H(P) \neq 0$.

Definição 6.2. *Sejam F, G curvas projetivas planas e $P \in \mathbb{P}^2$. Definimos o* ***número de interseção*** *$I(P, F \cap G)$ como $dim_k(\mathfrak{O}_P(\mathbb{P}^2)/(F_*, G_*))$. Isso independe da forma como F_* e G_* são formados, e satisfaz as Propriedades (1)−(8) de Curvas Afins com algumas ressalvas: na Propriedade (3), T deve ser uma mudança de coordenadas projetiva, e em (7), A deve ser uma forma com $deg(A) = deg(G) - deg(F)$.*

Podemos definir uma reta L como sendo tangente à curva F em P se $I(P, F \cap L) > m_P(F)$ (Proposição 4.1). Um ponto P em F é um ponto múltiplo ordinário de F se F possui $m_P(F)$ tangentes distintas em P.

Duas curvas F e G são ditas projetivamente equivalentes se existe uma mudança de coordenadas projetiva T tal que $G = F^T$. Todas as propriedades que destacarmos serão as mesmas para duas curvas projetivamente equivalentes.

6.1 Sistemas Lineares de Curvas

Muitas vezes queremos estudar todas as curvas de um dado grau $d \geq 1$. Seja $M_1, \ldots, M_N$ uma ordenação fixada do conjunto de monomios em $k[X, Y, Z]$ de grau d, onde N é $\frac{1}{2}(d + 1)(d + 2)$ (Proposição 6.45). Escolher uma curva F de grau d é o mesmo que escolher $a_1, \ldots, a_N \in k$, não todos nulos, e definindo $F = \sum a_i M_i$, exceto que $(a_1, \ldots, a_N)$ e $(\lambda a_1, \ldots, \lambda a_N)$ determinam a mesma curva. Em outras palavras, cada curva F de grau d corresponde a um único ponto em $\mathbb{P}^{N-1} = \mathbb{P}^{d(d+3)/2}$ e cada ponto de $\mathbb{P}^{d(d+3)/2}$ representa uma curva única. Frequentemente identificamos F com seu ponto correspondente em $\mathbb{P}^{d(d+3)/2}$, e diremos "as curvas de grau d formam um espaço projetivo de dimensão $d(d + 3)/2$".

Exemplo 6.1. *(1) Seja $d = 1$. Cada reta $aX + bY + cZ$ corresponde ao ponto $[a : b : c] \in \mathbb{P}^2$. As retas em $\mathbb{P}^2$ formam um espaço $\mathbb{P}^2$.*

(2) $d = 2$. A cônica $aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$ corresponde ao ponto $[a : b : c : d : e : f] \in \mathbb{P}^5$. As cônicas formam um espaço $\mathbb{P}^5$.

(3) As cúbicas formam um espaço $\mathbb{P}^9$ e as quarticas formam um espaço $\mathbb{P}^{14}$.

Lema 6.1. *(1) Seja $P \in \mathbb{P}^2$ um ponto fixo. O conjunto de curvas de grau d que contém P forma um hiperplano em $\mathbb{P}^{d(d+3)/2}$.*

(2) Se $T : \mathbb{P}^2 \to \mathbb{P}^2$ é uma mudança de coordenadas projetiva, então o mapa $F \to F^T$ de $\{$Curvas de grau $d\}$ para $\{$Curvas de grau $d\}$ é uma mudança de coordenadas projetiva em $\mathbb{P}^{d(d+3)/2}$.

Demonstração. Se $P = [x : y : z]$, então a curva correspondendo à $(a_1, \ldots, a_N) \in \mathbb{P}^{d(d+3)/2}$ passa por P se, e somente se, $\sum a_i M_i(x, y, z) = 0$. Como nem todo $M_i(x, y, z)$ é zero, os $[a_1 : \cdots : a_N]$ satisfazendo essa equação formam um hiperplano. $F \to F^T$ será linear pois se $F = \sum a_i M_i$ e $G = \sum b_i M_i$, então $(\alpha F + \beta G)^T = \sum(\alpha a_i + \beta b_i)M_i^T = \sum \alpha a_i M_i^T + \sum \beta b_i M^T = \alpha F^T + \beta G^T$, para todo $\alpha, \beta \in k$. Além disso, $F \to F^T$ será invertível, dado que sua inversa é $F \to F^{T^{-1}}$.

□

Segue disso que para qualquer conjunto de pontos, as curvas de grau d que o contém formam uma subvariedade linear em $\mathbb{P}^{d(d+3)/2}$. Como a intersecção de n hiperplanos de $\mathbb{P}^n$ é não vazia (Proposição 6.59), existe uma curva de grau d passando por quaisquer $d(d+3)/2$ pontos.

Suponha agora que fixamos um ponto P e um inteiro $r \leq d + 1$. Afirmamos que as curvas F de grau d tais que $m_P(F) \geq r$ formam uma subvariedade linear de dimensão $\dfrac{d(d+3)}{2} - \dfrac{r(r+1)}{2}$. Pelo item (2) do Lema 6.1, podemos assumir que $P = [0 : 0 : 1]$. Escreva $F = \sum F_i(X, Y)Z^{d-i}$, F_i uma forma de grau i. Então $m_P(F) \geq r$ se, e somente se, $F_0 = F_1 = \cdots = F_{r-1} = 0$, i.e., os coeficientes de todos os monômios $X^i Y^j Z^k$ com $i + j < r$ são zero (Proposição 6.70), e existem $1 + 2 + \cdots + r = \dfrac{r(r+1)}{2}$ tais coeficientes.

Seja $P_1, \ldots, P_n$ pontos distintos em $\mathbb{P}^2$, $r_1, \ldots, r_n$ inteiros não negativos. Definimos

$$V(d; r_1P_1, \ldots, r_nP_n) = \{\text{curvas de grau } d \mid m_{P_i}(F) \geq r_i, 1 \leq i \leq n\}.$$

Teorema 6.1. *(1) $V(d; r_1P_1, \ldots, r_nP_n)$ é uma subvariedade linear de $\mathbb{P}^{d(d+3)/2}$ de dimensão $\geq \dfrac{d(d+3)}{2} - \sum \dfrac{r_i(r_i+1)}{2}$.*

Demonstração. (1) segue diretamente da discussão do parágrafo anterior, pois para cada i teremos $\dfrac{r_i(r_i+1)}{2}$ coeficientes iguais a zero. Provaremos (2) por indução em $m = (\sum r_i) - 1$. Podemos assumir que $m > 1$, $d > 1$, pois caso contrário o resultado é trivial.

Caso 1: Cada $r_i = 1$. Seja $V_i = V(d; P_1, \ldots, P_i)$. Por indução, basta mostrar que $V_n \neq V_{n-1}$. Escolha retas L_i passando por P_i mas não por P_j, $j \neq i$ (Proposição 6.72), e uma linha L_0 que não passa por nenhum P_i. Então $F = L_1 \cdots L_{n-1} L_0^{d-n+1} \in V_{n-1}$, $f \notin V_n$.

Caso 2: Algum $r_i > 1$. Seja $r = r_1 > 1$, e $P = P_1 = [0 : 0 : 1]$. Seja

$$V_0 = V(d; (r-1)P, r_2P_2, \ldots, r_nP_n).$$

Para $F \in V_0$, seja $F_* = \sum_{i=0}^{r-1} a_i X^i Y^{r-1-i}$ + termos de maior grau. Seja $V_i = \{F \in V_0 \mid a_j = 0 \text{ para } j < i\}$. Então $V_0 \supset V_1 \supset \cdots \supset v_r = V(d; r_1P_1, r_2P_2, \ldots, r_nP_n)$, assim é suficiente mostrar que $V_i \neq V_{i+1}$, $i = 0, 1, \ldots, r-1$.

Seja $W_0 = V(d-1; (r-2)P, r_2P_2, \ldots, r_nP_n)$. Para $F \in W_0$, $F_* = a_i X^i Y^{r-2-i} + \cdots$. Defina $W_i = \{F \in W_0 \mid a_j = 0\}$. Por indução

$$W_0 \supsetneq W_1 \supsetneq \cdots \supsetneq W_{r-1} = V(d-1; (r-1)P, r_2P_2, \ldots, r_nP_n).$$

Se $F_i \in W_i$, $F_i \notin W_{i+1}$, então $YF_i \in V_i$, $YF_i \notin V_{i+1}$, e $XF_{r-2} \in V_{r-1}$, $XF_{r-2} \notin V_r$. Assim $V_i \neq V_{i+1}$ para $i = 0, \ldots, r-1$, e isso completa a prova. □

6.2 Teorema de Bézout

O plano projetivo foi construído de forma que quaisquer duas retas distintas se intersectem em um ponto. O Teorema de Bézout nos diz que temos mais uma propriedade:

Teorema 6.2. ***Teorema de Bézout.*** *Sejam F e G curvas planas projetivas de grau m e n respectivamente. Assuma que F e G não possuam componentes em comum. Então*

$$\sum_P I(P, F \cap G) = mn$$

Demonstração. Como $F \cap G$ é finito (Proposição 6.71), podemos assumir, por uma mudança de coordenadas projetiva se necessário, que nenhum dos pontos em $F \cap G$ está na reta no infinito $Z = 0$.

Então $\sum_P I(P, F \cap G) = \sum_P I(P, F_* \cap G_*) = dim_k k[X, Y]/(F_*, G_*)$, pela Propriedade (9) de Números de Interseção. Seja

$$\Gamma_* = k[X, Y]/(F_*, G_*), \quad \Gamma = k[X, Y, Z]/(F, G), \quad R = k[X, Y, Z]$$

e Γ_d (respectivamente R_d) o espaço vetorial das formas de grau d em Γ (respectivamente em R). O teorema será demonstrado se mostrarmos que $dim\ \Gamma_* = dim\ \Gamma_d$ e $dim\ \Gamma_d = mn$ para algum d suficientemente grande.

Passo 1: $dim\ \Gamma_d = mn$ para todo $d \geq m+n$: Seja $\pi : R \to \Gamma$ o mapa quociente natural, defina $\phi : R \times R \to R$ como $\phi(A,B) = AF + BG$ e $\psi : R \to R \times R$ como $\psi(C) = (GC, -FC)$. Utilizando o fato de que F e G não possuem fatores em comum, temos que a seguinte sequência é exata:

$$0 \to R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \xrightarrow{\pi} \Gamma \to 0.$$

Se restringirmos esses mapas para as formas de diferentes graus, temos a seguinte sequência exata:

$$0 \to R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \pi \Gamma_d \to 0.$$

Dado que $dim\ R_d = \dfrac{(d+1)(d+2)}{2}$, segue da Proposição 3.6 (com alguns cálculos) que $dim\ \Gamma_d = mn$ se $d \geq m+n$.

Passo 2: O mapa $\alpha : \Gamma \to \Gamma$ definido por $\alpha(\overline{H}) = \overline{ZH}$ (onde a barra denota o resíduo módulo (F,G)), é injetivo:

Devemos mostrar que se $ZH = AF + BG$, então $H = A'F + B'G$ para algum A' e B'. Para qualquer $J \in k[X,Y,Z]$, denote (temporariamente) $J(X,Y,0)$ como J_0. Como F, G e Z não possuem zeros em comum (pela suposição que $F \cap G$ não possui pontos na reta no infinito $Z = 0$), F_0 e G_0 são formas relativamente primas em $k[X,Y]$.

Se $ZH = AF + BG$, então $A_0F_0 = -B_0G_0$, assim $B_0 = F_0C$ e $A_0 = -G_0C$ para algum $C \in k[X,Y]$ (dado que F_0 e G_0 são relativamente primos). Seja $A_1 = A + CG$, $B_1 = B - CF$. Veja que $(A_1)_0 = A_0 + CG_0 = -G_0C + CG_0 = 0$ e $(B_1)_0 = B_0 - CF_0 = CF_0 - CF_0 = 0$. Logo temos que $A_1 = ZA'$ e $B_1 = ZB'$ para algum A' e B' pertencentes a $k[X,Y,Z]$, e como $A_1F + B_1G = FA + FCG + GB - GFC = AF + GB = ZH$, então segue que $H = A'F + B'G$ como desejado.

Passo 3: Seja $d \geq m+n$, e escolha $A_1, \ldots, A_{mn} \in R_d$ cujos resíduos em Γ_d formam uma base para Γ_d. Seja $A_{i*} = A_i(X,Y,1) \in k[X,Y]$, e a_i o resíduo de A_{i*} em Γ_*. Então $a_1, \ldots, a_{mn}$ formam uma base de Γ_*:

Notemos primeiro que o mapa α do Passo 2 se restringe a um isomorfismo de Γ_d para Γ_{d+1}, se $d \geq m+n$, dado que toda transformação linear injetiva entre espaços de mesma

dimensão é um isomorfismo. Disso segue que os resíduos de $Z^r A_1, \ldots, Z^r A_{mn}$ formam uma base para Γ_{d+r} para todo $r \geq 0$.

Os a_i's geram Γ_* : se $h = \overline{H} \in \Gamma_*$, $H \in k[X,Y]$, para algum N, $Z^N H^*$ é uma forma de grau $d+r$. Assim $Z^N H^* = \sum_{i=1}^{mn} \lambda_i Z^r A_i + BF + CG$ para algum $\lambda_i \in k$, $B, C \in k[X,Y,Z]$. Então $H = (Z^N H^*)_* = \sum \lambda_i A_{i*} + B_* F_* + C_* G_*$, e seu resíduo em (F,G) será $h = \sum \lambda_i a_i$, como desejado.

Além disso, os a_i's são linearmente independentes pois se $\sum \lambda_i a_i = 0$, então $\sum \lambda_i A_{i*} = BF_* + CG_*$. Logo, (pela Proposição 6.44) $Z^r \sum \lambda_i A_i = Z^s B^* F + Z^t C^* G$ para algum r, s e t. Mas então $\sum \lambda_i \overline{Z^r A_i} = 0$ em Γ_{d+r} e como os termos $\overline{Z^r A_i}$ formam uma base, cada $\lambda_i = 0$. Isso termina a demonstração.

□

Combinando a propriedade (5) de Números de Interseção da Seção 4.3 com o Teorema de Bézout, deduzimos os seguintes corolários:

Corolário 6.1. *Se F e G não possuem componentes em comum, então*

$$\sum_P m_P(F) m_P(G) = deg(F) \cdot deg(G)$$

Corolário 6.2. *Se F e G se intersectam em mn pontos distintos, $m = deg(F)$, $n = deg(G)$, então todos esses pontos são pontos simples em F e G.*

Corolário 6.3. *Se duas curvas de grau m e n possuem mais de mn pontos em comum, então elas possuem uma componente em comum.*

Conclusão

No primeiro capítulo foram estabelecidas as preliminares algébricas para o trabalho, foram definidas as estruturas algébricas principais bem como provados alguns resultados fundamentais da álgebra comutativa que foram utilizados ao longo de todo o trabalho. No segundo capítulo foram introduzidos os primeiros conceitos da geometria algébrica afim, definindo o espaço afim, os conjuntos algébricos, ideais de pontos no espaço e irredutibilidade, além disso foram demonstrados alguns teoremas principais como o Teorema de Base de Hilbert, que mostra que todo conjunto algébrico é uma interseção finita de hipersuperfícies, e ambas as versões do Teorema dos Zeros de Hilbert, que estabelecem uma conexão direta da geometria afim com a álgebra comutativa. O terceiro capítulo teve como foco abordar os conceitos das variedades afins, mostrando alguns resultados e também definindo as estruturas utilizadas para o estudo global e local das variedades (anel de coordenadas e anel local num ponto P respectivamente). No capítulo 4 foram estudados alguns conceitos importantes sobre curvas planas afins, como pontos singulares, retas tangentes, multiplicidades de pontos, números de interseção, e as respectivas conexões desses conceitos com as estruturas vistas anteriormente como a caracterização da multiplicidade das curvas em um ponto com o anel local nesse dado ponto. O capítulo 5 teve o objetivo de introduzir o espaço projetivo, dando sua motivação e definindo os conceitos já estudados no espaço afim em sua versão projetiva. Por fim o Capítulo 6 trata das curvas planas projetivas, trazendo os conceitos definidos no Capítulo 4 para o contexto projetivo, provando alguns resultados para sistemas lineares de curvas projetivas e finalizando com a demonstração do Teorema de Bézout, que mostra uma importante informação sobre o número de interseção de curvas projetivas sem componentes em comum.

