UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM MATEMÁTICA

Paulo Terra Silva Amorim

A Configuração das 27 retas

Juiz de Fora
2023

Paulo Terra Silva Amorim

A Configuração das 27 retas

Trabalho de Conclusão de curso apresentado ao Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Orientador: Prof. Dr. Frederico Sercio Feitosa

Juiz de Fora

2023

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

Amorim, Paulo Terra Silva.
A Configuração das 27 retas / Paulo Terra Silva Amorim. – 2023.
126 f. : il.

Orientador: Frederico Sercio Feitosa
Trabalho de Conclusão de Cruso – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Bacharelado em Matemática, 2023.

1. superfícies. 2. cúbicas. 3. retas. I. Feitosa, Frederico Sercio, orient. II. Título.

Paulo Terra Silva Amorim

A Configuração das 27 retas

Trabalho de Conclusão de curso apresentado ao Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Aprovada em 05 de Dezembro de 2023

BANCA EXAMINADORA

Prof. Dr. Frederico Sercio Feitosa - Orientador
Universidade Federal de Juiz de Fora

Profa. Dra. Flaviana Andrea Ribeiro
Universidade Federal de Juiz de Fora

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

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador, Frederico, pela imensa paciência e disposição. Aos meus amigos, Luiz, Luca, Fernando e Pedro pelo apoio e companhia durante o tempo em que trabalhei nesse projeto. À minha família pelo apoio e paciência. À Fernanda, pelo carinho e atenção.

When one has finished a substantial paper there is commonly a mood in which it seems that there is really nothing in it. Do not worry, later on you will be thinking "at least I could do something good then". (Littlewood, John E.; Littlewood's Miscellany 1986).

RESUMO

Este trabalho tem o objetivo de estudar conceitos iniciais de geometria algébrica. Começamos estudando variedades afins e a topologia de Zariski. Posteriormente, passamos a estudar variedades projetivas, pontos suaves e o conceito de dimensão. Depois, nos dedicamos ao estudo de curvas e à definição de uma superfície cúbica. Por fim, demonstramos que toda superfície cúbica possui uma reta e que toda superfície cúbica suave definida sobre um corpo algebricamente fechado contém exatamente 27 retas.

Palavras-chave: 27 retas, cúbica, superfície cúbica.

ABSTRACT

This work aims to study the initial concepts of algebraic geometry. We begin by examining affine varieties and the Zariski topology. Next, we move on to the study of projective varieties, smooth points, and the concept of dimension. Later, we delve into the analysis of curves and the definition of a cubic surface. In conclusion, we demonstrate that every cubic surface has a line and that every smooth cubic surface over a closed algebraic field has exactly 27 lines.

Keywords: 27 lines, cubic, cubic surface.

LISTA DE FIGURAS

Figura 1 – Curva cúbica. 15
Figura 2 – Um círculo $x^2 + y^2 - 1 = 0$, uma parábola $y - x^2 = 0$ e uma hipérbole $xy - 1 = 0$ respectivamente são exemplos de curvas não degeneradas. . 15
Figura 3 – Exemplos de cônicas degeneradas, cujas equaçoes são $(x - y)(x + y) = 0$, $x^2 - 1 = 0$ e $x^2 = 0$ ou $x = 0$, respectivamente. 16
Figura 4 – A parábola semicúbica $y^2 = x^3$. 16
Figura 5 – Deformações da curva C_λ. 17
Figura 6 – Eixos coordenados como um exemplo de variedade redutível. 22
Figura 7 – Diagrama. 30
Figura 8 – Diagrama. 31
Figura 9 – A variedade quasi-afim $\mathbb{A}^1_k \setminus \{1\} = (\mathbb{A}^1_k)_{(x-1)} \subset \mathbb{A}^1_k$ é isomorfa à variedade afim $W \subset \mathbb{A}^2_k$ dada por $t(x - 1) = 1$. 41
Figura 10 – A reta real projetiva $\mathbb{P}^1_{\mathbb{R}}$. 43
Figura 11 – Decomposição do espaço projetivo real $\mathbb{P}^2_{\mathbb{R}}$. 44
Figura 12 – Quádrica em $\mathbb{P}^3$ com suas decisões. 47
Figura 13 – Diagrama. 62
Figura 14 – Diagrama. 64
Figura 15 – O espaço tangente da variedade V no ponto P. 66
Figura 16 – Casos do Lema 5.1. 77
Figura 17 – Interseção da parábola semicúbica com os eixos coordenados. 80
Figura 18 – Cúbicas planas que se decompõe em uma cônica e uma reta. 82
Figura 19 – Cúbica plana com ponto um ponto duplo comum e cúbica plana com uma cúspide. 83
Figura 20 – A cúbica de Clebsch com suas retas. 88
Figura 21 – Possível configuração de retas em uma superfície cúbica, que estão contidas em um plano. 96
Figura 22 – A configuração de 10 retas em uma cúbica intersectando uma reta l. . 97
Figura 23 – Uma reta reversa m reversa à reta l. 100
Figura 24 – Retas em um cone quadrático (uma quádrica de posto 3 em $\mathbb{P}^3_k$). . . . 101
Figura 25 – As duas retas l_P e l_R na quádrica Q são transversais a l_1, l_2, l_3 e l_4. . . 102
Figura 26 – Configuração de retas não pode estar contida em uma superfície cúbica suave. 103
Figura 27 – A configuração de 18 das 27 retas em uma superfície cúbica. Os 20 pontos de interseção da forma $l'_i \cap l''_j$ para $1 \leq i < j \leq 5$ não são mostrados. . 104
Figura 28 – Caso 1. 105
Figura 29 – Caso 2. 105
Figura 30 – Caso 3. 106

Figura 31 – Significado geométrico da normalização de Noether: ϕ é sobrejetiva com fibras finitas. 115
Figura 32 – Diagrama. 123
Figura 33 – Diagrama. 123
Figura 34 – Diagrama. 125

LISTA DE SÍMBOLOS

$\forall$	Para todo.
$\in$	Pertence.
$\subset$	Está contido.
$\supset$	Contém.
$\emptyset$	Conjunto vazio.
$\iff$	Se e somente se.
$\rightarrow$	Implica que .
$\setminus$	Exclusão de conjunto
$\rightarrow$, $\mapsto$	Leva a.
$\cup$	União.
$\cap$	Interseção .
$J = (a_1, \ldots, a_n)$	Ideal gerado por $a_1, \ldots, a_n$.
$\hookrightarrow$	Inclusão.
$\sum$	Somatório.
$\prod$	Produtório.
$\equiv$	Identicamente.
mod	Módulo.
ker	Núcleo.
$:=$	Defini-se desta forma.
$\|_X$	Restrito ao conjunto X.
$\bigoplus$	Soma direta.
$\sim$	Se relacionam por uma relação de equivalência.
$\cong$	Isomorfismo.

SUMÁRIO

1 INTRODUÇÃO 12
2 VARIEDADES AFINS 13
2.1 CONCEITOS INICIAIS 13
2.2 O NULLSTELLENSATZ DE HILLBERT 19
2.2.1 A topologia de Zariski 21
2.2.2 Variedades afins 24
2.3 FUNÇÕES POLINOMIAIS E MAPAS 28
2.3.1 O anel de coordenadas de uma variedade 28
2.3.2 Mapas polinomiais 30
2.4 FUNÇÕES RACIONAIS E MORFISMOS 34
2.4.1 Localização de anéis 35
2.4.2 O feixe estrutural de uma variedade 37
2.4.3 Mapas racionais 38
2.4.4 Variedades quasi-afins 40
3 VARIEDADES PROJETIVAS 43
3.1 O ESPAÇO PROJETIVO 43
3.2 VARIEDADES PROJETIVAS 45
3.2.1 Anéis graduados e ideais homogêneos 48
3.3 FUNÇÕES RACIONAIS E MORFISMOS 53
3.3.1 Localização de anéis graduados 54
3.3.2 Funções regulares 55
3.3.3 Mapas racionais 59
3.3.4 Mapas birracionais 61
3.3.5 Produto de variedades projetivas 63
4 PONTOS SUAVES E DIMENSÃO 65
4.1 PONTOS SUAVES E SINGULARES 65
4.1.1 O espaço tangente de uma superfície em um ponto 65
4.1.2 O conceito de dimensão, pontos suaves e regulares de superfícies afins irredutíveis 67
4.1.3 Variedades afins arbitrárias 68
4.2 CARACTERIZAÇÃO ALGÉBRICA DE DIMENSÃO 69
4.2.1 Variedades quasi-projetivas 72
4.2.2 Dimensão de Krull 72
5 CURVAS CÚBICAS PLANAS 75
5.1 CURVAS PLANAS 75
5.2 MULTIPLICIDADE DA INTERSEÇÃO 78
5.3 CLASSIFICAÇÃO DE CÚBICAS SUAVES 84

6 AS 27 RETAS 88
6.1 A EXISTÊNCIA DE RETAS EM UMA CÚBICA 88
6.2 A CONFIGURAÇÃO DAS 27 RETAS 94
7 CONCLUSÃO 108
REFERÊNCIAS 109
APÊNDICE A – Alguns resultados de Álgebra Comutativa . 110
APÊNDICE B – O significado Geométrico da normalização de Noether 115
APÊNDICE C – Corpos de característica positiva 118
APÊNDICE D – Redução ao caso de uma hipersuperfície . . 120
APÊNDICE E – Conceitos básicos de categoria 121
APÊNDICE F – O produto de duas variedades 125

1 INTRODUÇÃO

Geometria algébrica é uma área da matemática que combina técnicas de álgebra abstrata para resolver problemas geométricos; classicamente, se preocupava em estudar o zeros de polinômios em várias variáveis. O espaço projetivo de dimensão n é visto como um espaço vetorial de dimensão $n+1$ tal que origem é removida. A partir disso, é possível chegar a resultados interessantes, como retas se encontrarem no infinito.

Uma superfície cúbica é definida pelos zeros de um polinômio homogêneo de grau três em quatro variáveis, que é um subconjunto do espaço projetivo $\mathbb{P}^3_k$, ou seja, pode ser identificado com o $\mathbb{R}^3$ e, dessa forma, pode ser visualizada.

Em 1849, Salmon e Cayley publicaram um resultado do número de retas em uma superfície cúbica. Cayley, em uma carta a Salmon, mostrou que deveria existir um número finito de retas em uma superfície cúbica. Posteriormente, Salmon provou que esse número é precisamente 27. Mais tarde, Steiner estudou e classificou as cúbicas, chegando à conclusão de que existem 23 tipos.

2 VARIEDADES AFINS

O objetivo desse capítulo é estabelecer uma relação entre **subconjuntos algébricos afins** de $\mathbb{A}_k^n$ e **ideias** no anel de coordenadas $k[x_1, \ldots, x_n]$. O resultado central é o Teorema dos Zeros de Hillbert (Nullstellensatz). A relação se estende para dar uma correspondência entre mapas polinomiais e homomorfismos de k-álgebras, interpretando, posteriormente, na linguagem de categorias. Por fim, discutiremos funções em conjuntos algébricos com mais detalhes. Durante o capítulo assumiremos que o corpo k é algebricamente fechado e os anéis são comutativos com unidade.

2.1 CONCEITOS INICIAIS

Geometria algébrica se preocupa em estudar **conjuntos algébricos**, ou seja, conjunto de soluções de equações polinomiais em várias variáveis:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ \vdots \qquad \vdots \qquad &= \vdots \\ f_m(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Para dar uma definição formal desse conceito, primeiro devemos fixar um corpo k.

Definição 2.1. *O **espaço afim** de dimensão n sobre k é definido como*

$$\mathbb{A}^n := \mathbb{A}_k^n := k^n = \{(a_1, \ldots, a_n) \mid a_i \in k\}.$$

Note que os espaços k^n e $\mathbb{A}_k^n$ são iguais como conjuntos. No entanto, enquanto pensamos em k^n equipado com a estrutura de espaço vetorial, pensamos em $\mathbb{A}_k^n$ como um espaço afim, i.e., não tem adição e não existem pontos especiais. Em particular a origem não é vista como algo a ser sobressaltado. Por outro lado vamos dar a $\mathbb{A}_k^n$ a estrutura de um espaço topológico, definindo a **topologia de Zariski**.

Todo polinômio $f \in k[x_1, \ldots, x_n]$ define um mapa

$$\begin{array}{rccc} f: & \mathbb{A}^n & \to & k, \\ & (a_1, \ldots, a_n) & \mapsto & f(a_1, \ldots, a_n), \end{array}$$

e um ponto $P = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$ é chamado de **zero** de f se $f(P) = 0$. Note que a menos que k tenha infinitos elementos, por exemplo, quando K é algebricamente fechado, vários polinômios podem definir um mesmo mapa. O **conjunto dos zeros de** f é

$$V(f) := \{P \in \mathbb{A}_k^n \mid f(P) = 0\}.$$

Agora seja $T \subset k[x_1, \ldots, x_n]$ um subconjunto do anel de polinômios.

Definição 2.2. *O* ***conjunto dos zeros de*** T *é*

$$V(f) := \{P \in \mathbb{A}_k^n \mid f(P) = 0 \text{ para todo } f \in T\}.$$

Definição 2.3. *Um subconjunto* $Y \subset \mathbb{A}^n$ *é chamado de* ***conjunto algébrico*** *(afim), um fechado, ou um conjunto fechado de Zariski em* $\mathbb{A}^n$*, se existe um subconjunto* $T \subset k[x_1, \ldots, x_n]$ *tal que*

$$Y = V(T).$$

Não é necessário considerar subconjuntos arbitrários $T \subset k[x_1, \ldots, x_n]$. Ao invés disso, vamos mostrar que podemos substituir T **pelo ideal gerado por** T, ou seja,

$$J := (T) \subset k[x_1, \ldots, x_n].$$

Mais ainda, já que $k[x_1, \ldots, x_n]$ é um anel Noetheriano, existe um número finito de polinômios $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ tais que

$$J = (f_1, \ldots, f_m).$$

Lema 2.4. *Para* T *e* J *como definidos anteriormente, vale:*

$$V(T) = V(J) = V(f_1, \ldots, f_m).$$

Prova. Claramente $V(J) \subset V(T)$. Para qualquer $g \in J$ existem polinômios $h_1, \ldots, h_l \in T$ e $q_1, \ldots, q_l \in k[x_1, \ldots, x_n]$ tal que

$$g = h_1 q_1 + \cdots + h_l q_l.$$

Se $P \in V(T)$ então $h_1(P) = \cdots = h_l(P) = 0$, e então, $g(P) = 0$. Então $V(T) \subset V(J)$. Um argumento similar mostra que $V(J) = V(f_1, \ldots, f_m)$. □

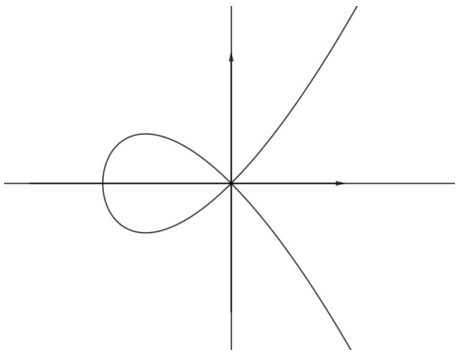
O lema acima nos mostra que podemos voltar nossa atenção para um **sistema de equações polinomiais finito**. Antes de continuar com uma investigação sistemática de conjuntos algébricos, vamos ver e discutir alguns exemplos.

Exemplo 2.5. O subconjunto algébrico mais simples possível de $\mathbb{A}_k^n$ é dado por um conjunto de equações lineares. Tal conjunto algébrico é chamado de **subespaço afim**.

Exemplo 2.6. A curva cúbica definida abaixo, também chamada de *cúbica nodal*, tem um "ponto duplo" na origem:

$$C : y^2 = x^3 + x^2, \text{ x, y} \in \mathbb{R}$$

Figura 1 – Curva cúbica.



Fonte: elaborado pelo autor (2023).

Essa curva tem uma parametrização

$$\begin{aligned} \varphi : \mathbb{R} &\longrightarrow \mathbb{R}^2 \\ t &\longmapsto (t^2 - 1, t^3 - t) \end{aligned}$$

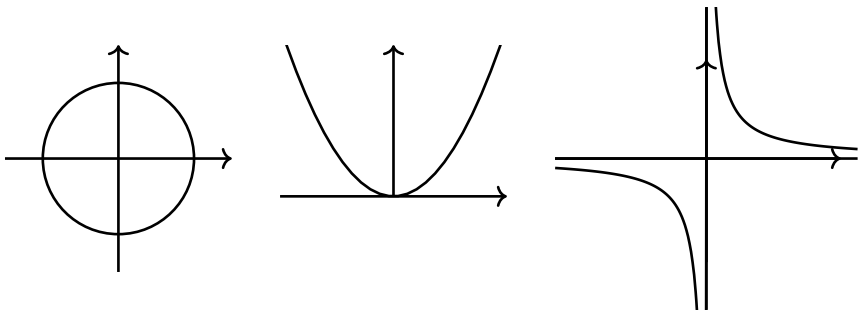
com $\varphi(\mathbb{R}) = C$. Essa aplicação é injetiva exceto em $\varphi(1) = \varphi(-1) = (0, 0)$, o que explica a terminologia "ponto duplo".

Exemplo 2.7. A cônica, dada por uma equação da forma

$$f(x, y) = a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y + a_6 = 0 \, (a_1, \ldots, a_6 \in \mathbb{R}),$$

é um exemplo famoso de conjunto algébrico, o círculo, parábola e hipérbole sendo casos especiais.

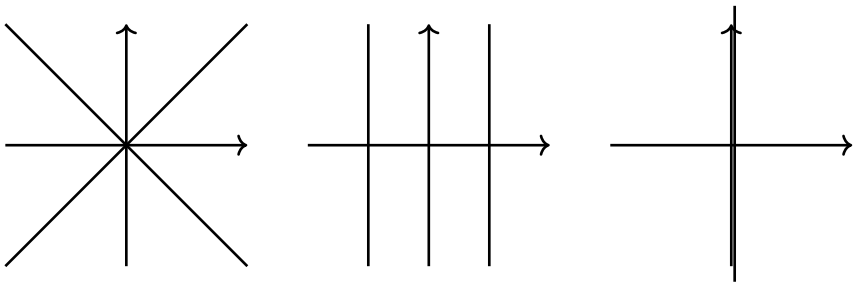
Figura 2 – Um círculo $x^2 + y^2 - 1 = 0$, uma parábola $y - x^2 = 0$ e uma hipérbole $xy - 1 = 0$ respectivamente são exemplos de curvas não degeneradas.



Fonte: elaborado pelo autor (2023).

No caso degenerado, ou seja, f sendo redutível, obtemos pares de retas como na figura abaixo.

Figura 3 – Exemplos de cônicas degeneradas, cujas equaçoes são $(x-y)(x+y)=0$, $x^2-1=0$ e $x^2=0$ ou $x=0$, respectivamente.



Fonte: elaborado pelo autor (2023).

Exemplo 2.8. A parábola semicúbica, conhecida também como a parábola de Neile ou cúbica cuspidal, é dada pela equação

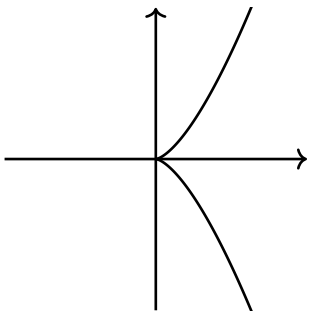
$$C:\ y^2=x^3,\ x,y\in\mathbb{R}.$$

Essa curva também admite a parametrização

$$\begin{aligned}\varphi: R &\longrightarrow \mathbb{R}^2\\ t &\longmapsto (t^2,t^3).\end{aligned}$$

Nesse caso φ nos dá uma bijeção entre $\mathbb{R}$ e C, no entanto, a derivada parcial de φ não existe na origem, que é chamada de cúspide de C.

Figura 4 – A parábola semicúbica $y^2=x^3$.



Fonte: elaborado pelo autor (2023).

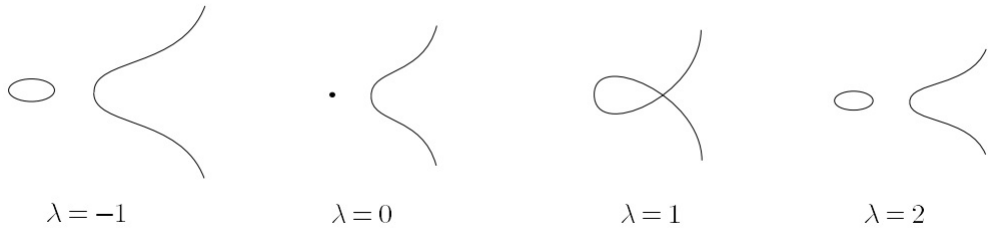
Neste exemplo, os pontos duplos e as "cúspides" são pontos singulares da curva, enquanto que os outros pontos são suaves. Veremos este assunto adiante.

Exemplo 2.9. Considere uma *família* de cúbicas planas, dada por

$$C_\lambda \ : \ y^2 = x(x-1)(x-\lambda) \ \ , (\lambda \in \mathbb{R}).$$

Para $\lambda = 0$ e 1 temos uma curva com um ponto duplo (sobre o corpo $\mathbb{C}$), e caso contrário C_λ é suave. A figura a seguir nos mostra C_λ para alguns valores de λ.

Figura 5 – Deformações da curva C_λ.



Fonte: Ver (1) página 6. (2000)

Sobre $\mathbb{R}$ a curva C_1 tem uma parametrização racional, e sobre $\mathbb{C}$ ambas C_0 e C_1 têm parametrizações racionais. Por outro lado, vamos mostrar que para $\lambda \neq 0, 1$ a curva lisa C_λ não tem uma parametrização racional sobre $\mathbb{R}$ ou $\mathbb{C}$, e por isso se comporta de maneira diferente de C_0 e C_1.

Proposição 2.10. *Seja $k \in \{\mathbb{R}, \mathbb{C}\}$, e seja $f, g \in k(t)$ funções racionais tais que*

$$g^2 = f(f-1)(f-\lambda) \ \ (\lambda \neq 0, 1). \tag{2.1}$$

Então f e g são constantes, i.e., $f, g \in k$.

Prova. Escreva

$$f = \frac{p}{q}, \quad g = \frac{r}{s}$$

onde r, s e $p, q \in k[t]$ são pares de polinômios coprimos. Depois que multiplicamos a equação (2.1) pelo denominador q e s, temos

$$r^2 q^3 = s^2 p(p-q)(p-\lambda q). \tag{2.2}$$

Logo $s^2 | q^3$, e como p e q são coprimos também temos que $q^3 | s^2$. Então $s^2 = aq^3$ para algum $a \in k$, e

$$aq = (s/q)^2 \in k[t]$$

é um quadrado. Multiplicando (2.2) por a e dividindo por s^2, obtemos

$$r^2 = ap(p-q)(p-\lambda q).$$

Considerando que o lado esquerdo é um quadrado, e que p e q são coprimos, deve existir um $b, c, d \in k$ tal que

$$bp, c(p-q), d(p-\lambda q)$$

são todos quadrados em $k[t]$. O próximo lema implica que $p, q \in k$, do qual segue que $f \in k$. De (2.2) temos também que $g \in k$. □

Lema 2.11. *Seja $p, q \in \mathbb{C}[t]$ coprimos. Se existem quatro valores distintos de razão $\lambda/\mu \in \mathbb{C} \cup \{\infty\}$ tal que $\lambda p + \mu q$ é um quadrado em $\mathbb{C}[t]$, então $p, q \in \mathbb{C}$.*

Prova. Vamos usar o método de Fermat de descida infinita. Primeiro note que as hipóteses não mudam por uma transformação linear

$$p' = \alpha p + \beta q, \;\; q' = \gamma p + \delta q, \quad \text{onde } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \; Gl(2, \mathbb{C}). \tag{2.3}$$

Suponha que o resultado é falso, e que $\{p, q\}$ é um contra exemplo com $\max\{\deg p, \deg q\}$ mínimo. Por uma transformação da forma (2.3), podemos assumir que as quatro razões em questão são $0, 1, \infty$ e que $\lambda \in \mathbb{C}$, i.e.,

$$p, q, p-q, p-\lambda q \; \in \; \mathbb{C}[t]$$

são quadrados. Então $p = u^2$ e $q = v^2$ para algum coprimo u e v. Pode-se ver que

$$\text{máx}\{\deg u, \deg v\} < \text{máx}\{\deg p, \deg q\}$$

Também temos $u - v, u + v, u - \mu v, u + \mu v$ são todos quadrados, onde $u^2 = \lambda$, como

$$p - q = u^2 - v^2 = (u - v)(u + v)$$
$$p - \lambda q = u^2 - \lambda v^2 = (u - \mu v)(u + \mu v).$$

Mas então $\{u, v\}$ é também um contra exemplo, contradizendo a minimalidade de $\{p, q\}$. □

Corolário 2.11.1. *Para $\lambda \neq 0, 1$ existe um mapa racional não constante*

$$(f, g) : k \longrightarrow C_\lambda \qquad , (f, g \in k(t)).$$

Em particular, não existe parametrização racional de C_λ para $\lambda \neq 0, 1$. Em outras palavras, C_λ é "racional" se, e somente se, $\lambda = 0$ ou 1, que será visto com mais detalhes no capítulo 2.

Exemplo 2.12. Outro exemplo de um conjunto algébrico é o grupo linear geral

$$Gl\ (n,k) := \{A \in Mat\ (n \times n, k) \mid det\ A \neq 0\}.$$

Para ver que $Gl\ (n,k)$ é um conjunto algébrico, consideremos o espaço afim $\mathbb{A}^{n^2+1}$ com coordenadas $(x_{ij})_{1\leq i,j\leq n}$ e t. O conjunto

$$V\ :=\ \{(x_{ij},t)\ \in\ \mathbb{A}^{n^2+1} \mid det(x_{ij})t - 1 = 0\}$$

é um conjunto algébrico, e o mapa

$$\begin{aligned} \varphi\ :\ Gl(n,k) &\longrightarrow V, \\ A = (a_{i,j}) &\longmapsto \left((a_{i,j}), \frac{1}{det\ A}\right) \end{aligned}$$

define uma bijeção de $Gl\ (n,k)$ para V, o que prova que $Gl\ (n,k)$ é de fato algébrico. Note que as aplicações a seguir

$$\begin{aligned} \mu\ :\ Gl(n,k) \times Gl(n,k) &\longrightarrow Gl(n,k) \\ (A,B) &\longmapsto AB, \end{aligned}$$

e o mapa inverso

$$\begin{aligned} i:\ Gl(n,k) &\longrightarrow Gl(n,k) \\ A &\longmapsto A^{-1}, \end{aligned}$$

são dadas em termos das entradas da matriz por um polinômio e uma função racional respectivamente. Devido a isso $Gl(n,k)$ é um *grupo algébrico*. De forma geral, um grupo algébrico é um conjunto algébrico que também é um grupo, tal que as operações consideradas entre os elementos e a inversa são dadas por funções racionais. Outros exemplos são o grupo linear especial $Sp(2n,k)$, o grupo ortogonal $O(n,k)$, o grupo simplético $Sp(2n,k)$, e o torus E_τ.

2.2 O NULLSTELLENSATZ DE HILLBERT

Seja $A := k[x_1,\ldots,x_n]$ o anel de polinômios em n variáveis sobre o corpo k. Anteriormente, definimos o conjunto dos zeros de um ideal $J \subset A$, como

$$V(J)\ :=\ \{P \in \mathbb{A}^n_k \mid f(P) = 0 \text{ para todo } f \in J\}$$

e mostramos que da origem a um mapa sobrejetivo

$$\begin{aligned} V\ :\ \{\text{ ideais em A }\} &\longrightarrow \{\text{ conjuntos algébricos em } \mathbb{A}^n_k\} \\ J\ &\longmapsto\ V(J). \end{aligned}$$

Na direção inversa, para cada subconjunto $X \subset \mathbb{A}_k^n$ definimos um ideal

$$I(X) := \{f \in A \mid f(P) = 0 \text{ para todo } P \in X\},$$

temos então o mapa

$$\begin{aligned} I : \{\text{subconjuntos de } \mathbb{A}_k^n\} &\longrightarrow \{\text{ideais em A}\} \\ X &\longmapsto I(X). \end{aligned}$$

O mapa V não é injetivo, por exemplo, considere que para todo $k \geq 1$ temos $V(x_1, \ldots, x_n) = V(x_1^k, \ldots, x_n^k)$. O mapa I não é injetivo nem sobrejetivo, considere $\mathbb{A}_k^1$, temos $I(\mathbb{Z}) = I(\mathbb{A}_k^1) = (0)$, enquanto para $n \geq 2$, o ideal (x^n) não é a imagem de I. No entanto, como um corolário de Nullstellensatz de Hillbert, quando restringimos para certos subconjuntos de ideais e conjuntos algébricos, V e I se tornam bijeções mutuamente inversas. Primeiro, investiguemos algumas propriedades básicas desses mapas.

Lema 2.13. *O mapa V satisfaz as seguintes propriedades:*

(1) $V(0) = \mathbb{A}_k^n$, $V(A) = \emptyset$;

(2) $I \subset J \implies V(J) \subset V(I)$;

(3) $V(J_1 \cap J_2) = V(J_1) \cup V(J_2)$;

(4) $V\left(\sum_{\lambda \in \Lambda} J_\lambda\right) = \bigcap_{\lambda \in \Lambda} V(J_\lambda)$.

Prova. Faremos a prova do item (3), a prova do item (4) encontra-se em ((4), p. 5)

" $\supset$ ": Seja $P \in V(J_1) \cup V(J_2)$. Sem perda de generalidade podemos assumir que $P \in V(J_1)$. Então para qualquer $g \in J_1 \cap J_2$ temos $g(P) = 0$, do qual segue que $P \in V(J_1 \cap J_2)$.

" $\subset$ " : Tome $P \notin V(J_1) \cup V(J_2)$. Então, existe $f \in J_1$ e $g \in J_2$ com $f(P) \neq 0$ e $g(P) \neq 0$, o que implica que $fg(P) \neq 0$. No entanto, $fg \in J_1 \cap J_2$, então $P \notin V(J_1 \cap J_2)$.

□

Lema 2.14. *Os mapas I e V têm as seguintes propriedades*

(1) $X \subset Y \implies I(X) \supset I(Y)$;

(2) *Para cada subconjunto $X \subset \mathbb{A}_k^n$ temos $X \subseteq V(I(X))$. A igualdade vale se, e somente se, X for um conjunto algébrico;*

(3) *Se $J \subset A$ é um ideal, então $J \subset I(V(J))$.*

Prova. Os itens (1) e (3) podem ser entendidos com mais facilidade, e a seguinte relação $X \subset V(I(X))$ também . Se $X = V(I(X))$, então X é algébrico por definição. Por outro lado, se X for fechado, então $X = V(J_0)$ para algum ideal J_0. Em particular $J_0 \subset I(X)$, logo $V(I(X)) \subset V(J_0) = X$. □

Em geral $J \subset I(V(J))$ é uma inclusão estrita, por exemplo, $J = (x_1^k, \ldots, x_n^k),\ k \geq 2$. Nesse caso, $I(V(J)) = (x_1, \ldots, x_n)$.

Definição 2.15. *Para um ideal J em um anel R, o **radical** de J é definido como*

$$\sqrt{J} \ := \ \{r \mid \textit{existe } k \geq 1 \textit{ com } r^k \in J\}.$$

*Nós chamamos este ideal J de **ideal radical** se $\sqrt{J} = J$.*

Segue do teorema binomial que $\sqrt{J}$ é um ideal. Temos que $J \subset \sqrt{J}$. Ideais radicais têm um papel importante na relação entre ideais e variedades, já que qualquer ideal da forma $I(X)$ é automaticamente um ideal radical. Um outro exemplo é dado por ideais primos, que também são ideais radicais.

2.2.1 A topologia de Zariski

Foi visto anteriormente que conjuntos algébricos são **fechados de Zariski**. O Lema 2.13 justifica essa terminologia, já que esse lema satisfaz os axiomas de conjuntos fechados de uma topologia. A topologia associada em $\mathbb{A}_k^n$ é chamada de **topologia de Zariski**. Um subconjunto de $\mathbb{A}_k^n$ é chamado de *aberto de Zariski* se seu complementar for um fechado de Zariski. A topologia de Zariski é bem diferente da topologia estudada em análise real ou complexa. Em particular, não é Hausdorff. Note que a topologia de Zariski em $\mathbb{A}_k^n$ induz uma topologia em cada subconjunto de $\mathbb{A}_k^n$.

Exemplo 2.16. Considere a topologia de Zariski em $\mathbb{A}_k^1$. O conjunto vazio e $\mathbb{A}_k^1$ são simultaneamente abertos e fechados. Como k é algebricamente fechado, todo ideal $J \subset k[x]$ é um ideal principal e pode ser escrito como

$$J = ((x - a_1) \ldots (x - a_n)).$$

Logo os subconjuntos fechados de Zariski de $\mathbb{A}_k^1$ diferentes de vazio e $\mathbb{A}_k^1$ são precisamente os subconjuntos finitos. Já que todo subconjunto fechado não vazio de Zariski em $\mathbb{A}_k^1$ é denso.