De modo geral, o trabalho foi uma introdução aos conceitos fundamentais da geometria algébrica clássica, estabelecendo uma primeira conexão da álgebra comutativa com a geometria e criando as bases para futuros estudos na área de geometria algébrica e álgebra

comutativa, além de uma primeira motivação para o estudo da teoria moderna de feixes e esquemas.

Referências Bibliográficas

[1] FULTON, William. Algebraic Curves: An Introduction to Algebraic Geometry. 2008.

[2] FRALEIGH, John B. *A first course in abstract algebra. Pearson Education India*, 7ª ed. 2003.

Apêndice

Resultados do Capítulo 1

Proposição 6.1. *Seja R um domínio*

(a) Se F e G são formas de grau r, s respectivamente em $R[X_1, \ldots, X_n]$, então FG é uma forma de grau $r + s$.

(b) Todo fator de uma forma em $R[X_1, \ldots, X_n]$ é também uma forma.

Demonstração. (a) Cada termo de F é da forma $aX_1^{i_1} \cdots X_n^{i_n}$, $a \in k$ e $a \neq 0$, tal que $i_1 + \cdots + i_n = r$ e cada termo de G é da forma $bX_1^{j_1} \cdots X_n^{j_n}$, $b \in k$ e $b \neq 0$, tal que $j_1 + \cdots + j_n = s$. Assim ao multiplicarmos cada termo de F e G

$$a_i X_1^{i_1} \cdots X_n^{i_n} b X_1^{j_1} \cdots X_n^{j_n} = ab X_1^{i_1+j_1} \cdots X_n^{i_n+j_n}$$

e o grau de cada termo de FG será $i_1 + \cdots + i_n + j_1 + \cdots + j_n = r + s$. Logo FG é uma soma de termos de grau $r + s$ e assim será uma forma de grau $r + s$.

(b) Seja $F \in R[X_1, \ldots, X_n]$ uma forma de grau d e que se fatora como $F = hg$. Suponha por absurdo que algum dos fatores de F não seja uma forma, no caso g. Então g pode ser escrito como $g = g_M + g_r$, onde g_M é o termo de maior grau de g e g_r o restante dos termos de menor grau (ou suas partes não homogêneas), e assim temos que $F = h(g_M + g_r) = hg_M + hg_r$. O grau de hg_r é menor que d, e como F é uma forma então $hg_r = 0$, porém $g_r \neq 0$ e $h \neq 0$, um absurdo.

□

Proposição 6.2. *Seja k um corpo infinito e $F \in k[X_1, \ldots, X_n]$. Se $F(a_1, \ldots, a_n) = 0$ para todos $a_1, \ldots, a_n \in k$, então $F = 0$.*

Demonstração. Podemos escrever F como um polinômio em $k[X_1, \ldots, X_{n-1}][X_n]$ e assim

$$F = \sum F_i X_n^i, \quad F_i \in R[X_1, \ldots, X_{n-1}]$$

E dados quaisquer $a_1, \ldots, a_{n-1} \in k$, $F(a_1, \ldots, a_{n-1}, X_n)$ possui somente finitas raízes se algum dos $F_i's$ for diferente de 0. Porém k é infinito e pela hipótese inicial, então $F(a_1, \ldots, a_{n-1}, X_n$ possui infinitas raízes. Logo $F_i = 0$ para todo i. Seguindo por indução, temos que $F_i \in k[X_1]$ é zero para todo $a_1 \in k$, logo deve ser igual a 0 (pois k é infinito e um polinômio de uma variável possui somente finitas raízes). Usando o argumento indutivo, temos que $F = 0$.

□

Proposição 6.3. *Seja R um DFU, K o corpo de frações de R. Então todo elemento $z \in K$ pode ser escrito $z = \frac{a}{b}$, onde $a, b \in R$ não possuem fatores em comum. Essa representação é única a menos de multiplicação por unidades.*

Demonstração. Dado $z \in K$, z é escrito como uma fração de elementos de R, assim $z = \frac{c}{d}$, $c, d \in R$. Como R é DFU então c e d possuem representação única como um produto de irredutíveis $c = p_{c_1} \cdots p_{c_n}$ e $d = p_{d_1} \cdots p_{d_m}$ e assim $z = \frac{p_{c_1} \cdots p_{c_n}}{p_{d_1} \cdots p_{d_m}}$ e eliminando os fatores irredutíveis em comum de c e d, temos que $z = \frac{a}{b}$, onde $a, b \in R$ e a e b não possuem fatores em comum. A representação será única a menos de de multiplicação por unidade pois a representação dos termos de R como produto de irredutíveis é única a menos de multiplicação por unidades.

□

Proposição 6.4. *Dado um corpo k, existem infinitos polinômios mônicos irredutíveis em $k[X]$.*

Demonstração. Suponha por absurdo que existam somente finitos polinômios mônicos irredutíveis $F_1, \ldots, F_n \in k[X]$. Agora dado o polinômio mônico $P = F_1 F_2 \cdots F_n + 1$, temos que P é redutível pois não é igual à nenhum F_i, mas se P é redutível, então P pode ser escrito como um produto de polinômios mônicos irredutíveis, logo deve ser divisível por algum F_i, o que não ocorre, e assim temos uma contradição.

□

Proposição 6.5. *Seja R um DIP e P um ideal primo não nulo de R.*

(a) P é gerado por um elemento irredutível;

(b) P é maximal.

Demonstração. (a) Assuma por absurdo que P não seja gerado por um elemento irredutível. Assim $P = (p)$ e p pode ser escrito como o produto de dois elementos $b, d \in R$ que não são unidades, $p = bd$. Logo $bd \in (p)$ e como (p) é ideal primo, então $b \in (p)$ ou $d \in (p)$. Seja $b \in (p)$. Então $p|b$ e $b = pc$ para algum $c \in R$, $p = pcd$ e d deve ser uma unidade, contradição.

(b) Seja M um ideal de R tal que $P = (p) \subseteq M = (m)$, $p, m \in R$ e p é irredutível pelo item (a). Logo $p \in (m)$ e $p = mc$ para algum $c \in R$. Porém p é irredutível, assim ou m é uma unidade e $(m) = R$ ou m e p são associados (isto é, diferem pela multiplicação de uma unidade) e $(m) = (p)$. Portanto P é maximal. □

Corolário 6.4. *Um corpo algebricamente fechado é infinito.*

Demonstração. Num corpo algebricamente fechado todo polinômio não constante cinde em fatores lineares, assim os polinômios mônicos irredutíveis de $k[X]$ serão da forma $X - \alpha$, $\alpha \in k$. Assim temos uma bijeção de k para o conjunto dos polinômios mônicos irredutíveis e pela Proposição 6.4 existem infinitos polinômios mônicos irredutíveis. □

Proposição 6.6. *Seja k um corpo, $F \in k[X_1, \ldots, X_n]$, $a_1, \ldots, a_n \in k$.*

(a) $F = \sum \lambda_{(i)}(X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$, $\lambda_i \in k$.

(b) Se $F(a_1, \ldots, a_n) = 0$, então $F = \sum_{i=1}^{n}(X_i - a_i)G_i$ para $G_i's \in k[X_1, \ldots, X_n]$ não únicos.

Demonstração. (a) Dado $F = \sum b_{(i)} X_1^{i_1} \cdots X_n^{i_n}$, podemos escrever

$$F = \sum b_{(i)}(X_1 - a_1 + a_1)^{i_1}(X_2 - a_2 + a_2)^{i_2} \cdots (X_n - a_n + a_n)^{i_n}$$

e podemos expandir os termos $(X_j - a_j + a_j)^{i_j}$ preservando os termos $X_j - a_j$ e disso segue o resultado.

(b) Escrevendo F como no item (a) para o ponto $(a_1, \ldots, a_n)$ temos que $F = \sum \lambda_i (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$ e como $F(a_1, \ldots, a_n) = 0$, então a parte constante de F deve ser igual a zero e cada termo de F deve ter alguma potência $i_j > 0$. Com isso podemos evidenciar cada termo $(X_j - a_j)$, e ter uma multiplicação $(X_j - a_j)G_j$ com $G_j \in k[X_1, \ldots, X_n]$ (com $G_j = 0$ possivelmente, caso não haja uma potência positiva de i_j).

□

Resultados do Capítulo 2

Proposição 6.7. *Os conjuntos algébricos de $\mathbb{A}^1(k)$ são somente os conjuntos finitos junto com $\mathbb{A}^1(k)$.*

Demonstração. Temos que para qualquer $S \subset k[X]$, $V(S) = V(I)$, onde I é o ideal gerado por S. Porém $k[X]$ é um DIP, logo $I = (F)$, com $F \in k[X]$, e $V(I) = V(F)$ e como F possui somente um número finito raízes então $V(I) = V(S)$ é finito. A única exeção caso k seja infinito e $S = \{0\}$, assim $V(S) = V(0) = \mathbb{A}^1(k)$.

□

Proposição 6.8. *Seja F um polinômio não constante em $k[X_1, \ldots, X_n]$, k algebricamente fechado. Então $\mathbb{A}^n(k) \setminus V(F)$ é infinito se $n \geq 1$ e $V(F)$ é infinito se $n \geq 2$.*

Demonstração. Provaremos que $V(F)$ é infinito se $n \geq 2$. Provaremos para $n = 2$ e o resultado seguirá por indução para $n > 2$. Fixe $a \in k$ e considere o polinômio $F(a)[Y] \in k[Y]$. Como $F(a)[Y]$ é um polinômio em uma variável e com coeficientes em um corpo algebricamente fechado k, $F(a)[Y]$ possui um número finito de raízes p_i em k, $i = 1, \ldots, n$. Assim (a, p_i) é uma raíz de $F \in k[X, Y]$ para cada i. Como k é algebricamente fechado, então é infinito pelo Corolário 6.4, e assim existem infinitos $a \in k$ tal que $(a, p_i) \in \mathbb{A}(k)^2$ é uma raíz de $F \in k[X, Y]$. Logo $V(F)$ é infinito.

Para $\mathbb{A}^n(K) \setminus V(F)$, quando $n = 1$ é um caso trivial pois todo polinômio não constante em uma variável possui somente um número finito raízes e como $\mathbb{A}^1(k)$ é infinito, então $\mathbb{A}^1(k) \setminus V(F)$ será infinito. Para os casos em que $n \geq 2$, como anteriormente provaremos que é válido para $n = 2$ e o restante seguirá por indução. Novamente fixe $a \in k$ e considere o polinômio $F(a)[Y]$. Temos que $F(a)[Y]$ possui um número finito de raízes $p_i \in k$, $i = 1, \ldots, n$. Assim para qualquer elemento $q \in k$, tal que $q \neq p_i$ para todo i, temos que $F(a, q) \neq 0$. Como k é infinito, $k \setminus \{p_1, \ldots, p_n\}$ é infinito, logo existem infinitas duplas $(a, q) \in \mathbb{A}^2(k)$ tal que $F(a, q) \neq 0$. Portanto $\mathbb{A}^2(k) \setminus V(F)$ é infinito. □

Proposição 6.9. *Sejam $U \subset A^n(k)$ e $W \subset A^m(k)$ conjuntos algébricos. Então*

$$U \times W = \{(a_1, \ldots, a_n, b_1, \ldots, b_m) |\ (a_1, \ldots, a_n) \in U,\ (b_1, \ldots, b_m) \in W\}$$

é um conjunto algébrico em $\mathbb{A}^{n+m}(k)$ e é chamado o produto de U e W.

Demonstração. Como U é um conjunto algébrico, então existe um conjunto $S \subset k[X_1, \ldots, X_n]$ tal que $V(S) = U$. Mas podemos ver S como um conjunto de polinômios em $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, com os coeficientes das variáveis $Y_1, \ldots, Y_m$ igual a zero. Assim todo ponto de U será um zero de $S \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Da mesma forma, podemos ver W como um conjunto algébrico de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, interpretando todo polinômio do conjunto $T \subset k[Y_1, \ldots, Y_m]$ tal que $V(T) = W$ como um polinômio em $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.

Então $U \times W$ será um conjunto algébrico pois o conjunto $S \cup T \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ é tal que $V(S \cup T) = U \times W$, pois se $P \in V(S \cup T)$, então P é um zero de todos polinômios em T e S. Então $F(P) = 0$ para todo $F \in S$. Sendo $P = (c_1, \ldots, c_n, d_1, \ldots, d_m)$, pela construção de S enquanto conjunto de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, $F(P) = F(c_1, \ldots, c_n) = 0$, então $(c_1, \ldots, c_n) \in U$. Da mesma forma, P será um zero de todo polinômio em T, assim $(d_1, \ldots, d_m) \in W$. Logo $P \in U \times W$. Reciprocamente, dado um ponto em $P \in U \times W$, com $P = (a_1, \ldots, a_n, b_1, \ldots, b_m)$, para todo polinômio $F \in S \cup T$, temos que se $F \in S$, então $F(P) = F(a_1, \ldots, a_n) = 0$ e se $F \in T$, então $F(P) = F(b_1, \ldots, b_m) = 0$. Logo $P \in V(S \cup T)$. □

Lema 6.2. *Sejam U, W conjuntos algébricos em $\mathbb{A}^n(k)$. Então $U = W$ se, e somente se, $I(U) = I(W)$.*

Demonstração. Se $U = W$ então o resultado é trivial. Se $I(U) = I(W)$, então temos que $V(I(U)) = V(I(W))$ mas pela Proposição 6.8 (vi) $U = V(I(U))$ e $W = V(I(W))$ e assim $U = W$.

□

Proposição 6.10. *(i) Seja V um conjunto algébrico em $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ um ponto que não pertence a V. Então existe um polinômio $F \in k[X_1, \ldots, X_n]$ tal que $F(Q) = 0$ para todo $Q \in V$, mas $F(P) = 1$*

(ii) Sejam $P_1, \ldots, P_r$ pontos distintos em $\mathbb{A}^n(k)$ que não pertencem a um conjunto algébrico V. Então existem polinômios $F_1, \ldots, F_r \in I(V)$ tal que $F_i(P_j) = 0$ se $i \neq j$, e $F_i(P_i) = 1$.

(iii) Sejam $P_1, \ldots, P_r \in \mathbb{A}^n(k)$ e V como em (ii), e $a_{ij} \in k$ para $1 \leq i, j \leq r$, então existem $G_i \in I(V)$ com $G_i(P_j) = a_{ij}$ para todo i e j.

Demonstração. **(i)** Temos que $I(V) \neq I(V \cup \{P\})$, logo existe $G \in I(V)$ tal que $G(Q) = 0$ $\forall Q \in V$ e $G(P) \neq 0$. Seja $G(P) = a$, $a \in k$. Então $a^{-1}G$ é tal que $a^{-1}G(Q) = a^{-1} \cdot 0 = 0$, $\forall Q \in V$ e $a^{-1}G(P) = a^{-1}a = 1$.

(ii) Para cada P_i, $I(V \bigcup_{j=1}^{r} \{P_j\}) \neq I(V \bigcup_{j=1}^{r} \{P_j\} \setminus \{P_i\})$, então aplicamos (i) para P_i e $V \bigcup_{j=1}^{r} \{P_j\} \setminus \{P_i\}$ e temos um polinômio F_i tal que $F_i(P_j) = 0$, $j \neq i$, $F_i(Q) = 0$, $\forall Q \in V$ e $F_i(P_i) = 1$.

(iii) Aplicando (ii) para os pontos $P_1, \ldots, P_r$ temos os polinômios $F_1, \ldots, F_r$ como em (ii). Tome $G_i = \sum_j a_{ij}F_j$. Então $G_i(P_j) = \sum_j a_{ij}F_j(P_j) = a_{ij}$, pois $F_i(P_j) = 0$ para $i \neq j$. □

Proposição 6.11. *Seja I um ideal de um anel R e $\pi : R \to R/I$ o homomorfismo natural. Então*

(i) Para todo ideal J' de R/I, $\pi^{-1}(J') = J$ é um ideal de R contendo I, e para todo ideal J de R contendo I, $\pi(J) = J'$ é um ideal de R/I. Assim existe uma correspondência um para um natural entre $\{$ideais de $R/I\}$ e $\{$ideais de R que contém $I\}$.

(ii) J' é um ideal radical se, e somente se, J é radical. Similarmente para ideais primos e maximais.

(iii) J' é finitamente gerado se, e somente se, J é finitamente gerado. Assim R/I é Noetheriano se R é Noetheriano, e todo anel da forma $k[X_1, \ldots, X_n]/I$ é Noetheriano.

Demonstração. (i) Dado J' ideal de R/I, temos que $J = \pi^{-1}(J')$ é um ideal de R pois a pré-imagem de um homomorfismo leva ideais em ideais. Além disso $I \subset J$, pois $I = \pi^{-1}(0 + I)$ e $0 + I \in J'$. Reciprocamente, dado J ideal de R que contém I, $\pi(J)$ será um ideal de R/I pois dados $a, b \in \pi(J)$ e $r \in R/I$, existem $c, d, r' \in J$ tal que $pi(c) = a$, $\pi(d) = b$ e $\pi(r') = r$ pois π é homomorfismo sobrejetivo. Então $\pi(c + d) = \pi(c) + \pi(d) = a + b \in \pi(J)$, $\pi(cd) = \pi(c)\pi(d) = ab \in \pi(J)$ e $\pi(r'c) = \pi(r')\pi(c) = ra \in \pi(J)$.

(ii) Seja J' ideal radical de R/I. Dado $a \in Rad(J)$, temos que $a^n \in J$ para algum n. Logo $a^n + I \in J'$ e $a + I \in J'$ pois J' é radical. Como π é sobrejetivo, então existe $c \in J$ tal que $\pi(c) = a + I$, isto é, $c + I = a + I$ o que implica que $a - c + I = I$. Como $I \subset J$, então $a - c \in J$ e $a \in J$. Reciprocamente seja J ideal radical. Então dado $a + I \in Rad(J')$, temos que $a^n + I \in J'$ para algum n. Logo existe $c \in J$ tal que $\pi(c) = a^n + I$, isto é, $c + I = a^n + I$.

Assim $a^n - c + I = 0 + I$ e $a^n - c \in I$, e como $I \subset J$, $a^n - c \in J$. Portanto $a^n \in J$ e como J é radical, $a \in J$, assim $\pi(a) \in J'$ e J' é ideal radical.

Seja J' ideal primo. Dados $a, b \in R$ tal que $ab \in J$, temos que $\pi(ab) = (a+I)(b+I) \in J'$ e como J' é primo, então $a + I \in J'$ ou $b + I \in J'$. Assuma, S.P.G, que $a + I \in J'$. Então existe $c \in J$ tal que $\pi(c) = c + I = a + I$ e assim $a - c \in I$. Como $I \subset J$, então $a - c \in J$ e $a \in J$. O mesmo processo implica que se $b + I \in J'$ então $b \in J$ e assim J é ideal primo. Reciprocamente, seja J ideal primo. Sejam $a + I, b + I \in R/I$ tal que $ab + I \in J'$. Então existe $c \in J$ tal que $\pi(c) = c + I = ab + I$ e assim $ab - c \in I$, mas como $I \subset J$, então $ab - c \in J$ e $ab \in J$. Como J é ideal primo, então $a \in J$ ou $b \in J$, assuma S.P.G, que $a \in J$. Então $a + I \in J'$. Portanto J' é ideal primo.

Seja J' ideal maximal. Seja U ideal próprio de R tal que $J \subset U \subset R$. Temos que $\pi(J) \subset \pi(U) \subset \pi(R)$, porém J' é maximal, então $\pi(U)$ deve ser igual a J' e assim $U = J$. Reciprocamente, seja J ideal maximal. Seja U' ideal próprio de R/I tal que $J' \subset U \subset R/I$. Temos que $\pi^{-1}(U')$ é um ideal de R que contém J, porém J é maximal, então $\pi^{-1}(U') = J$. Assim $U' = \pi(J) = J'$, e portanto J' é ideal maximal.

(iii) Se J é finitamente gerado, então existem $a_1, \ldots, a_n \in J$ tal que $J = \sum_{i=1}^{n} Ra_i$. Como todo elemento de J' tem um representante em J então $b + I \in J'$ pode ser escrito $\sum_{i=1}^{n} r_i a_i + I$ e J' será finitamente gerado por $a_1 + I, \ldots, a_n + I$.

□

Corolário 6.5. *$\mathbb{A}^n(k)$ é irredutível se k é infinito.*

Demonstração. Assuma que k é infinito. Pela Proposição 6.2 se $F \in I(\mathbb{A}^n(k))$ então $F = 0$. Assim $I(\mathbb{A}^n(k)) = (0)$, que é um ideal primo. Pela Proposição 2.6, $\mathbb{A}^n(k)$ é irredutível. □

Corolário 6.6. *Todo ideal próprio em um anel Noetheriano está contido em um ideal maximal.*

Demonstração. Seja I um ideal próprio de um anel Noetheriano R. Aplicando o Lema 2.2 para a coleção $\mathfrak{I} = \{J \subset R \mid J \text{ é próprio e } I \subset J\}$. Seja M o membro maximal de $\mathfrak{I}$, então $I \subset M$ e M é ideal maximal, pois se existe um ideal próprio N que contém M, então $I \subset N$ e isso contradiz a maximimalidade de M em $\mathfrak{I}$.

□

Proposição 6.12. *Se S é módulo-finito sobre R, então S é anel-finito sobre R.*

Demonstração. Sejam $s_1, \ldots, s_n \in S$ tal que $S = \sum Rs_i$. Temos que $R[s_1, \ldots, s_n] \subset S$, trivialmente pois R é subanel de S. Reciprocamente, dado $s \in S$ arbitrário, temos que $s = \sum_{i=1}^{n} r_i s_i$ para $r_i \in R$, pois S é módulo-finito sobre R. Mas $\sum_{i=1}^{n} r_i s_i \in R[s_1, \ldots, s_n]$, e assim $S \subset R[s_1, \ldots, s_n]$. □

Proposição 6.13. *Se L é anel-finito sobre K (K, L corpos) então L é uma extensão finitamente gerada de K.*

Demonstração. Sejam $v_1, \ldots, v_n \in L$ tal que $L = K[v_1, \ldots, v_n]$. Temos que $L \subset K(v_1, \ldots, v_n)$, pois dado $v \in L$, $v = \sum_i a_i v_1^{i_1} \cdots v_n^{i_n} = \sum_i a_i v_1^{i_1} \cdots v_n^{i_n}/1 \in K(v_1, \ldots, v_n)$. Reciprocamente, dado $b \in K(v_1, \ldots, v_n)$, então $b = \dfrac{p}{q}$ para $p, q \in K[v_1, \ldots, v_n]$ e $q \neq 0$. Como K é subcorpo de L, então $p, q \in L$. Como L é um corpo, $q^{-1} \in L$ e assim $p \cdot q^{-1} = \dfrac{p}{q} \in L$. □

Exemplo 6.2. *Um exemplo para o qual não vale a volta da Proposição 6.13 é o corpo $K(X)$, para K corpo. $K(X)$ é uma extensão finitamente gerada, pois $K(X)$ é o corpo de frações de $K[X]$. Mas $K(X)$ não é anel-finito sobre K. Suponha por absurdo que seja. Então existem $\dfrac{p_1}{q_1}, \ldots, \dfrac{p_n}{q_n} \in K(X)$, com $p_i, q_i \in K[X]$ e $q_i \neq 0$ para $i = 1, \ldots, n$, tal que $K(X) = K[\dfrac{p_1}{q_1}, \ldots, \dfrac{p_n}{q_n}]$. Temos então que $b = q_1 \cdots q_n \in K[X]$ é um denominador comum a todo $\dfrac{p_i}{q_i}$ e necessariamente para todo $z \in K(X)$, $z = \sum_i a_i (\dfrac{p_1}{q_1})^{i_1} \cdots (\dfrac{p_n}{q_n})^{i_n}$, para m suficientemente grande, $b^m z \in K[X]$. Porém tomando $z = \dfrac{1}{c}$ onde c é um polinômio mônico irredutível que não divide b (que sempre pode ser obtido, pela demonstração da Proposição 6.4) temos que para todo m inteiro positivo, $\dfrac{b^m}{c} \notin K[X]$, um absurdo.*

Proposição 6.14. *Seja R um subanel de S, S um subanel de T.*

(a) Se $S = \sum Rv_i$, $T = \sum Sw_j$, então $T = \sum Rv_i w_j$.

(b) Se $S = R[v_1, \ldots, v_n]$, $T = S[w_1, \ldots, w_m]$, então $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.

(c) Se R, S, T são corpos, $S = R(v_1, \ldots, v_n)$ e $T = S(w_1, \ldots, w_m)$, então $T = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$.

Então cada uma das três condições de finitude é uma relação transitiva.

Demonstração. (a) Dado $t \in T$ arbitrário, temos que $t = \sum s_j w_j$ para $s_j \in S$. Mas como S é módulo-finito sobre R, então cada $s_j = \sum r_i v_i$ para $r_i \in R$. Temos então que

$t = \sum_j (\sum_i r_i v_i) w_j$ e distribuindo os termos, temos então que $t = \sum r_i v_i w_j$, com $r_{i_j} \in R$. Portanto $T = \sum R v_i w_j$.

(b) Dado $t \in T$ arbitrário, temos que $t = \sum_j a_j w_1^{j_1} \cdots w_m^{j_m}$ para $a_j \in S$. Mas como S é anel-finito sobre R, então cada $a_j = \sum_i b_i v_1^{i_1} \cdots v_n^{i_n}$, com $b_i \in R$. Temos então que $t = \sum_j (\sum_i b_i v_1^{i_1} \cdots v_n^{i_n}) w_1^{j_1} \cdots w_m^{j_m}$, e distribuindo os termos $t = \sum b_i v_1^{i_1} \cdots v_n^{i_n} w_1^{j_1} \cdots w_m^{j_m}$ com $b \in R$ e assim $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.

(c) Dado $t \in T$ arbitrário, temos que $t = \dfrac{p}{q}$, $p, q \in S[w_1, \ldots, w_m]$ e $q \neq 0$. Seja $p = \sum_i a_i w_1^{i_1} \cdots w_m^{i_m}$ e $q = \sum b_j w_1^{j_1} \cdots w_m^{j_m}$ com $a_i, b_j \in S$. Mas como $S = R(v_1, \ldots, v_n)$, então $a_i = \dfrac{p_i'}{q_i'}$ e $b_j = \dfrac{p*_j}{q*_j}$ com $p_i', q_i', p_j^*, q_j^* \in R[v_1, \ldots, v_n]$ e $q_i', q_j^* \neq 0$. Assim $t = \dfrac{\sum_i (\frac{p_i'}{q_i'}) w_1^{i_1} \cdots w_m^{i_m}}{\sum_j (\frac{p_j^*}{q_j^*}) w_1^{j_1} \cdots w_m^{j_m}}$

e sendo $c = q_1' \cdots q_n' q_1^* \cdots q_n^*$, temos que $t = (c \cdot c^{-1})t = \dfrac{\sum_i Q_i' w_1^{i_1} \cdots w_m^{i_m}}{\sum_j Q_j^* w_1^{j_1} \cdots w_m^{j_m}}$, onde $Q_i', Q_j^* \in R[v_1, \ldots, v_n]$. Assim temos que $\sum_i Q_i' w_1^{i_1} \cdots w_m^{i_m}, \sum_j Q_j^* w_1^{j_1} \cdots w_m^{j_m} \in R[v_1, \ldots, v_n, w_1, \ldots, w_m]$ e $t \in R(v_1, \ldots, v_n, w_1, \ldots, v_m)$. Logo $T = R(v_1, \ldots, v_n, w_1, \ldots, v_m)$.

□

Proposição 6.15. *Seja R um subanel de S, S um subanel de um domínio T. Se S é integral sobre R e T é integral sobre S, então T é integral sobre R.*

Demonstração. Dado $z \in T$, temos que $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ para algum n e $a_i \in S$, pois T é integral sobre S. Logo z é integral sobre $R[a_1, \ldots, a_n]$ e pela Proposição 2.8, $R[a_1, \ldots, a_n, z]$ é módulo-finito sobre $R[a_1, \ldots, a_n]$. Como S é integral sobre R, então a_i é integral sobre R para todo i, assim a_i é integral sobre $R[a_1, \ldots, a_{i-1}]$ e pelo Lema 2.3, $R[a_1, \ldots, a_n]$ é módulo-finito sobre R. Pela transitividade da condição de finitude da Proposição 6.14 (a), $R[a_1, \ldots, a_n, z]$ é módulo-finito sobre R. Assim $R[a_1, \ldots, a_n, z]$ será um subanel de T que contém $R[z]$ e é módulo-finito sobre R, e pela Proposição 2.8, z é integral sobre R. □

Proposição 6.16. *Seja S um domínio anel-finito sobre R. Então S é módulo-finito sobre R se, e somente se, S é integral sobre R.*

Demonstração. Se S é módulo-finito sobre R, então para todo $z \in S$, S é um subanel de S que contém $R[z]$ e é módulo finito sobre R. Assim z será integral sobre R pela Proposição 2.8.

Reciprocamente, seja S integral sobre R. Temos que S é anel-finito sobre R por hipótese, seja $S = R[s_1, \ldots, s_n]$. Como S é integral sobre R, então s_i será integral sobre R e consequentemente integral sobre $R[s_1, \ldots, s_{i-1}]$. Então pelo Lema 2.3, $S = R[s_1, \ldots, s_n]$ é módulo-finito sobre R.

□

Proposição 6.17. *Seja L um corpo e k um subcorpo algebricamente fechado de L. Então todo elemento de L que é algébrico sobre k deve pertencer a k. Consequentemente, um corpo algebricamente fechado não possui uma extensão módulo-finito além de si mesmo.*

Demonstração. Seja $z \in L$ algébrico sobre k. Então existe $P \in k[X]$ tal que $P(z) = 0$. Mas como k é algebricamente fechado, então P cinde em fatores lineares, e assim P deve ter ao menos um fator $(X - z)$ logo $z \in k$.

Seja S uma extensão módulo-finito de k. Então S é anel-finito sobre k pela Proposição 6.12, e pela Proposição 6.16, então S deve ser integral (algébrico no caso de corpos) sobre k, e então $S \subset k$.