Definição 2.17 (Subconjunto denso)**.** *Um subconjunto $U \subset V$ é denso se, e somente se, ele tem interseção não vazia com todo subconjunto não vazio aberto de V.*

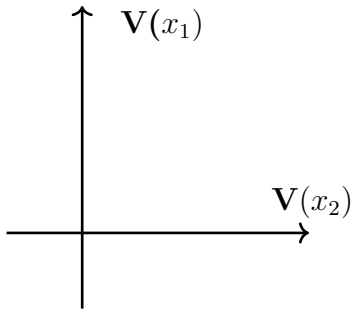
Definição 2.18. *Um conjunto algébrico X é chamado de* ***irredutível*** *se não existe a decomposição*

$$X = X_1 \cup X_2 \ \ (X_1, X_2 \subsetneq X)$$

em conjuntos algébricos próprios X_1, X_2. Do contrário X é chamado de ***redutível****.*

Exemplo 2.19. O subconjunto $V(x_1x_2) \subset \mathbb{A}_k^2$ é redutível, já que $V(x_1x_2) = V(x_1) \cup V(x_2)$.

Figura 6 – Eixos coordenados como um exemplo de variedade redutível.



Fonte: elaborado pelo autor (2023).

Proposição 2.20. *Seja $X \neq \emptyset$ um conjunto algébrico com ideal correspondente $I(X)$. Então*

$$X \text{ é irredutível } \iff I(X) \text{ é um ideal primo.}$$

Prova. (1) Assuma que X é redutível, então existe uma decomposição $X = X_1 \cup X_2$ para alguns conjuntos algébricos $X_1, X_2 \subsetneq X$. A inclusão $X_1 \subsetneq X$ implica a existência de um elemento, digamos, $f \in I(X_1) \setminus I(X)$. Similarmente, se $X_2 \subsetneq X$ existe um elemento $g \in I(X_2) \setminus I(X)$. Por isso, o produto fg, se anula em $X_1 \cup X_2 = X$, e então $fg \in I(X)$, o que implica que $I(X)$ não é um primo.

(2) Suponha que $I(X)$ não é um primo. Então existe $f, g \in A$ com $fg \in I(X)$, mas $f, g \notin I(X)$. Seja $J_1 := (I(X), f)$ e $J_2 := (I(X), g)$. Então $X_1 = V(J_1)$ e $X_2 = V(J_2)$ são conjuntos próprios de X. Por outro lado $X \subset X_1 \cup X_2$, supondo que $P \in X$, temos, $fg(P) = 0$, então $f(P) = 0$ ou $g(P) = 0$, o que implica que $P \in X_1$ ou $P \in X_2$. Logo X é redutível.

□

Sabe-se que $A = k[x_1, \ldots, x_n]$ é um anel noetheriano. Existem diversas definições equivalentes de anéis noetherianos, em particular:

Definição 2.21. *Um anel é* ***noetheriano*** *se, e somente se, satisfaz a condição da cadeia ascendente (acc), ou seja, toda cadeia ascendente de ideais*

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset I_n \subset \ldots$$

se torna estacionária, i.e., para algum n_0 é válido $I_{n_0+k} = I_{no}$ para todo $k \geq 0$.

Para qualquer cadeia descendente de conjuntos algébricos

$$X_1 \supset X_2 \supset \ldots \supset X_n \supset \ldots,$$

existe uma cadeia correspondente de ideais,

$$I(X_1) \subset I(X_2) \subset \ldots \subset I(X_n) \subset \ldots.$$

Se $X_n \supsetneq X_{n+1}$ é uma inclusão própria, e X_n e X_{n+1} são conjuntos algébricos, o Lema 2.14 implica que $I(X_n) \subsetneq I(X_{n+1})$ também é uma inclusão própria. Logo, toda sequência descendente de conjuntos fechados se torna estacionária. Um espaço topológico com essa propriedade é chamado de **espaço topológico Noetheriano**. Segue do axioma da escolha que todo sistema não trivial Σ de conjuntos algébricos $\mathbb{A}^n_k$ tem elemento mínimo (um elemento $X \in \Sigma$ é chamado de *mínimo* se não existe $Y \in \Sigma$ com $Y \subsetneq X$).

Proposição 2.22. *Todo conjunto algébrico $X \subset \mathbb{A}^n_k$ tem uma decomposição*

$$X = X_1 \cup \ldots \cup X_r,$$

onde os X_i são conjuntos algébricos irredutíveis e $X_i \not\subset X_j$ para $i \neq j$, que é único a menos da ordem dos fatores.

Prova. Primeiro é necessário mostrar a existência de tal decomposição. Seja Σ o conjunto de todos os conjuntos algébricos que não tem tal representação. Suponha que $\Sigma \neq \emptyset$. Então, como discutido anteriormente, Σ tem elemento mínimo X, que é redutível, caso contrário $X \notin \Sigma$. Logo, existem $X_1, X_2 \subsetneq X$ com $X = X_1 \cup X_2$. Como X é o elemento mínimo de Σ, segue que $X_1, X_2 \notin \Sigma$. Portanto X_1 e X_2 podem ser decompostos em uma união de componentes irredutíveis, o que significa que X também tem essa decomposição, contradizendo $X \in \Sigma$.

Resta mostrar que tal decomposição é única. Suponha que exista outra decomposição

$$X = Y_1 \cup \ldots \cup Y_l,$$

com Y_i irredutível e $Y_i \not\subset Y_j$ para $i \neq j$. Então

$$X_i = X_i \cap X = \bigcup_{m=1}^{l} (X_i \cap Y_m).$$

Já que X_i é irredutível, temos $X_i \cap Y_m = X_i$, para algum m. Em particular $Y_m \supset X_i$. Trocando os papéis das duas decomposições, de maneira similar podemos mostrar que para algum j temos $X_j \subset Y_m \subset X_i$. Logo $i = j$ e $X_i = Y_m$. □

Definição 2.23. *Os $X_i's$ do lema anterior são chamados de* ***componentes irredutíveis*** *de X.*

A proposição anterior é válida para qualquer espaço topológico Noetheriano, já que a prova usa somente o fato de que a topologia de Zariski é Noetheriana. Agora vamos mostrar outro fato sobre subconjuntos irredutíveis, que é válido para qualquer topologia.

Lema 2.24. *Para um conjunto fechado $V \subset \mathbb{A}_k^n$, as seguintes afirmações são equivalentes:*

(1) *V é irredutível;*

(2) *Para quaisquer dois subconjuntos abertos $U_1, U_2 \neq \emptyset$ de V, temos $U_1 \cap U_2 \neq \emptyset$;*

(3) *Todo subconjunto aberto $\emptyset \neq U \subset V$ é denso em V.*

Prova. A equivalência entre (1) e (2) segue de

$$U_1 \cap U_2 = \emptyset \iff (V - U_1) \cup (V - U_2) = V.$$

Por outro lado, por definição **um subconjunto $U \subset V$ é denso se, e somente se, ele tem interseção não vazia com todo subconjunto não vazio aberto de V.** Isto nos dá a equivalência de (2) e (3).

2.2.2 Variedades afins

Tendo discutido alguns aspectos das propriedades topológicas de $\mathbb{A}_k^n$ equipada com a topologia de Zariski, nos voltaremos para o ponto de vista algébrico. Precisaremos de mais ferramentas algébricas para discutir e entender o Nullstellensatz de Hillbert.

Definição 2.25. *Uma* ***variedade afim*** *(sobre k) é um conjunto algébrico afim (definição 2.3).*

A palavra "variedade" tem diversos significados na literatura. Para alguns autores, somente conjuntos algébricos irredutíveis são variedades, outros se referem a variedades abstratas, que são objetos cobertos por variedades afins.

Estamos prontos para enunciar o Nullstellensatz de Hillbert. A parte mais importante da demonstração é um resultado puramente algébrico (Teorema 2.28), o qual será enunciado a partir dos seguintes conceitos:

Definição 2.26. *Seja B um subanel de A.*

(1) *A é* ***finitamente gerada*** *sobre B (ou* ***finitamente gerada como uma B-álgebra***) *se existem finitos elementos $a_1, \ldots, a_n$ tal que $A = B[a_1, \ldots, a_n]$;*

(2) *A é **uma B-álgebra finita** se existem finitos elementos não constantes $a_1, \ldots, a_n$ com $A = Ba_1 + \ldots + Ba_n$.*

Exemplo 2.27. O anel de polinômios $k[x_1, \ldots, x_n]$ é uma k-álgebra finitamente gerada, mas não uma k-álgebra finita.

Teorema 2.28. *Seja k um corpo com infinitos elementos, e seja $A = k[a_1, \ldots, a_n]$ uma k-álgebra finitamente gerada. Se A é um corpo, então A é algébrica [1] sobre k.*

Como nosso objetivo é discutir o Nullstellensatz, vamos deixar a prova do teorema anterior para depois.

Teorema 2.29 (O Nullstellensatz de Hillbert). *Seja k um corpo algebricamente fechado e seja $A = k[x_1, \ldots, x_n]$. Então, as seguintes afirmações valem:*

(1) *Todo ideal maximal $m \subset A$ é da forma*

$$m = (x_1 - a_1, \ldots, x_n - a_n) = I(P)$$

para algum poto $P = (a_1, \ldots, a_n) \in \mathbb{A}_k^n$;

(2) *Se $J \subsetneq A$ é um ideal próprio, então $V(J) \neq \emptyset$;*

(3) *Para cada ideal $J \subset A$, temos*

$$I(V(J)) = \sqrt{J}.$$

O ponto crucial é o item (2), que diz que todo ideal não trivial tem ao menos um ponto que o anula, o que explica o nome do teorema (teorema dos zeros). Claramente não é verdade se o corpo considerado não for algebricamente fechado, por exemplo, o ideal $(x^2 + 1) \subset \mathbb{R}[x]$, é tal que $V(I) = \emptyset$.

Corolário 2.29.1. *Para $A = k[x_1, \ldots, x_n]$, os mapas V e I*

$$\{\textit{ideais de } A\} \overset{V,I}{\longleftrightarrow} \{\textit{ subconjuntos de } \mathbb{A}_k^n\}$$

induzem as seguintes bijeções:

$$\begin{array}{ccc} \{\textit{ideais radicais de } A\} & \overset{1:1}{\longleftrightarrow} & \{\textit{subvariedades de } \mathbb{A}_k^n\} \\ \cup & & \cup \\ \{\textit{ideais primos de } A\} & \overset{1:1}{\longleftrightarrow} & \{\textit{subvariedades irredutíveis de } \mathbb{A}_k^n\} \\ \cup & & \cup \\ \{\textit{ideais maximais de } A\} & \overset{1:1}{\longleftrightarrow} & \{\textit{pontos de } \mathbb{A}_k^n\} \end{array}$$

[1] Uma extensão A/k é algébrica se $\forall u \in A$, $\exists f \in k[t]$ não nulo tal que $f(u) = 0$.

Prova. Para cada conjunto algébrico $X \subset \mathbb{A}_k^n$ nós temos $V(I(X)) = X$, por outro lado, pelo Nullstellensatz de Hillbert (3), para cada ideal J temos $I(V(J)) = \sqrt{J}$. Obtemos então a primeira bijeção. A segunda bijeção segue da Proposição 2.20, e a terceira do primeiro item do Nullstellensatz.

Agora faremos a prova do Nullstellensatz.

Prova. (Nullstellensatz de Hillbert) Primeiro note que qualquer ideal da forma $(x_1 - a_n, \ldots, x_n - a_n)$ é maximal. Segue do fato que o mapa de avaliação

$$\begin{aligned} k[x_1, \ldots, x_n] &\longrightarrow k, \\ f &\longmapsto f(P), \end{aligned}$$

induz um isomorfismo $\dfrac{k[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong k$. Para ver isso, primeiro note que por uma transformação linear podemos assumir que todos os a_i são zero. Então o mapa $f \mapsto f(0, \ldots, 0)$ simplesmente leva f para seu termo constante, logo o núcleo é o conjunto das funções com constante igual a zero, que são precisamente os polinômios sem constantes.

Agora suponha que $m \subset k[x_1, \ldots, x_n]$ é um ideal maximal em A, o que implica

$$K := k[x_1, \ldots, x_n]/m$$

é um corpo. Mais ainda, K é uma k-álgebra finitamente gerada (gerada pela classe de resíduos $x_i \mod m$), então o Teorema 2.28 implica que K é algébrica sobre k. Como k é algebricamente fechado, o mapa natural

$$\varphi : k \hookrightarrow k[x_1, \ldots, x_n] \xrightarrow{\pi} k[x_1, \ldots, x_n]/m = K$$

é um isomorfismo entre k e K. Seja $b_i := x_i \mod m \in K$ e seja $a_i := \varphi^{-1}(b_i)$. Então para cada i temos

$$x_i - a_i \in \ker \pi = m,$$

logo

$$(x_1 - a_1, \ldots, x_n - a_n) \subset m.$$

Mas $(x_1 - a_1, \ldots, x_n - a_n)$ é um ideal maximal, portanto temos a igualdade $(x_1 - a_1, \ldots, x_n - a_n) = m$.

(1) $\Rightarrow$ (2) : Suponha que $J \subsetneq A = k[x_1, \ldots, x_n]$. Já que $k[x_1, \ldots, x_n]$ é um anel Noetheriano, existe um ideal maximal m com $J \subset m$. De (1) temos $m = I(P)$ para algum ponto $P \in \mathbb{A}_k^n$, então $\{P\} = V(I(P)) \subset V(J)$, logo $V(J)$ é não vazio.

(2) $\Rightarrow$ (3) : Este passo é geralmente feito usando o truque de Rabinowitsch. Para um ideal $J \subset k[x_1, \ldots, x_n]$ e qualquer elemento $f \in I(V(J))$, queremos mostrar que $f^N \in J$ para algum N. O truque introduz uma variável adicional t. Definimos então $J_f \supset J$ por

$$J_f := (J, ft - 1) \subset k[x_1, \ldots, x_n, t].$$

Pela definição de J_f fica claro que $V(J_f) = \{Q = (a_1, \ldots, a_n, b) = (P, b) \in \mathbb{A}_k^{n+1} \mid P \in V(J),\ bf(P) = 1\}$. A projeção nas primeiras n coordenadas leva $V(J_f)$ no subconjunto $V(J)$ de pontos P com $f(P) \neq 0$. Mas f é um elemento de $I(V(J))$, então $V(J_f) = \emptyset$. Logo, por (2) $J_f = k[x_1, \ldots, x_n, t]$. Em particular, $1 \in J_f$, o que significa que podemos escrever

$$1 = \sum_{i=1}^{r} g_i f_i + g_0(ft - 1) \ \in \ k[x_1, \ldots, x_n, t] \tag{2.4}$$

para algum $g_i \in k[x_1, \ldots, x_n, t]$ e $f_i \in J$. Seja t^N a maior potência de t aparecendo em polinômios g_i para $0 \leq i \leq r$. Multiplicando (2.4) por f^N temos

$$f^N = \sum_{i=1}^{r} G_i(x_1, \ldots, x_n, ft) f_i + G_0(x_1, \ldots, x_n, ft)(ft - 1), \tag{2.5}$$

onde os $G_i = f^N g_i$ são polinômios em $x_1, \ldots, x_n, ft$. Essa equação é válida em $k[x_1, \ldots, x_n, t]$. Considerando essa equação módulo $(ft - 1)$, ou seja, reduzindo ao anel $k[x_1, \ldots, x_n, t]/(ft - 1)$, obtemos a relação

$$f^N \equiv \sum h_i(x_1, \ldots, x_n) f_i \mod (ft - 1),$$

onde $h_i(x_1, \ldots, x_n) := G_i(x_1, \ldots, x_n, 1)$. O fato de que o mapa

$$k[x_1, \ldots, x_n] \longrightarrow k[x_1, \ldots, x_n, t]/(ft - 1)$$

é injetivo, implica que já temos a relação

$$f^N = \sum h_i(x_1, \ldots, x_n) f_i$$

no anel polinomial $k[x_1, \ldots, x_n]$, então $f^N \in J$.

□

Exemplo 2.30. Uma **hipersuperfície afim** em $\mathbb{A}_k^n$ é um subconjunto algébrico dado pela equação

$$V(f) = \{P \in \mathbb{A}_k^n \mid f(P) = 0\}; \qquad 0 \neq f \in k[x_1, \ldots, x_n].$$

Observação 2.31. *Se a decomposição de f em fatores primos é dada por $f = f_1^{r_1} \ldots f_m^{r_m}$, então $\sqrt{(f)} = (f_1 \ldots f_m)$. O ideal (f) é primo se, e somente se, f é irredutível, i.e., se $m = 1$ e $r_1 = 1$. Temos então a seguinte bijeção*

$$\{\textit{hipersuperfícies irredutíveis em } \mathbb{A}_k^n\} \overset{1:1}{\longleftrightarrow} \{f \in k[x_1, \ldots, x_n] \mid f \textit{ irredutível }\}/k^*.$$

A prova do Teorema 2.28 encontra-se no apêndice A.

2.3 FUNÇÕES POLINOMIAIS E MAPAS

2.3.1 O anel de coordenadas de uma variedade

Nesta seção, V denota uma variedade afim em $\mathbb{A}_k^n$.

Definição 2.32. *Uma* ***função polinomial*** *em V é um mapa $f : V \to k$ tal que existe um polinômio $F \in k[x_1, \ldots, x_n]$ com $f(P) = F(P)$ para todo $P \in V$.*

O polinômio F não é unicamente determinado pelos valores que toma em V. Em particular, para F e $G \in k[x_1, \ldots, x_n]$ temos

$$F|_V = G|_V \iff (F - G)|_V = 0 \iff F - G \in I(V).$$

Somos então levados à seguinte definição.

Definição 2.33. *O* ***anel de coordenada de V*** *é definido como*

$$k[V] := k[x_1, \ldots, x_n]/I(V).$$

Pelo que foi feito acima podemos fazer a seguinte identificação:

$$k[V] = \{f \mid f : V \longrightarrow k \text{ é uma função polinomial}\}.$$

Pela Proposição 2.20 temos

$$\text{V é irredutível} \iff k[V] \text{ é um domínio de integridade.}$$

Note que as funções coordenadas $x_1, \ldots, x_n$ geram $k[V]$, o que explica a terminologia "anel de coordenada". Na seção passada vimos a relação entre subconjuntos de $\mathbb{A}_k^n$ e ideais no anel de coordenada $k[\mathbb{A}_k^n] = k[x_1, \ldots, x_n]$. O anel $k[V]$ tem o mesmo papel para V que $k[x_1, \ldots, x_n]$ tem para $\mathbb{A}_k^n$. Em particular, existe uma correspondência entre conjuntos fechados W contidos em V e ideais de $k[V]$. Para descrever essa relação, primeiro note que a projeção $\pi : k[x_1, \ldots, x_n] \to k[V] = k[x_1, \ldots, x_n]/I(V)$ induz uma bijeção

$$\{\text{ideais } J \subset k[x_1, \ldots, x_n] \mid J \subset I(V)\} \overset{1:1}{\longleftrightarrow} \{\text{ideais } J' \subset k[V]\},$$

definida por $J \mapsto J/I(V)$, com inversa $J' \mapsto \pi^{-1}(J')$. Esse mapa preserva ideais radicais, ideais primos e ideais maximais. Por isso, exatamente como no Corolário 2.29.1 temos as seguintes correspondências:

$$\begin{array}{ccc}
\{\text{ideais radicais } J' \subset k[V]\} & \overset{1:1}{\longleftrightarrow} & \{\text{conjuntos fechados } W \subset V\} \\
\cup & & \cup \\
\{\text{ideais primos } J' \subset k[V]\} & \overset{1:1}{\longleftrightarrow} & \{\text{ conjuntos irredutíveis } W \subset V\} \\
\cup & & \cup \\
\{\text{ideais maximais } J' \subset k[V]\} & \overset{1:1}{\longleftrightarrow} & \{\text{pontos de } V\}.
\end{array}$$

Nós temos falado aqui sobre **conjuntos fechados de** V no sentido utilizado na topologia de Zariski em $\mathbb{A}_k^n$. Este resultado mostra que é equivalente à topologia definida tomando os fechados de V como conjuntos da forma $V(J)$, onde J é um ideal radical em $k[V]$.

Vamos discutir uma outra importante característica do anel de coordenada de uma variedade.

Definição 2.34. *Uma álgebra A é **reduzida** se A não contém elementos nilpotentes, i.e., para $x \in A$, se $x^n = 0$ para algum $n \geq 1$, então $x = 0$.*

Observação 2.35. *A álgebra $k[x_1, \ldots, x_n]/I$ é reduzida se, e somente se, I é um ideal radical, logo, já que $I(V)$ um ideal radical, o anel de coordenada é uma álgebra reduzida. Por construção, o anel de coordenada $k[V]$ de uma variedade afim V é uma k-álgebra finitamente gerada. Estas propriedades caracterizam os anéis de coordenadas, no sentido de que dado uma k-álgebra finitamente gerada A, podemos construir uma variedade algébrica correspondente como se segue. Escolhendo os geradores $a_1, \ldots, a_n$ podemos escrever $A = k[a_1, \ldots, a_n]$, temos o seguinte homomorfismo sobrejetivo*

$$\begin{aligned} \pi \ : \ k[x_1, \ldots, x_n] &\longrightarrow A = k[a_1, \ldots, a_n], \\ x_i &\longmapsto a_i. \end{aligned}$$

Seja $I = \ker(\pi)$. Então $V = V(I)$ é uma variedade que é irredutível se, e somente se, A é um domínio de integridade (Proposição 2.20). Já que A é reduzida, I é um ideal radical, então $I(V) = I$, e por construção $A = k[V]$.

Exemplo 2.36. Consideremos agora dois exemplos de anéis de coordenada, aos quais vamos retornar depois. Para a *parábola usual*

$$C_0 = \{(x, y) \in \mathbb{A}_2^k \mid y - x^2 = 0\}$$

temos

$$k[C_0] = k[x, y]/(y - x^2) \cong k[\mathbb{A}_k^1].$$

Para a parábola *semicúbica*, dada por

$$C_1 = \{(x, y) \in \mathbb{A}_k^2 \mid y^2 - x^3 = 0\},$$

temos

$$k[C_1] = k[x, y]/(y^2 - x^3).$$

Note que $k[C_1]$ não é um *domínio de fatoração única*[2]. Como conjuntos, existem bijeções entre cada C_0 e C_1 e $\mathbb{A}_k^1$, já que cada curva tem uma parametrização racional, dada por $t \mapsto (t, t^2)$ e $t \mapsto (t^2, t^3)$ respectivamente. No entanto, como variedades algébricas C_0 e C_1 se comportam de maneira diferente. Posteriormente veremos que C_0 é isomorfo a $\mathbb{A}_k^1$ mas C_1 não o é.

[2] Ver (6) página 360.

2.3.2 Mapas polinomiais

Agora vamos considerar mapas entre conjuntos algébricos. Durante esta seção $V \subset \mathbb{A}_k^n$ e $W \subset \mathbb{A}_k^m$ são conjuntos fechados, e x_i, para $1 \leq i \leq n$ e y_i, para $1 \leq j \leq m$, são as funções coordenadas em $\mathbb{A}_k^n$ e $\mathbb{A}_k^m$ respectivamente.

Definição 2.37. *Um mapa $f : V \longrightarrow W$ é chamado de **mapa polinomial** se existem polinômios $F_1, \ldots, F_m \in k[x_1, \ldots, x_n]$ tal que*

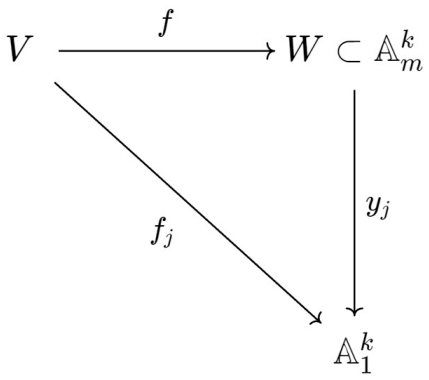
$$f(P) = (F_1(P), \ldots, F_m(P)) \in W \subset \mathbb{A}_k^m$$

para todos os pontos $P \in V$.

Lema 2.38. *Sejam $y_1, \ldots, y_m$ as funções coordenadas em $\mathbb{A}_k^m$. Um mapa $f : V \longrightarrow W$ é um mapa polinomial se, e somente se, $f_j := y_j \circ f \in k[V]$ para $j = 1, \ldots, m$.*

Prova. Compondo f com y_j obtemos a projeção na j-ésima coordenada:

Figura 7 – Diagrama.



Fonte: Ver (1) página 40. (2000)

Seja $f_j = y_j \circ f$. Então se f é um mapa polinomial, temos $f_j(P) = F_j(P)$ para algum $F_j \in k[x_1, \ldots, x_n]$. Logo f_j é um mapa polinomial, e por isso $f_j \in k[V]$.

Por outro lado, se $f_j = y_j \circ f$ é um mapa polinomial para cada j, então por definição exitem polinômios $F_1, \ldots, F_m$ com $f(P) = (F_1(P), \ldots, F_m(P))$ para todo $P \in V$. □

O próximo lema nos mostra que qualquer função polinomial $f : V \longrightarrow W$ pode ser escrito na forma $f = (f_1, \ldots, f_m)$ com $f_1, \ldots, f_m \in k[V]$.

Lema 2.39. *Um mapa polinomial $f : V \longrightarrow W$ é contínuo na topologia de Zariski.*

Prova. Devemos mostrar que se $Z \subset W$ é fechado, então $f^{-1}(Z)$ também é fechado. É possível ver isso já que $Z = \{h_1 = \ldots = h_r = 0\}$ então $f^{-1}(Z) = \{h_1 \circ f = \ldots = h_r \circ f = 0\}$, logo também é fechado. □

Exemplo 2.40. Neste exemplo, as curvas C_0 e C_1 são definidas como no Exemplo 2.36. O mapa de $\mathbb{A}^1_k$ para a parábola

$$\begin{aligned} f : \mathbb{A}^1_k &\longrightarrow C_0, \\ t &\mapsto (t, t^2), \end{aligned}$$

e o mapa

$$\begin{aligned} g : \mathbb{A}^1_k &\longrightarrow C_1, \\ t &\mapsto (t^2, t^3), \end{aligned}$$

são ambos mapas polinomiais bijetivos.

Exemplo 2.41. Para cada escolha de formas lineares $y_1, \ldots, y_m$ nas variáveis $x_1, \ldots, x_n$ o mapa

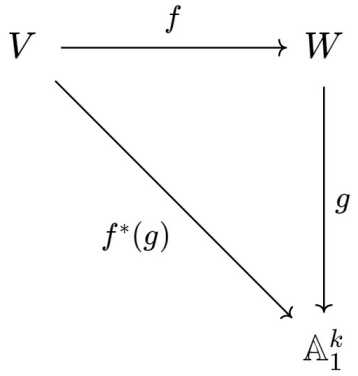
$$f = (y_1, \ldots, y_m) : \quad \mathbb{A}^n_k \longrightarrow \mathbb{A}^m_k$$

é um mapa polinomial. Como uma consequência da normalização de Noether, foi mostrado na Proposição 1 que para cada variedade irredutível V existe algum inteiro m tal que para uma escolha geral de $y_1, \ldots, y_m$ o mapa $\phi = f|_V$ é sobrejetivo com fibras finitas.

Se $V \subset \mathbb{A}^n_k, W \subset \mathbb{A}^m_k$ e $X \subset \mathbb{A}^l_k$ são conjuntos algébricos, e $f : V \longrightarrow W$ e $g : W \longrightarrow X$ são mapas polinomiais, então $g \circ f : V \longrightarrow X$ é também um mapa polinomial. Isto segue imediatamente do fato de que a composição de polinômios ainda é um polinômio.

Agora seja $f : V \longrightarrow W$ um mapa polinomial. Para $g \in k[W]$ definimos $f^*(g) := g \circ f$:

Figura 8 – Diagrama.



Fonte: Ver (1) página 41. (2000)

Como g é uma função polinomial, $g \circ f$ também o é. Logo temos o mapa

$$\begin{aligned} f^* : k[W] &\longrightarrow k[V], \\ g &\mapsto f^*(g) = g \circ f. \end{aligned}$$

Se $f : V \longrightarrow W,\ g : W \longrightarrow X$ são mapas polinomiais, então

$$(g \circ f)^* = f^* \circ g^* \ : \ k[X] \longrightarrow k[V].$$

Isto segue imediatamente do fato de que se $h \in k[X]$ temos

$$(g \circ f)^*(h) = h \circ (g \circ f) = (h \circ g) \circ f = g^*(h) \circ f = f^*(g^*(h)).$$

O mapa f^* é um **homomorfismo de anéis**, já que temos

$$f^*(g_1 + g_2) = (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f = f^*(g_1) + f^*(g_2),$$
$$f^*(g_1 \cdot g_2) = (g_1 \cdot g_2) \circ f = (g_1 \circ f) \cdot (g_2 \circ f) = f^*(g_1) \cdot f^*(g_2).$$

Para uma constante $c \in k$ temos $f^*(c) = c$, logo f^* é também um homomorfismo de k-álgebras. Logo todo mapa polinomial $f : V \longrightarrow W$ dá origem a um homomorfismo de k-álgebras $f^* \ : \ k[W] \longrightarrow k[V]$. O próximo teorema nos diz que este procedimento tem um inverso.

Proposição 2.42. *Se $\varphi \ : \ k[W] \longrightarrow k[V]$ é um homomorfismo de k-álgebras, então existe um único mapa polinomial $f : V \longrightarrow W$ tal que $\varphi = f^*$.*

Prova. Suponha que $W \subset \mathbb{A}_k^m$, e seja $y_1, \ldots, y_m$ as funções coordenadas em $\mathbb{A}_k^m$. Então

$$k[W] = k[y_1, \ldots, y_m]/I(W) = k[\bar{y}_1, \ldots, \bar{y}_m],$$

onde $\bar{y}_i = y_i + I(W)$. Defina $f_i := \varphi(\bar{y}_i) \in k[V]$ para $i = 1, \ldots, m$. Então

$$f := (f_1, \ldots, f_m) \ : \ V \longrightarrow \mathbb{A}_k^m$$

é um mapa polinomial (cf. Lema 2.38). Primeiro mostraremos que $f(V) \subset W$. Para ver isto, suponha que $G = G(y_1, \ldots, y_m) \in I(W)$. Então em $k[V]$ temos $G(\bar{y}_1, \ldots, \bar{y}_m) = 0$ e por isso

$$G(f_1, \ldots, f_m) = G(\varphi(\bar{y}_1), \ldots, \varphi(\bar{y}_m)) = \varphi(G(\bar{y}_1, \ldots, \bar{y}_m)) = 0,$$

o que implica que $f(V) \subset W$. Em seguida devemos mostrar que $\varphi = f^*$. Os elementos $\bar{y}_1, \ldots, \bar{y}_m$ geram a k-álgebra $k[W]$, e então é suficiente mostrar que $\varphi(\bar{y}_i) = f^*(\bar{y}_i) = f_i$. Mas isto é precisamente a definição de f_i. Este argumento mostra que $f = (f_1, \ldots, f_m)$ é o único mapa polinomial com $\varphi = f^*$.

Corolário 2.42.1. *Existe uma bijeção:*

$$\left\{ f \ \middle| \ \begin{array}{c} f : V \longrightarrow W \\ \text{é um mapa polinomial} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \varphi \ \middle| \ \begin{array}{c} \varphi : k[W] \longrightarrow k[V] \\ \text{é um homomorfismo de } k\text{-álgebras} \end{array} \right\}$$
$$f \longmapsto f^*.$$

Definição 2.43. *Um mapa polinomial $f : V \longrightarrow W$ é um* ***isomorfismo*** *se existe um mapa polinomial $g : W \longrightarrow V$ tal que $f \circ g = id_W$ e $g \circ f = id_V$.*

Corolário 2.43.1. *Um mapa polinomial $f : V \longrightarrow W$ é um isomorfismo de variedades se, e somente se, $f^* : k[W] \longrightarrow k[V]$ é um isomorfismo de $k-$álgebras.*

Prova. Segue do fato de que $(f \circ g)^* = g^* \circ f^*$. □

Exemplo 2.44. Seja $A = (\alpha_{ij})$ uma matriz inversível $(n \times n)$. Então as formas lineares

$$y_i = \sum_{j=1}^{n} \alpha_{ij} x_j$$

definem um mapa polinomial bijetivo

$$f = (y_1, \ldots, y_n) \ : \ \mathbb{A}_k^n \longrightarrow \mathbb{A}_k^n.$$

Exemplo 2.45. Considere a parábola $C_0 = \{y - x^2 = 0\}$ em $\mathbb{A}_k^2$ e a parametrização

$$\begin{aligned} f \ : \ \mathbb{A}_k^1 &\longrightarrow C_0, \\ t &\longmapsto (t, t^2). \end{aligned}$$

A projeção $p : \mathbb{A}_k^2 \longrightarrow \mathbb{A}_k^1$ para a primeira coordenada, restrita à C_0, nos dá o mapa inverso

$$\begin{aligned} g : C_0 &\longrightarrow \mathbb{A}_k^1, \\ (x, y) &\longmapsto x. \end{aligned}$$

Logo f é um isomorfismo. Podemos também ver isso considerando o mapa $f^* : k[C_0] \longrightarrow k[\mathbb{A}_k^1]$, já que

$$\begin{aligned} f^* : k[C_0] \cong k[x] &\longrightarrow k[\mathbb{A}_k^1] = k[t], \\ x &\longmapsto t, \end{aligned}$$

é um isomorfismo.