□

Proposição 6.18. *Seja K um corpo, $L = K(X)$ o corpo de funções racionais em uma variável sobre K. Então*

(i) Todo elemento de L que é integral sobre $K[X]$ pertence a $K[X]$.

(ii) Não existe nenhum elemento não nulo $F \in K[X]$ tal que para todo $z \in L$, $F^n z$ é integral sobre $K[X]$ para algum $n > 0$.

Demonstração. (i) Se $z \in L$ é tal que $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ para $a_i \in K[X]$, então escrevendo $z = \dfrac{F}{G}$, com $F, G \in K[X]$ e $G \neq 0$, temos que

$$\frac{F^n}{G^n} + \frac{a_1 F^{n-1}}{G^{n-1}} + \cdots + a_n = 0.$$

Multiplicando a equação por G^n, temos

$$F^n + a_1 F^{n-1} G + \cdots + a_n G^n = 0,$$

e assim

$$F^n = -a_1F^{n-1}G - a_2F^{n-2}G^2 - \cdots - a_nG^n = G(-a_1F^{n-1} - \cdots - a_nG^{n-1}).$$

Portanto G divide F e $z = \dfrac{F}{G} \in K[X]$.

(ii) Assuma por absurdo que exista tal F. Por (i), todo elemento de L integral sobre $K[X]$ deve pertencer a $K[X]$, logo para todo $z \in L$, $F^n z \in K[X]$ para algum n. Tome $c \in K[X]$ mônico e irredutível, tal que c não divide F (que sempre podemos obter pela Proposição 6.4). Então para qualquer m inteiro positivo $\dfrac{F^m}{c} \notin K[X]$, uma contradição.

□

Proposição 6.19. *Seja K um subcorpo de um corpo L. Então:*

(i) O conjunto de elementos de L que são algébricos sobre K é um subcorpo de L que contém K.

(ii) Suponha que L é módulo-finito sobre K e R um domínio tal que $K \subset R \subset L$. Então R é um corpo.

Demonstração. (i) Sejam $a, b \in L$ algébricos sobre K. Então b será algébrico sobre $K(a)$, que é uma extensão finita (logo, algébrica) sobre K. Assim, $[K(a,b) : K] = [K(a,b) : K(a)][K(a) : K]$ e $K(a,b)$ é uma extensão finita (e algébrica) sobre K. Assim, $a + b, ab \in K(a,b)$ são algébricos assim como os inversos multiplicativos de a e b, pois $K(a,b)$ é um corpo.

(ii) Pela Proposição 6.16 L é algébrico sobre K e então R também será. Dado $v \in R$, temos que $v^n + a_1v^{n-1} + \cdots + a_n = 0$ para $a_i \in K$, e $a_n \neq 0$. Logo $v(v^{n-1} + a_1v^{n-2} \cdots + a_{n-1}) = -a_n$ e multiplicando pelo inverso de $-a_n$, temos que

$$v(\frac{v^{n-1}}{a_n}v^{n-1} + \frac{a_1v^{n-2}}{a_n} + \cdots + \frac{a_{n-1}}{a_n}) = 1$$

e $(\dfrac{v^{n-1}}{a_n}v^{n-1} + \dfrac{a_1v^{n-2}}{a_n} + \cdots + \dfrac{a_{n-1}}{a_n}) \in R$, assim o inverso multiplicativo de v está em R e portanto R é um corpo. □

Proposição 6.20. *Suponha K um corpo de característica zero, F um polinômio mônico irredutível em $K[X]$ de grau $n > 0$. Seja L o corpo de raízes de F, então $F = \prod_{i=1}^{n}(X - x_i)$, $x_i \in L$. Então necessariamente os x_i's são distintos dois a dois.*

Demonstração. Suponha que existam x_i e x_j tal que $x_i = x_j$ (com $i \neq j$). Sendo $x = x_i$, temos então que $(X - x)^2$ divide F. Considere $G = F_X$, logo $G = \sum_{i=1}^{n} x_i \prod_{j \neq i}(X - x_j)$. Temos então que $G(x) = 0$ pois $(X - x)$ aparece mais de uma vez na representação de F em fatores lineares e assim $(X - x)$ aparece em cada fator do somatório de G. Pela Proposição 6.22 (iii) temos que F divide G, uma contradição pois $deg\ G < deg\ F$

□

Proposição 6.21. *Seja R um domínio integral, com corpo de frações K, e seja L uma extensão finita de K. Então:*

(i) Para todo $v \in L$, existe $a \in R$ não nulo tal que av é integral sobre R.

(ii) Existe uma base $\{v_1, \ldots, v_n\}$ de L sobre K (como espaço vetorial) tal que cada v_i é integral sobre R.

Demonstração. **(i)** Como L é extensão finita de K, então L é extensão algébrica de K. Dado $v \in L$, temos que $v^n + a_1 v^{n-1} + \cdots + a_n = 0$, com $a_i \in K$ para todo i. Como $a_i \in K$ e K é corpo de frações de R, então todo $a_i = \dfrac{b_i}{c_i}$ com $b_i, c_i \in R$ e $c_i \neq 0$ para todo i. Multiplicando a expressão

$$v^n + \frac{b_1}{c_1} v^{n-1} + \cdots + \frac{b_n}{c_n} = 0$$

por $(c_1 \cdots c_n)^n$, temos que

$$\begin{aligned}(c_1 \cdots c_n)^n v^n + (c_2 \cdots c_n)^n (c_1)^{n-1} b_1 v^{n-1} + (c_1 c_3 \cdots c_n)^n (c_2)^{n-1} b_2 v^{n-2} + \cdots \\ + (c_1 \cdots c_{n-2} c_n)^n (c_{n-1})^{n-1} b_{n-1} v + (c_1 \cdots c_{n-1})^n (c_n)^{n-1} b_n = 0\end{aligned}$$

E tomando $a = c_1 \cdots c_n$, vemos que

$$\begin{aligned}a^n v^n + (c_2 \cdots c_n) b_1 a^{n-1} v^{n-1} + (c_1 c_3 \cdots c_n)^2 (c_2) b_2 a^{n-2} v^{n-2} + \cdots \\ + (c_1 \cdots c_{n-2} c_n)^{n-1} (c_{n-1})^{n-2} b_{n-1} a v + (c_1 \cdots c_{n-1})^n (c_n)^{n-1} b_n = 0\end{aligned}$$

Como todos os coeficientes da expressão pertencem a R, temos que av é integral sobre R.

(ii) Dada uma base $\{x_1, \ldots, x_n\}$ de L sobre K (que existe pois L é extensão finita de K), temos que para cada x_i existe um $a_i \in R$ não nulo tal que $a_i x_i = v_i$ é integral sobre R. Mostraremos que $\{v_1, \ldots, v_n\}$ é LI, e portanto uma base de L sobre K. Dada uma combinação linear

$$\sum_{i=1}^{n} c_i v_i = 0$$

Então

$$\sum_{i=1}^{n} c_i a_i x_i = 0$$

E como $\{x_1, \ldots, x_n\}$ é LI então $c_i a_i = 0$ para todo i. Como $a_i \neq 0$ para todo i, então $c_i = 0$. Assim $\{v_1, \ldots, v_n\}$ é um conjunto LI e portanto será uma base de L sobre K.

□

Proposição 6.22. *Seja K um corpo, $F \in K[X]$ um polinômio mônico irredutível de grau $n > 0$. Então:*

(i) *$L = K/(F)$ é um corpo, e se x é a classe de X em L então $F(x) = 0$.*

(ii) *Suponha L' uma extensão de K, $y \in L'$ tal que $F(y) = 0$. Então o homomorfismo de $K[X]$ para L' que leva X para y induz um isomorfismo de L para $K(y)$.*

(iii) *Com L' e y como em (ii), suponha $G \in K[X]$ e $G(y) = 0$. Então F divide G.*

(iv) *$F = (X - x)F_1$, $F_1 \in L[X]$.*

Demonstração. (i) Pela Proposição 6.5 (F) será um ideal maximal de $K[X]$ e assim $K[X]/(F)$ será um corpo. Sendo $x = X + (F)$, temos que $F(x) = F + (F) = 0 + (F)$.

(ii) Seja $\phi : K[X] \to L'$ o homomorfismo que leva X à y. Temos que $Ker(\phi) = (G)$ com $G \in K[X]$ pois $K[X]$ é DIP. Como $F \in Ker(\phi) = (G)$, G divide F no entanto F é irredutível e assim $F = G$ ou $G = 1$, e como ϕ não é nulo, então $F = G$. Pelo Teorema do Isomorfismo, $L = K[X]/(F) \cong K[y]$ e como L é um corpo, então $K[y]$ também será. Assim $K[y] = K(y)$ e $L = K/(F) \cong K(y)$.

(iii) Dado o isomorfismo $\phi : L \to K(y)$, temos que $G+(F) \in Ker\ \phi$ e assim $G+(F) = (F)$ e F divide G.

(iv) Vendo F como um polinômio em $L[X]$, pelo algoritmo de Divisão de Euclides, temos que $F = (X - x)F_1 + r$, com $F_1, r \in L[X]$ e $deg(r) < deg(X - x)$ (logo $r \in L$). Como $F(x) = 0$, então $r = 0$ necessariamente, e assim $F = (X - x)F_1$. □

Proposição 6.23. *Seja K um corpo, $F \in K[X]$. Então existe um corpo L que contém K tal que $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$. L é chamado de corpo de raízes de F.*

Demonstração. Pela Proposição 6.22, para cada termo irredutível G de F podemos encontrar uma extensão M de K tal que $G = (X - x_i)G_1 \in M[X]$. Esse processo é finito pelo grau n de F, e assim existirá uma extensão L de K tal que $F = \prod_{i=1}^{n}(X - x_i)$.

□

Proposição 6.24. *Seja K um corpo, $F \in K[X]$ um polinômio de grau $n > 0$. Então os resíduos $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ formam uma base de $K[X]/(F)$ sobre K.*

Demonstração. Seja $F = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. Temos que o resíduo de $K[X]/(F)$ em (F) será $\overline{F} = \overline{X}^n + a_1\overline{X}^{n-1} + \cdots + \overline{a_n} = 0$, assim $\overline{X}^n$ será uma combinação linear de $\overline{1}, \overline{X}, \cdots, \overline{X}^{n-1}$. O resultado seguirá por indução a partir disso, pois se $\overline{X}^n = b_1\overline{X}^{n-1} + \cdots + \overline{b_n}$, então $\overline{X}^{n+1} = b_1\overline{X}^n + \cdots + \overline{X}b_n = b_1(b_1\overline{X}^{n-1} + \cdots + \overline{b_n}) + b_2\overline{X}^{n-1} + \cdots + b_n\overline{X}$ que é uma combinação linear de $\overline{1}, \overline{X}, \cdots, \overline{X}^{n-1}$. Assim $\overline{X}^m$ será uma combinação linear de $\overline{1}, \overline{X}, \cdots, \overline{X}^{n-1}$ para todo m e consequentemente $\overline{1}, \overline{X}, \cdots, \overline{X}^{n-1}$ gera $K[X]/(F)$ como espaço vetorial sobre K. Além disso $\overline{1}, \overline{X}, \cdots, \overline{X}^{n-1}$ é um conjunto LI, pois dada uma combinação linear $b_1\overline{X}^{n-1} + \cdots + \overline{b_n} = 0$, temos que

$$b_1\overline{X}^{n-1} + \cdots + \overline{b_n} = \overline{X}^n + a_1\overline{X}^{n-1} + \cdots + a_{n-1}\overline{X} + \overline{a_n}$$

e assim

$$(a_1 - b_1)\overline{X}^{n-1} + \cdots + (a_{n-1} - b_{n-1})\overline{X} + \overline{a_n - b_n} = a_1\overline{X}^{n-1} + \cdots + a_{n-1}\overline{X} + \overline{a_n}.$$

Portanto $\overline{b_i} = 0$ para todo i. □

Proposição 6.25. *Seja $R = k[X_1, \ldots, X_n]$, k algebricamente fechado, $V = V(I)$, com I ideal de R. Existe uma correspondência um para um entre conjuntos algébricos de V e e ideais radicais em R/I, e ideais primos (maximais respec.) correspondem a conjuntos algébricos irredutíveis (pontos respec.).*

Demonstração. Dado um ideal radical J em R/I, pela Proposição 6.11, temos um ideal radical J' em R que contém I. Pelo Teorema dos Zeros de Hilbert, temos um conjunto algébrico $V(J')$ que corresponde a J' e como $I \subset J'$, então $V(J') \subset V$, logo temos um conjunto algébrico de V. Reciprocamente, dado um conjunto algébrico $U \subset V$, teremos um ideal radical J' de R tal que $I \subset J'$ e novamente pela Proposição 6.11 teremos um ideal radical J de R/I.

As correspondência entre ideais primos de R/I e conjuntos algébricos irredutíveis de V vem diretamente da Proposição 6.11 e do Corolário 2.6, pois se temos um ideal primo de R/I temos um ideal primo de R que contém I, e assim teremos um conjunto algébrico irredutível que está contido em V. Se temos um conjunto algébrico irredutível de V, temos um ideal primo de R que contém I, assim tendo um ideal primo de R/I.

O mesmo é válido para ideais maximais de R/I e pontos em V. Se temos um ponto em V temos um ideal maximal que contém I, e assim teremos um ideal maximal em R/I. Se temos um ideal maximal em R/I, teremos um ideal maximal em R que contém I e assim teremos um ponto em V correspondente a esse ideal maximal. □

Resultados do Capítulo 3

Proposição 6.26. *O mapa que associa à cada $F \in k[X_1, \ldots, X_n]$ uma função polinomial em $\mathfrak{F}(V, k)$ é um homomorfismo de anéis cujo núcleo é $I(V)$.*

Demonstração. Sendo $\psi : k[X_1, \ldots, X_n] \to \mathfrak{F}(V, k)$ o mapa descrito, temos que dados $F, G \in k[X_1, \ldots, X_n]$: $\psi(F + G) = h \in \mathfrak{F}(V, k)$ tal que $h(a) = (F + G)(a) = F(a) + G(a)$ para todo $a \in V$. Logo $h = \psi(F) + \psi(G)$. De forma semelhante: $\psi(FG) = l \in \mathfrak{F}(V, k)$ tal que $l(a) = (FG)(a) = F(a)G(a)$ para todo $a \in V$ e assim $l = \psi(F)\psi(G)$. Portanto ψ é homomorfismo de anéis.

Dado $F \in Ker\ \psi$, temos que $\psi(F) = f \in \mathfrak{F}(V, k)$ tal que $f(a) = 0$ para todo $a \in V$. Como $f(a) = F(a)$ para todo $a \in V$, então $F \in I(V)$.

□

Proposição 6.27. *Existe uma correspondência um para um natural entre conjuntos algébricos (respec. subvariedades, respec. pontos) de V e ideais radicais (respec. ideais primos, respec. ideais maximais) de $\Gamma(V)$.*

Demonstração. Dado um conjunto algébrico U de V temos um ideal radical $I(U) = J$ de $k[X_1, \ldots, X_n]$, tal que $I(V) \subset J$. Logo pela Proposição 6.11 temos um ideal radical J' de $\Gamma(V)$. Reciprocamente, dado um ideal radical J' de $\Gamma(V)$, temos um ideal radical J de $k[X_1, \ldots, X_n]$ que contém $I(V)$. Assim $V(J)$ será um conjunto algébrico tal que $V(J) \subset V(I(V)) = V$.