Exemplo 2.46. Um comportamento diferente pode ser observado no caso da parábola semicúbica, $C_1 = \{(x, y) \mid y^2 = x^3\}$. Especificamente, o mapa

$$\begin{aligned} f : \mathbb{A}_k^1 &\longrightarrow C_0, \\ t &\mapsto (t^2, t^3), \end{aligned}$$

é uma bijeção, mas a imagem $f^*(k[C_1]) \subset k(\mathbb{A}_k^1) = k[t]$ é gerada por $f^*(x) = t^2$ e $f^*(y) = t^3$, logo $f^*(k[C_1]) \neq k[t]$, por isso f não é um isomorfismo. No entanto f é uma bijeção com mapa inverso

$$\begin{aligned} g : C_1 \ &\longrightarrow \ \mathbb{A}_k^1, \\ g(x, y) \ &= \ \begin{cases} y/x & \text{se } (x, y) \neq (0, 0) \\ 0 & \text{se } (x, y) = (0, 0), \end{cases} \end{aligned}$$

que não é um mapa polinomial.

2.4 FUNÇÕES RACIONAIS E MORFISMOS

Vamos assumir agora que V é uma **variedade irredutível**. Isto implica que o anel de coordenadas $k[V]$ é um domínio de integridade e portanto tem um corpo de frações.

Definição 2.47. *O* ***corpo de funções*** *de V é o corpo de frações de $k[V]$, e é denotado por $k(V)$. Elementos $f \in k(V)$ são chamados de* ***funções racionais*** *de V.*

Qualquer função racional pode ser escrita como $f = g/h$ com $g, h \in k[V]$. Em geral $k[V]$ não precisa ser um domínio de fatoração única, logo tal representação não é necessariamente única. Podemos dar a f um valor definido no ponto P se existe tal representação $f = g/h$ com $h(P) \neq 0$.

Definição 2.48. *Seja $f \in k(V)$ e $P \in V$. A função racional f é chamada de* ***regular*** *em P se existe uma representação $f = g/h$ com $h(P) \neq 0$. O* ***domínio de definição de*** *f é definido como sendo o conjunto*

$$dom\,(f) := \{P \in V \mid f \text{ é regular em } P\}.$$

Definição 2.49. *Para cada função polinomial $h \in k[V]$ definimos*

$$V_h := \{P \in V \mid h(P) \neq 0\}.$$

Claramente V_h é um conjunto aberto de V, já que seu complementar é fechado.

Teorema 2.50. *Para uma função racional $f \in k(V)$ as seguintes afirmações são válidas:*

(1) *dom (f) é aberto e denso em V.*

(2) *dom $(f) = V \iff f \in k[V]$.*

(3) *dom $(f) \supset V_h \iff f \in k[V][h^{-1}]$.*

Prova. (1) Para $f \in k(V)$ definimos o **ideal de denominadores de** f por

$$D_f := \{h \in k[V] \mid fh \in k[V]\} \subset k[V].$$

Por definição temos

$$D_f = \{h \in k[V] \mid \text{existe uma representação } f = g/h\} \cup \{0\},$$

e

$$V \setminus \text{dom } (f) = \{P \in V \mid h(P) = 0 \text{ para todo } h \in D_f\} = V(D_f).$$

Logo dom (f) é aberto. Como dom (f) é não vazio, é também denso em V pelo Lema 2.24.

(2) Temos que dom $(f) = V$ se, e somente se, $V(D_f) = \emptyset$. Pelo Nullstellensatz de Hillbert isso é equivalente a $1 \in D_f$, que é equivalente a $f \in k[V]$.

(3) Temos que dom $(f) \supset V_h$ se, e somente se, h se anula em $V(D_f)$. De novo, pelo Nullstellensatz de Hillbert isso é equivalente a $h^n \in D_f$ para algum $n \geq 1$, o que implica que $f = g/h^n \in k[V][h^{-1}]$.

□

A parte dois do teorema anterior dos diz que funções polinomiais são precisamente função racionais que são "regulares em todo lugar". No futuro vamos nos referir às funções polinomiais como **funções regulares**. A seguir, vamos definir o anel $\mathcal{O}(U)$ das funções regulares em um aberto $U \subset V$, o que eventualmente levará ao conceito de *feixe estrutural de uma variedade.* Primeiro devemos definir o anel de funções em V regulares no ponto $P \in V$.

Definição 2.51. *O* ***anel local de*** V *em um ponto* $P \in V$ *é o anel*

$$\mathcal{O}_{V,P} = \{f \in k(V) \mid f \text{ é regular em } P\}$$

O anel local $\mathcal{O}_{V,P} \subset k(V)$ *é um subanel de* $k(V)$*, e temos*

$$\mathcal{O}_{V,P} = k[V]\{h^{-1} \mid h(P) \neq 0\}.$$

O anel $\mathcal{O}_{V,P}$ *é um anel local, i.e., tem um único ideal maximal:*

$$m_P := \left\{ \frac{f}{g} \in k(V) \;\middle|\; f, g \in k[V],\ f(P) = 0,\ g(P) \neq 0 \right\}.$$

2.4.1 Localização de anéis

Tendo definido o anel local $\mathcal{O}_{V,P}$, que terá um papel importante na teoria, agora é um momento adequado para introduzir o conceito de *localização*, que é uma maneira de produzir anéis locais a partir de anéis arbitrários.

Definição 2.52. *Um* ***sistema multiplicativo fechado*** *em* R *é um subconjunto* $S \subset R^* = R \setminus \{0\}$ *com as seguintes propriedades:*

(1) $a, b \in S \implies ab \in S$.

(2) $1 \in S$.

Exemplo 2.53. Um anel R é um domínio de integridade se $R^* = R \setminus \{0\}$ é um sistema multiplicativo fechado.

Exemplo 2.54. Um ideal $\mathfrak{p} \neq R$ é um ideal primo se, e somente se, $R \setminus \mathfrak{p}$ é um sistema multiplicativo fechado.

Vamos agora aumentar o anel R "permitindo que elementos de S apareçam no denominador". Isto generaliza a construção de um corpo de frações de um domínio de integridade. Definimos a seguinte relação de equivalência no produto cartesiano $R \times S$:

$$(r', s') \sim (r'', s'') \iff \text{existe } s \in S \text{ com } s(r's'' - r''s') = 0.$$

O conjunto das classes de equivalência é denotado por

$$R_S := R \times S/\sim .$$

Escrevemos r/s para denotar a classe de equivalência de (r, s). Podemos então definir adição e multiplicação em R_S da seguinte forma:

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}; \qquad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

É possível verificar que estas operações estão bem definidas. O anel R_S é um anel comutativo com unidade $1 = \dfrac{1}{1}$ e o mapa

$$\begin{aligned} R &\longrightarrow R_S, \\ r &\longmapsto \frac{r}{1}, \end{aligned}$$

é um homomorfismo de anéis.

Definição 2.55. *O anel R_S é chamado de **localização** de R com respeito ao conjunto multiplicativo S.*

Exemplo 2.56. Seja R um domínio de integridade e $S = R^* = R \setminus \{0\}$. Então R_S é o corpo de frações de R, e o mapa $R \longrightarrow R_S$ descrito acima é injetivo, e R, portanto, pode ser identificado com sua imagem em R_S.

Exemplo 2.57. Seja $\mathfrak{p} \subsetneq R$ um ideal primo e seja $S_\mathfrak{p} = R \setminus \mathfrak{p}$. Frequentemente é escrito

$$R_\mathfrak{p} := R_{S_\mathfrak{p}},$$

e chamamos $R_\mathfrak{p}$ de **localização** de R em $\mathfrak{p}$. Na verdade $R_\mathfrak{p}$ é um anel local, i.e., tem um único ideal maximal, o ideal:

$$m_\mathfrak{p} := \left\{ \mathfrak{p}s \;\middle|\; p \in \mathfrak{p}, s \in S_\mathfrak{p} \right\} \subsetneq R_\mathfrak{p}.$$

Para ver que $m_\mathfrak{p}$ é um ideal maximal, note que um elemento $R_\mathfrak{p}$ que não esteja em $m_\mathfrak{p}$ é da forma s'/s com $s' \in S_\mathfrak{p}$, e portanto tem inverso s/s' e dessa forma é uma unidade.

Exemplo 2.58. Dado um domínio de integridade R e para $0 \neq f \in R$, seja $S_f := \{f^n \mid n \geq 0\}$. Definimos

$$R_f := R_{S_f}.$$

Já que R é um domínio de integridade, o mapa $R \longrightarrow R_f, r \mapsto \frac{r}{1}$ é injetivo. Identificando R com sua imagem em R_f e no corpo de frações, temos a igualdade

$$R_f = R[f^{-1}] \subset \text{ corpo de frações de R.}$$

2.4.2 O feixe estrutural de uma variedade

O anel local $\mathcal{O}_{V,P}$, definido acima como um subcorpo do corpo de funções $k(V)$, também pode ser construído por localização. Ou seja, para um ponto $P \in V$ o ideal correspondente,

$$\bar{M}_P = \{f \in k[V] \mid f(P) = 0\} = \overline{I(\{P\})} = I(\{P\}) + I(V) \subset k[V],$$

é maximal pelo Corolário 2.29.1, temos então uma igualdade

$$\mathcal{O}_{V,P} = k[V]_{\bar{M}_P},$$

i.e. $\mathcal{O}_{V,P}$ surge através da localização do anel de coordenadas em $\bar{M}_P$. O ideal maximal em $\mathcal{O}_{V,P}$ é dado por $m_P = \{f \in \mathcal{O}_{V,P} \mid f(P) = 0\}$. Para cada conjunto aberto não vazio $U \subset V$ definimos

$$\mathcal{O}(U) := \mathcal{O}_V(U) := \{f \in k(V) \mid \ f \text{ é regular em } U\},$$

e definimos também $\mathcal{O}_V(\emptyset) := \{0\}$. Então $\mathcal{O}_V(U)$ é um anel, mais ainda, uma k-álgebra. O conjunto dos anéis $\mathcal{O}_V(U)$, junto com a restrição de homomorfismos, forma o **feixe estrutural** de $\mathcal{O}_V$. O anel local $\mathcal{O}_{V,P}$ é chamado de **stalk** do feixe estrutural no ponto P, e os seus elementos são chamados de **funções germes**. Agora podemos escrever o Teorema 2.50 da seguinte forma:

$$\mathcal{O}(V) = k[V] \qquad \text{(Teorema 2.50 (2))} \tag{2.6}$$

e

$$\mathcal{O}(V_h) = k[V][h^{-1}] = k[V]_h \qquad \text{(Teorema 2.50 (3))},$$

onde o anel $k[V]_h$ é a localização do anel de coordenadas $k[V]$ com respeito ao sistema multiplicativo $\{h^n \mid n \geq 0\}$. Pode-se ver uma discussão mais detalhada e rigorosa sobre feixes em (7).

2.4.3 Mapas racionais

Vamos frequentemente precisar considerar mapas em V que não são definidos em todo lugar, e portanto, introduzimos esse novo conceito.

Definição 2.59. (1) *Um* ***mapa racional*** $f : V \dashrightarrow \mathbb{A}_k^n$ *é uma* $n-$*upla* $f = (f_1, \ldots, f_n)$ *de funções racionais* $f_1, \ldots, f_n \in k(V)$. *O mapa* f *é chamado de* ***regular*** *no ponto* P *se todos os* f_i *são regulares em* P. *O* ***domínio de definição*** $dom\,(f)$ *é o conjunto de todos os pontos regulares de* f, *i.e.,* $dom\,(f) = \bigcap_{i=1}^{n} = dom\,(f_i)$.

(2) *Para uma variedade* $W \subset \mathbb{A}_k^n$, *um mapa racional* $f : V \dashrightarrow W$ *é uma mapa racional* $f : V \dashrightarrow \mathbb{A}_k^n$ *tal que* $f(P) \in W$ *para todos os pontos regulares* $P \in dom\,(f)$.

Segue do Teorema 2.50 que o domínio de definição de um mapa racional é um conjunto aberto não vazio de V.

Em contraste com a situação de mapas polinomiais, para mapas racionais $f : V \dashrightarrow W$ e $g : W \dashrightarrow X$ a composição

$$g \circ f : V \overset{f}{\dashrightarrow} W \overset{g}{\dashrightarrow} X$$

não pode ser sempre definida. Isto é ilustrado no seguinte exemplo.

Exemplo 2.60. Para os mapas racionais f e g definidos da seguinte forma

$$\begin{aligned} f : \mathbb{A}_k^1 \to \mathbb{A}_k^2, \qquad & g : \mathbb{A}_k^2 \dashrightarrow \mathbb{A}_k^1, \\ f(x) = (x, 0) \qquad & g(x, y) = \frac{x}{y}, \end{aligned}$$

a composição não é definida em nenhum lugar, já que $f(\mathbb{A}_k^1) \cap \text{dom}\,(g) = \emptyset$.

Formulando algebricamente o problema, temos: dado um mapa racional $f : V \dashrightarrow W$, queremos definir o mapa

$$f^* : k(W) \longrightarrow k(V)$$

com $f^*(g) = g \circ f$. No Exemplo 2.41 foi construído um homomorfismo

$$f^* : k[W] \longrightarrow k[V],$$

logo sabemos que para $g \in k[W]$ a função $f^*(g) \in k(V)$ é bem definida. No entanto é possível que $f^*(h) = 0$ para algum $h \in k[W]$, com $h \neq 0$, neste caso não podemos definir $f^*(g/h)$ como $f^*(g)/f^*(h)$. Nosso objetivo agora é construir mapas em que a composição pode ser definida.

Definição 2.61. *Um mapa racional* $f : V \dashrightarrow W$ *é chamado de* ***dominante*** *se* $f(dom\,(f))$ *é um subconjunto de Zariski denso de* W.

Definição 2.62. *Para um mapa racional $f : V \dashrightarrow W$ e um subconjunto $U \subset W$, definimos a* ***imagem inversa*** *de U sobre f como*

$$f^{-1}(U) := \{P \in dom\,(f) \mid f(P) \in U.\}$$

Suponha que $f : V \dashrightarrow W$ seja dominante[3], e que $g : W \dashrightarrow \mathbb{A}^1_k$ é um mapa racional. O Teorema 2.50 parte (1) nos diz que dom (g) é um conjunto não vazio aberto de W, e o Lema 2.39 implica que $f^{-1}(\text{dom }(g))$ é um subconjunto aberto denso de dom (f). Logo a composição $g \circ f : V \dashrightarrow \mathbb{A}^1_k$ é definida no subconjunto denso aberto $f^{-1}(\text{dom }(g))$ de V.

Algebricamente temos a seguinte situação. Para um mapa racional $f : V \dashrightarrow W$ com homomorfismo correspondente

$$f^* : k[W] \longrightarrow k(V),$$

para todo $g \in k[W]$, temos

$$f^*(g) = 0 \iff f(\text{dom }(f)) \subset V(g).$$

Segue que

$$f^* : k[W] \to k(V) \text{ é injetivo} \iff f \text{ é dominante,}$$

e por isso se f é dominante podemos estender f^* a um homomorfismo

$$f^* : k(W) \longrightarrow k(V)$$

definindo $f^*(g/h) := f^*(g)/f^*(h)$. Note que se $f : V \dashrightarrow W$ e $g : W \dashrightarrow X$ são dominantes, então $g \circ f : V \dashrightarrow X$ é também dominante. Temos então o seguinte resultado.

Teorema 2.63. *Para variedades afins irredutíveis V e W,*

(1) *Todo mapa racional dominante $f : V \dashrightarrow W$ define um $k-$homomorfismo linear $f^* : k(W) \longrightarrow k(V)$.*

(2) *Por outro lado, se $\varphi : k(W) \longrightarrow k(V)$ é um $k-$homomorfismo linear, então existe um único mapa racional dominante $f : V \dashrightarrow W$ com $\varphi = f^*$.*

(3) *Se $f : V \dashrightarrow W$ e $g : W \dashrightarrow X$ são dominantes, então $g \circ f : V \dashrightarrow X$ é também dominante e $(g \circ f)^* = f^* \circ g^*$.*

Prova. Já discutimos (1) e (3) anteriormente. A prova de (2) é similar à prova da Proposição 2.42. Suponha que $W \subset \mathbb{A}^m_k$, então as funções coordenadas $y_1, \ldots, y_m$ geram o corpo $k(W)$. Definimos $f_i := \varphi(y_i) \in k(V)$ e $f := (f_1, \ldots, f_m) : V \dashrightarrow W$. Este mapa tem imagem em W como mostrado na prova da Proposição 2.42. Por construção temos $f^* = \varphi$. Resta mostrar que f é dominante. Já que $f^* = \varphi$ temos $f^*|_{k[W]} = \varphi|_{k[W]}$. Já que φ é um homomorfismo de corpos, φ é injetiva, logo $f^*|_{k[W]} : k[W] \longrightarrow k(V)$ é também injetiva, e por isso f é dominante. □

[3] f é dominante se sua imagem é densa.

2.4.4 Variedades quasi-afins

Como subconjuntos abertos de variedades afins se comportam da mesma forma que as próprias variedades, vamos introduzir a seguinte terminologia.

Definição 2.64. *Uma **variedade quase afim** é um subconjunto aberto de uma variedade afim.*

Definição 2.65. *A seguir U_1 e U_2 são variedades quasi-afins irredutíveis, contidas nas variedades V e W respectivamente.*

(1) *Um **morfismo** $f : U_1 \longrightarrow W$ é um mapa racional $f : V \dashrightarrow W$ com $U_1 \subset dom\,(f)$, i.e., f é regular em todo ponto $P \in U_1$.*

(2) *Um **morfismo** $f : U_1 \longrightarrow U_2$ é um morfismo $f : U_1 \longrightarrow W$ com $f(U_1) \subset U_2$.*

(3) *Um **isomorfismo** de variedades quasi-afins é um morfismo f: $U_1 \longrightarrow U_2$ tal que existe um morfismo $g : U_2 \longrightarrow U_1$ com $g \circ f = id_{U_1}$ e $f \circ g = id_{U_2}$.*

Para cada duas variedades irredutíveis V e W, o Teorema 2.50 diz que os morfismos entre V e W são mapas polinomiais, portanto temos a seguinte igualdade de conjuntos:

$$\{f \mid f : V \longrightarrow W \text{ é um morfismo}\} = \{f \mid f : V \longrightarrow W \text{ é um mapa polinomial}\}.$$

Exemplo 2.66. Esta parábola semicúbica

$$C_1 = \{(x, y) \in \mathbb{A}^2_k \mid y^2 - x^3 = 0\}$$

tem a parametrização

$$\begin{aligned} f : \mathbb{A}^1_k &\longrightarrow C_1, \\ t &\longmapsto (t^2, t^3), \end{aligned}$$

e foi visto anteriormente que não é um isomorfismo, logo $k[\mathbb{A}^1_k]$ e $k[C_1]$ não são isomorfos (Corolário 2.43.1). No entanto, a restrição $f : \mathbb{A}^1_k \setminus \{0\} \longrightarrow C_1 \setminus \{(0, 0)\}$ é um isomorfismo de variedades quasi-afins, com inversa $g(x, y) = y/x$. Na terminologia vista anteriormente temos que $\mathbb{A}^1_k$ e C_1 são **birracionalmente equivalentes**. O Teorema 2.63 nos dá um mapa

$$f^* : k(C_1) \longrightarrow k(\mathbb{A}^1_k),$$

com $f^*(y/x) = t$. Logo f^* é sobrejetiva, e sendo um homomorfismo de corpos não nulo, f^* também é injetiva, e portanto o corpo de funções de $k(\mathbb{A}^1_k) = k(t)$ e $k(C_1)$ são isomorfos.

Uma variedade quasi-afim pode ser isomorfa a uma variedade afim, por exemplo, na Definição 2.49, foi introduzido para uma variedade afim V e para $f \in k[V]$,

$$V_f = V \setminus V(f) = \{P \in V \mid f(P) \neq 0\}.$$

Proposição 2.67. *A variedade quasi-afim V_f é isomorfa a uma variedade afim com anel de coordenadas $k[V_f] = k[V][f^{-1}] = k[V]_f$.*

Prova. Usaremos novamente o truque de Rabinowitsch. Seja $J := I(V) \subset k[x_1, \ldots, x_n]$ o ideal da variedade $V \subset \mathbb{A}^n_k$, e seja $F \in k[x_1, \ldots, x_n]$ um polinômio com $F|_V = f$. Definimos

$$J_F := (J, tF - 1) \subset k[x_1, \ldots, x_n, t].$$

Afirmamos que V_f é isomorfa a uma variedade afim

$$W = V(J_F) \subset \mathbb{A}^{n+1}_k.$$

Isto segue do fato de que os mapas

$$\begin{aligned} p : W &\longrightarrow V_f, \\ (x_1, \ldots, x_n, y) &\longmapsto (x_1, \ldots, x_n), \end{aligned}$$

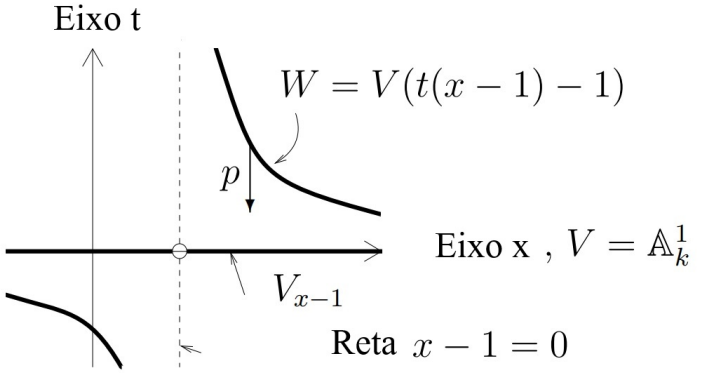
e

$$\begin{aligned} q : V_f &\longrightarrow W, \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_n, \frac{1}{F(x_1, \ldots, x_n)}), \end{aligned}$$

são claramente morfismos mutuamente inversos. □

A figura a seguir ilustra essa proposição onde $V = \mathbb{A}^1_k$ e $f = x - 1$. Neste caso o mapa p é a projeção no eixo-x.

Figura 9 – A variedade quasi-afim $\mathbb{A}^1_k \setminus \{1\} = (\mathbb{A}^1_k)_{(x-1)} \subset \mathbb{A}^1_k$ é isomorfa à variedade afim $W \subset \mathbb{A}^2_k$ dada por $t(x-1) = 1$.



Fonte: Ver (1) página 57. (2000)

Note que cada conjunto aberto de V é uma união conjuntos da forma V_f, implicando que os conjuntos V_f formam uma **base** para a topologia de Zariski de V. Temos então o seguinte corolário.

Corolário 2.67.1. *A Topologia de Zariski em V tem uma* ***base de conjuntos afins.***

Observação 2.68. *Existem variedades quasi-afins que não são afins, um exemplo simples seria* $\mathbb{A}_k^2 \setminus \{(0,0)\}$.

3 VARIEDADES PROJETIVAS

3.1 O ESPAÇO PROJETIVO

Seja V um espaço vetorial de dimensão finita sobre um corpo k. Considere a seguinte relação de equivalência:

$$u \sim v \iff \text{existe } \lambda \in k^* \text{ com } u = \lambda v.$$

Definição 3.1. *O **espaço projetivo** associado a V é definido como*

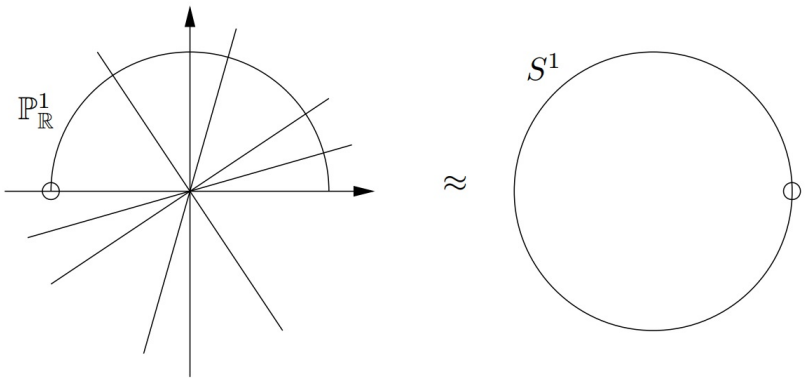
$$\mathbb{P}(V) := (V \setminus \{0\})/\sim .$$

A **dimensão** de $\mathbb{P}(V)$ é definida como $\dim \mathbb{P}(V) := \dim V - 1$. Dois vetores são equivalentes se, e somente se, geram a mesma reta em V. Geometricamente o espaço projetivo associado a V é o conjunto de todas as retas que passam pela origem de V. Em particular, tomando $V = k^{n+1}$ definimos

$$\mathbb{P}^n := \mathbb{P}^k_n := \mathbb{P}(k^{n+1}).$$

Exemplo 3.2. O espaço $\mathbb{P}^1_{\mathbb{R}} = \mathbb{P}(\mathbb{R}^2)$ é homeomorfo a S^1.

Figura 10 – A reta real projetiva $\mathbb{P}^1_{\mathbb{R}}$.



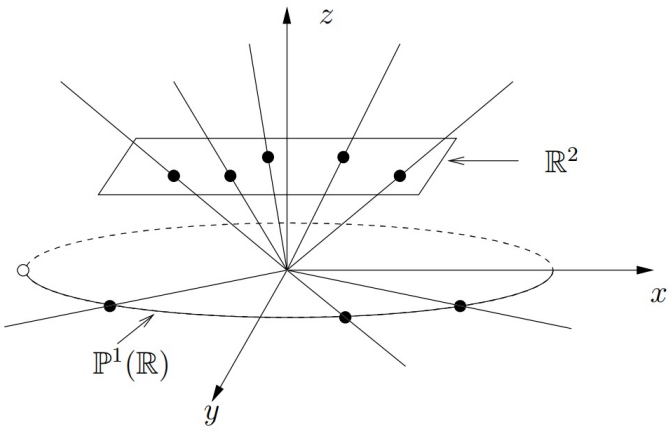
Fonte: Ver (1) página 64. (2000)

Exemplo 3.3. O plano projetivo real tem uma decomposição

$$\mathbb{P}^2_{\mathbb{R}} = \mathbb{P}(\mathbb{R}^3) = \mathbb{R}^2 \cup \mathbb{P}^1(\mathbb{R}).$$

Sob esta decomposição $\mathbb{R}^2$ corresponde ao conjunto de retas que não se encontram no plano-(x, y), e $\mathbb{P}^1_{\mathbb{R}}$ corresponde ao conjunto de retas que estão no plano-(x, y), como mostrado a seguir.

Figura 11 – Decomposição do espaço projetivo real $\mathbb{P}^2_{\mathbb{R}}$.



Fonte: Ver (1) página 64. (2000)

Nesta seção vamos denotar o mapa da classe de resíduos como

$$\pi : V \setminus \{0\} \longrightarrow \mathbb{P}(V).$$

Para o caso especial $\mathbb{P}(V) = \mathbb{P}^n = \mathbb{P}^n_k$, usamos a notação

$$(x_0 : \ldots : x_n) := \pi((x_0, \ldots, x_n)),$$

e chamamos $(x_0 : \ldots : x_n)$ de **coordenada homogêneas** do ponto $P = \pi((x_0, \ldots, x_n)) \in \mathbb{P}^n_k$. Os pontos estão bem definidos a menos de multiplicação por escalar. Veremos que poderemos calculá-las mais a frente.

No exemplo acima, vimos que $\mathbb{P}^2_{\mathbb{R}}$ se decompõe em uma união de um conjunto afim e outro projetivo. De fato, qualquer espaço projetivo pode ser decomposto dessa forma, em um subespaço afim e um subespaço projetivo de dimensão menor. Para $\mathbb{P}^n_k$ tal decomposição é dada definindo

$$U_l := \{(x_0 : \ldots : x_n) \in \mathbb{P}^n_k \mid x_l \neq 0\},$$
$$H_l := \{(x_0 : \ldots : x_n) \in \mathbb{P}^n_k \mid x_l = 0\}.$$

O espaço H_l pode ser identificado com $\mathbb{P}^{n-1}_k$, e U_l pode ser identificado com $\mathbb{A}^n_k$, por exemplo, pelos mapas mutuamente inversos

$$\begin{aligned} i_l : \quad & \mathbb{A}^n_k \longrightarrow U_l, \\ & (x_1, \ldots, x_n) \longmapsto (x_1 : \ldots : x_{l-1} : 1 : x_l : \ldots : x_n), \end{aligned}$$

e

$$\begin{aligned} j_l : \quad & U_l \longrightarrow \mathbb{A}^n_k, \\ (x_0 : \ldots : x_{l-1} : x_l : \ldots : x_n) & \longmapsto \Big(\frac{x_0}{x_l}, \ldots, \frac{x_{l-1}}{x_l}, \frac{x_l + 1}{x_l}, \ldots, \frac{x_n}{x_l}\Big). \end{aligned}$$

Temos a decomposição

$$\mathbb{P}_k^n = U_l \cup H_l = \mathbb{A}_k^n \cup \mathbb{P}_k^{n-1}.$$

De modo geral fixamos o valor de l (usualmente $l = 0$ ou $l = n$), e nos referimos a U_l como **a parte afim de** $\mathbb{P}_k^n$ e a H_l como o **hiperplano no infinito**. Pontos em H_l são chamados de "pontos no infinito". Enquanto essa decomposição particular em um espaço afim e um projetivo é convencional, qualquer hiperplano projetivo pode ser tomado em $\mathbb{P}_k^n$, e seu complemento será sempre um espaço afim.

Definição 3.4. *Um* ***subespaço projetivo*** *de* $\mathbb{P}(V)$ *é um subespaço da forma* $\pi(W \setminus \{0\})$, *onde* $W \subset V$ *é um subespaço linear e* π *é o mapa da classe de resíduos. Escrevemos* $\mathbb{P}(W) \subset \mathbb{P}(V)$.

Um subespaço projetivo é naturalmente um espaço projetivo. Se $\dim W = \dim V - 1$, então chamamos $\mathbb{P}(W)$ de um **hiperplano** em $\mathbb{P}(V)$. Espaços projetivos de dimensão 1 e 2 são chamados de **retas projetivas** e **planos projetivos**.

Lema 3.5. *Seja* $\mathbb{P}(W_1)$ *e* $\mathbb{P}(W_2)$ *subespaços projetivos de um espaço projetivo n-dimensional* $\mathbb{P}(V)$. *Se* $\dim \mathbb{P}(W_1) + \dim \mathbb{P}(W_2) \geq n$, *então* $\mathbb{P}(W_1)$ *e* $\mathbb{P}(W_2)$ *se intersectam, i.e.,* $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) \neq \emptyset$.

Prova. Temos que $\dim W_1 + \dim W_2 \geq n + 2 = \dim V + 1$ então W_1 e W_2 se intersectam em pelo menos uma reta. □

Em particular, duas retas no plano projetivo sempre se intersectam em contraste com a situação no plano afim, onde duas retas podem ser paralelas. No caso projetivo a distinção entre retas paralelas e retas não paralelas não existe.

Qualquer espaço projetivo tem uma cobertura por espaços afins

$$\mathbb{P}_k^n = U_0 \cup U_1 \cup \ldots \cup U_n,$$

onde

$$U_i := \{(x_0 : \ldots : x_n) \in \mathbb{P}_k^n \mid x_i \neq 0\}.$$

3.2 VARIEDADES PROJETIVAS

Queremos considerar agora o conjunto dos zeros em um espaço projetivo de equações polinomiais definidas em $\mathbb{P}_k^n$. Já que as coordenadas homogêneas de um ponto $P = (x_0 : \ldots : x_n) \in \mathbb{P}_k^n$ são unicamente determinadas a menos da multiplicação por um escalar, devemos fazer a restrição a **polinômios homogêneos**. Um polinômio

$$f(x_0, \ldots, x_n) = \sum a_{\nu_o \ldots \nu_n} x_0^{\nu_0} \ldots x_n^{\nu_n}$$

é chamado de **homogêneo de grau** d se todos os monômios têm o mesmo grau $d = \nu_0 + \ldots + \nu_n$. Usaremos também a palavra **forma** para nos referirmos a polinômios homogêneos, e.g., formas lineares, formas quadráticas, formas cúbicas, etc. Se f é homogêneo de grau d, temos

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Em particular os **zeros** de f são

$$V(f) := \{(x_0 : \ldots : x_n) \in \mathbb{P}_k^n \mid f(x_0, \ldots, x_n) = 0\} \subset \mathbb{P}_k^n,$$

estão bem definidos.

Definição 3.6. *Uma **variedade projetiva** é um subconjunto $V \subset \mathbb{P}_k^n$ para o qual existe um conjunto de polinômios homogêneos $T \subset k[x_0, \ldots, x_n]$ com*

$$V = \{P \in \mathbb{P}_k^n \mid f(P) = 0 \text{ para todo } f \in T\}.$$

Como no caso afim, podemos assumir que T tem um número finito de elementos. Agora daremos alguns exemplos de variedades projetivas.

Exemplo 3.7. Já vimos a subvariedade projetiva de $\mathbb{P}_k^n$ dada pelo hiperplano no infinito,

$$H_n = \{(x_0 : x_1 : \ldots : x_n) \in \mathbb{P}_k^n \mid x_n = 0\}$$

Exemplo 3.8. As curvas a seguir são exibidas em (1) página 12,

$$C_1 = \{(x : y : z) \in \mathbb{P}_{\mathbb{C}}^2 \mid y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3\}$$

e

$$C_2 = \{(x : y : z) \in \mathbb{P}_{\mathbb{C}}^2 \mid y^2 z = x(x - z)(x - \lambda z)\}.$$

Essas curvas foram descritas considerando equações afins em duas variáveis, aqui elas foram homogenizadas. O processo de obter equações projetivas é chamado de **homogenização**, na prática multiplica-se cada termo por uma nova variável adequada de modo que todos os termos da equação tenham o mesmo grau.

Exemplo 3.9. Considere o mapa

$$\begin{aligned} \varphi : \quad \mathbb{P}_k^1 &\longrightarrow \mathbb{P}_k^3, \\ \varphi(t_0 : t_1) &= (t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3). \end{aligned}$$

A imagem $C := \varphi(\mathbb{P}_k^1)$ é uma variedade projetiva, dada por

$$C = \left\{ (x_0 : x_1 : x_2 : x_3) \in \mathbb{P}_k^3 \;\middle|\; \text{posto} \begin{pmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix} \leq 1 \right\}.$$

Isto significa que C é a interseção de três quádricas

$$C = Q_1 \cap Q_2 \cap Q_3,$$

onde

$$\begin{aligned} Q_1 &:= \{(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3_k \mid x_0x_2 - x_1^2 = 0\}, \\ Q_2 &:= \{(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3_k \mid x_0x_3 - x_1x_2 = 0\}, \\ Q_3 &:= \{(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3_k \mid x_1x_3 - x_2^2 = 0\}. \end{aligned}$$

A curva C não pode ser definida por somente duas equações quadráticas. Por outro lado, temos

$$C = Q_1 \cap F,$$

onde

$$F := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2_k \mid x_0x_3^2 - 2x_1x_2x_3 + x_2^3 = 0\},$$

ou seja, a quádrica Q_1 e a cúbica F se encontram ao longo da curva C. A curva C é chamada de **curva racional normal de grau 3**.

Exemplo 3.10. A imagem do mapa

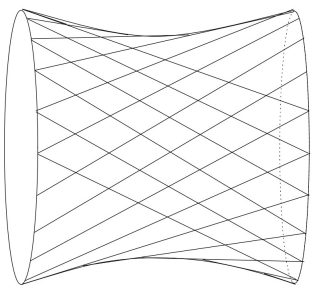
$$\begin{aligned} \varphi : \quad & \mathbb{P}^1_k \times \mathbb{P}^1_k \longrightarrow \mathbb{P}^3_k, \\ & \varphi((x_0 : x_1), (y_0 : y_1)) = (x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1), \end{aligned}$$

é dada pela quádrica

$$Q := \{(z_0 : z_1; z_2 : z_3) \in \mathbb{P}^3_k \mid z_0z_3 - z_1z_2 = 0\}.$$

Existem duas famílias de retas em Q, uma é dada pela família de retas de $\varphi(\mathbb{P}^1_k \times \{P\})$, e a outra pela família de retas de $\varphi(\{P\} \times \mathbb{P}^1_k)$, onde em cada caso o ponto P segue pelos pontos de $\mathbb{P}^1_k$. Cada uma dessas famílias de retas é chamada de **decisão** [1] **de Q**. Quaisquer duas retas em uma mesma decisão são disjuntas, e quaisquer duas retas em decisões diferentes se intersectam.

Figura 12 – Quádrica em $\mathbb{P}^3$ com suas decisões.



Fonte: Ver (1) página 68. (2000)

[1] Do inglês "ruling".

3.2.1 Anéis graduados e ideais homogêneos

Introduziremos agora o conceito de anel graduado e vamos aplicá-lo à variedades projetivas.

Definição 3.11. *Um **anel graduado**[2] é um anel S junto com um decomposição em grupos abelianos*

$$S = \bigoplus_{d \geq 0} S_d$$

tal que para $d \neq e$ temos

$$S_d \cap S_e = \{0\},$$

e tal que a multiplicação entre elementos de S_d e S_e implica que

$$S_d \cdot S_e \subset S_{d+e}.$$

*Os elementos de S_d são chamados de **homogêneos de grau d**.*

Exemplo 3.12. Um exemplo anel graduado é o de polinômios homogêneos

$$S = k[x_0, \ldots, x_n] = \bigoplus_{d \geq 0} k^d[x_0, \ldots, x_n],$$

onde

$$k^d[x_0, \ldots, x_n] = \{f \in k[x_0, \ldots, x_n] \mid f \text{ é homogêneo de grau d}\} \cup \{0\}.$$

Definição 3.13. *Um **ideal homogêneo I** em um anel graduado S é um ideal que satisfaz*

$$I = \bigoplus_{d \geq 0} (I \cap S_d).$$

Um ideal I é homogêneo se, e somente se, todo elemento $f \in I$ tem uma decomposição única

$$f = f_0 + \ldots + f_N,$$

onde $f \neq 0$, os d_i são distintos e os f_i são não nulos.

Lema 3.14. *Para um ideal I em um anel graduado S, temos:*

(1) *O ideal I é homogêneo se, e somente se, pode ser gerado por elementos homogêneos;*

(2) *Se I é homogêneo, então I é primo se, e somente se, para cada par de elementos homogêneos $f, g \in S$ temos:*

$$fg \in I \iff f \in I \text{ ou } g \in I;$$

[2] Para um estudo mais profundo sobre anéis graduados ver (9).

(3) *A soma, produto, interseção e radical de ideais homogêneos são também ideais homogêneos.*

Definimos uma variedade projetiva como o conjunto de zeros de um sistema de polinômios homogêneos, poderíamos também, de forma equivalente, ter definido uma variedade projetiva como o conjunto de zeros de um ideal homogêneo, ou um número finito de ideais homogêneos: se T é um conjunto de polinômios homogêneos e $I(T)$ é o ideal homogêneo gerado por T, então temos

$$V(T) = V(I(T)) = V(f_1, \ldots, f_k)$$

para geradores homogêneos $f_1, \ldots, f_k$ de $I(T)$. O próximo resultado mostra que para espaços afins o conjunto dos zeros projetivos define uma topologia em $\mathbb{P}^n_k$.

Lema 3.15. *Variedades projetivas satisfazem o axioma de conjuntos fechados de uma topologia em $\mathbb{P}^n_k$, i.e., satisfazem as seguintes condições:*

(1) *A união de um número finito de variedades projetivas ainda é uma variedade projetiva;*

(2) *A interseção de qualquer número de variedades projetivas é uma variedade projetiva;*

(3) *O conjunto vazio e $\mathbb{P}^n_k$ são variedades projetivas.*

Essa topologia é chamada de **topologia de Zariski em** $\mathbb{P}^n_k$. Assim como no caso afim, podemos decompor variedades projetivas em componentes irredutíveis. Tendo definido a topologia em uma variedade projetiva podemos fazer a seguinte definição:

Definição 3.16. *Uma **variedade quasi-projetiva** é um subconjunto aberto de uma variedade projetiva.*

Exploraremos agora a relação entre variedades projetivas e ideais homogêneos. Similarmente ao caso afim, temos as correspondências

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{ideais homogêneos}\\ I \subset k[x_0, \ldots, x_n]\end{array}\right\} & \longrightarrow & \left\{\begin{array}{c}\text{variedades projetivas}\\ V \subset \mathbb{P}^n_k\end{array}\right\}, \\ I & \longmapsto & V(I), \end{array}$$

e

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{variedades projetivas}\\ V \subset \mathbb{P}^n_k\end{array}\right\} & \longrightarrow & \left\{\begin{array}{c}\text{ideais homogêneos}\\ I \subset k[x_0, \ldots, x_n]\end{array}\right\}, \\ V & \longmapsto & I(V), \end{array}$$

com

$$V(I) := \left\{ (x_0, \ldots, x_n) \in \mathbb{P}_k^n \;\middle|\; \begin{array}{c} f(x_0, \ldots, x_n) = 0 \\ \text{para } f \in I,\ f \text{ homogêneo} \end{array} \right\}$$

e

$$I(V) := \begin{array}{l} \text{ideal gerado por polinômios} \\ \text{homogêneos } f \text{ com } f|_V = 0. \end{array}$$

No caso afim vimos que os mapas correspondentes I e V são mutuamente inversos se fizermos uma restrição a ideais radicais. Para que possamos fazer uma versão projetiva do Nullstellensatz precisamos considerar o seguinte: assim como no caso afim, temos $V((1)) = \emptyset$, por outro lado, existe outro ideal homogêneo

$$m = (x_0, \ldots, x_n) = \bigoplus_{d \geq 1} k^d[x_0, \ldots, x_n],$$

tal que $V(m) = \emptyset$.

Definição 3.17. *O ideal m é chamado de **ideal irrelevante**.*

Note que se I é um ideal homogêneo, podemos considerar não somente o conjunto de zeros projetivo $V = V(I) \subset \mathbb{P}_k^n$, mas também o conjunto de zeros afim, $V^a = V(I) \subset \mathbb{A}_k^{n+1}$. Geometricamente, se $I \neq k[x_1, \ldots, x_n]$ temos

$$V^a = \pi^{-1}(V) \cup \{0\},$$

onde como antes, π é o mapa classe de resíduos

$$\pi : \mathbb{A}_k^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_k^n.$$

Em particular, temos

$$(x_0, \ldots, x_n) \in V^a \iff (\lambda x_0, \ldots, \lambda x_n) \in V^a \text{ para } \lambda \in k^*.$$

Definição 3.18. *O conjunto V^a é chamado de **cone afim** sobre a variedade projetiva $V(I) \subset \mathbb{P}_k^n$.*

Teorema 3.19 (Nullstellensatz Projetivo.)**.** *Seja k um corpo algebricamente fechado. Então para um ideal homogêneo J temos as seguintes afirmações:*

(1) $V(J) = \emptyset \iff \sqrt{J} \supset (x_0, \ldots, x_n)$.

(2) *Se $V(J) \neq \emptyset$ então $I(V(J)) = \sqrt{J}$.*

Prova. (1) Temos

$$V(J) = \emptyset \iff V^a(J) \subset \{0\} \iff \sqrt{J} \supset (x_0, \ldots, x_n),$$

onde a segunda equivalência segue do Nullstellensatz afim.

(2) Suponha que $V(J) \neq \emptyset$. Então

$$\begin{aligned} f \in I(V(J)) &\iff f \in I(V^a(J)) \\ &\iff \exists\, n \geq 1,\ f^n \in J \iff f \in \sqrt{J}, \end{aligned}$$

aplicando o Nullstellensatz afim de novo. Aqui usamos o seguinte: se $f = \sum f_i$ é um polinômio com componentes homogêneas f_i, então $f(\lambda x_0, \ldots, \lambda x_n) = 0$ para todo λ se, e somente se, $f_i(x_0, \ldots, x_n) = 0$ para todo i.

Corolário 3.19.1. *Os mapas $J \longmapsto V(J)$ e $V \longmapsto I(V)$ nos dão as bijeções*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{ideais radicais homogêneos} \\ J \subsetneq k[x_0, \ldots, x_n] \end{array} \right\} & \overset{1:1}{\longleftrightarrow} & \left\{ \begin{array}{c} \textit{variedades projetivas} \\ V \subset \mathbb{P}^n_k \end{array} \right\}, \\ \cup & & \cup \\ \left\{ \begin{array}{c} \textit{ideais primos homogêneos} \\ J \subsetneq k[x_0, \ldots, x_n] \end{array} \right\} & \overset{1:1}{\longleftrightarrow} & \left\{ \begin{array}{c} \textit{variedades projetivas} \\ \textit{irredutíveis } V \subset \mathbb{P}^n_k \end{array} \right\} \end{array}$$

Aqui o ideal irrelevante m corresponde ao conjunto vazio.

Prova. Resta mostrar que V é irredutível se, e somente se, $I(V)$ é primo. Utilizando o Lema 3.14 item (2), a prova se torna análoga à prova da Proposição 2.20. □

Retornamos agora à cobertura finita de $\mathbb{P}^n_k$ por conjuntos afins

$$\mathbb{P}^n_k \ = \ U_0 \cap \ldots \cap U_n, \tag{3.1}$$

onde

$$U_i := \{(x_0 : \ldots : x_n) \in \mathbb{P}^n_k \mid x_i \neq 0\}.$$

Para cada conjunto aberto U_i temos a bijeção

$$\begin{aligned} j_i : \qquad U_i &\longrightarrow \mathbb{A}^n_k, \\ (x_0 : \ldots : x_i : \ldots x_n) &\longmapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right). \end{aligned}$$

A topologia de Zariski em $\mathbb{P}^n_k$ induz uma topologia em U_i, e $\mathbb{A}^n_k$ é equipado com a topologia de Zariski introduzida anteriormente.

Proposição 3.20. *O mapa $j_i : U_i \longrightarrow \mathbb{A}^n_k$ é um* ***homeomorfismo.***

Prova. Por simplicidade tomamos $i = 0$. Devemos mostrar que j_0 e j_0^{-1} são ambos contínuos, i.e., que j_0^{-1} e j_0 levam conjuntos fechados em conjuntos fechados.

Os conjuntos fechados de U_i e $\mathbb{A}^n_k$ são definidos por polinômios nos seguintes anéis

$$S^h := \{f \in k[x_0, \ldots, x_n] \mid f \text{ é homogêneo}\},$$
$$A := k[x_1, \ldots, x_n].$$

Existem mapas entre esses anéis dados por

$$\alpha : \qquad S^h \longrightarrow A,$$
$$\alpha(f) := f(1, x_1, \ldots, x_n),$$

e

$$\beta : \qquad A \longrightarrow S^h,$$
$$\beta(g) := x_0^{\deg g} g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$$

que satisfazem $\alpha \circ \beta(g) = g$.
Qualquer conjunto fechado de U_o tem a forma $X = \bar{X} \cap U_o$, onde $\bar{X} \subset \mathbb{P}^n_k$ é o fecho de X em $\mathbb{P}^n_k$. Já que $\bar{X}$ é uma variedade projetiva, existe um subconjunto $T \subset S^h$ com $\bar{X} = V(T)$, e $j_0(X) = V(\alpha(T))$.

Qualquer subconjunto fechado de $\mathbb{A}^n_k$ tem a forma $W = V(T')$ para um subconjunto $T' \subset A$, e $j_0^{-1}(W) = V(\beta(T')) \cap U_0$.

Logo j_0 e j_0^{-1} levam subconjuntos fechados em subconjuntos fechados do seguinte modo:

$$V(T) \cap U_0 \xrightarrow{j_0} V(\alpha(T)),$$
$$V(\beta(T')) \cap U_0 \xleftarrow{j_0^{-1}} V(T').$$

Portanto j_0 é um homeomorfismo. □

Qualquer variedade projetiva $X \subset \mathbb{P}^n_k$ tem uma cobertura

$$X = X_0 \cup \ldots \cup X_n, \qquad X_i := X \cap U_i. \tag{3.2}$$

Pelos j_i podemos identificar U_i com $\mathbb{A}^n_k$, então os X_i podem ser tomados como variedades afins. Essa cobertura é chamada de **cobertura afim padrão de** X. O próximo resultado segue imediatamente da prova da Proposição 3.20.

Corolário 3.20.1. *O mapa $X \mapsto X_0 = X \cap U_0$ define uma bijeção*

$$\left\{ \begin{array}{c} \textit{variedades projetivas irredutíveis} \\ X \subset \mathbb{P}^n_k \textit{ com } X \not\subset \{x_0 = 0\} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \textit{variedades afins} \\ \textit{irredutíveis } X_0 \subset \mathbb{A}^n_k \end{array} \right\}$$

O inverso deste mapa é dado tomando o fecho de Zariski.

O corolário acima implica que podemos considerar tanto variedades afins e variedades quasi-afins como variedades quasi-projetivas.

Exemplo 3.21. Retornamos a uma curva já vista anteriormente, dada por

$$\{(x_1, x_2) \in \mathbb{A}_k^2 \mid x_2^2 - x_1(x_1 - 1)(x_1 - \lambda) = 0\} \subset \mathbb{A}_k^2 \cong U_0 \subset \mathbb{P}_k^2.$$

Definimos $f(x_1, x_2) := x_2^2 - x_1(x_1 - 1)(x_1 - \lambda)$, de onde segue

$$\beta(f) = x_0 x_2^2 - x_1(x_1 - x_0)(x_1 - \lambda x_0),$$

onde β é o mapa definido na Proposição 3.20. Logo, o fecho de Zariski C_0 em $\mathbb{P}_k^2$ é dado por

$$\bar{C_0} = \{(x_0 : x_1 : x_2) \in \mathbb{P}_k^2 \mid x_0 x_2^2 - x_1(x_1 - x_0)(x_1 - \lambda x_0) = 0\}.$$

Seja $H_0 := V(x_0) = \mathbb{P}_k^n \setminus U_0$. Temos

$$\bar{C_0} \cap H_0 = \{(0 : 0 : 1)\},$$

e então nesse caso $\bar{C_0}$ é obtido de C_0 adicionando um único ponto no infinito.

3.3 FUNÇÕES RACIONAIS E MORFISMOS

O objetivo agora é definir funções em variedades projetivas $V \subset \mathbb{P}_k^n$. Embora polinômios homogêneos não determinem funções bem definidas em $\mathbb{P}_k^n$, se f e g são ambos polinômios homogêneos de grau d, o quociente

$$\frac{f(\lambda x_0, \ldots, \lambda x_n)}{g(\lambda x_0, \ldots, \lambda x_n)} = \frac{\lambda^d f(x_0, \ldots, x_n)}{\lambda^d f(x_0, \ldots, x_n)} = \frac{f(x_0, \ldots, x_n)}{g(x_0, \ldots, x_n)},$$

é uma função bem definida em V. Logo para uma variedade projetiva irredutível V definimos

$$k(V) := \left\{ \frac{f}{g} \;\middle|\; \begin{array}{c} f, g \in k[x_0, \ldots, x_n] \text{ homogêneos} \\ \deg f = \deg g,\ g \notin I(V) \end{array} \right\} \Big/ \sim,$$

onde

$$\frac{f}{g} \sim \frac{f'}{g'} \iff fg' - gf' \in I(V).$$

Pode-se verificar que $k(V)$ é um corpo.

Definição 3.22. *$k(V)$ é chamado de **corpo de funções de** V. Os elementos de $k(V)$ são chamados de **funções racionais.***

Lema 3.23. *Para uma variedade projetiva irredutível V com cobertura afim padrão $V = V_0 \cap \ldots \cap V_n$ como visto anteriormente, se $V \not\subset V(x_0)$ então temos um isomorfismo de corpos de funções afins e projetivos, $k(V) \cong k(V_0)$.*

Prova. Temos os seguintes mapas que são mutuamente inversos:

$$\begin{aligned} k(V) &\longrightarrow k(V_0), \\ \frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)} &\longmapsto \frac{f(1,x_1,\ldots,x_n)}{g(1,x_1,\ldots,x_n)}, \end{aligned}$$

e

$$\begin{aligned} k(V_0) &\longrightarrow k(V), \\ \frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} &\longmapsto \frac{f\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)}{g\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)}. \end{aligned}$$

□

O corpo de funções $k(V)$ também pode ser definido por **localização**[3] do anel de coordenadas, que definiremos agora como um anel graduado. Se $V \subset \mathbb{P}_k^n$ é um variedade irredutível com cone afim $V^a \subset \mathbb{A}_k^{n+1}$, então o anel

$$S(V) := k[V^a] := k[x_0,\ldots,x_n]/I(V)$$

é equipado com a estrutura de anel graduado,

$$S(V) = \bigoplus_{d\geq 0} S_d(V),$$

onde

$$S_d(V) := \{\bar{f} \in S(V) \mid f \text{ é homogêneo com } \deg f = d\} \cup \{0\}.$$

Para mostrar que $S_d(V) \cap S_e(V) = \{0\}$ para $e \neq d$, note que se $\bar{f} = \bar{g}$ então $f - g \in I(V)$, então se $\deg f \neq \deg g$, como $I(V)$ é homogêneo, temos que $f, g \in I(V)$, e $\bar{f} = \bar{g} = 0$.

Definição 3.24. *$S(V)$ é o anel de coordenada homogêneo de V.*

3.3.1 Localização de anéis graduados

Já definimos a localização de um anel arbitrário, agora para aplicar no contexto projetivo precisamos entender o que significa **localização de anéis graduados.** Seja $S = \bigoplus_{d\geq 0} S_d$ um anel graduado arbitrário, seja $T \subset S$ um sistema multiplicativo fechado de elementos homogêneos. Com o objetivo de dar ao anel local S_T a estrutura de anel graduado tomamos elementos $f \in S$ e $g \in T$ e definimos f/g sendo homogêneo com grau

$$\deg \frac{f}{g} := \deg f - \deg g.$$

[3] Ver (8) capítulo 11. para um estudo mais aprofundado.

Isto está bem definido já que se $f/g = f'/g'$, existe por definição $h \in S$ tal que $h(fg'-gf') = 0$, i.e., $hfg' = hf'g$. Logo

$$\deg h + \deg f + \deg g' = \deg h + \deg f' + \deg g,$$

e dessa forma vemos que o grau $\deg(f/g)$ está bem definido.

Definição 3.25. *Para qualquer sistema multiplicativo fechado $T \subset S$ de um anel graduado S definimos*

$$S_{(T)} := \left\{ \frac{f}{g} \in S_T \;\middle|\; \frac{f}{g} \text{ é homogêneo de grau } 0 \right\}.$$

Para um ideal primo homogêneo $\mathfrak{p} \subset S$, o conjunto

$$T_{\mathfrak{p}} := \{f \in S \mid f \text{ é homogêneo, } f \notin \mathfrak{p}\}$$

é um sistema multiplicativo fechado, definimos

$$S_{(\mathfrak{p})} := S_{(T_{\mathfrak{p}})}.$$

Se S é um domínio de integridade, então para um elemento homogêneo não nulo $f \in S$, o conjunto

$$T_f := \{f^n \mid n \geq 0\}$$

é multiplicativamente fechado, e definimos

$$S_{(f)} := S_{(T_f)}.$$

Retornando agora às variedades projetivas $V \subset \mathbb{P}^n_k$.

Lema 3.26. *Existe um isomorfismo de anéis graduados*

$$k(V) \cong S(V)_{((0))}.$$

Prova. Segue imediatamente da definição de $k(V)$. □

3.3.2 Funções regulares

Vamos agora discutir funções regulares em subconjuntos abertos de V. Ao contrário do caso afim, o anel de coordenada homogêneo não corresponde às funções regulares em V, já que seus elementos não são funções em V. Veremos adiante que toda função regular em uma variedade projetiva irredutível V é constante.

Definição 3.27. *Uma função racional $f \in k(V)$ é chamada de **regular em** P se existe uma representação $f = f/h$ com $h(P) \neq 0$.*

Definição 3.28. *O* ***domínio de definição, dom*** (f) ***,****de* $f \in k(V)$ *é o conjunto de todos os pontos onde* f *é regular.*

Assim como no caso afim, dom (f) é um conjunto não vazio e aberto de V.

Definição 3.29. *O* ***anel local de*** V *em um ponto* $P \in V$ *é definido como*

$$\mathcal{O}_{V,P} := \{f \in k(V) \mid f \text{ é regular em } P\}.$$

Definição 3.30. *O* ***ideal maximal de*** V *em um ponto* $P \in V$ *é definido como*

$$m_{V,P} := \{f \in \mathcal{O}_{V,P} \mid f(P) = 0\} \subset \mathcal{O}_{V,P}.$$

Observação 3.31. *De fato,* $m_{V,P}$ *é o único ideal maximal, já que todo elemento* $g \in \mathcal{O}_{V,P}$ *com* $g(P) \neq 0$ *é uma unidade. Logo* $\mathcal{O}_{V,P}$ *é um anel local.*

Se V é uma variedade irredutível com $V \not\subset V(x_0)$, então para cada ponto $P \in V_0 = V \cap U_0$ temos dois anéis locais $O_{V_0,P}$ e $O_{V,P}$, dependendo de como interpretamos P, podemos vê-lo como um ponto na variedade projetiva V ou na variedade afim V_0. O isomorfismo dado no Lema 3.23 induz outro isomorfismo

$$\mathcal{O}_{V,P} \cong \mathcal{O}_{V_0,P}.$$

Para $P \in V$ podemos considerar o seguinte ideal maximal

$$M_P := \{f \in S(V) \mid f(P) = 0\} \subset S(V).$$

Lema 3.32.

$$\mathcal{O}_{V,P} \cong S(V)_{(M_P)}$$

Prova. Segue imediatamente das definições anteriores. □

Definição 3.33. *Para uma variedade quasi-projetiva dada por um subconjunto aberto* $U \subset V$*, o* ***anel de funções regulares*** *em* U *é definido por*

$$\mathcal{O}(U) := \{f \in k(V) \mid U \subset \textit{dom}\,(f)\}.$$

Observação 3.34. *Considerando* $\mathcal{O}(U)$ *como um subconjunto de* $k(V)$*, temos*

$$\mathcal{O}(U) = \bigcap_{P \in U} \mathcal{O}_{V,P}.$$

Teorema 3.35. *Se* V *é uma variedade projetiva irredutível definida sobre um corpo algebricamente fechado* k*, então toda função regular em* V *é constante, i.e.,* $\mathcal{O}(V) \cong k$*.*

Para dar uma prova algébrica precisamos introduzir o conceito de módulo Noetheriano. Seja R um anel com unidade.

Definição 3.36. *Um* ***módulo sobre R*** *(ou R-módulo) é um grupo abeliano M junto com um mapa de multiplicação*

$$\begin{aligned} R \times M &\longrightarrow M, \\ (r, m) &\longmapsto rm, \end{aligned}$$

tal que as seguintes afirmações são válidas

(1) $r(m_1 + m_2) = rm_1 + rm_2$,

(2) $(r_1 + r_2)m = r_1m + r_2m$,

(3) $(r_1r_2)m = r_1(r_2m)$,

(4) $1m = m$.

Definição 3.37. *Um R-módulo M é* ***finitamente gerado*** *se existem um número finito de elementos $m_1, \ldots, m_n$ com*

$$M = Rm_1 + \ldots + Rm_k.$$

Definição 3.38. *Um R-módulo M é* ***Noetheriano*** *se todos os submódulos $U \subset M$ são finitamente gerados.*

Lema 3.39. *Se R é um anel Noetheriano e M é um R-módulo finitamente gerado, então M é um módulo Noetheriano.*

Prova. Suponha que $M = Rm_1 + \ldots + Rm_k$. Então existe um homomorfismo sobrejetivo

$$\begin{aligned} \varphi : R^k &\longrightarrow M, \\ e_i &\longmapsto m_i \qquad \text{para } 1 \leq i \leq k, \end{aligned}$$

onde $e_i, 1 \leq i \leq k$, é uma base para R^k, com $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, i.e., todas as componentes são 0 exceto uma na i-ésima coordenada que assume o valor de 1. Se U é um submódulo de M, então $\varphi^{-1}(U)$ é um submódulo de R^k, logo é suficiente mostrar o resultado para R^k.

Provaremos o resultado utilizando indução sobre k. Se $k = 1$, então um submódulo de $M \cong R$ é isomorfo a um ideal de R, o resultado segue da hipótese de que R é um anel Noetheriano. Agora tome $U \subset R^k$ com $k \geq 2$. As primeiras componentes dos vetores em U geram o ideal I em R,

$$I := (u_1 \mid (u_1, \ldots, u_k) \in U).$$

Já que R é Noetheriano, este ideal é finitamente gerado, então existem elementos $u^{(i)} \in U$, $1 \leq i \leq l$, com primeiras componentes $u_1^{(i)}$, tal que

$$I = (u_1^{(1)}, \ldots, u_1^{(l)}).$$

Logo para $u \in U$ existem elementos $r_1, \ldots, r_l \in R$ tal que

$$u - r_1 u^{(1)} - \ldots - r_l u^{(l)} = (0, u_2^*, \ldots, u_k^*).$$

Agora seja $R^{k-1} \subset R^k$ o submódulo de elementos R^k com primeira componente 0, e considere o submódulo

$$U' := U \cap R^{k-1}.$$

Por indução U' é finitamente gerado por elementos $v_1, \ldots, v_m$. Logo $u^{(1)}, \ldots, u^{(l)}, v_1, \ldots, v_m$ geram U. □

Agora estamos prontos para fazer a prova do Teorema 3.35.

Prova (do Teorema 3.35)**.** Seja V uma variedade projetiva irredutível em $\mathbb{P}_k^n$. Podemos assumir que V não está contida em um hiperplano $H_i := V(x_i)$, caso contrário $V \subset H_i \cong \mathbb{P}_k^{n-1}$, e podemos substituir $\mathbb{P}_k^n$ por $\mathbb{P}_k^{n-1}$.

Seja $f \in \mathcal{O}(V)$. Nosso objetivo é mostrar que $f \in k$. Considere a cobertura afim

$$V = V_0 \cup \ldots V_n.$$

Já que f é regular em V, a restrição $f|_{V_i}$ é regular em V_i. Utilizando o isomorfismo $k(V) \cong (V_i)$, dado na prova do Lema 3.23, e o item (2) do Teorema 2.50, temos que $f|_{V_i}$ é um polinômio em x_j/x_i, $1 \leq j \neq i \leq n$. Então, para $1 \leq i \leq n$, podemos escrever

$$f|_{V_i} = \frac{g_i}{x_i^{N_i}}, \qquad \text{onde } g_i \in S(V) \text{ é homogêneo de grau } N_i. \tag{3.3}$$

Como V é irredutível, $I(V)$ é um ideal primo. Isto implica que $S(V) = k[x_0, \ldots, x_n]/I(V)$ é um domínio de integridade, e dessa forma podemos considerar o corpo de frações

$$L := \text{Quot } S(v) = k(V^a),$$

onde V^a é cone afim sobre V. Os anéis $\mathcal{O}(V), k(V)$ e $S(V)$ estão contidos em L. Por (3.3) temos

$$x_i^{N_i} \ f \in S_{N_i}(V), \tag{3.4}$$

onde $S_d(V)$ denota a parte homogênea de grau d do anel graduado $S(V)$. Agora tome um inteiro $N \geq \sum N_i$. Então $S_N(V)$ é um espaço vetorial de dimensão finita, gerado pelos monômios de grau N. Todo monômio m em $S_N(V)$ é divisível por $x_i^{N_i}$ para algum i, por (3.4) temos que $mf \in S_N(V)$, então

$$S_N(V)f \subset S_N(V).$$

Isto mostra que para $q \geq 1$ temos uma sequência de inclusões,

$$S_N(V)f^q \subset S_N(V)f^{q-1} \subset \ldots \subset S_N(V)f \subset S_N(V).$$

Em particular, que

$$x_0^N f^q \in S_N(V) \qquad \text{para todo } q \geq 1.$$

Logo,

$$S(V)[f] \subset x_o^{-N} S(V) \subset L.$$

Já que $x_0^{-N}S(V)$ é um $S(V)$-módulo finitamente gerado, o Lema 3.39 implica que $x_0^{-N}S(V)$ é Noetheriano, e o submódulo $S(V)[f]$ é também finitamente gerado sobre $S(V)$. Pelo Lema 1 item (2) f é integral sobre $S(V)$, e portanto satisfaz uma equação da forma

$$f^m + a_{m-1}f^{m-1} + \ldots + a_1 f + a_0 = 0 \qquad (a_i \in S(V)).$$

Já que f é homogêneo de grau 0, podemos assumir o mesmo para os a_i, podemos considerar também a componente de grau 0 dos a_i. Portanto $a_i \in S_0(v) = k$. Logo f é algébrico sobre k, já que estamos assumindo que $k = \bar{k}$, segue que $f \in k$. □

3.3.3 Mapas racionais

Definição 3.40. *Seja V uma variedade projetiva irredutível.*

(1) *Um mapa racional $f : V \dashrightarrow \mathbb{A}_k^m$ é uma m-upla $f = (f_1, \ldots, f_m)$ de funções racionais $f_1, \ldots, f_m \in k(V)$. O **domínio de definição** de f é dado por*

$$dom\,(f) := \bigcap_{i=1}^{m} dom\,(f_i).$$

Neste conjunto f é bem definida, com $f(P) = (f_1(P), \ldots, f_m(P))$.

(2) *Um **mapa racional** $f : V \dashrightarrow W \subset \mathbb{A}_k^m$ é dado por um mapa racional $f : V \dashrightarrow \mathbb{A}_k^m$ com $f(dom\,(f)) \subset W$.*

Seja V uma variedade algébrica irredutível.