A correspondência entre ideais primos e subvariedades, bem como a correspondência entre ideias maximais e pontos vem diretamente da Proposição 6.11 e do Corolário 2.6. □

Proposição 6.28. *Seja W uma subvariedade de uma variedade V, e seja $I_V(W)$ o ideal de $\Gamma(V)$ correspondente à W. Então:*

(a) Toda função polinomial em V se restringe a uma função polinomial em W.

(b) O mapa de $\Gamma(V)$ para $\Gamma(W)$ definido em (a) é um homomorfismo sobrejetivo com núcleo $I_V(W)$, tal que $\Gamma(W)$ é isomorfo à $\Gamma(V)/I_V(W)$.

Demonstração. **(a)** Dada uma função polinomial $f \in \mathfrak{F}(V, k)$, então $f(P) = F(P)$, $F \in k[X_1, \ldots, X_n]$, para todo $P \in V$. Em particular para todo $P \in W$. Assim $f|_W \in \mathfrak{F}(W, k)$ será uma função polinomial em W. Isso caracteriza um homomorfismo $\phi : \Gamma(V) \to \Gamma(W)$, definido como $F + I(V) \mapsto F + I(W)$.

(b) O homomorfismo ϕ definido em (a) será sobrejetivo, pois para todo $F+I(W) \in \Gamma(W)$, temos que $F+I(W) = \phi(F+I(V))$. Já o núcleo de ϕ será igual a dado $F+I(V) \in \Gamma(V)$ tal que $phi(F+I(V)) = 0$, então $F+I(W) = 0$ e portanto $F \in I(W)$, logo $F+I(V) \in I_V(W)$. Pelo Teorema do Isomorfismo $\Gamma(W) \cong \Gamma(V)/I_V(W)$.

□

Proposição 6.29. *Seja $V \subset \mathbb{A}^n$ uma variedade não vazia. Então são equivalentes:*

(i) V é um ponto;

(ii) $\Gamma(V) = k$;

(iii) $dim_k \Gamma(V) < \infty$.

Demonstração. $((i) \Rightarrow (ii))$ Se V é um ponto, então $I(V)$ é um ideal maximal de $k[X_1, \ldots, X_n]$. Assim $k[X_1, \ldots, X_n]/I(V)$ é um corpo que possui k como subcorpo. Como a passagem ao

quociente de $k[X_1, \ldots, X_n]$ para $k[X_1, \ldots, X_n]/I(V)$ é um homomorfismo sobrejetivo que é a identidade restrito a k. Assim pelo Lema 2.4, $\Gamma(V) = k[X_1, \ldots, X_n]/I(V) = k$.

$((ii) \Rightarrow (iii))$ Vem do fato de k ser um espaço vetorial sobre si mesmo de dimensão 1.

$((iii) \Rightarrow (i))$ Como $dim_k \Gamma(V) < \infty$, então $\Gamma(V)$ é módulo-finito sobre k e assim é integral sobre k pela Proposição 6.16. Assim para todo $a \in \Gamma(V)$, existe um polinômio $F \in k[X]$ tal que $F(a) = 0$. Mas como k é algebricamente fechado, então F cinde em fatores lineares e F deve possuir ao menos um termo $(X - a)$ em sua fatoração, logo $a \in k$. Portanto $\Gamma(V) \subset k$ e $\Gamma(V) = k$. Como $\Gamma(V)$ é um corpo, então $I(V)$ deve ser um ideal maximal e como ideias maximais correspondem a pontos pelo Corolário 2.6, então V deve ser igual a um ponto. □

Proposição 6.30. *Sejam $\phi : V \to W$, $\psi : W \to Z$ mapas entre variedades. Então $\widetilde{\psi \circ \phi} = \widetilde{\phi} \circ \widetilde{\psi}$. Temos também que a composição de mapas polinomiais será um mapa polinomial.*

Demonstração. Temos que $\psi \circ \phi : V \to Z$ induzirá o homomorfismo $\widetilde{\psi \circ \phi} : \mathfrak{F}(Z, k) \to \mathfrak{F}(V, k)$, definido por $\widetilde{\psi \circ \phi}(f) = f \circ \psi \circ \phi = \widetilde{\phi}(f \circ \psi) = \widetilde{\phi}(\widetilde{\psi}(f)) = \widetilde{\phi} \circ \widetilde{\psi}(f)$.

Se ϕ e ψ são mapas polinomiais, então $\widetilde{\phi} : \Gamma(W) \to \Gamma(V)$ e $\widetilde{\psi} : \Gamma(Z) \to \Gamma(W)$ são homomorfismos entre seus anéis coordenados e sua composição $\widetilde{\phi} \circ \widetilde{\psi} = \widetilde{\psi \circ \phi} : \Gamma(Z) \to \Gamma(V)$ será um homomorfismo de anéis coordenados. Pela Proposição 3.1, $\psi \circ \phi : V \to Z$ será um mapa polinomial.

□

Proposição 6.31. *Se $\phi : V \to W$ é um mapa polinomial, e X é um subconjunto algébrico de W, então $\phi^{-1}(X)$ é um subconjunto algébrico de V. Se $\phi^{-1}(X)$ é irredutível, e X está contido na imagem de ϕ, então X é irredutível.*

Demonstração. Como X é conjunto algébrico, existe $S \subset k[X_1, \ldots, X_m]$ tal que $X = V(S)$. Seja $p \in \phi^{-1}(X)$, então $\phi(p) \in X = V(S) \iff (T_1(p), \ldots, T_m(p)) \in V(S)$. Assim $\forall F \in S$, $F(T_1, \ldots, T_m)(p) = 0$ e $p \in V(J)$, onde $J = \{F(T_1, \ldots, T_m) \mid F \in S\}$. Logo $\phi^{-1}(X) \subset V(J)$. Dado $p \in V(J)$, temos que $F(T_1, \ldots, T_m)(p) = 0$, $\forall F \in S \iff (T_1(p), \ldots, T_m(p)) \in V(S) \iff \phi(p) \in X$. Portanto $p \in \phi^{-1}(X)$. Assim $\phi^{-1}(X) = V(J)$ e $\phi^{-1}(X)$ é conjunto algébrico.

Assumindo $\phi^{-1}(X)$ irredutível, temos que $I_V(\phi^{-1}(X))$ é ideal primo de $\Gamma(V)$, e assim $\widetilde{\phi}^{-1}(I_V(\phi^{-1}(X)))$ é ideal primo de $\Gamma(W)$. Mostraremos que $\widetilde{\phi}^{-1}(I_V(\phi^{-1}(X))) = I_W(X)$.

Seja $F + I(W) \in \widetilde{\phi}^{-1}(I_V(\phi^{-1}(X)))$, então $\widetilde{\phi}(F + I(W)) \in I_V(\phi^{-1}(X)) \Rightarrow F(T_1, \ldots, T_m) + I(V) \in I_V(\phi^{-1}(X))$. Temos que $\forall p \in \phi^{-1}(X)$, $\phi(p) \in X \iff (T_1(p), \ldots, T_m(p)) \in X$. Logo

$\forall p \in \phi^{-1}(X)$, $F(T_1, \ldots, T_m)(p) = 0$. Como $X \subset Im\ \phi$, então $\phi(\phi^{-1}(X)) = X$ e $F(x) = 0$, $\forall x \in X$. Portanto $F + I(W) \in I_W(X)$.

Reciprocamente, seja $F + I(W) \in I_W(X)$. Assim $F(x) = 0$, $\forall x \in X$. Temos que $\forall p \in \phi^{-1}(X) \Rightarrow (T_1(p), \ldots, T_m(p)) \in X$. Assim $F(T_1(p), \ldots, T_m(p)) = 0$, $\forall p \in \phi^{-1}(X)$. Logo $F + I(W) \in \widetilde{\phi}^{-1}(I_V(\phi^{-1}(X)))$.

Portanto $I_W(X) = \widetilde{\phi}^{-1}(I_V(\phi^{-1}(X)))$ e $I_W(X)$ é ideal primo de $\Gamma(W)$, então X é subvariedade de W.

□

Proposição 6.32. *Seja $\phi : V \to W$ um mapa polinomial de variedades afins, $V' \subset V$, $W' \subset W$ subvariedades. Suponha $\phi(V') \subset W'$. Então:*

(a) $\widetilde{\phi}(I_W(W')) \subset I_V(V')$;

(b) A restrição de ϕ à V' é um mapa polinomial de V' para W'.

Demonstração. **(a)** Sejam $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ tal que $\phi(v) = (T_1(v), \ldots, T_m(v))$ para todo $v \in V$. Como $\phi(V') \subset W'$, temos que para todo $v' \in V'$, $(T_1(v'), \ldots, T_m(v')) \in W'$. Agora dado $F+I(W) \in I_W(W')$, temos que $\widetilde{\phi}(F+I(W)) = F(T_1, \ldots, T_m)+I(V)$. Como necessariamente $F \in I(W')$, então $F(T_1, \ldots, T_m) \in I(V')$, pois para todo v', $F(T_1(v'), \ldots, T_m(v')) = 0$. Assim $F(T_1, \ldots, T_m) + I(V) \in I_V(V')$, e portanto $\widetilde{\phi}(I_W(W')) \subset I_V(V')$.

(b) A restrição $\phi' : V' \to W'$ será um mapa polinomial pois $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ são tais que $\phi'(v') = (T_1(v'), \ldots, T_m(v')) \in W'$ para todo $v' \in V$ (dado que $\phi(V') \subset W'$, por hipótese).

□

Proposição 6.33. *O mapa de projeção $pr : \mathbb{A}^n \to \mathbb{A}^r$, $n \geq r$, definido por $pr(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$ é um mapa polinomial.*

Demonstração. Temos que para todo $(a_1, \ldots, a_n) \in \mathbb{A}^n$

$$pr(a_1, \ldots, a_n) = (F_1(a_1, \ldots, a_n), \ldots, F_r(a_1, \ldots, a_n)),$$

onde $F_i = X_i \in k[X_1, \ldots, X_n]$.

□

Proposição 6.34. *Dado $V \subset \mathbb{A}^n$ subvariedade linear. Temos que:*

(a) Se T é uma mudança afim de coordenadas, então V^T é também uma subvariedade linear de $\mathbb{A}^n$.

(b) Se $V \neq \emptyset$, então existe uma mudança afim de coordenadas T de $\mathbb{A}^n$ tal que $V^T = V(X_{m+1}, \ldots, X_n)$. Assim V^T é uma variedade.

(c) O número m que aparece em (b) não depende da mudança afim de coordenadas T escolhida. Denominamos m como a dimensão de V. Então V é isomorfo à $\mathbb{A}^m$ como uma variedade.

Proposição 6.35. *(a) Se L é a reta que passa por P e Q, e T é uma mudança afim de coordenadas, então $T(L)$ é a reta que passa por $T(P)$ e $T(Q)$.*

(b) Uma reta é uma subvariedade linear de dimensão 1, e qualquer subvariedade linear de dimensão 1 é uma reta que passa por dois pontos.

(c) Em $\mathbb{A}^2$ uma reta é o mesmo que um hiperplano.

(d) Sejam $P, P' \in \mathbb{A}^2$, L_1, L_2 duas retas distintas que passam por P e L_1', L_2' que passam por P'. Existe uma mudança afim de coordenadas T de $\mathbb{A}^2$ tal que $T(P) = P'$ e $T(L_i) = L_i'$, $i = 1, 2$.

Proposição 6.36. *Seja $\phi : V \to W$ um mapa polinomial entre variedades afins, $\widetilde{\phi} : \Gamma(W) \to \Gamma(V)$ o mapa induzido em anéis coordenados. Suponha $P \in V$, $\phi(P) = Q$. Então $\widetilde{\phi}$ se estende unicamente a um homomorfismo de anéis (também descrito $\widetilde{\phi}$) de $\mathfrak{O}_Q(W)$ para $\mathfrak{O}_P(V)$ e $\widetilde{\phi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$.*

Demonstração. Dado $f \in \mathfrak{O}_Q(W)$, temos que $f = \dfrac{a + I(W)}{b + I(W)}$, para algum $a + I(W), b + I(W) \in \Gamma(W)$ com $(b + I(W))(Q) \neq 0$. Assim definimos $\widetilde{\phi}(f) = \dfrac{\widetilde{\phi}(a + I(W))}{\widetilde{\phi}(b + I(W))}$. Temos que $\widetilde{\phi}(a + I(W)) = a(\phi) + I(V) \in \Gamma(V)$ e $\widetilde{\phi}(b + I(W)) = b(\phi) + I(V) \in \Gamma(V)$, assim $\widetilde{\phi}(b + I(W))(P) = b(\phi(P)) + I(V) = b(Q) + I(V) \neq 0$. Portanto $\widetilde{f} \in \mathfrak{O}_P(V)$, e como $\widetilde{\phi} : \Gamma(W) \to \Gamma(V)$ é homomorfismo, então $\widetilde{\phi} : \mathfrak{O}_Q(W) \to \mathfrak{O}_P(V)$ também será.

Agora dada $f \in \mathfrak{m}_Q(W)$, com $f = \dfrac{a + I(W)}{b + I(W)}$, temos que $f(Q) = 0$. Aplicando $\widetilde{\phi}$, $\widetilde{\phi}(f) = \dfrac{\widetilde{\phi}(a + I(W))}{\widetilde{\phi}(b + I(W))} = \dfrac{a(\phi) + I(V)}{b(\phi) + I(V)}$ e assim $\widetilde{\phi}(f)(P) = \dfrac{a(\phi)(P) + I(V)}{b(\phi)(P) + I(V)} = \dfrac{a(Q) + I(V)}{b(Q) + I(V)} = f(Q) = 0$. Logo $\widetilde{\phi}(f) \in \mathfrak{m}_P(V)$. □

Proposição 6.37. *Seja $T : \mathbb{A}^n \to \mathbb{A}^n$ uma mudança afim de coordenadas, $T(P) = Q$. Então $\widetilde{T} : \mathfrak{O}_Q(\mathbb{A}^n) \to \mathfrak{O}_P(\mathbb{A}^n)$ é um isomorfismo. Além disso, $\widetilde{T}$ induz um isomorfismo de $\mathfrak{O}_Q(V)$ para $\mathfrak{O}_P(V^T)$ se $P \in V^T$, para V uma subvariedade de $\mathbb{A}^n$.*

Proposição 6.38. *A função de ordem em K que leva um elemento em de K em sua ordem em $\mathbb{Z}$ é independente da escolha do parâmetro do uniformizante.*

Demonstração. A demonstração vem diretamente do fato que dado dois parâmetros uniformizantes t e r em R, temos que $r = ut$ e $t = vr$ para v, u unidades em R. Isso é verdade pois se $r = ut$, então como r é parâmetro uniformizante, então $r = u(vr^n)$ para alguma unidade v de R e n inteiro positivo. Logo $uvr^{n-1} = 1$ e como uv é unidade em R e r não é uma unidade, temos que $r^{n-1} = 1$. Portanto $n = 1$ e $t = vr$.

Então dado $z \in K$, se $z = ut^n$, então $z = u(vr)^n = uv^n r^n$ e a ordem é a mesma para os parâmetros t e r. □

Proposição 6.39. *Seja $V = \mathbb{A}^1$, $\Gamma(V) = k[X]$, $K = k(V) = k(X)$.*

(a) Para cada $a \in k = V$, $\mathfrak{O}_a(V)$ é um AAD com parâmetro uniformizante $t = X - a$.

(b) $\mathfrak{O}_\infty = \{F/G \in k(X) \mid deg(G) \geq deg(F)\}$ é um AAD, com parâmetro uniformizante $t = \dfrac{1}{X}$

Demonstração. **(a)** Dado $z \in \mathfrak{O}_a(V)$ temos que $z = \dfrac{P}{Q}$, com $Q(a) \neq 0$. Temos dois casos a se considerar: se $P(a) \neq 0$ e $P(a) = 0$.