Definição 3.41. *Um mapa racional $f : V \dashrightarrow \mathbb{P}_k^m$ em V é dado por*

$$f(P) = (f_0(P) : \ldots : f_m(P))$$

para funções racionais $f_0, \ldots, f_m \in k(V)$.

Note que se $0 \neq g \in k(V)$, então $(f_0, \ldots, f_m)$ e $(gf_0, \ldots, gf_m)$ definem o mesmo mapa racional.

Definição 3.42. *Um mapa racional $f : V \dashrightarrow \mathbb{P}_k^m$ é **regular** em um ponto P se existe uma representação $f = (f_0 : \ldots : f_m)$ tal que:*

(1) *Para $1 \leq i \leq m$ a função f_i é regular em P.*

(2) *Existe algum i tal que $f_i(P) \neq 0$.*

Definição 3.43. *Um mapa racional $f : V \dashrightarrow W \subset \mathbb{P}_k^m$ é um mapa racional $f : V \dashrightarrow \mathbb{P}_k^m$ com $f(dom\,(f)) \subset W$.*

Definição 3.44. *Sejam V_1 e V_2 variedades projetivas ou afins e irredutíveis contendo subconjuntos abertos U_1 e U_2, respectivamente.*

(1) *Um **morfismo** $f : U_1 \longrightarrow U_2$ é um mapa racional $f : V_1 \dashrightarrow V_2$ com $U_1 \subset dom\,(f)$ e $f(U_1) \subset U_2$.*

(2) *Um morfismo $f : U_1 \longrightarrow U_2$ é um **isomorfismo** se existe um morfismo $g : U_2 \longrightarrow U_1$ com $g \circ f = id_{U_1}$ e $f \circ g = id_{U_2}$.*

Essa definição nos permite falar de morfismos de variedades quasi-projetivas e isomorfismos entre variedades quasi-projetivas.

Exemplo 3.45. Considere a **curva racional normal de grau n**, parametrizada pelo mapa

$$\begin{aligned} \varphi : \quad & \mathbb{P}_k^1 \to \mathbb{P}_k^n, \\ & \varphi(t_0 : t_1) = (t_0^n : t_0^{n-1}t_1 : \ldots : t_1^n). \end{aligned}$$

Já que podemos escrever

$$\varphi(t_0 : t_1) = \left(\left(\frac{t_0}{t_1}\right)^n : \left(\frac{t_0}{t_1}\right)^{n-1} : \ldots : 1\right) = \left(1 : \ldots : \left(\frac{t_1}{t_0}\right)^n\right),$$

o mapa φ é racional e regular em todo lugar.

Retornamos à cobertura afim de $\mathbb{P}_k^n$. Lembremos que temos os mapas

$$\begin{aligned} i_l : \quad & \mathbb{A}_k^n \longrightarrow U_l = \{(x_0 : \ldots : x_n) \mid x_l \neq 0\} \subset \mathbb{P}_k^n, \\ & (x_1, \ldots, x_n) \longmapsto (x_1 : \ldots : x_{l-1} : x_l : \ldots : x_n), \end{aligned}$$

$$\begin{aligned} j_l : \quad & U_l \longrightarrow \mathbb{A}_k^n \\ (x_0 : \ldots : x_{l-1} : x_l : \ldots : x_n) & \longmapsto \left(\frac{x_0}{x_l}, \ldots, \frac{x_{l-1}}{x_l}, \frac{x_{l+1}}{x_l}, \ldots, \frac{x_n}{x_l}\right). \end{aligned}$$

Vimos na Proposição 3.20 que j_l é um homeomorfismo.

Proposição 3.46. *$j_l : U_l \longrightarrow \mathbb{A}_k^n$ é um isomorfismo.*

Prova. Pode-se ver que os mapas i_l e j_l são inversos um do outro. □

3.3.4 Mapas birracionais

Sejam V e W variedades quasi-projetivas irredutíveis.

Definição 3.47. *Um mapa racional $f : V \dashrightarrow W$ é chamado de **birracional** (ou uma equivalência birracional) se existe um mapa racional $g : W \dashrightarrow V$ com $f \circ g = id_W$ e $g \circ f = id_V$.*

Definição 3.48. *Duas variedades V e W são ditas **birracionalmente equivalentes** se existe uma equivalência birracional $f : V \dashrightarrow W$.*

Teorema 3.49. *Para um mapa racional $f : V \dashrightarrow W$ as seguintes afirmações são equivalentes:*

(1) *f é birracional.*

(2) *f é dominante e $f^* : k(W) \longrightarrow k(V)$ é um isomorfismo.*

(3) *Existem conjuntos abertos $V_0 \subset V$ e $W_o \subset W$ tais que a restrição $f|_{V_0} : V_0 \longrightarrow W_0$ é um isomorfismo.*

Prova. A equivalência entre (1) e (2) é provada do mesmo jeito que no Teorema 2.63.

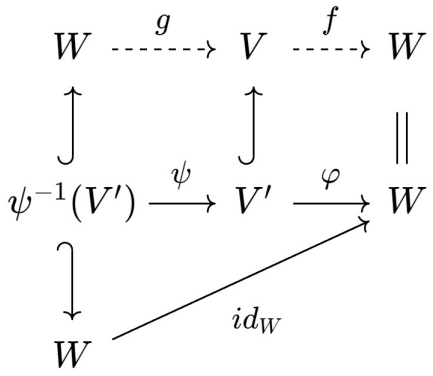
Para mostrar que (3) $\implies$ (1), é necessário notar que $f|_{V_0} : V_0 \longrightarrow W_0$ tem inversa $g : W_0 \longrightarrow V_0$, e por definição $g : W \dashrightarrow V$ é um mapa racional. Então $g \circ f : V \dashrightarrow V$ e $f \circ g : W \dashrightarrow W$ são mapas racionais que são os mapas identidade em V_0 e W_0 respectivamente. Já que V_0 e W_0 são densos, segue que $g \circ f = id_V$ e $f \circ g = id_W$.

Resta mostrar que (1) $\implies$ (3). Seja $g : W \dashrightarrow V$ um mapa racional inverso de f. Definimos $V' := \text{dom } (f)$ e $W' = \text{dom } (g)$. Então $\varphi := f|_{V'} : V' \longrightarrow W$ e $\psi := g|_{W'} : W' \to V$ são morfismos. Já que temos uma igualdade de mapas racionais, $f \circ g = id_W$, temos

$$\varphi(\psi(P)) = P, \qquad \text{para todo } P \in \psi^{-1}(V'). \tag{3.5}$$

Portanto temos o seguinte diagrama comutativo:

Figura 13 – Diagrama.



Fonte: Ver (1) página 84.
(2000)

Seja $V_0 := \varphi^{-1}(\psi^{-1}(V'))$ e $W_0 := \psi^{-1}(\varphi^{-1}(W'))$. Se $Q \in V_0$, então $\varphi(Q) \in \varphi^{-1}(V')$, por (3.5) temos $\varphi(\psi(\varphi(Q))) = \varphi(Q)$. Logo, $\varphi(Q) \in W'$ e $\varphi(Q) \in \psi^{-1}(\varphi^{-1}(W')) = W_0$. Assim, o mapa $\varphi : V_0 \longrightarrow W_0$ é um morfismo. De modo similar, $\psi : W_0 \longrightarrow V_0$ é um morfismo. Pode-se ver que φ e ψ são inversos um do outro. □

Na linguagem de categorias pode-se reformular o teorema anterior da seguinte forma:

Corolário 3.49.1. *Existe uma equivalência contravariante entre a categoria das variedades quasi-afins irredutíveis com mapas racionais dominantes como morfismos, e a categoria de extensões finitas de corpos de k e k-homomorfismos, dada por*

$$V \longmapsto k(V),$$
$$(f : V \dashrightarrow W) \longmapsto (f^* : k(W) \longrightarrow k(V)).$$

Proposição 3.50. *Toda variedade quasi-projetiva irredutível é birracionalmente equivalente a uma hipersuperfície afim.*

Prova. Ver (1) página 85.

Definição 3.51. *Uma variedade quasi-projetiva V é chamada de **racional** se V é birracionalmente equivalente a $\mathbb{A}^n_k$ (ou equivalentemente, a $\mathbb{P}^n_k$).*

Proposição 3.52. *As seguintes afirmações são equivalentes.*

(1) *V é racional.*

(2) *$k(V) \cong k(x_1, \ldots, x_n)$.*

(3) *Existem conjuntos abertos isomorfos $V_0 \subset V$ e $U_0 \subset \mathbb{A}^n_k$.*

Prova. Segue do Teorema 3.49. □

Exemplo 3.53. O mapa

$$\begin{aligned} f : \mathbb{A}^1_k &\longrightarrow C := \{(x,y) \in \mathbb{A}^2_k \mid y^2 - x^3 = 0\}, \\ t &\longmapsto (t^2, t^3), \end{aligned}$$

é um mapa birracional, mas não um isomorfismo. A restrição

$$f_0 := f|_{\mathbb{A}^1_k \setminus \{0\}} \ : \ \mathbb{A}^1_k \setminus \{0\} \longrightarrow C \setminus \{0\}$$

é um isomorfismo de conjuntos abertos de Zariski.

Exemplo 3.54. Um mapa birracional de $\mathbb{P}^2_k$ para $\mathbb{P}^2_k$ é chamado de transformação de Cremona. Um exemplo é dado pelo mapa

$$\begin{aligned} \varphi \qquad & \mathbb{P}^2_k \dashrightarrow \mathbb{P}^2_k, \\ \varphi(x_0 : x_1 : x_2) &= (x_1x_2 : x_0x_2 : x_0x_1) \\ &= \left(\frac{1}{x_0} : \frac{1}{x_1} : \frac{1}{x_2}\right), \end{aligned}$$

que é birracional, com $\varphi = \varphi^{-1}$. O mapa φ não é definido nos pontos $(1:0:0), (0:1:0)$ e $(0:0:1)$, e transforma as três retas $V(x_i)$ em pontos.

3.3.5 Produto de variedades projetivas

Definição 3.55. *Definimos o* ***mapa de Segre*** *como*

$$\begin{aligned} s_{n,m} : \qquad & \mathbb{P}^n_k \times \mathbb{P}^m_k \longrightarrow \mathbb{P}^N_k \\ ((x_0 : \ldots : x_n), (y_0, \ldots, y_m)) &\mapsto (x_0y_0 : \ldots x_iy_j : \ldots : x_ny_m), \end{aligned}$$

onde $N = (n+1)(m+1) - 1$ *e* $0 \leq i \leq n,\ 0 \leq j \leq m$. *Este mapa é bem definido, e a imagem*

$$\sum n, m := s_{n,m}(\mathbb{P}^n_k \times \mathbb{P}^n_k),$$

é chamada de ***variedade de Segre****.*

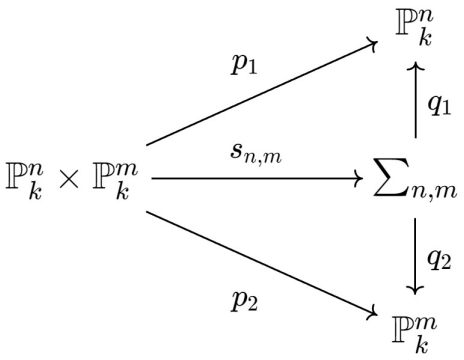
Lema 3.56. *O mapa de Segre* $s_{n,m} : \mathbb{P}^n_k \times \mathbb{P}^m_k \longrightarrow \sum_{n,m}$ *é bijetivo e a imagem* $\sum_{n,m}$ *é uma variedade projetiva em* $\mathbb{P}^N_k$.

Prova. Ver (1) página 88.

Lema 3.57. *A variedade de Segre* $\sum n, m$ *é irredutível.*

Prova. As projeções $\mathbb{P}_k^n \times \mathbb{P}_k^m$ para $\mathbb{P}_k^n$ e para $\mathbb{P}_k^m$ formam um diagrama comutativo

Figura 14 – Diagrama.



Fonte: Ver (1) página 89.
(2000)

Onde $p_1 = q_1 \circ s_{n,m}$ e $p_2 = q_2 \circ s_{n,m}$, além disso, q_1 e q_2 existem pela propriedade universal do produto. A prova do Lema 3.56 mostra que q_1 e q_2 são morfismos. Para quaisquer pontos $P \in \mathbb{P}_k^n$ e $Q \in \mathbb{P}_k^m$ temos as seguintes restrições de $s_{n,m}$:

$$s_{n,m}^Q : \mathbb{P}_k^n \times \{Q\} \longrightarrow \sum_{n,m},$$
$$s_{n,m}^P : \{P\} \times \mathbb{P}_k^m \longrightarrow \sum_{n,m}.$$

Estes mapas induzem isomorfismos entre $\mathbb{P}_k^n$ e $\mathbb{P}_k^m$ os subespaços projetivos de $\mathbb{P}_k^N$. Logo, via $s_{n,m}^P$ e $s_{n,m}^Q$, as fibras de q_1 e q_2 são variedades projetivas isomorfas a $\mathbb{P}_k^m$ e $\mathbb{P}_k^n$ respectivamente. Em particular, as fibras de q_1 e q_2 são irredutíveis. A irredutibilidade de $\sum_{n,m}$ pode ser mostrada do mesmo que foi feito na Proposição 4. □

Exemplo 3.58. Considere o mapa já visto anteriormente:

$$\begin{aligned} s_{1,1} : \quad & \mathbb{P}_k^1 \times \mathbb{P}_k^1 \longrightarrow \mathbb{P}_k^3 \\ & ((x_0 : x_1), (y_0 : y_1)) \mapsto (x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1). \end{aligned}$$

Neste caso a variedade de Segre $\sum_{1,1}$ é a quádrica $\sum_{1,1} = Q = V(z_{00}z_{11} - z_{01}z_{10})$.

Proposição 3.59. *Sejam V e W variedades projetivas. Então:*

(1) *O produto $V \times W$ também é uma variedade projetiva.*

(2) *Se V, W são irredutíveis, $V \times W$ também o é.*

Prova. Ver (1) página 90.

4 PONTOS SUAVES E DIMENSÃO

4.1 PONTOS SUAVES E SINGULARES

4.1.1 O espaço tangente de uma superfície em um ponto

Inicialmente, vamos considerar o caso no qual V é uma hipersuperfície afim irredutível, ou seja, tem a seguinte forma

$$V = V(f) = \{(x_1, \ldots, x_n) \in \mathbb{A}_k^n | f(x_1, \ldots, x_n) = 0\},$$

onde $f \in k[x_1, \ldots, x_n]$ é um polinômio não constante irredutível.

Definição 4.1. *Seja $P = (a_1, \ldots, a_n) \in V$. O **espaço tangente** da hipersuperfície V no ponto P é definido como*

$$T_P V := \left\{ (x_1, \ldots, x_n) \in \mathbb{A}_k^n \Big| \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)(x_1 - a_i) = 0 \right\},$$

onde $\dfrac{\partial f}{\partial x_i}$ é a derivada formal de f com respeito a x_i.

O espaço $T_P(V)$ é um subespaço afim de $\mathbb{A}_k^n$ tal que $P \in T_P V$. Na literatura, frequentemente, o espaço tangente de V em P é munido com a estrutura adicional de espaço vetorial com a origem em P.

Lema 4.2. *Seja $L \subset \mathbb{A}_k^n$ uma reta afim que passa pelo ponto P. Então P é raiz múltipla de $f|_L$ se, e somente se, $L \subset T_P V$.*

Prova. A reta L tem uma parametrização

$$L : x_i = a_i + b_i t$$

onde $P = (a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$ é um vetor na direção de L. Seja $g := f|_L$, i.e.,

$$g(t) = f(a_1 + b_1 t, \ldots, a_n + b_n t),$$

como $P = (a_1, \ldots, a_n) \in V$. Temos,

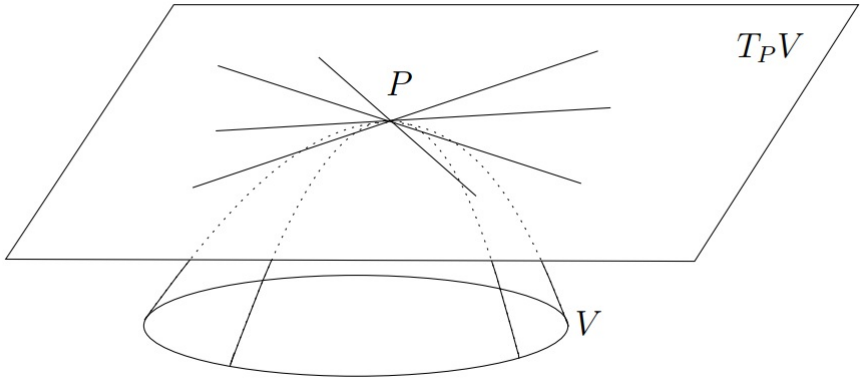
$$g(0) = f(P) = 0.$$

Logo g tem raiz múltipla no 0 se, e somente se,

$$\frac{\partial g}{\partial t}(0) = 0 \iff \sum_{i=1}^{n} b_i \frac{\partial f}{\partial x_i}(P) = 0 \iff L \subset T_P V$$

onde a última equivalência segue diretamente da equação para $T_P V$. □

Figura 15 – O espaço tangente da
variedade V no ponto P.



Fonte: Ver (1) página 98. (2000)

Definição 4.3. *P é chamado de **ponto suave** (ou regular) da hipersuperfície V se existe algum índice i, tal que $\dfrac{\partial f}{\partial x_i}(P) \neq 0$. Caso contrário, P é chamado de **ponto singular** (ou singularidade) de V.*

A definição anterior nos dá a seguinte caracterização de pontos suaves e singulares em hipersuperfícies:

$$P \text{ é um ponto suave de } V \iff T_PV \text{ é hiperplano afim.}$$
$$P \text{ é um ponto singular de } V \iff T_PV = \mathbb{A}^n_k.$$

O próximo resultado mostra que pontos singulares são especiais, no sentido que, de modo geral, os pontos de uma variedade são suaves.

Proposição 4.4. *Para uma hipersuperfície afim $V \subset \mathbb{A}^n_k$ o conjunto*

$$V_{suave} := \{P \in V |\ P \text{ é um ponto suave de } V\ \}$$

é aberto e denso em V.

Prova. O conjunto $V_{\text{singular}} = V \setminus V_{\text{suave}}$ é dado por

$$V_{\text{singular}} = V\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \subset \mathbb{A}^n_k$$

Logo esse conjunto é fechado e V_{suave} é aberto. Como estamos assumindo que V é irredutível, para mostrar que V_{suave} é denso temos que mostrar que $V_{\text{singular}} \neq V$. Se $V_{\text{singular}} = V$, então todas as derivadas $\partial f/\partial x_i$ se anulam em V, i.e., $\partial f/\partial x_i \in (f)$. Já que o grau de $\partial f/\partial x_i$ é menor que o grau de f, temos que $\partial f/\partial x_i = 0$. Nesse caso, se char $(k) = 0$, f é

constante, uma contradição. Se char $(k) = p > 0$, segue que f é constante ou um polinômio da forma x_i^p (ver o apêndice C). Mas como assumimos que o corpo k é algebricamente fechado, isso implica que $f = g^p$, contradizendo a irredutibilidade de f. □

4.1.2 O conceito de dimensão, pontos suaves e regulares de superfícies afins irredutíveis

Tendo definido pontos singulares e suaves para hipersuperfícies, nos voltamos para o caso de uma variedade arbitrária $V \subset \mathbb{A}_k^n$. Para um polinômio $f \in k[x_1, \ldots, x_n]$ e um ponto $P = (a_1, \ldots, a_n)$, a **parte linear de** f em $P = (a_1, \ldots, a_n)$ é definida como

$$f_P^{(1)} := \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)(x_i - a_i).$$

Definição 4.5. *O **espaço tangente** de uma variedade irredutível V em um ponto $P \in V$ é definido como a seguinte interseção de hiperplanos:*

$$T_P V := \bigcap_{f \in I(V)} V\left(f_P^{(1)}\right) \subset \mathbb{A}_k^n.$$

Isso é um subespaço afim de $\mathbb{A}_k^n$ contendo P. Se V é uma hipersuperfície então essa definição se resume à definição inicial de espaço tangente (Definição 4.1).

Definição 4.6. *Para uma variedade irredutível V, definimos a **dimensão** de V por*

$$dim\ V = min\ \{dim\ T_P V | P \in V\}$$

Com essa definição temos que $\dim T_P V \geq \dim V$ para todo $P \in V$. A seguir mostraremos que de fato $\dim V$ é igual a dimensão do espaço tangente $\dim T_P V$ para um ponto geral de V.

Proposição 4.7. *A função $V \to \mathbb{N}$, $P \mapsto dim\ T_P V$, é superiormente semicontínua na topologia de Zariski, i.e., para todo $r \in \mathbb{N}$ o conjunto*

$$S_r(V) := \{P \in V | dim\ T_P V \geq r\} \tag{4.1}$$

é fechado

Prova. Suponha que $g_1, \ldots, g_m$ gere o ideal $I(V)$. Então para cada $f \in I(V)$ a parte linear $f_P^{(1)}$ pode ser escrita como uma combinação linear de $g_{i,P}^{(1)}$, logo

$$T_P V = \bigcap_{i=1}^{m} V\left(g_{i,p}^{(1)}\right)) \subset \mathbb{A}_k^n.$$

Temos

$$\dim T_P V = n - \text{posto}\left(\frac{\partial g_i}{\partial x_j}(P)\right)_{ij}, \tag{4.2}$$

então

$$P \in S_r(V) \iff \text{posto}\left(\frac{\partial g_i}{\partial x_j}(P)\right)_{ij} \leq n - r.$$

Onde a última desigualdade acontece se todos os $(n - r + 1) \times (n - r + 1)$ menores[1] de

[1] Ver "menor", no contexto de álgebra linear.

$\left(\dfrac{\partial g_i}{\partial x_j}(P)\right)_{ij}$ se anulam. Como são equações polinomiais, segue que $S_r(V)$ é fechado. □

Proposição 4.8. *Seja $V \subset \mathbb{A}_k^n$ uma variedade afim irredutível. Então existe subconjunto aberto e denso $V_0 \subset V$ tal que $\dim T_P V = \dim V$ para todo $P \in V_0$.*

Prova. Seja $r = \dim(V)$. Pela definição de dimensão, com a notação usada em (4.1), temos $S_r(V) = V$ e $S_{r+1}(V) \neq V$. Como $S_{r+1}(V)$ é fechado, podemos tomar $V_0 := V \setminus S_{r+1}(V)$, que é aberto e não vazio. □

Definição 4.9. *Para uma variedade afim irredutível V, um ponto $P \in V$ é um ponto **suave** (regular) de V se $\dim T_P V = \dim V$, caso contrário o ponto é dito **singular**.*

Para uma hipersuperfície $V(f) \subset \mathbb{A}_k^n$, isso é equivalente à Definição 4.3, já que temos

$$\frac{\partial f}{\partial x_i}(P) \neq 0 \text{ para algum } i \iff \operatorname{posto}\left(\frac{\partial f}{\partial x_i}(P)\right)_i = 1.$$

Por (5.2) isso também mostra que a hipersuperfície V em $\mathbb{A}_k^n$ tem dimensão $\dim V = n - 1$.

Definição 4.10. *A **codimensão** de uma variedade afim V em $\mathbb{A}_k^n$ é definida por*

$$\textit{codim } V = n - \dim V.$$

Observação 4.11. *Suponha que $V \subset \mathbb{A}_k^n$ é definida por r polinômios $f_1, \ldots, f_r$. Pela equação (4.2) e pela Proposição 4.8, a codimensão é dada pelo posto da matriz $(\partial f_i/\partial x_j)_{ij}$ em um ponto suave P, e então $\operatorname{codim} V \leq r$. Então para definir uma variedade afim irredutível de codimensão r é necessário pelo menos r equações. Esse é também o caso se V for redutível.*

4.1.3 Variedades afins arbitrárias

Agora vamos considerar o caso de uma variedade afim arbitrária V com uma decomposição em componentes irredutíveis

$$V = V_1 \cup \cdots \cup V_l.$$

Definição 4.12. *Um ponto $P \in V$ é um ponto **suave** (regular) de V se*

(1) *P está exatamente em uma componente irredutível V_i de V, e*

(2) *P é suave em V_i.*

Definição 4.13. *A **dimensão** de V é definida como o máximo da dimensão das componentes irredutíveis V_i.*

4.2 CARACTERIZAÇÃO ALGÉBRICA DE DIMENSÃO

Vamos mostrar que a dimensão de uma variedade é igual ao grau de transcendência do seu corpo de funções. No caso de uma hipersuperfície irredutível $V \subset \mathbb{A}_k^n$ podemos ver isso da seguinte maneira, se f é uma equação irredutível para V, então o anel de coordenadas de V é dado por $k[V] = k[x_1, \ldots, x_n]/(f)$. Depois de uma possível renumeração, podemos assumir que f contém a variável x_1. Então

$$k(V) = k(x_2, \ldots, x_n)[x_1]/(f),$$

i.e, $x_2, \ldots, x_n$ forma uma base transcendente para $k(V)$. Temos então

$$\text{tr } deg_k\, k(V) = n - 1 = \dim V.$$

Vamos mostrar que essa igualdade é válida para variedades algébricas em geral e o primeiro passo é dar uma definição mais algébrica do espaço tangente.

A seguir, o espaço tangente T_PV é considerado como espaço vetorial com origem em P. Na Definição 4.5, o espaço tangente T_PV foi dado a partir de equações explícitas. Vamos dar uma caracterização intrínseca do espaço tangente em termos do ideal maximal m_P no anel local $\mathcal{O}_{V,P}$. Isso nos permite ver que os conceitos de "regular"e "singular" não dependem da imersão de uma variedade afim em $\mathbb{A}_k^n$. Lembremos que m_P pode ser construído do seguinte modo. O ideal maximal de P em $\mathbb{A}_k^n$ é dado por

$$M_P = \{f \in k[x_1, \ldots, x_n] | f(P) = 0\} \subset k[x_1, \ldots, x_n]. \tag{4.3}$$

Isso nos dá um ideal maximal no quociente,

$$\bar{M}_P = M_P/I(V) \subset k[V],$$

e a localização nos da o ideal maximal m_P em $\mathcal{O}_{V,P}$,

$$m_P = \left\{ \frac{f}{g} \in k(V) \middle| f(P) = 0,\ g(P) \neq 0 \right\} \subset \mathcal{O}_{V,P} \subset k(V).$$

Teorema 4.14. *Existe um isomorfismo de espaços vetoriais*

$$T_PV \cong (m_P/m_P^2)^* := Hom_k(m_P/m_P^2, k),$$

que é natural, no sentido de não depender da escolha de base.

Prova. Por simplicidade, vamos assumir que P está na origem, $(0, \ldots, 0)$, então $M_P = (x_1, \ldots, x_n)$, o que sempre pode ser feito através de uma translação. Seja $(k^n)^*$ o espaço dual de k^n. As coordenadas $x_1, \ldots, x_n$ são formas lineares de k^n, podemos considerá-las como uma base de $(k^n)^*$. Para todo $f \in k[x_1, \ldots, x_n]$ temos a função linear

$$f_P^{(1)} = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(0) x_i \in (k^n)^*,$$

logo obtemos o mapa linear

$$d : M_P \to (k^n)^*,$$
$$f \mapsto f_P^{(1)}.$$

Esse mapa é sobrejetivo já que $d(x_i) = x_i$, e os x_i formam uma base para $(k^n)^*$. O núcleo é M_P^2, já que para $f(P) \in M_P$ temos $f_P^{(1)} = 0$ se, e somente se, todos os termos de f tem ordem ao menos 2, i.e., $f \in M_P^2$. Então d induz um isomorfismo

$$M_P/M_P^2 \cong (k^n)^*.$$

Agora seja $V \subset \mathbb{A}_k^n$ uma variedade afim. A inclusão $T_PV \subset k^n$ corresponde a uma sobrejeção

$$(k^n)^* \to (T_PV)^*,$$

dada pela restrição de formas lineares de k^n em T_PV. Então a composição

$$D : M_P/M_P^2 \to (k^n)^* \to (T_PV)^*$$

também é sobrejetiva. Afirmamos que

$$\ker\,(D) = M_P^2 + I(V), \tag{4.4}$$

o que pode ser visto pelas seguintes equivalências

$$\begin{aligned} f \in \ker D &\iff f_P^{(1)}|_{T_P(V)} = 0 \\ &\iff f_P^{(1)} = \sum a_i g_{i,P}^{(1)} \text{ para algum } g_i \in I(V), a_i \in k \\ &\iff f - \sum a_i g_i \in M_P^2 \text{ para algum } g_i \in I(V), a_i \in k \\ &\iff f \in M_P^2 + I(V). \end{aligned}$$

Onde a igualdade (4.4) implica que

$$\bar{M}_P/\bar{M}_P^2 \cong M_P/(M_P^2 + I(V)) \cong (T_PV)^*,$$

portanto para completar a prova é necessário mostrar que

$$\bar{M}_P/\bar{M}_P^2 \cong m_P/m_P^2, \tag{4.5}$$

e o resultado vai seguir por dualidade. Para mostrar (4.5), note que a inclusão $\bar{M}_P \subset m_P$ induz uma bijeção

$$\varphi : \bar{M}_P/\bar{M}_p^2 \to m_P/m_P^2.$$

Para ver que φ é sobrejetiva, tome $f/g \in m_P$. Então $c := g(0) \neq 0$ e

$$\frac{f}{c} - \frac{f}{g} = f\Big(\frac{1}{c} - \frac{1}{g}\Big) \in m_P^2,$$

logo $\varphi(f/c) = (\overline{f/g}) \in m_P/m_P^2$. □

Corolário 4.14.1. *O espaço tangente T_PV depende somente de uma vizinhança de P em V, i.e., se $f : V \dashrightarrow W$ é um mapa birracional que leva uma vizinhança de V_0 de P isomorficamente a uma vizinhança de W_0 em $Q = f(P)$, então existe um isomorfismo $T_PV \cong T_PW$.*

Prova. Já que $f : V \dashrightarrow W$ é birracional e $f(P) = Q$, nós temos um isomorfismo

$$f^* : k(W) = k(W_0) \to k(V) = k(V_0),$$

que leva funções regulares em Q em funções regulares em funções regulares em P. Claramente as funções que se anulam em P se anulam também em Q, e então m_Q é levado em m_P. Logo f^* induz um isomorfismo

$$\begin{array}{rccc} \bar{f}^* : & m_Q/m_Q^2 & \longrightarrow & m_P/m_P^2 \\ & || & & || \\ & (T_QW)^* & & (T_PV)^* \end{array}$$

□

Corolário 4.14.2. *Se V e W são variedades birracionalmente equivalentes, então* $\dim V = \dim W$.

Definição 4.15. *Se $f : V \to W$ é um isomorfismo com $f(P) = Q$, então dualizando o mapa $\bar{f}^* : m_Q/m_Q^2 \to m_P/m_P^2$ nos dá um homomorfismo*

$$df(P) : T_PV \longrightarrow T_QW,$$

*chamado de **diferencial** de f em P.*

Teorema 4.16. *Se V é uma variedade afim irredutível, então* $\dim V = tr\, deg_k\, k(V)$

Prova. Pela Proposição 3.50, V é birracionalmente equivalente a uma hipersuperfície, o que pelo Corolário 4.2 tem a mesma dimensão de V e é isomorfa ao corpo de funções (Teorema 3.49). Portanto o resultado segue da prova para hipersuperfícies que foi dada no começo da seção. □

Podemos agora generalizar a Proposição 4.4.

Corolário 4.16.1. *Para toda variedade afim V, o conjunto dos pontos suaves é um subconjunto aberto e denso de V.*

Prova. Isso pode ser inferido diretamente da Proposição 4.8 e pela definição de ponto regular, ou podemos reduzir ao caso de uma hipersuperfície e aplicar o Corolário 4.14.1.

4.2.1 Variedades quasi-projetivas

Podemos considerar agora o caso de variedades quasi-projetivas.

Definição 4.17. *Seja V uma variedade quasi-projetiva. Um ponto $P \in V$ é dito um ponto* ***suave*** *(ou regular) de V se existe uma vizinhança afim $U \subset V$ de P tal que P é um ponto suave de U.*

Prova. Segue imediatamente do Corolário 4.14.1 que isso é válido para todas as vizinhanças afins contendo P. Nesse caso o conjunto dos pontos suaves é um subconjunto aberto e denso.

A dimensão de uma variedade quasi-projetiva é definida da seguinte forma.

Definição 4.18. *Suponha que V é uma variedade projetiva irredutível em $\mathbb{P}^n_k$, com cobertura afim $V = V_0 \cup \cdots \cup V_n$. Podemos assumir que V não está contida em nenhum hiperplano $H_i \subset \mathbb{P}^n_k$. Segue então que todos os V_i tem a mesma dimensão, e chamamos isso de dimensão de V.*

Se V for redutível, como no caso afim definimos a dimensão de V como sendo o máximo da dimensão de suas componentes.

4.2.2 Dimensão de Krull

Vamos agora discutir numa nova maneira de definir dimensão e pontos suaves. Como qualquer variedade é birracionalmente equivalente ao uma variedade afim (Proposição 3.50), a partir de agora V é sempre uma variedade afim irredutível. Foi visto anteriormente que V é um espaço topológico Noetheriano, ou seja, toda cadeia

$$V = V_0 \supsetneq V_1 \supsetneq V_2 \cdots \supsetneq V_l \neq \emptyset \tag{4.6}$$

de conjuntos fechados irredutíveis tem comprimento finito l.

Definição 4.19. *A* ***Dimensão de Krull*** *de V, denotada por kr dim(V), é o supremo dos comprimentos de todas as cadeias descendentes da forma* (4.6) *acima.*

Definição 4.20. *Seja A um anel.*

(1) *A* ***altura****, $ht(I)$, de um ideal primo I é o supremo sobre os comprimentos l de todas as cadeias de ideais primos das forma*

$$I_0 \subsetneq I_1 \subsetneq I_2 \cdots \subsetneq I_l = I.$$

(2) *A* ***Dimensão de Krull de A****, denotada por dim A, é o supremo sobre as alturas $ht(I)$ de todos os ideais primos $I \neq A$.*

Tomando $I_i = I(V_i)$, uma cadeia descendente de ideais da forma 4.6 da origem a uma cadeia ascendente de ideias primos

$$\{0\} \subsetneq I_1 \subsetneq I_2 \cdots \subsetneq I_l \tag{4.7}$$

no anel de coordenadas $k[V] = k[x_1, \ldots, x_n]/I(V)$. Reciprocamente, uma cadeia da forma (4.7) da origem a uma cadeia da forma (4.6). Logo segue imediatamente que

$$\text{kr } dim(V) = dim\, k[V] \tag{4.8}$$

O fato de que a dimensão de Krull é a mesma que a maneira que foi definida anteriormente (Definição 4.6) vem de um teorema conhecido em álgebra comutativa:

Teorema 4.21. *Seja A um domínio de integridade que é uma k-álgebra finitamente gerada, e seja K o corpo de frações de A. Então*

$$dim\, A = tr\, deg_k\, A$$

Prova. Ver **[Ma]**(2) capítulo 5 seção 14.

Corolário 4.21.1. *Se V é uma variedade afim irredutível, então*

$$kr\, dim(V) = tr\, deg_k\, k(V) = dim\, V$$

Prova. Segue da equação (4.8), Teorema 4.21 e do Teorema 4.16.

O resultado a seguir mostra que a dimensão de uma variedade V também é igual a dimensão de Krull do anel local $\mathcal{O}_{V,P}$ no ponto $P \in V$.

Proposição 4.22. *Se V é uma variedade afim irredutível, então para todos os pontos $P \in V$ a seguinte igualdade é válida:*

$$dim\, \mathcal{O}_{V,P} = dim\, k[V].$$

Prova. Segue diretamente dos teoremas "going-up"e "going-down"de Cohen e Seidenberg. Para mais detalhes ver (3) Teorema 11.25.

Para discutir pontos singulares e suaves em termos das dimensão de Krull, vamos precisar de outro resultado de álgebra comutativa:

Proposição 4.23. *Seja A um anel local Noetheriano com ideal maximal m e corpo de resíduos $k = A/m$. Então*

$$dim_k\, (m/m^2) \geq dim\, A.$$

Prova. Ver (2) página 78.

A proposição anterior motiva a seguinte definição.

Definição 4.24. *Um anel Noetheriano local A com ideal maximal m é chamado de anel local regular se $dim_k\,(m/m^2) = dim\,A$.*

Corolário 4.24.1. *Um ponto $P \in V$ é suave se, e somente se, $\mathcal{O}_{V,P}$ é um anel regular.*

Prova. Pelo Teorema 4.14, P é suave se, somente se,

$$dim_k\,(m/m^2) = dim\,V.$$

Pela equação 2.1, pelo Corolário 4.21.1 e pela Proposição 4.22 temos que

$$dim\,V = dim\,k[V] = dim\,\mathcal{O}_{V,P}.$$

□

5 CURVAS CÚBICAS PLANAS

Neste capítulo, iremos classificar curvas cúbicas planas e mostrar que uma curva plana irredutível é racional se, e somente se, é singular. Consideraremos aqui k um corpo algebricamente fechado com característica diferente de 2 ou 3.

5.1 CURVAS PLANAS

Um polinômio homogêneo não nulo $f \in k^d[x_0, x_1, x_2]$ de grau d define uma variedade projetiva de dimensão dois

$$V(f) = \{(x_0 : x_1 : x_2) | f(x_0, x_1, x_2) = 0\} \subset \mathbb{P}^2_k$$

que vamos chamar de **curva plana**. Para $c \in k^*$ os polinômios f e cf definem a mesma curva. No entanto, ao contrário dos capítulos anteriores, queremos distinguir entre f e potências de f. Suponha que f tenha uma decomposição em fatores irredutíveis (que é única ao não ser por uma permutação e fatores constantes)

$$f = f_1^{d_1} \dots f_r^{d_r}.$$

Podemos escrever C como uma soma formal

$$C = d_1 C_1 + \dots + d_r C_r,$$

onde $C_i := V(f_i)$. As curvas C_i são chamadas de **componentes irredutíveis** de C. Se f não tem componentes repetidas, então isso corresponde a decomposição de $V(f)$ em componentes irredutíveis dado pela Proposição 2.22. Usamos a notação

$$C = \{f = 0\}$$

para denotar o conjunto das curvas C_i contadas com multiplicidade, e chamamos C de uma **curva plana de grau** d. Temos uma bijeção

$$\{\text{Curvas planas de grau } d\} \overset{1:1}{\longleftrightarrow} \mathbb{P}(k^d[x_0, x_1, x_2]).$$

Logo, o conjunto de curvas planas de grau d forma um espaço projetivo de dimensão $\binom{d+2}{2} - 1$. O espaço de retas, i.e., o espaço de retas projetivas de grau 1, é o **espaço projetivo dual** $(\mathbb{P}^2_k)^*$.

Se f não tem fatores repetidos, então por nossa definição anterior, um ponto $P \in C$ é singular se, e somente se,

$$f(P) = 0 \text{ e } \frac{\partial f}{\partial x_i}(P) = 0,\ i = 0, 1, 2.$$

A relação

$$d \cdot f = \sum x_i \frac{\partial f}{\partial x_i},$$

conhecida como fórmula de Euler, implica que se a característica de k é igual a 0 ou é positiva maior que d, então P é um ponto singular se, e somente se, $\dfrac{\partial f}{\partial x_i}(P) = 0$ para $i = 0, 1, 2$. Também vamos usar a definição de pontos singulares e suaves quando f tiver fatores repetidos. Note que em contraste com os capítulos anteriores (c.f Corolário 4.16.1), C pode não ter pontos suaves; por exemplo, esse é o caso quando $f = x_0^2$.

Para $P \in C$, definimos o **espaço tangente** de C em P como

$$T_P C := \left\{ (x_0 : x_1 : x_2) \in \mathbb{P}_k^2 \;\middle|\; \sum_{i=0}^{2} \frac{\partial f}{\partial x_i}(P) x_i = 0 \right\} \subset \mathbb{P}_k^2.$$

Esse é o **fecho projetivo** do espaço tangente afim definido anteriormente. Um ponto P em C é um ponto suave de C se, e somente se, $T_P C$ é uma reta.

Um mapa $A \in \mathrm{Gl}(3, k)$ leva retas através da origem em retas através da origem, e induz uma **transformação projetiva**

$$\varphi = \varphi_A : \mathbb{P}_k^2 \longrightarrow \mathbb{P}_k^2.$$

Dizemos que duas curvas C e C', com equações f e f' respectivamente, são **projetivamente equivalentes** se existe uma transformação de coordenadas $A \in \mathrm{Gl}(3, k)$ tal que a transformação correspondente de $\mathbb{P}(k[x_0, x_1, x_2])$ leva $\{f = 0\}$ em $\{f' = 0\}$.

Este capítulo é dedicado **à classificação de curvas planas de grau 3** (curvas cúbicas) a menos de uma equivalência projetiva. O primeiro passo é dado pelo lema a seguir.

Lema 5.1. *Seja C uma curva cúbica plana que é decomposta em três retas. Então C é projetivamente equivalente a uma das seguintes curvas:*

(1) $C = \{x_0 x_1 x_2 = 0\}$,

(2) $C = \{x_0 x_1 (x_0 + x_1) = 0\}$,

(3) $C = \{x_0^2 x_1 = 0\}$,

(4) $C = \{x_0^3 = 0\}$.

Prova. Assumindo que $C = l_1 \cup l_2 \cup l_3$, onde l_i são considerados como pontos do espaço dual $(\mathbb{P}_k^2)^*$. Temos os seguintes casos:

(1) As três retas l_i são diferentes e não se intersectam em um ponto comum. Isso é equivalente a afirmação de que os pontos $l_1, l_2, l_3 \in (\mathbb{P}_k^2)^*$ não se encontram em uma

reta. Vamos então usar a transitividade da ação de $\mathrm{Gl}(3,k)$ em $(\mathbb{P}^2_k)^*$. Explicitamente, as coordenadas desses pontos definem as linhas de uma matriz em $\mathrm{Gl}(3,k)$ que leva x_0, x_1, x_2 em l_1, l_2, l_3.

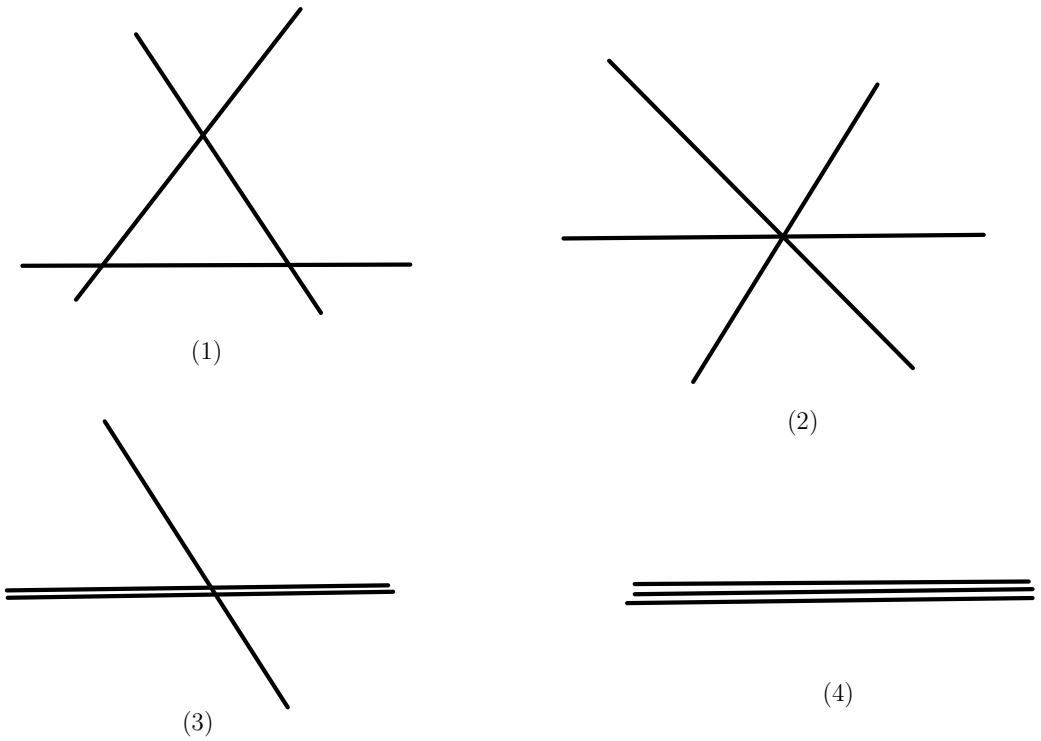
(2) As três retas são diferentes, e se intersectam em um ponto comum. Logo, existe uma reta nos distintos pontos $l_i \in (\mathbb{P}^2_k)^*$. Todos esse conjuntos são equivalentes sobre a ação de $(\mathbb{P}^2_k)^*$, já que $\mathrm{Gl}(3,k)$ age transitivamente em $(\mathbb{P}^2_k)^*$ e $\mathrm{Gl}(2,k)$ age 3-transitivamente em $(\mathbb{P}^1_k)^*$, i.e., quaisquer três pontos distintos são equivalentes sobre a ação de $\mathrm{Gl}(2,k)$.

(3) $l_1 = l_2 \neq l_3$. Um argumento similar a (2) nos dá (3).

(4) $l_1 = l_2 = l_3$. Isso nos dá o caso (4).

□

Figura 16 – Casos do Lema 5.1.



Fonte: elaborado pelo autor. (2023)

5.2 MULTIPLICIDADE DA INTERSEÇÃO

Nesta seção, C e C' são duas curvas planas definidas por polinômios f e g, respectivamente. Para começar, assumimos que C e C' não têm componentes em comum.

Definição 5.2. *A **multiplicidade da interseção** de C e C' em um ponto $P \in \mathbb{P}^2_k$ é definida como*

$$I_P(C, C') := \dim_k \mathcal{O}_{\mathbb{P}^2_k, P}/(f, g).$$

Lembremos que para uma variedade V e um ponto $P \in V$ temos:

$$\mathcal{O}_{V,P} = \{f \in k(V) | f \text{ é regular em } P\},$$

e o ideal maximal de V em $P \in V$ é definido como

$$m_{V,P} = \{f \in \mathcal{O}_{V,P} | f(P) = 0\} \subset \mathcal{O}_{V,P}.$$

Temos o seguinte lema:

Lema 5.3.

$$I_P(C, C') \geq 1 \iff P \in C \cap C'.$$

Prova. Se $P \notin C \cap C'$, então ou $P \notin C$, e f é uma unidade em $\mathcal{O}_{\mathbb{P}^2_k, P}$, ou $P \notin C'$, e g é uma unidade em $\mathcal{O}_{\mathbb{P}^2_k, P}$. Então $(f, g) = \mathcal{O}_{\mathbb{P}^2_k, P}$, i.e. $\dim \mathcal{O}_{\mathbb{P}^2_k, P}/(f, g) = 0$ e portanto menor do que 1.

Reciprocamente, se $P \in C \cap C'$ então $f, g \in m_P$, então $(f, g) \subset m_P$. Logo $(f, g) \subset m_P$. Portanto

$$\dim_k \mathcal{O}_{\mathbb{P}^2_k, P}/(f, g) \geq \dim_k \mathcal{O}_{\mathbb{P}^2_k, P}/m_P = 1.$$

□

Para uma reta $L \subset \mathbb{P}^2_k$ que passa por um ponto P de C temos

$$I_P(C, L) = \text{mult}_P(f|_L). \tag{5.1}$$

Para ver isso, primeiro faremos uma transformação linear tal que $P = (0 : 0 : 1)$ e L é dado por $x_1 = 0$. Então em termos de coordenadas afins $x = x_0/x_2$ e $y = x_1/x_2$ para o subespaço afim $\mathbb{A}^2_k$ de $\mathbb{P}^2_k$, onde $x_2 \neq 0$, a reta $L \cap \mathbb{A}^2_k$ é dada por $y = 0$, e temos

$$\begin{aligned} I_P(C, L) &= \dim_k \mathcal{O}_{\mathbb{P}^2_k, P}/(f, x_1) \\ &= \dim_k \mathcal{O}_{\mathbb{A}^2_k, 0}/(f(x, y, 1), y) \\ &= \text{mult}_P(f|_L). \end{aligned}$$

De (5.1) e do Lema 4.2 podemos ver que

$$I_P(C, L) \geq 2 \iff L \subset T_P C.$$

Definição 5.4. *As curvas C e C' se **intersectam transversalmente** em um ponto $P \in C \cap C'$ se C e C' são ambos suaves em P e as retas tangentes em P são distintas, i.e.,*

$$T_P C \cap T_P C' = \{P\}$$

O próximo lema é uma versão do Lema de Nakayama (Lema 2).

Lema 5.5. *Seja V uma variedade quasi-projetiva e seja $P \in V$. Se os elementos $f_1, \ldots, f_r \in m_P$ geram o k-espaço vetorial m_P/m_P^2, então eles também geram o ideal m_P.*

Prova. Como isso é uma afirmação local, e como uma variedade quasi-projetiva é coberta por conjuntos afins, podemos assumir que V é uma variedade afim em $\mathbb{A}_k^n$. Definimos $B := \mathcal{O}_{V,P}/(f_1, \ldots, f_r)$ e $A := m_P/(f_1, \ldots, f_r)$. Se $P = (a_1, \ldots, a_n)$ então a classe de resíduos de $x_1 - a_1, \ldots, x_n - a_n$ gera o módulo A sobre B. Logo A é uma B-álgebra, logo pelo Lema de Nakayama ou $A = 0$ ou $m_P A \neq A$. No entanto

$$m_P A = ((f_1, \ldots, f_r) + m_P^2)/(f_1, \ldots, f_r) = m_P/(f_1, \ldots, f_r) = A,$$

e logo devemos ter $A = 0$, i.e., $m_P = (f_1, \ldots, f_r)$. □

Lema 5.6. *Duas curvas C e C' se intersectam transversalmente em P se, e somente se, $I_P(C, C') = 1$.*

Prova. Podemos assumir que $P = (0 : 0 : 1)$, e trabalhar com as coordenadas afins x, y. Como $P \in C \cap C'$ nós temos $(f, g) \subset m_P$, portanto $I_P(C, C') = 1$ é equivalente a afirmação de que $(f, g) = m_P$. Logo, se $I_P(C, C') = 1$ então as partes lineares de f e g devem gerar o espaço vetorial de dimensão dois m_P/m_P^2. Em particular eles são linearmente independentes e as retas tangentes de C e C' em P são distintas. Agora de forma recíproca assuma que C e C' se intersectam transversalmente em P, depois de uma troca de coordenadas adequada as partes lineares de f e g são dadas por $f_P^{(1)} = x$ e $g_P^{(1)} = y$ respectivamente. Pode-se então aplicar o Lema 5.5, ou usar um argumento elementar, para mostrar que f e g geram o ideal m_P.

Se omitirmos a condição de que C e C' não têm componentes em comum, podemos definir a multiplicidade de interseção local $I_P(C, C')$, que assume o valor ∞ se P está sobre uma componente comum de C e C'.

Exemplo 5.7. Voltemos à parábola semicúbica C, dada em coordenadas projetivas por

$$z_0^2 z_2 - z_1^3 = 0,$$

ou em coordenadas locais em uma vizinhança de $P = (0 : 0 : 1)$ por

$$x^2 - y^3 = 0.$$

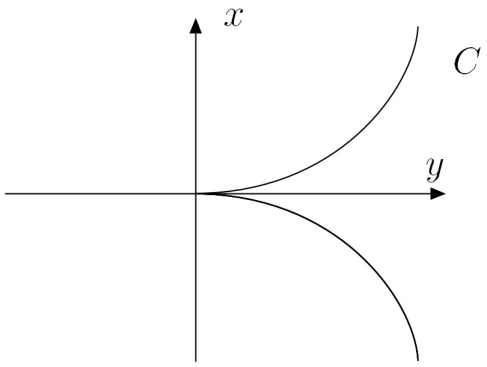
Seja L_1 e L_2 as retas dadas por $z_0 = 0$ e $z_1 = 0$ respectivamente. Então

$$I_P(C, L_1) = \dim_k \mathcal{O}_{\mathbb{P}^2_k,P}/(x^2 - y^3, x) = \dim_k \mathcal{O}_{\mathbb{P}^2_k,P}/(x, y^3) = 3,$$

e

$$I_P(C, L_2) = \dim_k \mathcal{O}_{\mathbb{P}^2_k,P}/(x^2 - y^3, y) = \dim_k \mathcal{O}_{\mathbb{P}^2_k,P}/(x^2, y) = 2.$$

Figura 17 – Interseção da parábola semicúbica
com os eixos coordenados.



Fonte: Ver (1) página 121. (2000)

Para continuar a classificação de curvas cúbicas planas vamos precisar utilizar o Teorema de Bézout:

Teorema 5.8 (Bézout)**.** *Sejam C e C' duas curvas planas projetivas de grau d e d' respectivamente, que não tem componentes em comum. Então C e C' se intersectam em dd' pontos, contados com multiplicidade, i.e.,*

$$C.C' := \sum_P I_P(C, C') = dd'.$$

Não faremos a prova deste teorema neste trabalho, uma prova pode ser encontrada em (12) página 57. Precisaremos de um caso particular:

Proposição 5.9. *Seja $C \in \mathbb{P}^2_k$ uma curva de grau d e L uma reta não contida em C. Então C e L se intersectam em d pontos (contados com a multiplicidade), i.e.,*

$$\sum_P I_P(C, L) = d.$$

Prova. Seja $L = \{x_2 = 0\}$ e $C = \{f = 0\}$, onde $f = f(x_0, x_1, x_2)$ é um polinômio homogêneo de grau d. Então

$$f|_L = f(x_0, x_1, 0) = a_0 x_0^d + a_1 x_0^{d-1} x_1 + \ldots + a_d x_1^d$$

é um polinômio homogêneo de grau d em duas variáveis. Podemos assumir que as coordenadas foram escolhidas de modo que $(1:0) \in L$ não é um zero em $f|_L$. Logo, pela equação (5.1) o número de pontos em que C e L se intersectam é obtido contando, levando em conta a multiplicidade, os zeros do polinômio

$$f(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d.$$

Pelo Teorema Fundamental da Álgebra, existem exatamente d zeros. □

Voltando agora para a classificação de cúbicas planas. Primeiro relembremos a classificação projetiva de cônicas. Toda equação quadrática homogênea pode ser escrita da forma

$$q(x_0, x_1, x_2) = q_A(x_0, x_1, x_2) = xA^tx$$

com $x = (x_0 : x_1 : x_2)$ e $A = {}^tA \in Mat\ (3 \times 3, k)$. Já que estamos assumindo que k é algebricamente fechado, o único invariante sob uma mudança de coordenadas é o posto da matriz. A não ser por uma equivalência, temos os seguintes casos

(1) $q(x_0, x_1, x_2) = x_0^2 + x_1^2 + x_2^2$ (cônica suave),

(2) $q(x_0, x_1, x_2) = x_0^2 + x_1^2$ (par de retas),

(3) $q(x_0, x_1, x_2) = x_0^2$ (retas duplas).

Note que a cônica $x_0^2 + x_1^2 + x_2^2$ é projetivamente equivalente a

$$x_0x_2 - x_1^2 = 0. \tag{5.2}$$

Proposição 5.10. *Seja C uma cúbica plana que se decompõe em uma cônica irredutível (uma curva de grau 2) e uma reta. Então, C é projetivamente equivalente a uma das seguintes curvas:*

(1) $C_1 = \{(x_0x_2 - x_1^2)x_1 = 0\}$,

(2) $C_2 = \{(x_0x_2 - x_1^2)x_0 = 0\}$.

Prova. Assumindo que $C = C_0 + L$, onde C_0 é uma cúbica irredutível e L uma reta. A cônica C_0 é dada por uma quádrica irredutível $\{q(x_0, x_1, x_2) = 0\}$. Por (5.2), C_0 é projetivamente equivalente à cônica $\{x_0x_2 - x_1^2 = 0\}$. Pela Proposição 5.9 a reta L intersecta a cônica em dois pontos. Como C_0 é suave, temos as seguintes possibilidades:

(1) L intersecta C_0 transversalmente em dois pontos,

(2) L é tangente a C_0 em um ponto P_0.

A curva C_0 é a imagem de $\mathbb{P}^1_k$ sobre a aplicação

$$\begin{aligned} \varphi : \quad & \mathbb{P}^1_k \longrightarrow C_0 \subset \mathbb{P}^2_k \\ & (t_0 : t_1) \longmapsto (t_0^2 : t_0t_1 : t_1^2). \end{aligned}$$

A transformação $t_0 \mapsto at_0 + bt_1,\ t_1 \mapsto ct_0 + dt_1$ induz o mapa

$$\begin{aligned} t_0^2 &\longmapsto a^2t_0^2 + 2abt_0t_1 + b^2t_1^2, \\ t_0t_1 &\longmapsto act_0^2 + (ad + bc)t_0t_1 + bdt_1^2, \\ t_1^2 &\longmapsto c^2t_0^2 + 2cdt_0t_1 + d^2t_1^2. \end{aligned}$$

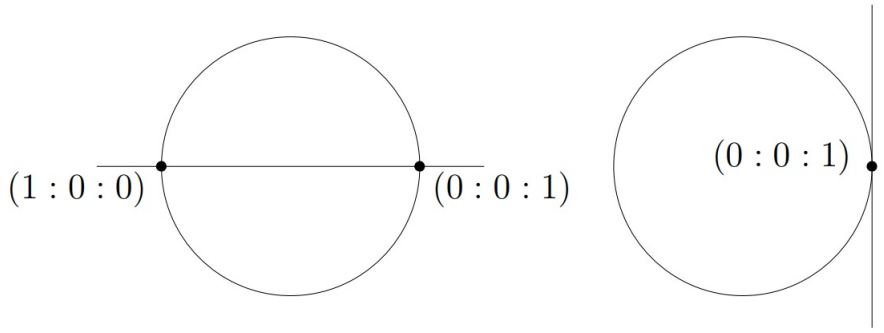
Podemos ver que a matriz

$$\begin{pmatrix} a^2 & 2ab & b^2 \\ ac & (ad+bc) & bd \\ c^2 & 2cd & d^2 \end{pmatrix}$$

define uma transformação de $\mathbb{P}^2_k$ que leva a cônica C_0 nela mesma. Utilizando uma matriz adequada $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, no caso (1), os pontos da interseção são levados em $(1 : 0 : 1)$ e $(0 : 0 : 1)$, no caso (2) podemos levar P_0 ao ponto $(0 : 0 : 1)$. Como a reta passando por $(1 : 0 : 0)$ e $(0 : 0 : 1)$ é $\{x_1 = 0\}$, e como a tangente da cônica C_0 em $(0 : 0 : 1)$ é $\{x_0 = 0\}$, a prova está completa. □

Obtemos as curvas C_1 e C_2 respectivamente, como ilustrado a seguir:

Figura 18 – Cúbicas planas que se decompõe em uma cônica e uma reta.



Fonte: Ver (1) página 123. (2000)

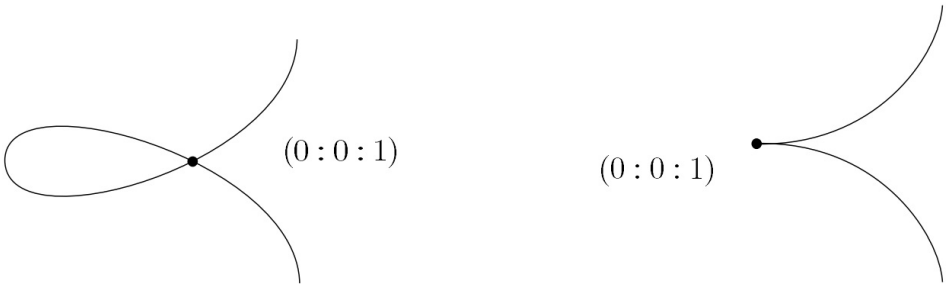
Agora, abordaremos a classificação de cúbicas singulares.

Proposição 5.11. *Seja C uma cúbica singular irredutível. Então C tem exatamente uma singularidade e é projetivamente equivalente a uma das seguintes curvas:*

(a) $C = \{x_1^2x_2 - x_0^3 - x_0^2x_2 = 0\}$,

(b) $C = \{x_2x_1^2 - x_0^3 = 0\}$.

Figura 19 – Cúbica plana com ponto um ponto duplo comum e cúbica plana com uma cúspide.



Fonte: Ver (1) página 124. (2000)

Prova. A curva C tem no máximo uma singularidade. Caso contrário a reta que passa pelas duas singularidades intersectaria C em ao menos 4 pontos, contados com multiplicidade, contradizendo a Proposição 5.9.

Podemos assumir que a singularidade de C em P está em $P = (0 : 0 : 1)$. Isso significa que a equação f para C tem a forma

$$f = x_2q(x_0, x_1) + bx_0^3 + cx_0^2x_1 + dx_0x_1^2 + ex_1^3,$$

com $q(x_0, x_1) \neq 0$. De fato, caso contrário f poderia ser fatorada em três formas lineares. Os termos quadráticos q poderem ser fatorados em formas lineares

$$q(x_0, x_1) = l_0(x_0, x_1)l_1(x_0, x_1),$$

e há dois casos a se considerar:

(a) O caso em que $l_0(x_0, x_1) \neq cl_1(x_0, x_1)$. Aplicando uma transformação de coordenadas podemos considerar que

$$l_0(x_0, x_1) = x_0 \qquad\qquad l_1(x_0, x_1) = x_1,$$

de modo que f tenha a forma

$$f = x_2x_0x_1 + b'x_0^3 + c'x_0^2x_1 + d'x_0x_1^2 + e'x_1^3.$$

Já que f é irredutível, $b'e' \neq 0$. Definindo

$$\begin{aligned} x_2 =& \beta\gamma(x_2' - 6x_0') + \frac{c'}{\beta}(x_0' + x_1') + \frac{d'}{\gamma}(x_0' - x_1'), \\ x_0 =& -\frac{1}{\beta}(x_0' + x_1'), \\ x_1 =& -\frac{1}{\gamma}(x_0' - x_1'), \end{aligned}$$

com $\beta^3 = b'$, $\gamma^3 = e'$, obtemos

$$f = x_2'((x_0')^2 - (x_1')^2) - 8(x_0')^3,$$

que é projetivamente equivalente a $x_1^2x_2 - x_0^2x_2 - x_0^3$.

(b) O caso $l_0(x_0, x_1) = cl_1(x_0, x_1)$. Podemos assumir que $l_0(x_0, x_1) = l_1(x_0, x_1) = x_1$, de modo que

$$f = x_2x_1^2 + b'x_0^3 + c'x_0^2x_1 + d'x_0x_1^2 + e'x_1^3.$$

Temos $b' \neq 0$, caso contrário x_1 dividiria f. Definindo

$$x_0 = x_0' - \frac{c'}{3b'}x_1$$

nos dá

$$f = x_2x_1^2 + b'(x_0')^3 + d''x_0'x_1^2 + e''x_1^3, \quad b' \neq 0,$$

e definindo

$$x_2 = -b'x_2' - d''x_0' - e''x_1$$

nos leva a

$$f = -b'(x_2'x_1^2 - (x_0')^3),$$

que é projetivamente equivalente a $x_2x_1^2 - x_0^3$.

□

5.3 CLASSIFICAÇÃO DE CÚBICAS SUAVES

A classificação de cúbicas planas suaves é baseada no fato de que toda curva deste tipo tem um ponto de inflexão, que é definido da seguinte maneira.

Definição 5.12. *Seja C uma curva plana de grau arbitrário. Um ponto suave $P \in C$ é chamado de* ***ponto de inflexão*** *de C se $I_P(C, T_PC) \geq 3$. A tangente T_PC a C em um ponto P é chamada de* ***reta tangente de inflexão*** *ou* ***tangente de inflexão de*** *C.*

Vamos mostrar que os pontos de inflexão de C são determinados pela interseção de C com a sua Hessiana, que é definida a seguir.

Definição 5.13. *Para uma curva plana $C = \{f = 0\}$, a* ***Hessiana*** *de C é dada por*

$$H_f := \det\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{0 \leq i,j \leq 2}$$

Se H_f não é identicamente nula, H_f é um polinômio homogêneo de grau $3(d-2)$. Seja

$$H = \{H_f = 0\} \subset \mathbb{P}^2_k.$$

Se $d = 2$, então H pode ser vazia. Por outro lado ou $H = \mathbb{P}^2_k$ ou H é uma curva plana de grau $3(d-2)$ chamada de **curva Hessiana de** C.

Proposição 5.14. *Seja C uma curva plana suave de grau $d \geq 3$ com Hessiana H. Assuma que o máximo divisor comum entre char (k) e $d-1$ seja igual a 1. Então $H \cap C$ é igual ao conjunto dos pontos de inflexão de C.*

Prova. Primeiro vamos considerar como a afirmação se comporta com uma mudança de coordenadas. Considere a transformação

$$A : \begin{pmatrix} x_0 \\ x_2 \\ x_2 \end{pmatrix} \longmapsto A \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}, \qquad A \in Gl(3,k).$$

Para qualquer polinômio $f \in k[x_0, x_1, x_2]$ denotamos o polinômio transformado como $f \circ A$ por f^*. Usando a regra da cadeia é possível mostrar que

$$H_{f^*} = (\det A)^2 (H_f)^*.$$

Logo o que queremos provar é invariante por mudança de coordenadas, e podemos assumir que $P = (0:0:1)$ e que $T_P C = \{x_1 = 0\}$. Em termos de coordenadas afins $x = x_0/x_2$ e $y = x_1/x_2$ temos

$$f(x,y) = y(a + bx + cy + g(x,y)) + ex^2 + h(x),$$

onde $a, b, c, e \in k$, $a \neq 0$, todos os termos $g(x,y)$ tem ordem ≥ 2 e todos os termos de h tem ordem ≥ 3. Em coordenadas homogêneas temos

$$f(x_0,x_1,x_2) = ax_2^{d-1}x_1 + bx_2^{d-2}x_0x_1 + cx_2^{d-2}x_1^2 + ex_2^{d-2}x_0^2 + \text{ termos de ordem } \geq 3 \text{ em } x_0, x_1.$$

Logo temos

$$H_f(0:0:1) = \det \begin{pmatrix} 2e & b & 0 \\ b & 2c & (d-1)a \\ 0 & (d-1)a & 0 \end{pmatrix} = -2ea^2(d-1)^2.$$

Já que $(\text{char }(k), d-1) = 1$ e $a \neq 0$, temos

$$H_f(0:0:1) = 0 \iff e = 0.$$

Segue que

$$\mathcal{O}_{\mathbb{P}^2_k, P}/(f, x_1) = \mathcal{O}_{\mathbb{A}^2_k, 0}/(ex^2 + h(x), y).$$

Portanto

$$I_P(C, T_P C) \geq 3 \iff e = 0 \iff P \in H.$$

□

Observação 5.15. *A mesma prova é válida sem a hipótese de que C é suave, é necessário somente de que P seja um ponto suave de C.*

Precisamos mostrar a existência de pelo menos um ponto de inflexão em uma curva suave de grau $d \geq 3$, i.e., precisamos mostrar que a interseção de uma curva suave de grau maior ou igual a 3 com sua Hessiana é não vazia. Isto é trivial se a Hessiana é todo o $\mathbb{P}^2_k$, caso contrário devemos utilizar uma versão fraca do Teorema de Bézout.