Se $P(a) \neq 0$, então $\dfrac{P}{Q}$ é uma unidade em $\mathfrak{O}_a(V)$, pois $\dfrac{Q}{P} \in \mathfrak{O}_a(V)$. Assim $z = \dfrac{P}{Q}(X-a)^0$.

Se $P(a) = 0$, então $P = (X - a)^n J$, $J \in k[X]$ e $J(a) \neq 0$. Assim $\dfrac{J}{Q}$ é uma unidade em $\mathfrak{O}_a(V)$ pois $\dfrac{Q}{J} \in \mathfrak{O}_a(V)$. E então $z = \dfrac{P}{Q} = \dfrac{J}{Q}(X - a)^n$.

Logo todo $z \in \mathfrak{O}_a(V)$ pode ser escrito como $u(X - a)^n$ para $u \in \mathfrak{O}_a(V)$ uma unidade e n inteiro não negativo.

(b) Dado $z \in \mathfrak{O}_\infty(V)$, temos que $z = \dfrac{F}{G}$ com $deg(G) \geq deg(F)$. Temos dois casos a considerar: se $deg(F) = deg(G)$ e se $deg(F) < deg(G)$.

Se $deg(F) = deg(G)$, então z é uma unidade em $\mathfrak{O}_\infty(V)$, pois $\dfrac{G}{F} \in \mathfrak{O}_\infty(V)$. Assim $z = \dfrac{F}{G}(\dfrac{1}{X})^0$.

Se $deg(F) < deg(G)$, então $deg(G) - deg(F) = m$ natural. Então multiplicando F por X^m, temos que $deg(FX^m) = deg(G)$. Isso implica que $\frac{FX^m}{G}$ é uma unidade em $\mathfrak{O}_\infty(V)$. Logo $z = \frac{F}{G} = \frac{F}{G}\frac{X^m}{X^m} = \frac{FX^m}{G}(\frac{1}{X})^m$.

Portanto todo $z \in \mathfrak{O}_\infty(V)$ pode ser representado como $z = u(\frac{1}{X})^n$ para algum n inteiro positivo e u unidade em $\mathfrak{O}_\infty(V)$. □

Proposição 6.40. *Seja R um AAD com corpo de frações K, e $\mathfrak{m}$ o ideal maximal de R.*

(a) Se $z \in K$ e $z \notin R$, então $z^{-1} \in \mathfrak{m}$.

(b) Suponha $R \subset S \subset K$ e S também é AAD. Suponha que o ideal maximal de S contém $\mathfrak{m}$. Então $S = R$.

Demonstração. **(a)** Seja t o parâmetro uniformizante de R. Se $z \in K$ e $z \notin R$, então $z = ut^n$ com u unidade em R e n inteiro negativo. Assim $z^{-1} = (ut^n)^{-1} = vt^{-n}$, com v tal que $vu = 1$ (logo unidade de R), e $-n > 0$. Portanto $z^{-1} = vt^{-n} \in \mathfrak{m}$.

(b) Seja r parâmetro uniformizante de S. Como $S \subset K$, então $r = ut^n$, n inteiro e u unidade em R e em S consequentemente. Como $t \in S$, então $t = vr^m$, v unidade em S e m inteiro não negativo. Assim $r = uvr^{mn}$, o que implica que $uvr^{mn-1} = 1$. Portanto $mn = 1$, como $m > 0$, então $m = n = 1$. Assim $r = ut$, e $r \in R$.

Seja v uma unidade de S tal que $v \notin R$. Então $v = ut^m$, com u unidade em R e m inteiro negativo, pois $S \subset K$ e $v \notin R$. Mas então $u^{-1}t^{-m} \in R$ seria o inverso de v em S, e $u^{-1}t^{-m}$ seria uma unidade de S, uma contradição pois $\mathfrak{m}$ está contindo no ideal maximal de S, logo toda não unidade de R é uma não unidade em S. Portanto não existem unidades em S que não estão em R. E assim todo elemento de S, que pode ser escrito como vr^n com v unidade de R e n inteiro não negativo, é um elemento de R e $R = S$. □

Proposição 6.41. *Dado um corpo K e uma função de ordem $\phi : K \to \mathbb{Z} \cup \{\infty\}$, temos que o conjunto $R = \{z \in K \mid \phi(z) \geq 0\}$ é um AAD com ideal maximal $\mathfrak{m} = \{z \in K \mid \phi(z) > 0\}$. Reciprocamente, dado um AAD R com corpo de frações K, a função $ord : K \to \mathbb{Z} \cup \{\infty\}$ é uma função de ordem em K. Com isso concluímos que dar um AAD com corpo de frações K é equivalente a definir uma função de ordem em K.*

Demonstração. Pela Definição 3.13 R será um subanel de K, pois será fechado para a soma e o produto (visto que a soma e o produto de elementos de ordem não negativa geram

elementos de ordem não negativa). Provaremos que R é um AAD. Temos que $\mathfrak{m}$ é um ideal, pois dados quaisquer elementos $m_1, m_2 \in \mathfrak{m}$ e $r \in R$, $\phi(m_1 + m_2) \geq min(\phi(m_1), \phi(m_2)) > 0$ e $\phi(rm_1) = \phi(r) + \phi(m_1) > 0$.

Agora se 1_R é a unidade de R, temos que $\phi(1_R) = 0$ pois para todo $z \in R$, $\phi(z) = \phi(z * 1_R) = \phi(z) + \phi(1_R)$. Logo para u uma unidade em R, temos que $\phi(1) = \phi(u^{-1}u) = \phi(u^{-1}) + \phi(u) = 0$. Então $\phi(u) = \phi(u^{-1})$, mas como $u, u^{-1} \in R$, então $\phi(u) \geq 0$ e $\phi(u^{-1}) \geq 0$, logo $\phi(u) = \phi(u^{-1}) = 0$.

Então $\mathfrak{m}$ será o conjunto das não unidades de R, então o conjunto das não unidades de R forma um ideal e pelo Lema 3.1, $\mathfrak{m}$ será o único ideal maximal de R.

Provaremos que $\mathfrak{m}$ é ideal principal. Tome $\pi \in \mathfrak{m}$ tal que $\phi(\pi) = 1$ (que existe pois a função ϕ é sobrejetora). Assim para $\pi^{-1} \in K$, $\phi(\pi^{-1}) = -1$, logo dado $z \in \mathfrak{m}$, tal que $\phi(z) = n$, então $\phi((\pi^{-1})^n z) = \phi((\pi^{-1})^n) + \phi(z) = 0$. Logo $v = (\pi^{-1})^n z$ é uma unidade de R e $\pi^n v = z$. Portanto todo $z \in \mathfrak{m}$ pode ser escrito como $u\pi^n$ para uma unidade u de R e n natural. Assim $\mathfrak{m} = (\pi)$, e R é um AAD.

Reciprocamente, seja R é AAD com corpo de frações K, e parâmetro uniformizante t. Então temos que $ord(z) = \infty$ se, e somente se, $z = 0$. Além disso dados $z, h \in K$ com $z = ut^n$ e $h = vt^m$, temos que $ord(zh) = ord(uvt^{m+n}) = m + n = ord(z) + ord(h)$. Assumindo S.P.G que $n \geq m$, temos que $\phi(z+h) = \phi(ut^n + vt^m) = \phi(t^m(ut^{n-m} + v)) = \phi(t^m) + \phi(ut^{n-m} + v) = m + \phi(ut^{n-m} + v) \geq m = min(\phi(z), \phi(h))$. Portanto $ord : K \to \mathbb{Z} \cup \{\infty\}$ é uma função de ordem em K. □

Proposição 6.42. *Seja R um AAD com corpo de frações K, ord a função de ordem em K. Então:*

(a) Se $ord(a) < ord(b)$, então $ord(a + b) = ord(a)$.

(b) Se $a_1, \ldots, a_n \in K$ e para algum i, $ord(a_i) < ord(a_j)$ para todo $j \neq i$, então $a_1 + \cdots + a_n \neq 0$.

Demonstração. **(a)** Seja $ord(a) = n$ e $ord(b) = m$. Então $a = ut^n$ e $b = vt^m$ com u, v unidades em R. Assim $a + b = ut^n + vt^m = t^n(u + vt^{m-n})$. Então $ord(a + b) = ord(t^m(u + vt^{m-n})) = ord(t^m) + ord(u + vt^{m-n})$, e $u + vt^{m-n}$ é uma unidade, pois se $u + vt^{m-n} \in \mathfrak{m}$, então $u \in \mathfrak{m}$ uma contradição. Portanto $ord(a+b) = ord(t^m) + ord(u+vt^{m-n}) = m+0 = m$.

(b) Assuma que para algum i, $ord(a_i) < ord(a_j)$, para todo $j \neq i$. Considere a soma $a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n$. Por indução na propriedade (iii) da Definição 3.13, temos que

$ord(a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n) \geq min(ord(a_1), \ldots, ord(a_{i-1}), ord(a_{i+1}), \ldots, ord(a_n)) > ord(a_i)$. Assim pelo item (a), temos que $ord(a_1 + \cdots + a_n) = ord(a_i)$ e como $ord(a_i) \neq \infty$ (pois $ord(a_i) < ord(a_j)$), então $a_1 + \cdots a_n \neq 0$.

□

Proposição 6.43. *Seja R um AAD com ideal maximal $\mathfrak{m}$ e corpo de frações K. Suponha que um corpo k é subanel de R, e que a composição $k \to R \to R/\mathfrak{m}$ é um isomorfismo de k com $R/\mathfrak{m}$. Então:*

(a) Para qualquer $z \in R$, existe um único $\lambda \in k$ tal que $z - \lambda \in \mathfrak{m}$.

(b) Seja t um parâmetro uniformizante para R, $z \in R$. Então para qualquer $n \geq 0$, existem únicos $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ e $z_n \in R$ tais que $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}$.

Demonstração. **(a)** Dado $z \in R$, considere o resíduo de z em $R/\mathfrak{m}$, $z + \mathfrak{m}$. Como $k \cong R/\mathfrak{m}$, então existe um único $\lambda \in k$ tal que o resíduo de λ em $R/\mathfrak{m}$ é igual a $z+\mathfrak{m}$, assim $\lambda+\mathfrak{m} = z+\mathfrak{m}$, o que implica que $0 + \mathfrak{m} = z - \lambda + \mathfrak{m}$. Portanto $z - \lambda \in \mathfrak{m}$.

(b) Primeiro, provaremos a existência dos $\lambda_0, \ldots, \lambda_n \in k$ e $z_n \in R$ por indução.

Seja $n = 0$. Então existe um único $\lambda_0 \in k$ tal que $z - \lambda_0 \in \mathfrak{m}$ pelo item (a). Assim $z - \lambda_0 = bt^m$ para $b \in R$ unidade e $m \geq 1$ (pois $z - \lambda_0$ não é unidade). Assim $z = \lambda_0 + bt^m = \lambda_0 + (bt^{m-1})t$, como queríamos. Assuma que o resultado vale para um n positivo arbitrário. Então existem $\lambda_0, \ldots, \lambda_n \in k$ e $z_n \in R$ tais que

$$z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}$$

Podemos assumir que $z_n \notin k$, pois caso fosse bastaria tomar $z_n = \lambda_{n+1}$ e teríamos

$$z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + \lambda_{n+1} t^{n+1} + 0 * t^{n+2}$$

e o resultado seguiria.

Como $z_n \in R$, pelo item (a), existe único $\lambda \in k$ tal que $z_n - \lambda \in \mathfrak{m} \Rightarrow z_n - \lambda = bt^m$, para b unidade de R e $m \geq 1$. Assim $\lambda = z_n - bt^m$. Subtraindo $t^{n+1}bt^m$ à expressão de z, temos:

$$z - bt^{m+n+1} = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1} - bt^{m+n+1} =$$
$$\lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + (z_n - bt^m)t^{n+1} =$$
$$\lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + \lambda t^{n+1}$$

Então

$$z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + \lambda t^{n+1} + bt^{m+n+1} =$$
$$\lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + \lambda t^{n+1} + (bt^{m-1})t^{n+2}$$

E como $bt^{m-1} \in R$, temos o resultado.

Para provar a unicidade, sejam $\lambda_0, \ldots, \lambda_n, \gamma_0, \ldots, \gamma_n \in k$ e $z_n, y_n \in R$ tais que

$$\lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1} = z = \gamma_0 + \gamma_1 t + \cdots + \gamma_n t^n + y_n t^{n+1}$$

Então

$$(\lambda_0 - \gamma_0) + (\lambda_1 - \gamma_1)t + \cdots + (\lambda_n - \gamma_n)t^n + (z_n - y_n)t^{n+1} = 0$$

Se i é o menor indice tal que $(\lambda_i - \gamma_i) \neq 0$, então $ord((\lambda_i - \gamma_i)t^i) < ord((\lambda_j - \gamma_j)t^j))$ para todo $j \neq i$, e então pela Proposição 6.42 (b),

$$(\lambda_0 - \gamma_0) + (\lambda_1 - \gamma_1)t + \cdots + (\lambda_n - \gamma_n)t^n + (z_n - y_n)t^{n+1} \neq 0$$

Logo $\lambda_i = \gamma_i$ para todo $i = 1, \ldots, n$ e $z_n = y_n$, e temos a unicidade.

□

Proposição 6.44. *(1)* $(FG)_* = F_* G_*$; $(fg)^* = f^* g^*$.

(2) Se $F \neq 0$ *e* r *é a maior potência de* X_{n+1} *que divide* F, *então* $X_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

(3) $(F + G)_* = F_* + G_*$; $X_{n+1}^t (f + g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, *onde* $r = deg(g)$, $s = deg(f)$, *e* $t = r + s - deg(f + g)$.

Proposição 6.45. *(a) Existem $d+1$ monomios de grau d em $R[X,Y]$, e $\dfrac{(d+1)(d+2)}{2}$ monomios de grau d em $R[X,Y,Z]$.*

(b) Seja $V(d,n) = \{$formas de grau d em $k[X_1,\ldots,X_n]\}$, k um corpo. Então $V(d,n)$ é um espaço vetorial sobre k e os monomios de grau d formam uma base. Assim dim $V(d,1) = 1$; dim $V(d,2) = d+1$; dim $V(d,3) = \dfrac{(d+1)(d+2)}{2}$.

(c) Sejam $L_1, L_2, \ldots$ e $M_1, M_2, \ldots$ sequências de formas lineares em $k[X,Y]$ e assuma que não existe $L_i = \lambda M_j$, $\lambda \in k$. Seja $A_{ij} = L_1L_2\cdots L_iM_1M_2\cdots M_j$, $i,j \geq 0$ (e $A_{00} = 1$). Então $\{A_{ij} \mid i+j = d\}$ forma uma base de $V(d,2)$.

Demonstração. Para o item (a), basta um argumento de combinatória, dado que o número de monômios em $k[X,Y]$ de grau d é o mesmo número de soluções não negativas da equação $a+b=d$ (onde cada X^aY^b é um monômio), que será $d+1$. De forma semelhante, o número de monômios de grau d em $k[X,Y,Z]$ será o número de soluções não negativas da equação $a+b+c=d$ (onde cada $X^aY^bZ^c$ é um monômio) que será $\dfrac{(d+1)(d+2))}{2}$.

O item (b) é resultado direto do fato de que a dado duas formas de grau d, $F, G \in V(d,n)$, $F+G$ também é uma forma de grau d e para qualquer $\lambda \in k$, $\lambda \cdot F$ será uma forma de grau d. Além disso o conjunto dos monômios de grau d forma uma base pois dada qualquer forma $F \in V(d,n)$, temos que $F = \sum \lambda_i X_1^{a_{1i}} \cdots X_n^{a_{ni}}$, com $\sum_{j=1}^{n} a_{ij} = d$ para todo i. Logo os monômios de grau d geram $V(d,n)$, e como os monômios são $L.I$ (dado que se a soma de qualquer dois monômios distintos é igual a zero, então ambos devem ser multiplicados por zero), então os monômios de grau d formam uma base para $V(d,n)$.

Para o item (c) note que cada A_{ij} tal que $i+j=d$ terá a forma $\alpha_0X^d + \alpha_1X^{d-1}Y + \cdots + \alpha_1XY^{d-1} + \alpha_dY^d$ dado que será uma mutiplicação de d formas lineares em $k[X,Y]$. Note também que para os $d+1$ A_{ij} distintos tais que $i+j=d$, e com $A_{ij} = \alpha_0X^d + \alpha_1X^{d-1}Y + \cdots + \alpha_1XY^{d-1} + \alpha_dY^d$ podemos por uma sequência finita de combinações lineares entre os A_{ij} obter qualquer monômio X^aY^b de grau d , num processo de "escalonar" todos os monômios distintos de X^aY^b. Assim podemos gerar a base para $V(d,2)$ e o conjunto $\{A_{ij} \mid i+j=d\}$ gera $V(d,2)$.

□

Lema 6.3. *Para ideais I_1, I_2, J de um anel R*

(a) $(I_1 + I_2)J = I_1J + I_2J$;

(b) $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$

Demonstração. **(a)** O ideal $(I_1 + I_2)J$ é gerado pelos elementos $(a_1 + a_2)b$, onde $a_1 \in I_1$, $a_2 \in I_2$ e $b \in J$. Como $(a_1 + a_2)b = a_1b + a_2b \in I_1J + I_2J$, então $I_1J + I_2J$ contém todos os geradores de $(I_1 + I_2)J$ e assim $(I_1 + I_2)J \subset I_1J + I_2J$.

Temos que I_1J é gerado por elementos a_1b, com $a_1 \in I_1$ e $b \in J$. Como $a_1b \in (I_1 + I_2)J$, então $(I_1+I_2)J$ contém todos os geradores de I_1J, e assim $I_1J \subset (I_1+I_2)J$. Da mesma forma, $(I_1 + I_2)J$ contém todos os elementos da forma a_2c, onde $a_2 \in I_2$ e $c \in J$, logo $(I_1 + I_2)J$ contém todos os geradores de I_2J e $I_2J \subset (I_1 + I_2)J$. Como $I_1J + I_2J$ é o menor ideal que contém ambos I_1J e I_2J, então $I_1J + I_2J \subset (I_1 + I_2)J$. Portanto $(I_1 + I_2)J = I_1J + I_2J$.

(b) Primeiro veja que dados quaisquer ideais I_1 e I_2 de um anel comutativo, temos que $I_1I_2 = I_2I_1$ pois ambos são gerados pelos elementos $ab = ba$, com $a \in I_1$ e $b \in I_2$. Provaremos o resultado por indução. Para $n = 1$ temos a igualdade diretamente. Assuma que o resultado é válido para algum n positivo qualquer, logo $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$. Então $(I_1 \cdots I_N)^{n+1} = I_1 \cdots I_N I_1^n \cdots I_N^n$. Pela comutatividade da multiplicação de ideais em um anel comutativo, temos que $I_1 \cdots I_N I_1^n \cdots I_N^n = I_1 I_1^n \cdots I_N I_N^n$. E $I_j I_j^n = I_j^{n+1}$ por definição, logo $(I_1 \cdots I_N)^{n+1} = I_1^{n+1} \cdots I_N^{n+1}$. □

Proposição 6.46. *Sejam I, J ideais em um anel R. Suponha que I é finitamente gerado e $I \subset Rad(J)$. Então $I^m \subset J$ para algum m.*

Demonstração. Como I é finitamente gerado, então existem x_i, $i = 1, \ldots, n$, tais que $I = \sum_{i=1}^n Rx_i$. Como $I \subset Rad(J)$, então para cada x_i existe um m_i tal que $x_i^{m_i} \in J$. Assim, tomando $M = max(\{m_i : i = 1, \ldots, n\})$, temos que $x_i^M \in J$ para todo i.

Considere então o ideal I^{nM}. Temos que I^{nM} é gerado pelos elementos $x_1^{i_1} \cdots x_n^{i_n}$, tais que $\sum_{j=1}^n i_j = nM$. Assim para qualquer $x_1^{i_1} \cdots x_n^{i_n}$, deve existir algum x_i com potência maior ou igual a M, pois se todo $x_j^{i_j}$ for tal que $i_j < M$, então $\sum_{j=1}^n i_j < nM$, uma contradição.

Logo todo elemento gerador de I^{nM} pertence a J e portanto $I^{nM} \subset J$.

□

Proposição 6.47. *(a) Suponha I, J ideais comaximais de R. Então $I + J^2 = R$. Além disso, para quaisquer m, n, I^m e J^n são comaximais.*

(b) Suponha $I_1, \ldots, I_N$ são ideais em R e I_i e $J_i = \cap_{j \neq i} I_j$ são comaximais para todo i. Então $I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n$ para todo n.

Proposição 6.48. *(a) Sejam $I \subset J$ ideais de um anel R. Então existe um homomorfismo natural de R/I para R/J.*

(b) Seja I um ideal de um anel R, R um subanel de um anel S. Então existe um homomorfismo natural entre R/I e S/IS

Demonstração. **(a)** A função $T : R/I \to R/J$ que leva $x+I$ em $T(x+I) = x+J$ será uma aplicação entre aneis bem definida, pois se $x+I = y+I$, temos que $x-y \in I$, logo $x-y \in J$ e $x+J = y+J$. Além disso será um homomorfismo pois dados $x+I, y+I \in R/I$ temos:

(i) $T((x+I)+(y+I)) = T(x+y+I) = x+y+J = (x+J)+(y+J) = T(x+I)+T(y+I)$

(ii) $T((x+I)(y+I)) = T(xy+I) = xy+J = (x+J)(y+J) = T(x+I)T(y+I)$

(b) Dado $x+I \in R/I$, temos que a aplicação $T : R/I \to S/IS$ que leva $x+I$ em $x+IS$ é bem definida, pois se $x+I = y+I$, então $x-y \in I$ o que implica que $x-y \in IS$ (pois $I \subset IS$), e assim $x+IS = y+IS$. Além disso para quaisquer $x+I, y+I \in R/I$ temos:

(i) $T((x+I)+(y+I)) = T(x+y+I) = x+y+IS = (x+IS)+(y+IS) = T(x+I)+T(y+I)$

(ii) $T((x+I)(y+I)) = T(xy+I) = xy+IS = (x+IS)(y+IS) = T(x+I)T(y+I)$

□

Proposição 6.49. *Seja $P = (0, \ldots, 0) \in \mathbb{A}^n$, $\mathfrak{O} = \mathfrak{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Seja $I \subset k[X_1, \ldots, X_n]$ o ideal gerado por $X_1, \ldots, X_n$. Então $I\mathfrak{O} = \mathfrak{m}$, assim $I^r\mathfrak{O} = m^r$ para todo r.*

Demonstração. Dado um elemento $\dfrac{f}{g} \in \mathfrak{m}$, temos que $\dfrac{f}{g}$ não é inversível em $\mathfrak{O}$ o que implica que $\dfrac{g}{f} \notin \mathfrak{O}$ e temos que $f(P) = 0$. Assim temos que f deve ser tal que $f = \sum X_1^{i_1} \cdots X_n^{i_n}$ com $i_j > 0$ para algum j em todo i e assim $f \in I$. Logo $\dfrac{f}{g} \in I\mathfrak{O}$ e portanto $\mathfrak{m} \subset I\mathfrak{O}$. Como $\mathfrak{O}$ é ideal maximal e $I\mathfrak{O}$ é um ideal de $\mathfrak{O}$, então $\mathfrak{m} = I\mathfrak{O}$.

□

Proposição 6.50. *Seja V uma variedade em $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n], P \in V$ e seja J um ideal de $k[X_1, \ldots, X_n]$ que contém I. Seja J' a imagem de J em $\Gamma(V)$. Então existe um homomorfismo natural ϕ de $\mathfrak{O}_P(\mathbb{A}^n)/J\mathfrak{O}_P(\mathbb{A}^n)$ para $\mathfrak{O}_P(V)/J'\mathfrak{O}_P(V)$ e ϕ é um isomorfismo. Em particular, $\mathfrak{O}_P(\mathbb{A}^n)/I\mathfrak{O}_P(\mathbb{A}^n)$ é isomorfo a $\mathfrak{O}_P(V)$.*

Demonstração. Seja $\pi : k[X_1, \ldots, X_n] \to \Gamma(V)$ a projeção natural. Considere a função $\phi : \mathfrak{O}_P(\mathbb{A}^n)/J\mathfrak{O}_P(\mathbb{A}^n) \to \mathfrak{O}_P(V)/J'\mathfrak{O}_P(V)$, defina como: dado $\frac{a}{b}+J\mathfrak{O}_P(\mathbb{A}^n) \in \mathfrak{O}_P(\mathbb{A}^n)/J\mathfrak{O}_P(\mathbb{A}^n)$, tome

$$\phi(\frac{a}{b} + J\mathfrak{O}_P(\mathbb{A}^n)) = \frac{\pi(a)}{\pi(b)} + J'\mathfrak{O}_P(V) \in \mathfrak{O}_P(V)/J'\mathfrak{O}_P(V)$$

Temos que se $\frac{a}{b} \in \mathfrak{O}_P(\mathbb{A}^n)$, então $a, b \in \Gamma(\mathbb{A}^n) = k[X_1, \ldots, X_n]$, assim $\pi(a), \pi(b) \in \Gamma(V)$, e note que como $b(P) \neq 0$, então $\pi(b)(P) \neq 0$. A função ϕ estará bem definida pois se $\frac{a}{b}$ e $\frac{c}{d}$ são representantes da mesma classe em $\mathfrak{O}_P(\mathbb{A}^n)/J\mathfrak{O}_P(\mathbb{A}^n)$, então $\frac{ad-cb}{bd} \in J\mathfrak{O}_P(\mathbb{A}^n)$, e $ad - cb \in J$. Logo $\pi(ad - cb) \in J'$, o que implica que

$$\phi(\frac{ad-cb}{bd} + \mathfrak{O}_P(\mathbb{A}^n)/J\mathfrak{O}_P(\mathbb{A}^n)) = \frac{\pi(ad-cb)}{\pi(bd)} + \mathfrak{O}_P(V)/J'\mathfrak{O}_P(V) = 0$$

como desejado. Além disso será um homomorfismo pois π é um homomorfismo.

Seguindo, mostraremos que ϕ é um isomorfismo. Se $\phi(\frac{a}{b}+J\mathfrak{O}_P(\mathbb{A}^n)) = 0+\mathfrak{O}_P(V)/J'\mathfrak{O}_P(V)$, então $\frac{\pi(a)}{\pi(b)} \in J'\mathfrak{O}_P(V)$, o que implica que $\pi(a) \in J'$, mas como J' é a imagem de J em $\Gamma(V)$, temos que $a \in J$. Logo $\frac{a}{b} + J\mathfrak{O}_P(\mathbb{A}^n) = 0 + J\mathfrak{O}_P(\mathbb{A}^n)$ e ϕ é injetiva.

Dado $\frac{c}{d} + J'\mathfrak{O}_P(V) \in \mathfrak{O}_P(V)/J'\mathfrak{O}_P(V)$, temos que $c, d \in \Gamma(V)$. Como o homomorfismo natural π é sobrejetor, então existem $a, b \in k[X_1, \ldots, X_n]$ tais que $\pi(a) = c$ e $\pi(b) = d$. Logo

$$\pi(\frac{a}{b} + J\mathfrak{O}_P(\mathbb{A}^n)) = \frac{c}{d} + J'\mathfrak{O}_P(V),$$

e ϕ será sobrejetora, e portanto um isomorfismo.

□

Proposição 6.51. *Dados $I, J \subset k[X_1, \ldots, X_n]$ com k algebricamente fechado, então I e J são comaximais se, e somente se, $V(I) \cap V(J) = \emptyset$.*

Demonstração. ($\Rightarrow$) Se $V(I) \cap V(J) \neq \emptyset$, então existe $P \in \mathbb{A}^n$ tal que $P \in V(I)$ e $P \in V(J)$. Logo como para todo elemento $f \in I + J$ temos que $f = h + g$ com $h \in I$ e $g \in J$, então $f(P) = h(P) + g(P) = 0$ e $I + J$ não pode ser igual a $k[X_1, \ldots, X_n]$ (pois dada qualquer constante não nula $a \in k$, $a \in k[X_1, \ldots, X_n]$ e $a(P) = a \neq 0$).

($\Leftarrow$) Se $V(I) \cap V(J) = \emptyset$, então $V(I \cup J) = V(I) \cap V(J) = \emptyset$. Como $V(I \cup J) = V(I + J)$

(pois $I+J$ é gerado pelos elementos de $I \cup J$), então $V(I+J) = \emptyset$ e pela versão fraca do Teorema dos Zeros $I+J$ não é um ideal próprio, logo $I+J = k[X_1, \ldots, X_n]$ e I e J são comaximais. □

Proposição 6.52. *Seja $I = (X, Y) \subset k[X, Y]$. Então $dim_k(k[X, Y]/I^n) = 1+2+\cdots+n = \frac{n(n+1)}{2}$*

Demonstração. Temos que I^n é o ideal gerado por todos os elementos X^iY^{n-i}, com $i = 0, 1, \ldots, n$. Considerando então $k[X, Y]/I^n$, temos que para toda classe de equivalência com representate X^iY^j com $i + j >= n$ é a mesma classe do elemento nulo pois, $X^iY^j + I^n = X^{i-k}Y^{j-l}X^kY^l + I^n$ (aqui $k + l = n$, logo $X^kY^l \in I^n$) e então

$$X^iY^j + I^n = (X^{i-k}Y^{j-l} + I^n)(X^kY^l + I^n) = (X^{i-k}Y^{j-l} + I^n)(0 + I^n) = I^n.$$

Portanto para obter uma base de $k[X, Y]/I^n$ como um espaço vetorial sobre k, basta considerar $\{X^iY^j + I^n \in k[X, Y]/I^n \mid i + j < n\}$, isto é as classes cujos representantes são monômios de grau menor que n. Pela Proposição 6.45 (a) existem $d+1$ monômios de grau d em $k[X, Y]$, logo para cada $i = 0, 1, \cdots, n-1$, teremos $i+1$ monômios de grau i, totalizando $\sum_{i=0}^{n+1} i + 1 = \frac{n(n+1)}{2}$ elementos na base. Logo $dim_k(k[X, Y]/I^n) = \frac{n(n+1)}{2}$.

□

Proposição 6.53. *(a) Seja N um submódulo de M, $\pi : M \to M/N$ o homomorfismo natural de M para M/N. Suponha $\phi : M \to M'$ um homomorfismo tal que $\phi(N) = 0$. Então existe um único homomorfismo $\overline{\phi} : M/N \to M'$ tal que $\overline{\phi} \circ \pi = \phi$.*

(b) Se N e P são submódulos de M com $P \subset N$ então existem homomorfismos naturais de M/P para M/N e de N/P para M/P e a sequência

$$0 \to N/P \to M/P \to M/N \to 0$$

é exata.