Lema 5.16. *A interseção de duas curvas planas projetivas C e C' é não vazia.*

Para provar esse lema, usaremos o seguinte resultado:

Lema 5.17. *O complemento $\mathbb{P}^2_k \setminus C$ de uma curva plana C é afim.*

Prova. Considere o **mapa de Veronese**

$$v_d : \mathbb{P}^2_k \longrightarrow \mathbb{P}^N_k, \quad N = \binom{d+2}{2} - 1,$$

dado por

$$v_d(x_0 : x_1 : x_2) = (x_0^d : x_0^{d-1}x_1 : \ldots : x_2^d) = (\ldots : x_I : \ldots)_{I \in \Lambda_d}$$

onde

$$\Lambda_d := \{(i_0, i_1, i_2) \in \mathbb{N}_0^3 \mid i_0 + i_1 + i_2 = d\}$$

e $x_I = x_{(i_0,i_1,i_2)} = x_0^{i_0}x_1^{i_1}x_2^{i_2}$. É possível mostrar que $|\Lambda_d| = \binom{d+2}{2}$. Denotamos as coordenadas de $\mathbb{P}^N_k$ por z_I para $I \in \Lambda_d$. Assim como no mapa de Segre, pode ser verificado que v_d é uma imersão com imagem dada pelas equações

$$z_I z_J = z_K z_L \text{ para } I + J = K + L.$$

Seja f uma equação para C com grau d. Podemos escrever isso da seguinte forma:

$$f = \sum_{I \in \Lambda_d} a_I x_I.$$

Consideremos o hiperplano

$$H = \Big\{ \sum a_I z_I = 0 \Big\}$$

em $\mathbb{P}^N_k$. Então temos

$$v_d(C) = v_d(\mathbb{P}^2_k) \cap H.$$

Esse argumento mostra que $\mathbb{P}^2_k \setminus C$ é afim. □

Agora faremos a prova do Lema 5.16.

Prova (Lema 5.16)**.** Seja C uma curva de grau d. Pelo Lema 5.17, $\mathbb{P}^2_k \setminus C$ é afim. Se $C \cap C' = \emptyset$, teríamos $C' \subset \mathbb{P}^2_k \setminus C \subset \mathbb{A}^N_k$. Como C' não consiste de um ponto, existiria uma uma função coordenada w em $\mathbb{A}^N_k$ que, por restrição, nos daria uma função não constante em C', o que contradiz o Teorema 3.35 □.

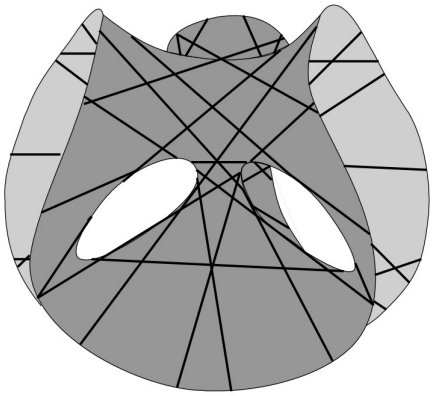
Corolário 5.17.1. *Toda curva suave C de grau $d \geq 3$ com $mdc(d-1, char(k)) = 1$ tem pelo menos um ponto de inflexão.*

Prova. Do Lema 5.17 segue que $C \cap H \neq \emptyset$. A afirmação segue da Proposição 5.14. □

6 AS 27 RETAS

Chegamos ao capítulo do objetivo deste trabalho. Agora vamos mostrar que toda superfície cúbica suave em $\mathbb{P}^3_k$ contém 27 retas. Primeiro vamos verificar que existem retas em uma superfície cúbica e depois determinar sua configuração. A partir de agora vamos assumir que o corpo k é algebricamente fechado, e que a característica é diferente de 2 ou 3.

Figura 20 – A cúbica de Clebsch com suas retas.



Fonte: Ver (1) página 143. (2000)

6.1 A EXISTÊNCIA DE RETAS EM UMA CÚBICA

Seja $f = f(x_0, x_1, x_2, x_3) \in k^3[x_0, x_1, x_2, x_3]$ um polinômio homogêneo de grau 3. Vamos considerar a **superfície cúbica** correspondente (também conhecida simplesmente como cúbica)

$$S = \{(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3_k \mid f(x_0, x_1, x_2, x_3) = 0\}.$$

A seguir vamos assumir que S é suave, que é o caso para cúbicas f genéricas, mais precisamente, existe um conjunto aberto de Zariski de polinômios cúbicos f tal que S é suave.

Teorema 6.1. *Toda superfície cúbica suave $S \subset \mathbb{P}^3_k$ contém uma reta.*

Há dois passos nessa prova. Primeiros vamos mostrar que para algum ponto $P \in S$ a interseção $C_P := S \cap T_P S$ ou contém um reta, ou é uma cúbica plana com uma cúspide. No primeiro caso, temos a reta como queremos. No segundo, vamos mostrar que existe uma reta em S passando por um ponto de C_P.

Lema 6.2. *Duas superfícies em $\mathbb{P}^3_k$ tem interseção não vazia.*

Prova. A prova é similar à prova do Lema 5.16.

Lema 6.3. *Seja S uma superfície cúbica suave. Então para cada ponto $P \in S$ a interseção $C_P := S \cap T_P S$ é uma curva plana cúbica singular. Existe um ponto P em S tal que C_P ou é redutível, ou é uma cúbica plana com uma cúspide (uma parábola semicúbica).*

Prova. Primeiro note que C_P é uma curva. De fato, como uma superfície cúbica redutível é singular, então, sendo suave, S é irredutível e por isso não contém $T_P S$. Já que S é definida por uma cúbica, a restrição a um subespaço linear é também dada por uma cúbica, logo C_P é um curva cúbica plana.

Vamos mostrar que P é uma singularidade em C_P. Escolhemos coordenadas de maneira que $P = (0:0:0:1) \in S$ e $T_P S = \{x_2 = 0\}$. Em coordenadas afins x, y, z a equação f de S é dada por

$$f = z + q(x, y, z) + h(x, y, z),$$

onde q é uma quádrica homogênea e h é um polinômio cúbico homogêneo. Em coordenadas homogêneas temos

$$f = x_2 x_3^2 + q(x_0, x_1, x_2)x_3 + h(x_0, x_1, x_2). \tag{6.1}$$

Logo $f|_{\{x_2=0\}}$ se anula quadraticamente em P, então C_P é singular em P.

Agora suponha que C_P é irredutível para todos os pontos $P \in S$. Então devemos mostrar que para algum P a curva C_P é uma cúbica cuspidal (i.e., tem uma cúspide). Assim como na prova da Proposição 5.11, as tangentes de C_P no ponto P são dadas pelos fatores da forma quadrática

$$\tilde{q}(x_0, x_1) = q(x_0, x_1, 0),$$

e C_P tem uma cúspide se, e somente se, as duas retas tangentes são iguais, i.e., se, e somente se, q é o quadrado de uma forma linear. Se escrevermos

$$q(x_0, x_1, x_2) = \sum_{i,j=0}^{2} a_{ij} x_i x_j, \qquad \text{com } a_{ij} = a_{ji}, \tag{6.2}$$

$\tilde{q}$ é um quadrado se, e somente se, a matriz $\tilde{A} = (a_{ij})_{i,j=0,1}$ tem posto 1. Como $\tilde{q}$ não é identicamente nulo, é equivalente ao determinante de $\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ ser igual a zero.

Consideremos a Hessiana de f,

$$H_f := \det\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{i,j}.$$

De modo similar à Hessiana de uma curva cúbica dada na Proposição 5.14, o comportamento dessa Hessiana sob uma mudança de coordenadas dada por uma matriz $M \in Gl(4, k)$, é :

$$H_{f^*} = (\det M)^2 (H_f)^*,$$

onde $f^* = f \circ M$ e $(H_f)^* = H_f \circ M$.

No nosso caso, f tem a forma de (6.1) com q, como em (6.2), e portanto temos

$$H_f(P) = \det \begin{pmatrix} 2a_{00} & 2a_{01} & 2a_{02} & 0 \\ 2a_{10} & 2a_{11} & 2a_{12} & 0 \\ 2a_{20} & 2a_{21} & 2a_{22} & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

Da forma dessa matriz temos

$$H_f(P) = 0 \iff \det \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} = 0.$$

Por isso C_P é uma cúbica com uma cúspide se, e somente se, $P \in S \cap H$, onde $H = \{H_f = 0\}$. Resta mostrar que $S \cap H = S \neq \emptyset$. Como f é uma cúbica, H ou é $\mathbb{P}^3_k$, nesse caso $S \cap H \neq \emptyset$, ou uma superfície cúbica, e o resultado segue do Lema 6.2. □

Queremos saber quando uma reta está contida em uma superfície cúbica. Como qualquer reta pode ser dada como uma reta $\overline{PQ}$ que passa por dois pontos P e Q, introduzimos o seguinte conceito que nos ajudará a determinar quando a reta $\overline{PQ}$ está contida na superfície $\{f = 0\}$.

Definição 6.4. *Para um polinômio cúbico homogêneo $f \in k[x_0, x_1, x_2, x_3]$ e pontos $P = (x_0, x_1, x_2, x_3)$ e $Q = (y_0, y_1, y_2, y_3)$, a "polar" de f é definida como*

$$f_1(x_0, \ldots, x_3; y_0, \ldots, y_3) = f_1(P; Q) := \sum_{i=0}^{3} \frac{\partial f}{\partial x_i}(P) y_i.$$

Vamos explicar o significado geométrico da polar. Lembremos que para $P \in C$, o espaço tangente de C em P foi definido como

$$T_P C := \left\{ (x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3_k \;\middle|\; \sum_{i=0}^{3} \frac{\partial f}{\partial x_i}(P) x_i = 0 \right\} \subset \mathbb{P}^3_k.$$

Para $P \in S$, por definição de espaço tangente, temos

$$\overline{PQ} \subset T_P S \iff f_1(P; Q) = 0.$$

Para pontos arbitrários $P \neq Q$, um cálculo nos mostra que

$$f(\lambda P + \mu Q) = \lambda^3 f(P) + \lambda^2 \mu f_1(P; Q) + \lambda \mu^2 f_1(Q; P) + \mu^3 f(Q).$$

Logo temos

$$\overline{PQ} \subset S \iff f(P) = f_1(P;Q) = f_1(Q;P) = f(Q) = 0. \tag{6.3}$$

Essa condição nos permite identificar quando dois polinômios terão os mesmos zeros. Isso é um problema clássico resolvido por meio de **resultantes.**

Definição 6.5. *Para polinômios homogêneos r e s nas variáveis u e v, dados por*

$$\begin{aligned} r(u,v) =& a_0u^2 + a_1uv + a_2v^2, \\ s(u,v) =& b_0u^3 + b_1u^2v + b_2uv^2 + b_3v^3, \end{aligned}$$

*a **resultante** de r e s é dada por*

$$R(r,s) := \det \begin{pmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{pmatrix}. \tag{6.4}$$

A importância da resultante é dada pelo seguinte fato.

Lema 6.6. *Dois polinômios homogêneos r e s de graus 2 e 3, respectivamente, têm um zero em comum em $\mathbb{P}^1_k$ se, e somente se, $R(r,s) = 0$.*

Prova. Considere o espaço vetorial V de 5 dimensões de todos os polinômios homogêneos de grau 4 em u e v. As linhas da matriz (6.4) acima são os coeficientes dos cinco polinômios

$$u^2r, uvr, v^2r, us, vs$$

em termos da base de monômios padrão para esse espaço. O determinante é zero se, e somente se, existe uma relação linear entre esses polinômios. Tal relação pode ser escrita da como

$$qr = ls,$$

onde $q = q(u,v)$ é homogêneo de grau 2 e $l = l(u,v)$ é linear. Essa igualdade implica que qr e ls têm os mesmos zeros, o que é possível somente se r e s têm zeros em comum. Por outro lado, se r e s têm zeros em comum, então os outros 5 polinômios também, o que significa que não podem gerar V, portanto são linearmente dependentes. □

Agora podemos fazer a prova do Teorema 6.1.

Prova (Teorema 6.1)**.** Se $C_P = S \cap T_PS$ é redutível para algum ponto $P \in S$, então C_P, e logo S, contém uma reta, como se quer. Caso contrário pelo Lema 6.3 podemos assumir que existe um ponto P tal que C_P tem uma cúspide. Por uma mudança de coordenadas

podemos assumir que $P = (0 : 0 : 1 : 0)$ e $T_P S = \{x_3 = 0\}$, e pela Proposição 5.11 podemos assumir que

$$C_P = \{x_0^2 x_2 - x_1^3 = x_3 = 0\}.$$

Por isso, a equação f de S tem a forma

$$f = x_0^2 x_2 - x_1^3 + x_3 g$$

para algum polinômio homogêneo $g = g(x_0, x_1, x_2, x_3)$ de grau 2. Como S é suave em P, temos $g(0, 0, 1, 0) \neq 0$, multiplicando por um escalar podemos assumir que $g(0, 0, 1, 0) = 1$.

Vamos mostrar que S contém uma reta que passa por um ponto em C_P. Os pontos em C_P são parametrizados por $P_\alpha := (1 : \alpha : \alpha^3 : 0)$ para $\alpha \in k$. Note que podemos representar qualquer reta que passa por P_α por uma reta $\overline{P_\alpha Q}$ e $Q = (0 : x_1 : x_2 : x_3)$ por algum ponto Q no plano $\{x_0 = 0\}$. Como $f(P_\alpha) = 0$, nesse caso, a equação (6.3) nos dá

$$\overline{P_\alpha Q} \subset S \iff f_1(P_\alpha; Q) = f_1(Q; P_\alpha) = f(Q) = 0.$$

Denotamos $f_1(P_\alpha; Q),\ f_1(Q; P_\alpha), f(Q) \in k[\alpha][x_1, x_2, x_3]$ por A_α, B_α e C_α respectivamente. Esses são polinômios homogêneos nas variáveis x_1, x_2, x_3 de grau 1,2 e 3, respectivamente, com coeficientes dados por polinômios em α. Vimos anteriormente que a teoria de resultantes pode ser usada para determinar se dois polinômios têm um uma raiz em comum. Nesse caso, definimos o polinômio $R_{27}(\alpha)$ como sendo a resultante

$$R_{27}(\alpha) := R\Big(\underbrace{B_\alpha(x_1, \tilde{A}_\alpha(x_1, x_3), x_3)}_{\text{grau 2}}, \underbrace{C_\alpha(x_1, \tilde{A}_\alpha(x_1, x_3), x_3)}_{\text{grau 3}}\Big),$$

onde $x_2 = \tilde{A}_\alpha(x_1, x_3)$ é uma relação determinada pelo polinômio linear A_α. (Veremos a seguir que $R_{27}(\alpha)$ é um polinômio de grau 27). O Lema 6.6 implica que $R_{27}(\alpha)$ satisfaz a seguinte propriedade:

$$R_{27}(\alpha) = 0 \iff A_\alpha, B_\alpha, C_\alpha \text{ têm um zero em comum } (\eta_\alpha : \xi_\alpha : \tau_\alpha).$$

Para provar o teorema é suficiente provar que R_{27} tem uma raiz, já que para cada raiz a_0 de $R_{27}(\alpha)$ a reta $\overline{P_{\alpha_0} Q}$ com $Q = (0 : \eta_{\alpha_0} : \xi_{\alpha_0} : \tau_{\alpha_0})$ está em S.

Para mostrar que R_α tem uma raiz, é suficiente mostrar que R_α é não constante. Faremos isso explicitamente calculando R_α.

Em nossa situação a polar da equação

$$f = f(x_0, \ldots, x_3) = x_0^2 x_2 - x_1^3 + x_3 g$$

é dado por

$$f_1 = 2x_0 x_2 y_0 - 3x_1^2 y_1 + x_0^2 y_2 + g(x_0, \ldots, x_3) y_3 + x_3 g_1(x_0, \ldots; \ldots, y_3),$$

onde g_1 é a polar da equação quadrática g. Os polinômios $A_\alpha, B_\alpha, C_\alpha$ são dados por

$$\begin{aligned} A_\alpha &= -3\alpha^2 x_1 + x_2 + g(1, \alpha, \alpha^3, 0)x_3, \\ B_\alpha &= -3\alpha x_1^2 + x_3 g_1(1, \alpha, \alpha^3, 0; 0, x_1, x_2, x_3), \\ C_\alpha &= -x_1^3 + x_3 g(0, x_1, x_2, x_3). \end{aligned}$$

Como g é quadrático e $g(0, 0, 1, 0) = 1$, segue que

$$g(1, \alpha, \alpha^3, 0) = \alpha^6 + \text{ termos de ordem menor.}$$

Definimos

$$a^{(6)} := g(1, \alpha, \alpha^3, 0).$$

De $A_\alpha = 0$ temos a relação

$$x_2 = 3\alpha^2 x_1 - a^{(6)} x_3. \tag{6.5}$$

Substituindo em B_α temos a expressão

$$B_\alpha = -3\alpha x_1^2 + x_3 g_1(1, \alpha, \alpha^3, 0; 0, x_1, 3\alpha^2 x_1 - a^{(6)} x_3, x_3).$$

Já que $g_1(1, \alpha, \alpha^3; 0, x_1, x_2, x_3)$ é linear em x_1, x_2 e x_3, temos

$$B_\alpha = b_0 x_1^2 + b_1 x_1 x_3 + b_2 x_3^2$$

com

$$\begin{aligned} b_0 &= -3\alpha, \\ b_1 &= g_1(1, \alpha, \alpha^3, 0; 0, 1, 3\alpha^2, 0) = 6\alpha^5 + \ldots, \\ b_2 &= g_1(1, \alpha, \alpha^3, 0; 0, 0, -a^{(6)}, 1) = -2\alpha^9 + \ldots, \end{aligned}$$

onde as reticências representam termos de ordem menor. De modo similar, substituindo (6.5) em C_α temos

$$C_\alpha = -x_1^3 + x_3 g(0, x_1, 3\alpha^2 x_1 - a^{(6)} x_3, x_3),$$

obtemos

$$C_\alpha = c_0 x_1^3 + c_1 x_1^2 x_3 + c_2 x_1 x_3^2 + c_3 x_3^3,$$

onde

$$\begin{aligned} c_0 &= -1, \\ c_1 &= g(0, 1, 3\alpha^2, 0) = 9\alpha^4 + \ldots, \\ c_2 &= g_1(0, 1, 3\alpha^2, 0; 0, 0, -a^{(6)}, 1) = -6\alpha^8 + \ldots, \\ c_3 &= g(0, 0, -a^{(6)}, 1) = a^{12} + \ldots \end{aligned}$$

Por definição temos

$$R_{27}(\alpha) = \det \begin{pmatrix} b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 & c_3 & 0 \\ 0 & c_0 & c_1 & c_2 & c_3 \end{pmatrix}.$$

O termo líder de R_{27} é dado pelo termo líder do determinante da matriz dos termos líderes, i.e., a matriz obtida substituindo b_i e c_j pelos termos líderes, assumindo que esse determinante é diferente de zero. Por isso o termo líder de R_{27} é dado por

$$\det \begin{pmatrix} -3\alpha & 6\alpha^5 & -2\alpha^9 & 0 & 0 \\ 0 & -3\alpha & 6\alpha^5 & -2\alpha^9 & 0 \\ 0 & 0 & -3\alpha & 6\alpha^5 & -2\alpha^9 \\ -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} & 0 \\ 0 & -1 & 9\alpha^4 & -6\alpha^8 & \alpha^{12} \end{pmatrix} = \alpha^{27} \det \begin{pmatrix} -3 & 6 & -2 & 0 & 0 \\ 0 & -3 & 6 & -2 & 0 \\ 0 & 0 & -3 & 6 & -2 \\ -1 & 9 & -6 & 1 & 0 \\ 0 & -1 & 9 & -6 & 1 \end{pmatrix} = \alpha^{27}.1 = \alpha^{27}.$$

Segue que $R_{27}(\alpha)$ é um polinômio de grau 27 e, em particular, é não constante, portanto há uma raiz e, dessa forma, existe uma reta. □

6.2 A CONFIGURAÇÃO DAS 27 RETAS

Começamos com uma observação de que se S é uma superfície cúbica contendo um ponto P tal que $S \cap T_P S$ é uma cúbica cuspidal, a prova do Teorema 6.1 mostra que existe um polinômio R_α de grau 27 tal que cada raiz de R_α dá origem a pelo menos uma reta em S. Se as raízes de R_α forem distintas, devemos esperar que S contenha ao menos 27 retas.

Vamos mostrar que existem 27 retas em uma cúbica suave e determinar sua configuração.

Vamos precisar de um resultado sobre pontos singulares de uma quádrica. Considere a quádrica

$$Q = \left\{ \sum_{i,j=0}^{n} a_{ij} x_i x_j = 0 \right\} \subset \mathbb{P}_k^n, \qquad a_{ij} = a_{ji}. \tag{6.6}$$

Lema 6.7. *A quádrica Q dada por* (6.6) *tem o conjunto de pontos singulares dados pelo subespaço linear*

$$Sing\ Q\ = \mathbb{P}(\ker(A)) = \{x \in \mathbb{P}_k^n \mid Ax = 0\},$$

onde a matriz simétrica $A = (a_{ij})$ é a matriz da forma quadrática correspondente a Q. Em particular, Q é suave se, e somente se, A tem posto máximo igual a $n+1$.

Prova. Pelo teorema do eixo principal[1], existe uma matriz invertível [2] M tal que

$$(M)(A)(M^t) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} = E_{r+1}$$

A matriz M induz uma transformação de coordenadas, que leva Q à quádrica [3]

$$Q_{r+1} = \{x_0^2 + \ldots + x_r^2 = 0\},$$

onde $r =$ posto$(A) - 1$. Pode-se ver que

$$\text{Sing } Q_{r+1} = \{x_0 = \ldots = x_r = 0\} = \mathbb{P}(\ker E_{r+1}) = \{x \in \mathbb{P}_k^n \mid E_{r+1}x = 0\}.$$

Logo, se o posto de A é $n+1$ o único ponto $x \in Q \subset \mathbb{P}_k^n$ tal que $E_{n+1}x = 0$ seria $x = 0$, mas esse ponto não pertence à $\mathbb{P}_k^n$, portanto Q não tem pontos singulares e é suave. □

Definição 6.8. *Para a quádrica Q em (6.6), o **posto de** Q é definido como o posto da matriz correspondente $A = (a_{ij})$. Note que o posto é bem definido, apesar de A ser determinada a menos de multiplicação por um escalar não nulo.*

Proposição 6.9. *Seja S uma superfície cúbica suave.*

(1) *Se E é um plano, então $E \cap S$ é uma cúbica irredutível, ou uma cônica e uma reta, ou três retas distintas.*

(2) *A superfície S contém no máximo três retas que passam por qualquer ponto dado $P \in S$. Se S contém duas ou três retas passando por por $P \in S$, então essas retas estão em um plano E. E $E \cap S$ tem uma das possíveis configurações mostradas na figura a seguir.*

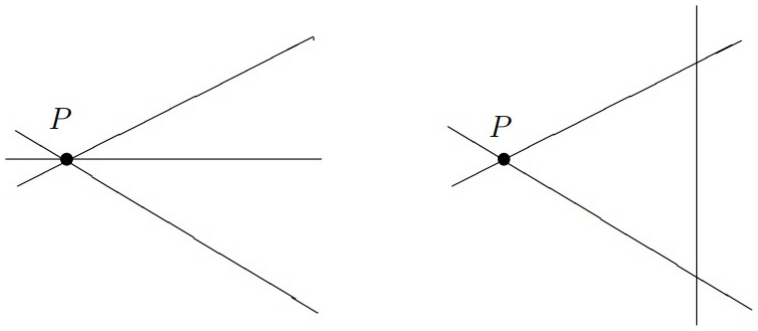
---

[1] O teorema diz: se A é uma matriz simétrica, então existe uma matriz ortogonal P e uma matriz diagonal D tal que $P^T AP = D$.

[2] O teorema do eixo principal utiliza matrizes ortogonais, mas uma matriz ortogonal A é uma matriz tal que $A^T = A^{-1}$.

[3] Note que para se chegar à equação da quádrica a partir de sua matriz, é necessário fazer a operação matricial xAx^t, onde $x = (x_0 : \ldots : x_n) \in \mathbb{P}_k^n$.

Figura 21 – Possível configuração de retas em uma superfície cúbica, que estão contidas em um plano.



Fonte: Ver (1) página 152. (2000)

Prova. (1) Note que, assim como na prova do Lema 6.3, a interseção $E \cap S$ é curva cúbica plana. Temos que mostrar que $E \cap S$ não contém uma reta dupla (por reta dupla, queremos dizer que L, com a notação da seção 5.1, deve satisfazer à seguinte equação $E \cap S = 2L + M$ para alguma reta M, possivelmente com $M = L$). Suponha que esse não é o caso, ou seja, que $E \cap S$ tem essa forma. Escolhemos mudanças de coordenadas tal que $E = \{x_3 = 0\}$ de modo que a reta dupla é dada por $l = \{x_2 = x_3 = 0\} \subset E \cap S$. Isso implica que a equação de S tem a forma

$$f = x_2^2 g(x_0, x_1, x_2) + x_3 h(x_0, x_1, x_2, x_3),$$

onde $\deg g = 1$ e $\deg h = 2$. Note que na primeira parcela, g não contém a variável x_3, se fosse esse o caso f conteria o plano. Como k é algebricamente fechado, o conjunto

$$\Delta := l \cap \{h = 0\} = \{(x_0 : x_1 : 0 : 0) \mid h(x_0, x_1, 0, 0) = 0\}$$

é não vazio. No "pior" dos casos $h(x_0, x_1, x_2, x_3) = x_2.g_1 + x_3.g_2$, onde $g_i \in k[x_0, x_1, x_2, x_3]$, e a restrição seria identicamente nula, o que significa que qualquer ponto satisfaria a equação $h(x_0, x_1, 0, 0)$. Perceba que se $f = x_2^2 g(x_0, x_1, x_2) + x_3 h(x_0, x_1, x_2, x_3)$ então

$$\begin{aligned}
\frac{\partial f}{\partial x_0} &= x_2^2.\frac{\partial g}{\partial x_0} + x_3.\frac{\partial h}{\partial x_0} \\
\frac{\partial f}{\partial x_1} &= x_2^2.\frac{\partial g}{\partial x_1} + x_3.\frac{\partial h}{\partial x_1} \\
\frac{\partial f}{\partial x_2} &= 2x_2.g + x_2^2.\frac{\partial g}{\partial x_2} + x_3.\frac{\partial h}{\partial x_2} \\
\frac{\partial f}{\partial x_3} &= h + x_3.\frac{\partial h}{\partial x_3}.
\end{aligned}$$

Cada parcela de cada derivada parcial deve ser zerada para que o ponto considerado seja singular. Olhando a restrição temos que isso vai acontecer imediatamente para quase todas as parcelas das 4 equações ($x_2 = x_3 = 0$), a não ser na última equação, aí deve-se ter $h(x_0, x_1, 0, 0) = 0$.

Portanto os pontos de Δ são pontos singulares de S, o que contradiz o fato de que S é suave.

(2) Qualquer reta $l \subset S$ passando por P se encontra na espaço tangente $T_P S$, já que

$$l = T_P l \subset T_P S.$$

Então é suficiente tomar $E = T_P S$. Como S é suave, $T_P S$ é um plano, e portanto o resultado segue de (1). □

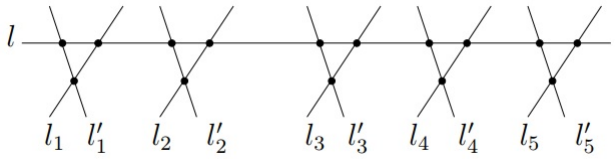
Proposição 6.10. *Seja S uma cúbica suave e $l \subset S$ uma reta. Então existem exatamente 10 retas em S que intersectam l. Essas retas são dadas por 5 pares de retas (l_i, l_i'), $1 \leq i \leq 5$, que têm as seguintes propriedades:*

(1) *$l \cup l_i \cup l_i'$ se encontram num plano. Em particular, as retas l_i e l_i' intersectam a reta l para $i = 1, \ldots, 5$.*

(2) *$(l_i \cup l_i') \cap (l_j \cup l_j') = \emptyset$ para $i \neq j$.*

Tal configuração é ilustrada a seguir. (Note que também é possível que l, l_i e l_i' se encontrem em um único ponto.)

Figura 22 – A configuração de 10 retas em uma cúbica intersectando uma reta l.



Fonte: Ver (1) página 153. (2000)

Prova. Seja E um plano contendo l. Então $E \cap S = l \cup q$, onde $q \subset E$ é uma cônica. Ou q é irredutível, ou, pela Proposição 6.9, $E \cap S$ tem uma das configurações da Figura 19. Então devemos mostrar que existem exatamente cinco planos $E \supset l$ tais que a cônica q se decompõe. Cada um desses planos nos dá um par de retas, e pela Proposição 6.9, implica que eles têm essa configuração.

Podemos assumir que $l = \{x_2 = x_3 = 0\}$. Logo, o conjunto dos planos que contém l é dado pela família de planos

$$E_{\lambda,\mu} : \{\lambda x_3 - \mu x_2 = 0\}.$$

Queremos determinar para que valores de $(\lambda : \mu) \in \mathbb{P}^1_k$ a interseção $E_{\lambda,\mu} \cap S$ consiste de três retas.

Como S contém l, a equação que define S tem a forma

$$f = Ax_0^2 + Bx_0x_1 + Cx_1^2 + Dx_0 + Ex_1 + F, \tag{6.7}$$

onde $A, \ldots, F \in k[x_2, x_3]$ são polinômios homogêneos, com A,B e C lineares, D,E quadráticos e F cúbico.

Pontos do plano $E_{\lambda,\mu}$ tem a forma $(x_0 : x_1 : \lambda t : \mu t)$ para algum $t \in k$. Logo, podemos tomar coordenadas homogêneas[4] $(x_0 : x_1 : t)$ em $E_{\lambda,\mu}$. Em termos dessas coordenadas $l|_{E_{\lambda,\mu}} = \{t = 0\}$ e

$$f|_{E_{\lambda,\mu}} = tq(x_0, x_1, t),^{5}$$

onde

$$\begin{aligned} q(x_0, x_1, t) =& A(\lambda,\mu)x_0^2 + B(\lambda,\mu)x_0x_1 + C(\lambda,\mu)x_1^2 \\ &+ D(\lambda,\mu)x_0t + E(\lambda,\mu)x_1t + F(\lambda,\mu)t^2. \end{aligned}$$

Pode-se calcular a matriz que define a quádrica q realizando a operação matricial e comparando coeficientes, lembrando que tal matriz é simétrica, i.e, $a_{ij} = a_{ji}$:

$$\begin{pmatrix} x_0 & x_1 & t \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ t \end{pmatrix} = q(x_0, x_1, t).$$

Temos então que a matriz A que define a quádrica é

$$A = \begin{pmatrix} A & \frac{1}{2}B & \frac{1}{2}D \\ \frac{1}{2}B & C & \frac{1}{2}E \\ \frac{1}{2}D & \frac{1}{2}E & F \end{pmatrix}.$$

Sabe-se que se o posto de uma matriz $n \times n$ é menor que n, então há pelo menos uma linha nula, ou seja, $\det A = 0$. Obtivemos então uma condição equivalente para se aplicar o Lema 6.7.

Pelo Lema 6.7, essa cônica é singular se, e somente se,

$$\Delta(\lambda, \mu) = 0,$$

[4] Considerando uma correspondência um por um.