(c) Sejam $U \subset W \subset V$ espaços vetoriais com V/U de dimensão finita. Então $dim V/U = dim\ V/W + dim\ W/U$.

(d) Se $J \subset I$ são ideais de um anel R, então existe uma sequência exata

$$0 \to I/J \to R/J \to R/I \to 0$$

(e) Se $\mathfrak{O}$ é um anel local com ideal maximal $\mathfrak{m}$, existe uma sequência exata natural de $\mathfrak{O}$-módulos

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathfrak{O}/\mathfrak{m}^{n+1} \to \mathfrak{O}/\mathfrak{m}^n \to 0$$

Demonstração. (a) : Assuma que existam dois homomorfismos $\overline{\psi}$ e $\overline{\phi}$ respeitando a igualdade. Como π é sobrejetora, para todo $b' \in M/N$, existe $b \in M$ tal que $\pi(b) = b'$. Logo para qualquer $b' \in M/N$, $\overline{\phi}(b') = \overline{\phi}(\pi(b)) = \phi(b)$ (note que a igualdade é válida sem problemas pois para todo $z \in N$, $\phi(z) = 0$). Da mesma forma $\overline{\psi}(b') = \overline{\psi}(\pi(b)) = \phi(b)$, portanto $\overline{\phi}(b') = \overline{\psi}(b')$, $\forall b' \in M/N$, assim $\overline{\psi} = \overline{\phi}$.

(b) : Considere o homomorfismo $\phi : N/P \to M/P$, definido como $\phi(m + P) = m + P \in M/P$, para todo $m + P \in N/P$, e o homomorfismo $\psi : M/P \to M/N$ definido como $\psi(m+P) = m+N$. Ambos estarão bem definidos pois se ϕ é a inclusão (logo se elementos são representantes de classes equivalentes em N/P também serão em M/P), e dados elementos $m, l \in M$ tais que $m - l \in P$, então $m - l \in N$ e assim $\psi(m - l + P) = m - l + N = 0 + N$ e ψ está bem definida. Ambos serão homomorfismos pois ϕ é a inclusão e $\psi(\alpha \cdot m + l + P) = \alpha \cdot m + l + N = \alpha\psi(m + P) + \psi(l + P)$. Seguindo, mostraremos que a sequência

$$0 \to N/P \xrightarrow{\phi} M/P \xrightarrow{\psi} M/N \to 0,$$

é exata mostrando que ϕ é injetiva e ψ é sobrejetora. Seja $m + P \in N/P$ tal que $\phi(m + P) = 0 + P$, como $\phi(m + P) = m + P = 0 + P$, então $m \in P$ e assim $m + P = 0 + P$, logo ϕ é injetiva. Dado $l + N \in M/N$, então $l \in M$ e assim $\psi(l + P) = l + N$, e temos que ψ é sobrejetora.

(c) : Segue diretamente do item (b) e do item (1) da Proposição 3.6.

(d) : Análogo ao item (b), os homomorfismos naturais $\phi : I/J \to R/J$ e $\psi : R/J \to R/I$ serão definidos da mesma forma que no item (b), porém os considerando como homomorfismos de anéis.

(e) : É resultado direto do item (b), vendo $\mathfrak{m}^n$, $\mathfrak{m}^{n+1}$ e $\mathfrak{O}$ como $\mathfrak{O}$-módulos, pois $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n \subset \mathfrak{O}$.

□

Proposição 6.54. *Seja R um AAD satisfazendo as condições da Proposição 6.43. Então $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ é um R-módulo e também um k-módulo dado que $k \subset R$.*

(a) para todo $n \geq 0$, $dim_k\ (\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$.

(b) para todo $n > 0$, $dim_k(R/\mathfrak{m}^n) = n$.

(c) Seja $z \in R$, então $ord(z) = n$ se $(z) = \mathfrak{m}^n$ e assim $ord(z) = dim_k\ (R/(z))$

Demonstração. (a): Seja t o parâmetro uniformizante de R. Então, $\mathfrak{m}^n$ é o ideal que possui todos os elementos ut^j com $j \geq n$ e u unidade de R. Ao quocientar por $\mathfrak{m}^{n+1}$ que possui todos os elementos da forma ut^l com $l \geq n+1$, então todo elemento não nulo $ut^j + \mathfrak{m}^{n+1} \in \mathfrak{m}^n/\mathfrak{m}^{n+1}$ terá como representante um elemento da forma ut^n, com u unidade de R. Assim tem como base um único elemento t^n e $dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$.

(b): Provaremos por indução. Temos que $dim_k(R/\mathfrak{m}^1) = dim_k(k) = 1$. Assuma que para um dado $n > 0$, $dim_k(R/\mathfrak{m}^n) = n$. Utilizando o item (c) da Proposição 6.53, temos a seguinte relação $dim_k(R/\mathfrak{m}^{n+1}) = dim_k(R/m^n) + dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ e pela hipótese de indução e o item (a), temos que $dim_k(R/m^n) + dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1$, assim $dim_k(R/\mathfrak{m}^{n+1}) = n + 1$ como desejado.

(c) : Seja t o parâmetro uniformizante de R. Seja $z = ut^j$, $j \in \mathbb{N}$. Então (z) é gerado por ut^j, mas como $(z) = \mathfrak{m}^n$ que é gerado por t^n, então temos que $z = ut^j = ht^n$, com $h \in R$, logo $j \geq n$ e temos que $t^n = aut^j$, com $a \in R$, assim $n \geq j$ e $j = n$. Portanto $z = ut^n$ e $ord(z) = n$. □

Resultados do Capítulo 5

Proposição 6.55. *Seja $F \in k[X_1, \ldots, X_{n+1}]$ (k infinito). Escreva $F = \sum F_i$, onde F_i é uma forma de grau i. Seja $P \in \mathbb{P}^n(k)$, e suponha $F(x_1, \ldots, x_{n+1}) = 0$ para toda escolha de coordenadas homogêneas $(x_1, \ldots, x_{n+1})$ de P. Então para todo i, $F_i(x_1, \ldots, x_{n+1}) = 0$ para todas as coordenadas homogêneas de P.*

Demonstração. Fixe coordenadas $(x_1, \ldots, x_{n+1})$ homogêneas de P. Note que o polinômio, $G \in k[Y]$, com $G(Y) = \sum Y^i F_i(x_1, \ldots, x_{n+1})$ é tal que $\forall \lambda \in k$, $G(\lambda) = \sum \lambda^i F_i(x_1, \ldots, x_{n+1}) = \sum F_i(x_1, \ldots, \lambda x_{n+1}) = F(\lambda x_1, \ldots, \lambda x_{n+1}) = 0$, pois $(\lambda x_1, \ldots, \lambda x_{n+1})$ também serão coordenadas homogêneas de P. Assim $G(\lambda) = 0$ para todo elemento λ de k e $G = 0$ pela Proposição

6.2. Assim $F_i(x_1, \ldots, x_{n+1}) = 0$, para todo i e o resultado é válido para todas coordenadas homogêneas de P, como desejado.

□

Proposição 6.56. *Seja I um ideal homogêneo de $k[X_1, \ldots, X_{n+1}]$. Então I é primo se, e somente se, a seguinte condição é satisfeita: dadas quaisquer formas $F, G \in k[X_1, \ldots, X_{n+1}]$, se $FG \in I$ então $F \in I$ ou $G \in I$*

Demonstração. Se I é ideal primo temos a condição da própria definição de ideal primo, pois se $FG \in I$, então $F \in I$ ou $G \in I$ para quaisquer $F, G \in k[X_1, \ldots, X_{n+1}]$.

Reciprocamente, seja a condição válida e assuma por absurdo que I não é ideal primo, isto é, existem $F, G \in k[X_1, \ldots, X_{n+1}]$ tais que $FG \in I$ mas $F \notin I$ e $G \notin I$. Podemos assumir que F e G sejam os polinômios de menor grau tal que isso aconteça. Como I é ideal homogêneo, então ao escrevermos $FG = \sum H_i$, com H_i uma forma de grau i, então $H_i \in I$ para todo i. Em particular, a forma H_m de maior grau será o produto dos termos de maior grau de F e G, digamos a_F e a_G. Assim $a_F a_G \in I$, mas como isso é um produto de formas, pela condição temos que $a_F \in I$ ou $a_G \in I$. Seja, S.P.G, $a_F \in I$. Então $FG - a_F G = (F - a_F)G \in I$, mas note que $G \notin I$ e $(F - a_F) \notin I$ (pois caso contrário $F = (F - a_F) + a_F \in I$), mas isso é uma contradição com a minimalidade do grau de FG. □

Proposição 6.57. *Seja I um ideal homogêneo em $k[X_1, \ldots, X_{n+1}]$ e*

$$\Gamma = k[X_1, \ldots, X_{n+1}]/I.$$

As formas de grau d de Γ (unidas da constante nula) formam um espaço vetorial de dimensão finita sobre k.

Demonstração. É fácil ver que as formas de grau d de Γ, formarão um espaço vetorial sobre k, dado que se $f, g \in \Gamma$ são formas de grau d, então $f + g$ é uma forma de grau d de Γ e o mesmo para λf (com $\lambda \in k$).

Uma base (finita) para o dado espaço vetorial é a base formada por todos os produtos $X_1^{i_1} \cdots X_{n+1}^{i_{n+1}}$ tais que $\sum_{j=1}^{n+1} i_j = d$.

□

Proposição 6.58. *Um conjunto $V \subset \mathbb{P}^n(k)$ é chamado de uma subvariedade linear se $V = V(H_1, \ldots, H_r)$, onde cada H_i é uma forma de grau* 1.

(a) *Se T é uma mudança de coordenadas projetivas, então $V^T = T^{-1}(V)$ também é uma subvariedade linear.*

(b) *Existe uma mudança de coordenadas projetiva T de $\mathbb{P}^n$ tal que $V^T = V(X_{m+2}, \ldots, X_{n+1})$, então V é uma variedade.*

(c) *O número m que aparece no item (b) é independente da escolha de T. m então é chamado de dimensão de V ($m = -1$ se $V = \emptyset$).*

Proposição 6.59. *Sejam $H_1, \ldots, H_m$ hiperplanos em $\mathbb{P}^n$, $m \leq n$. Então $H_1 \cap H_2 \cap \cdots \cap H_m \neq \emptyset$.*

Proposição 6.60. *Sejam $P = [a_1 : \cdots : a_{n+1}]$, $Q = [b_1 : \cdots : b_{n+1}]$ pontos distintos de $\mathbb{P}^n$. A reta que passa por P e Q é definida como*

$$L = \{[\lambda a_1 + \mu b_1 : \cdots : \lambda a_{n+1} + \mu b_{n+1}] \mid \lambda, \mu \in k,\ \lambda \neq 0 \text{ ou } \mu \neq 0\}$$

São válidos os mesmos resultados, na versão projetiva, da Proposição 6.35.

Proposição 6.61. *Quaisquer duas retas distintas em $\mathbb{P}^2$ se intersectam em um ponto.*

Proposição 6.62. *Seja z uma função racional em uma variedade projetiva V. O conjunto de polos de z é um subconjunto algébrico de V.*

Proposição 6.63. *Sejam P_1, P_2, P_3 (respectivamente, Q_1, Q_2, Q_3) três pontos em $\mathbb{P}^2$ que não estão em uma mesma reta. Existe uma mudança de coordenadas $T : \mathbb{P}^2 \to \mathbb{P}^2$ tal que $T(P_i) = Q_i$, $i = 1, 2, 3$. Adicionalmente, podemos estender esse resultado para $n + 1$ pontos em $\mathbb{P}^n$ que não estão em um mesmo hiperplano.*

Proposição 6.64. *Se $I = (F)$ é o ideal de uma hipersuperfície afim, então $I^* = (F^*)$.*

Demonstração. Por definição I^* será o ideal gerado por G^*, onde $G \in (F)$. Assim $G = HF$, $H \in k[X_1, \ldots, X_n]$, pela Proposição 6.44, $G^* = (HF)^* = H^*F^*$. Logo todo gerador de I^* é gerado por F^* e temos o resultado.

□

Proposição 6.65. *Seja V uma variedade em $\mathbb{P}^n$ e $V \supset H_\infty$. Então $V = \mathbb{P}^n$ ou $V = H_\infty$. Se $V = \mathbb{P}^n$, então $V_* = \mathbb{A}^n$, enquanto $V_* = \emptyset$ se $V = H_\infty$.*

Demonstração. Assuma que $H_\infty \subsetneq V \subsetneq \mathbb{P}^n$, e tome $F \in I(V)$ $(F \neq 0)$. Como $H_\infty \subsetneq V$, então $I(V) \subset I(H_\infty) = (X_{n+1})$, assim $F = X_{n+1}^r G$ (com r a maior potência de X_{n+1} que divide F). Como V é uma variedade, $I(V)$ é ideal primo, assim $X_{n+1} \in I(V)$ ou $G \in I(V)$. Temos que $X_{n+1} \notin I(V)$ pois $H_\infty \subsetneq V$, logo existe $P \in V$ tal que $P \in U_{n+1}$. Portanto $G \in I(V)$, porém isso é uma contradição pois claramente existe algum ponto Q em H_∞ (logo em V) tal que $G(Q) \neq 0$ (pela Proposição 6.2). Portanto $V = H_\infty$ ou $V = \mathbb{P}^n$.

Se $V = \mathbb{P}^n$, então $I(V) = \{0 \in k[X_1, \ldots, X_{n+1}]\}$ e $I_*(V) = \{0 \in k[X_1, \ldots, X_n]\}$, logo $V_* = V(I_*(V)) = \mathbb{A}^n$.

Caso $V = H_\infty$, então $I(V) = (X_{n+1})$ e $I_*(V) = k[X_1, \ldots, X_n]$, logo $V_* = V(I_*(V)) = \emptyset$. □

Proposição 6.66. *Seja $P = [0 : 1 : 0] \in \mathbb{P}^2(k)$. Então as retas que passam por P são:*

(a) As retas "verticais" $L_\lambda = V(X - \lambda Z) = \{[\lambda : t : 1] \mid t \in k\} \cup \{P\}$

(b) A reta no infinito $L_\infty = V(Z) = \{[x : y : 0] \mid x, y \in k\}$

Proposição 6.67. *Seja $P = [x : y : z] \in \mathbb{P}^2$. Então:*

(a) $\{(a, b, c) \in \mathbb{A}^3 \mid ax + by + cz = 0\}$ é um hiperplano em $\mathbb{A}^3$.

(b) Para qualquer conjunto finito de pontos em $\mathbb{P}^2$, existe uma reta que não passa por nenhum deles.

Resultados do Capítulo 6

Proposição 6.68. *Seja F uma curva plana projetiva. Um ponto P é um ponto múltiplo de F se, e somente se, $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$.*

Proposição 6.69. *Seja P um ponto simples em F. A reta tangente à F em P tem a equação $F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$.*

Proposição 6.70. *Seja $P = [0 : 1 : 0]$, F uma curva de grau n, $F = \sum F_i(X, Z)Y^{n-i}$, F_i uma forma de grau i. Então $m_P(F)$ é o menor m tal que $F_m \neq 0$, e os fatores de F_m determinam as tangentes de F em P.*

Proposição 6.71. *Duas curvas planas sem componentes em comum intersectam apenas em um número finito de pontos.*

Proposição 6.72. *Sejam $P_1, \ldots, P_n \in \mathbb{P}^2$. Existem infinitas retas passando por P_1, mas que não passam por $P_2, \ldots, P_n$. Se P_1 é um ponto simples em F, podemos tomar essas retas transversais à F em P_1.*