[5] Perceba que existe um fator de t em A, B, C, D e F, que foi colocado em evidência para se chegar a essa forma.

onde $\Delta(\lambda,\mu)$ é o polinômio homogêneo de grau 5 dado por

$$\begin{aligned}\Delta(\lambda,\mu) :=& 4\det\begin{pmatrix} A(\lambda,\mu) & \frac{1}{2}B(\lambda,\mu) & \frac{1}{2}D(\lambda,\mu) \\ \frac{1}{2}B(\lambda,\mu) & C(\lambda,\mu) & \frac{1}{2}E(\lambda,\mu) \\ \frac{1}{2}D(\lambda,\mu) & \frac{1}{2}E(\lambda,\mu) & F(\lambda,\mu)\end{pmatrix} \\ =& 4A(\lambda,\mu)C(\lambda,\mu)F(\lambda,\mu) + B(\lambda,\mu)E(\lambda,\mu)D(\lambda,\mu) \\ & - C(\lambda,\mu)D^2(\lambda,\mu) - A(\lambda,\mu)E^2(\lambda,\mu) - F(\lambda,\mu)B^2(\lambda,\mu).\end{aligned}$$

Para mostrar a proposição, precisamos mostrar que $\Delta(\lambda,\mu) \neq 0$ e que Δ não tem raiz múltipla.

Por uma mudança de coordenadas, podemos tomar $\lambda = 0$ como sendo um zero de $\Delta(\lambda,\mu)$. Precisamos mostrar que λ^2 não divide $\Delta(\lambda,\mu)$. A Proposição 6.9 nos dá as possíveis configurações para as cúbicas correspondentes $E_{0,1} \cap S$. Podemos escolher coordenadas de modo que $E_{0,1} \cap S$ é dado por

$$l = \{x_3 = 0\}, l_1 = \{x_0 = 0\}, l_1' = \{x_1 = 0\} \tag{6.8}$$

ou

$$l = \{x_3 = 0\}, l_1 = \{x_0 = 0\}, l_1' = \{x_0 - x_3 = 0\}. \tag{6.9}$$

Trataremos do caso (6.9). Os cálculos do caso (6.8) podem ser vistos em (10) página 107. No caso (6.9) temos

$$f = x_0x_3(x_0 - x_3) + x_2g, \tag{6.10}$$

onde g é quadrático. Comparando (6.10) com (6.7) vemos que

$$D(x_2, x_3) = -x_3^2 + x_2\beta(x_2, x_3),$$

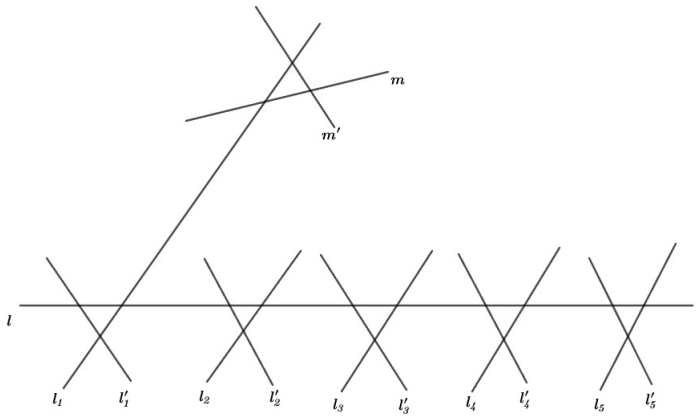
para algum $\beta \in k^1[x_2, x_3]$, e que os polinômios B, C, E e $F \in k[x_2, x_3]$ devem ser divisíveis por x_2. Por isso

$$\Delta \equiv -C(\lambda,\mu)D^2(\lambda,\mu) \mod \lambda^2.$$

Como C é linear, $C(x_2, x_3) = cx_2$ para algum $c \in k$, e como S é suave em $P = (0 : 1 : 0 : 0)$ segue que $c \neq 0$. Logo $\Delta(\lambda,\mu)$ não é divisível por λ^2 como se quer. □

Corolário 6.10.1. *Dada uma reta l existe uma reta m reversa a l.*

Figura 23 – Uma reta reversa m reversa à reta l.



Fonte: Elaborado pelo autor (2023).

Prova. Aplicando a proposição a l_1 temos que as retas m e m' existem. Suponha que m não seja reversa a l_1, nesse caso existiria um plano E_i tal que E_i contém m, l, l_i, l'_i, teríamos $E_i \cap S = \{m, l, l_i, l'_i\}$, um absurdo pela Proposição 2.1. □

Para discutir como retas se encontram em uma cúbica precisamos dos próximos resultados. Dizer que duas retas se intersectam transversalmente significa que elas se intersectam em um único ponto.

Lema 6.11. *Se as retas $l_1, \ldots, l_4$ em $\mathbb{P}^3_k$ são disjuntas, então uma, e apenas uma, das afirmações a seguir é válida:*

(1) *$l_1, \ldots, l_4$ se encontram sobre uma quádrica suave Q. Nesse caso, existem infinitas retas que intersectam $l_1, \ldots, l_4$ transversalmente.*

(2) *$l_1, \ldots, l_4$ não estão em nenhuma quádrica. Então existem uma ou duas retas transversais comuns.*

Prova. Primeiro vamos mostrar que as retas l_1, l_2 e l_3 estão contidas em uma superfície quádrica Q. Como a dimensão do espaço de polinômios homogêneos de grau 2 em 4 variáveis é dado por[6]

$$\dim k^2[x_0, x_1, x_2, x_3] = 10,$$

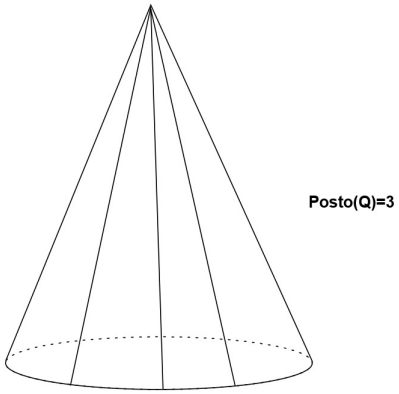
o espaço das quádricas em $\mathbb{P}^3_k$ pode ser considerado como um espaço projetivo de dimensão 9. O requisito de que a quádrica $Q = \{f = 0\}$ passe por um ponto dado, é uma condição

[6] A dimensão de um polinômio homogêneo em n variáveis de grau d é dada por $D = \binom{(n-1)+d}{(n-1)}$.

linear nos coeficientes de f. Para uma reta l se encontrar em uma quádrica Q, é suficiente mostrar que três pontos distintos em l estão em Q, caso contrário, $l \cap Q$ consistiria de no máximo 2 pontos. Logo, o requisito para que três retas se encontrem em uma quádrica pode ser expresso exibindo 9 condições lineares. Como o espaço das quádricas é uma espaço projetivo de dimensão 9, significa que existe ao menos uma quádrica Q contendo as três retas.

Precisamos mostrar que Q é suave. Como as retas l_1, l_2, l_3 são disjuntas, Q não é a união de dois planos, já que quaisquer duas retas em um plano se intersectam. De modo similar Q não pode ser uma quádrica de posto 3, pelo Lema 6.7 Q é suave se, e somente se, tem posto máximo igual a 4, em uma quádrica de posto 3 toda reta passa pela única singularidade de Q, i.e., pelo vértice do cone, como mostrado na figura a seguir. Isso pode ser visto considerando a projeção a partir do vértice. Retas passam pelo vértice, ou são levadas a pontos, ou são levadas a retas. Mas a imagem é uma curva quádrica suave, e portanto não contém quaisquer retas.

Figura 24 – Retas em um cone quadrático
(uma quádrica de posto 3 em $\mathbb{P}^3_k$).



Fonte: Ver (1) página 156. (2000)

Logo Q é uma quádrica suave contendo l_1, l_2, l_3. Sendo disjuntas, essas retas se encontram na mesma decisão em Q. (Ver Exemplo 3.10 para a definição de decisão em uma quádrica.)

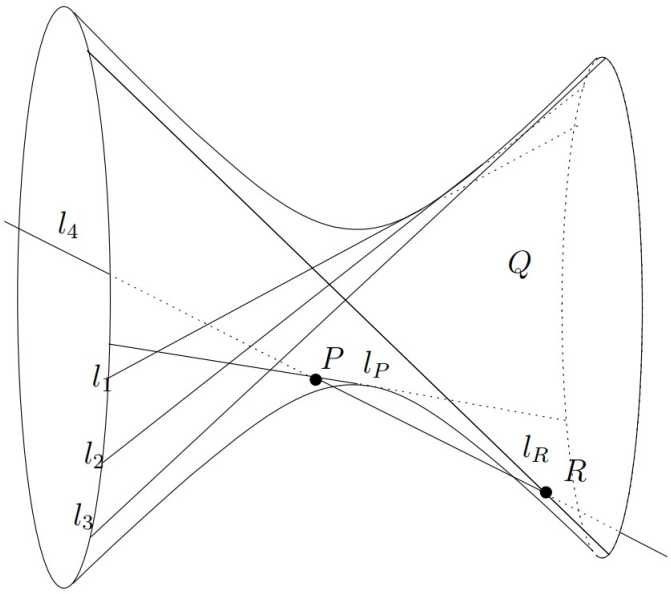
Temos as seguintes possibilidades:

(1) $l_4 \subset Q$. Então, l_4 deve estar na mesma decisão que l_1, l_2, l_3 e existem infinitas retas transversais, dadas pelas retas na outra decisão em Q.

(2) $l_4 \not\subset Q$. Então, $l_4 \cap Q$ consiste de um ou dois pontos. Se l_4 encontra Q em pontos distintos P e R, como mostrado na figura a seguir, então as retas l_P e l_R em Q passando por P e R, respectivamente, que não estão na mesma decisão que l_1, l_2 e l_3,

intersectam todas as quatro retas transversalmente. Se l_4 encontra Q em um único ponto, obtemos uma uma reta em Q transversal às quatro retas l_1, l_2, l_3, l_4. Note que qualquer reta intersectando l_1, l_2 e l_3, intersecta Q em ao menos 3 pontos, por isso está contida em Q, e, portanto, descrevemos todas as possíveis retas que intersectam l_1, l_2, l_3, l_4 transversalmente.

Figura 25 – As duas retas l_P e l_R na quádrica Q são transversais a l_1, l_2, l_3 e l_4.



Fonte: Ver (1) página 157. (2000)

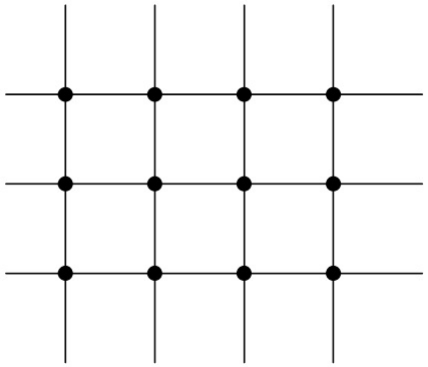
□

Observação 6.12. *Uma quádrica singular e uma quádrica suave são projetivamente equivalentes às quádricas mostradas nas respectivas figuras.*

Como um corolário do lema acima, temos o seguinte resultado sobre a possível configuração de retas em uma superfície cúbica suave.

Lema 6.13. *Se S é uma cúbica suave, então S não pode conter quatro retas reversas m_1, m_2, m_3, m_4 as quais são todas intersectadas por três retas n_1, n_2, n_3. Ou seja, S não pode conter 7 retas com a configuração da figura abaixo.*

Figura 26 – Configuração de retas não pode estar contida em uma superfície cúbica suave.



Fonte: Ver (1) página 158. (2000)

Prova. Suponha que tenhamos tal configuração em S. Como $m_1, \ldots, m_4$ são intersectadas por três retas, o Lema 6.11 implica que elas se encontram em uma quádrica Q. Então, m_i estão em uma decisão em Q, e n_i estão na outra. Todo ponto $P \in Q$ está contido em uma reta L na mesma decisão que n_i. A reta L intersecta m_1, m_2, m_3 e m_4. Isso nos dá 4 pontos em $L \cap S$. Mas uma cúbica e uma reta se intersectam no máximo em três pontos, a menos que $L \subset S$. Por isso, $P \in S$ para todo $P \in Q$, logo $Q \subset S$. Portanto existe uma decomposição $S = Q \cup H$ para algum hiperplano H. Mas $Q \cup H$ é singular ao longo de interseção $Q \cap H$, se $f = g.h$, os pontos $x \in V(g) \cap V(h)$ são pontos singulares, basta olhar para as derivadas parciais, por exemplo, $\dfrac{\partial f}{\partial x_i} = \dfrac{\partial g}{\partial x_i}.h + g.\dfrac{\partial h}{\partial x_i}$. Obtemos uma contradição. □

Vamos precisar do resultado sobre retas em uma superfície cúbica dada pela Proposição 6.10.

Lema 6.14. *Se l, l_i e l_i' são retas em uma superfície cúbica S como na Proposição 6.10, então qualquer outra reta m em S deve intersectar exatamente uma delas, l, l_i ou l_i'.*

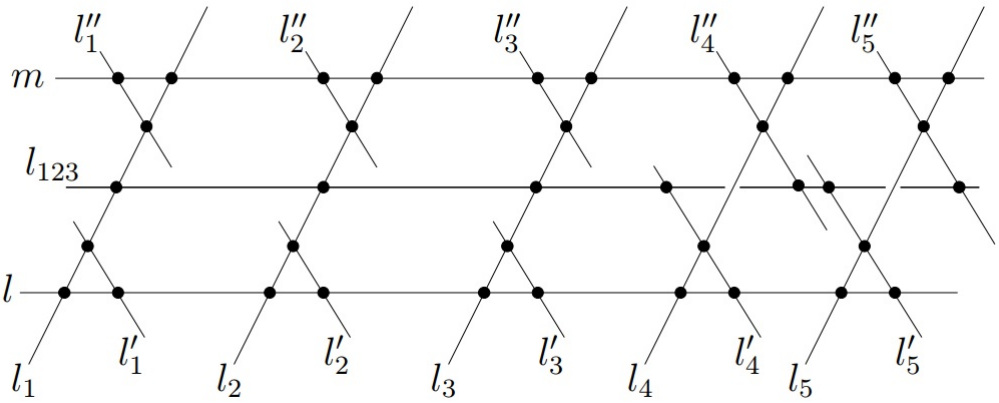
Prova. Seja E_i um plano com $E_i \cap S = l \cup l_i \cup l_i'$. Então, m intersecta o plano E_i, já que uma reta e um plano em $\mathbb{P}_k^3$ sempre se intersectam. Por isso $\mathbf{m} \cap (\mathbf{l} \cup \mathbf{l_i} \cup \mathbf{l_i'}) = \mathbf{m} \cap (\mathbf{E_i} \cap \mathbf{S})$ $= (\mathbf{m} \cap \mathbf{S}) \cap \mathbf{E_i} = \mathbf{m} \cap \mathbf{E_i} \neq \emptyset$. Logo, m intersecta ao menos uma das três retas. **Se m intersecta mais de uma reta**, m intersecta E_i em dois pontos, nesse caso está contida em E_i, contradizendo a Proposição 6.9(1), ou m intersecta duas das retas em um único ponto em S, e pela Proposição 6.9(2) implica que m está contido em E_i, novamente contradizendo a Proposição 6.9(1), logo m deve intersectar somente uma delas. □

Teorema 6.15. *Uma superfície cúbica suave S contém exatamente 27 retas.*

Prova. Pelo Teorema 6.1, S contém uma reta l. A Proposição 6.10 nos dá 5 pares de retas $(l_i, l'_i),\ i = 1, \ldots, 5$, intersectando l.

Seja $m \subset S$ uma reta reversa a l, que existe pela aplicação do Corolário 6.10.1 a l_1. Pelo Lema 6.14, a reta m intersecta exatamente uma das retas l_i e l'_i para $i = 1, \ldots, 5$. Por renomeação, se necessário, podemos assumir que m intersecta cada uma das retas $l_1, l_2, \ldots, l_5$ e não intersecta nenhuma das retas $l'_1, l'_2, \ldots, l'_5$. Pela Proposição 6.10, existem 5 pares de retas intersectando m, que devem ser da forma (l_i, l''_i), para $i = 1, \ldots, 5$. Temos que l''_i são todas diferentes de l'_j, caso contrário, se $l''_i = l'_i$, l e m estariam no plano $l_i \cup l'_i = l_i \cup l''_i$, nos dando quatro retas coplanares l, m, l_i, l'_i, contradizendo a Proposição 6.9. Até agora, encontramos 17 retas, l, m, l_i, l'_i e l''_i para $i = 1, \ldots, 5$.

Figura 27 – A configuração de 18 das 27 retas em uma superfície cúbica. Os 20 pontos de interseção da forma $l'_i \cap l''_j$ para $1 \leq i < j \leq 5$ não são mostrados.



Fonte: Ver (1) página 159. (2000)

Pelo Lema 6.14, cada l''_i deve intersectar uma das retas l, l_j ou l'_j. Mas a Proposição 6.10(2) implica que $l''_i \cap l_j = \emptyset$ para $i \neq j$ e, como foi visto, $l''_i \cap l = \emptyset$. Logo $l''_i \cap l'_j \neq \emptyset$ para $i \neq j$.

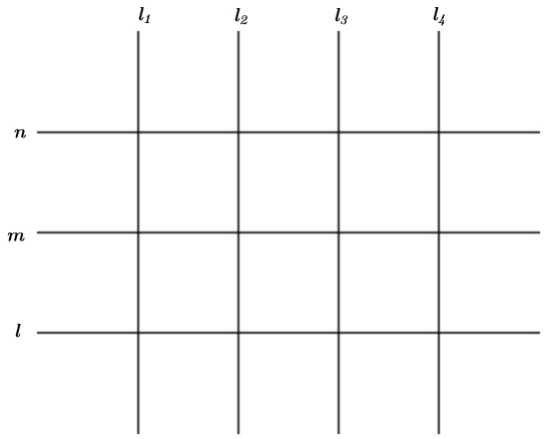
Nos resta encontrar mais 10 retas. Para cada uma das 10 triplas (i, j, k) com $1 \leq i < j < k \leq 5$[7], seja $l_{i,j,k}$ um reta diferente de e reversa com respeito a l e m, que intersecta l_i, l_j e l_k. Vamos mostrar que existe exatamente uma reta desse tipo para cada tripla (i, j, k) e que qualquer reta em S que não é igual a uma das 17 retas já encontradas deve ser igual a uma dessas 10 retas.

Suponha que n é uma reta em S que não é igual a uma das 17 retas já encontradas. Note que n não pode intersectar l ou m, já que todas as retas intersectando l ou m são dadas pelas l_i, l'_i e l''_i. Vamos mostrar agora que n intersecta exatamente 3 das retas l_i, excluindo as alternativas.

[7] (3,4,5),(2,4,5),(1,4,5),(2,3,5),(1,3,5),(1,2,5),(2,3,4),(1,3,4),(1,2,4),(1,2,3).

(1) n não pode intersectar 4 das retas l_i. Se fosse esse o caso, as três retas reversas l, n e m seriam todas transversais a essas quatro l_i reversas, contradizendo o Lema 6.13.

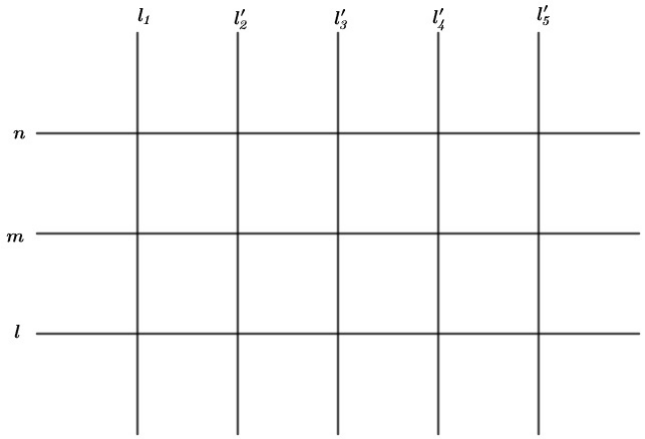
Figura 28 – Caso 1.



Fonte: elaborado pelo autor. (2023)

(2) n não pode intersectar menos que duas das l_i. Nesse caso, pelo Lema 6.14, a reta n intersectaria ao menos 4 das l'_i, o que de novo entra em contradição com o Lema 6.13.

Figura 29 – Caso 2.

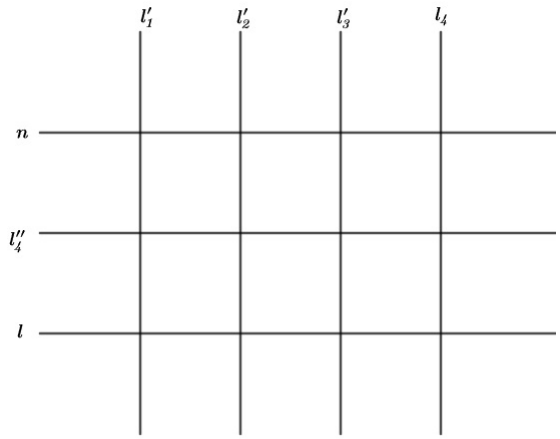


Fonte: elaborado pelo autor. (2023)

(3) n não pode intersectar exatamente duas das retas l_i. Nesse caso, podemos assumir que n não intersecta l'_1, l'_2, l'_3, l_4 e l_5. Mas agora n, l e l''_4 seriam transversais comuns[8] a l'_1, l'_2, l'_3 e l_4, contradizendo novamente o Lema 6.13

[8] $l''_i \cap l'_j \neq \emptyset$ para $i \neq j$.

Figura 30 – Caso 3.



Fonte: elaborado pelo autor. (2023)

Por isso, n intersecta exatamente três das retas l_i para $i = 1, \ldots, 5$.

Precisamos mostrar agora que l_{ijk} é única. Suponha que existam duas retas l_{ijk} e l'_{ijk} diferente de e reversa às retas l e m, as quais intersectam l_i, l_j e l_k. Se l_{ijk} e l'_{ijk} se intersectam, então todas as 5 retas l_i, l_j, l_k, l_{ijk} e l'_{ijk} estão em um mesmo plano, contradizendo a Proposição 6.9. Logo, temos três retas reversas l_i, l_j e l_k as quais intersectam 4 retas reversas l, m, l_{ijk} e l'_{ijk} transversalmente. Novamente, pelo Lema 6.13 isso é uma contradição.

Finalmente, devemos mostrar que todas as retas l_{ijk} existem. Pela Proposição 6.10, l_1 intersecta 10 retas distintas. Quatro dessas retas são dadas por l, l'_1, m e l''_1. Pelo argumento acima, as seis retas remanescentes devem ser da forma l_{1jk} para alguma tripla $(1, j, k)$ com $1 < j < k \leq 5$. Mas essas são exatamente $\binom{4}{2} = 6$ triplas dessa forma e, portanto, todas as retas l_{1jk} existem. Um argumento similar prova a existência de todas as retas l_{ijk}.

Acabamos de construir as 27 retas em S, dadas por

$$\{l, m, l_i, l'_i, l''_i, l_{ijk} \mid 1 \leq i < j < k \leq 5\}.$$

□

Resumindo, temos que uma superfície cúbica suave S contém 27 retas,$l, m, l_i, l'_i, l''_i, l_{ijk}$

para $i < j < k \leq 5$. Cada reta intersecta 10 outras, como se segue:

$$
\begin{aligned}
l &\text{ intersecta } l_1, \ldots, l_5 \text{ e } l'_1, \ldots, l'_5, \\
m &\text{ intersecta } l''_1, \ldots, l''_5 \text{ e } l_1, \ldots, l_5, \\
l_1 &\text{ intersecta } l, m, l'_1, l''_1, \text{ e } l_{1jk} \text{ para } 2 \leq j < k \leq 5, \\
l'_1 &\text{ intersecta } l, l_1, l''_j \text{ para } 2 \leq j \leq 5 \text{ e } l_{234}, l_{235}, l_{245}, l_{345}, \\
l''_1 &\text{ intersecta } m, l_1, l'_j \text{ para } 2 \leq j \leq 5 \text{ e } l_{234}, l_{235}, l_{245}, l_{345}, \\
l_{123} &\text{ intersecta } l_1, l_2, l_3, l'_4, l''_4, l'_5, l''_5 \text{ e } l_{145}, l_{245}, l_{345}.
\end{aligned}
$$

A interseção das demais retas é encontrada pela permutação adequada dos índices.

7 CONCLUSÃO

Pode-se ver, então, que toda superfície cúbica sobre um corpo algebricamente fechado contém, de fato, 27 retas. As ferramentas aqui apresentadas, mesmo que não tenham sido utilizadas explicitamente para este resultado, ainda são de caráter importante para o estudo de curvas e para o que se segue no contexto de geometria algébrica.

REFERÊNCIAS

1 [Hu] K. Hulek. *Elementary Algebraic Geometry*. American Mathematical Society 2003.

2 [Ma] H. Matsumura.*Commutative Algebra*. W.A Benjamin 1970.

3 [AM] M. F. Atiyah e I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley 1969.

4 [Ue] K. Ueno. *Algebraic Geometry I: From algebraic varieties to schemes; American Mathematical Society 1997.*

5 [La] S. Lang *Algebra; Graduate Texts in Mathematics 2002.*

6 [Ar] M. Artin *Algebra; Segunda edição; Pearson 2014.*

7 [Rh] R. Hartshorne *Algebraic Geometry; Springer; Primeira edição 1977.*

8 [AS] A. Altman, S.Kleiman.*A Term of Commutative Algebra*. World Center of Mathematics 2013.

9 [Rh] R. Hazrat.*Graded Rings and Graded Grothendieck Groups*. London Mathematical Society 2016.

10 [Rm] M. Reid. *Undergraduate Algebraic Geometry*. LMS Student Texts 12,Cambridge University Press 1988.

11 [Co] Sobre a história das superfícies cúbicas: https://mathshistory.st-andrews.ac.uk/HistTopics/Cubic_surfaces/.

12 [Fu] W. Fulton. *Algebraic Curves: an introduction to algebraic geometry* 2008.

APÊNDICE A – Alguns resultados de Álgebra Comutativa

Neste apêndice abordaremos alguns conceitos de álgebra comutativa, normalização de Noether, corpos de característica positiva e e redução ao caso de uma hipersuperfície.

Lema 1. *Seja $C \subset B \subset A$ anéis.*

(1) *Se B é uma C-álgebra finita e A é uma B-álgebra finita, então A também é uma C-álgebra finita;*

(2) *Se A é uma B-álgebra finita, então A é* ***integral sobre B****, i.e, todo elemento $x \in A$ satisfaz uma equação da forma*

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 = 0. \qquad (b_i \in B).$$

(3) *Por outro lado, se $x \in A$ satisfaz uma equação da forma acima, então $B[x]$ é uma B-álgebra finita.*

Prova. (1) Se $B = Cb_1 + \ldots + Cb_m$ e $A = Ba_1 + \ldots + Ba_n$, então $A = Ca_1b_1 + \ldots + Ca_nb_m$.

(2) Provaremos isso usando um "truque de determinante". Suponha que

$$A = Ba_1 + \ldots + Ba_n.$$

Então para cada $x \in A$ temos $xa_i \in A$ para $i = 1, \ldots, n$. Portanto existem elementos $b_{ij} \in B$ tal que

$$xa_i = \sum_{j=1}^{n} b_{ij}a_j. \qquad (.1)$$

Para obter uma única equação polinomial para x destas n equações lineares, a expressamos em notação matricial, e tomamos o determinante da matriz. Primeiro note que (.1) é equivalente a

$$\sum_{j=1}^{n}(x\delta_{ij} - b_{ij})a_j = 0,$$

o que em notação matricial pode ser escrito como

$$Ma = 0, \qquad (.2)$$

onde M é a matriz dada por

$$M := (x\delta_{ij} - b_{ij})_{i,j}$$

e a é o vetor coluna com transposta ${}^t a = (a_1, \ldots, a_n)$. Se M^{adj} é a matriz adjunta de M, então segue de (.2) que

$$\det Ma = M^{\mathrm{adj}} Ma = 0,$$

então $\det Ma_i = 0$ para $i = 0, \ldots, n$. Como os a_i geram a B-álgebra A, temos

$$\det M = \det M \cdot 1 = 0.$$

No entanto, expandindo o determinante, também temos

$$\det M = x^n + b_{n-1}x^n + \ldots + b_1 x + b_0$$

para algum $b_i \in B$. Logo x satisfaz uma equação polinomial com coeficientes em B.

(3) Nesse caso temos $B[x] = B + Bx + \ldots + Bx^{n-1}$, e $B[x]$ é uma B-álgebra finita.

□

Definição 1. *Um polinômio $f \in B[x]$ é chamado de* ***mônico*** *se o coeficiente do termo líder é igual a 1, como no item* (2) *do Lema 1.*

Lema 2 (Lema de Nakayama)**.** *Seja $A \neq 0$ uma B-álgebra finita. Então para todos os ideais próprios m de B temos $mA \neq A$.*

Prova. Como no Lema 1 item (2), consideramos o determinante de uma matriz. Já que A é uma B-álgebra finita, podemos escrever $A = Ba_1 + \ldots + Ba_n$ para algum $a_i \in A$. Suponha que $mA = A$. Então existe $b_{ij} \in m$ para $1 \leq i, j \leq n$ tal que

$$a_i = \sum_{j=1}^{n} b_{ij} a_j, \qquad 1 \leq i \leq n.$$

Desse resultado podemos concluir que

$$\det(\delta_{ij} - b_{ij}) = 0.$$

Expandindo o determinante pode-se ver que $1 \in m$, que é uma contradição. □

Lema 3. *Seja A um corpo e $B \subset A$ um subanel tal que A é uma B-álgebra finita. Então B também é um corpo.*

Prova. Seja $0 \neq b \in B$. Já que A é um corpo, existe $b^{-1} \in A$. Devemos mostrar que b^{-1} está em B. Pelo item (2) do Lema 1, temos que

$$b^{-n} + b_{n-1}b^{-(n-1)} + \ldots + b_1 b^{-1} + b_0 = 0 \qquad \text{para } b_i \in B, \forall i = 0, \ldots, n-1.$$

Multiplicando por b^{n-1} temos

$$b^{-1} = -(b_{n-1} + b_{n-2}b + \ldots + b_0 b^{n-1}) \in B.$$

□

Observação 1. *O* ***grau*** *de um monômio $x_1^{\nu_1} \dots x_n^{\nu_n}$ é definido como a soma $\sum \nu_i$, e o grau de um polinômio é o máximo dos graus de seus monômios.*

Para a prova da Normalização de Noether, precisaremos do próximo lema.

Lema 4. *Suponha que f é um elemento não nulo de $k[x_1, \dots, x_n]$ com $d = \deg f$. Então existe uma mudança de variáveis $x_i' = x_i - \alpha_i x_n$ para $1 \leq i \leq n-1$, onde $\alpha_1, \dots, \alpha_{n-1} \in k$, tal que o polinômio $f(x_1' + \alpha_1 x_n, \dots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \in k[x_1', \dots, x_{n-1}', x_n]$ tem um termo da forma cx_n^d para algum $0 \neq c \in k$.*

Prova. De fato, "quase" qualquer escolha de α_i vai funcionar (veremos numa observação à frente). Seja $x_i' = x_i - \alpha_i x_n$ para alguma escolha de $\alpha_i \in k$ para $1 \leq i \leq n-1$. Como $d = \deg f$, podemos escrever

$$f = F_d + G,$$

onde F_d é uma soma de monômios de grau d (i.e., F é homogêneo de grau d), e $\deg G \leq d-1$. Logo

$$\begin{aligned} &f(x_1' + \alpha_1 x_n, \dots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \\ &= F_d(\alpha_1, \dots, \alpha_{n-1}, 1) x_n^d + \text{ termos de ordem inferior em } x_n. \end{aligned}$$

Agora $F_d(\alpha, \dots, \alpha_{n-1}, 1)$ é um polinômio em $\alpha_1, \dots, \alpha_{n-1}$ diferente de zero, logo o conjunto dos zeros é diferente de $\mathbb{A}_k^{n-1}$ (aqui usamos o fato de que k tem infinitos elementos). Isto significa que podemos escolher $\alpha_1, \dots, \alpha_{n-1} \in k$ com $F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. Isto completa a prova, pois obtemos $c = F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. □

Chegamos ao Teorema da normalização de Noether, veremos a seguir que esse teorema tem um importante significado geométrico, em particular, a interpretação geométrica da normalização de Noether nos dá uma indicação de como a ideia geométrica de dimensão está relacionada com a estrutura algébrica do anel de coordenadas de uma variedade, que será visto mais à frente.

Teorema 1 (**Normalização de Noether**). *Seja k um corpo com infinitos elementos e seja $A = k[a_1, \dots, a_n]$ uma k-álgebra finitamente gerada. Então existem $y_1, \dots, y_m \in A$, com $m \leq n$, tal que*

(1) *$y_1, \dots, y_m$ são algebricamente independentes sobre k, e*

(2) *A é uma $k[y_1, \dots, y_m]$-álgebra finita.*

Antes da prova, uma observação:

Observação 2. *O fato de que os $y_1, \dots, y_m$ serem algebricamente independentes (i.e, eles não satisfazem nenhuma equação polinomial com coeficiente em k), é equivalente à*

afirmação de que o mapa do anel de polinômios $k[t_1, \ldots, t_m]$ em m variáveis sobre k para $k[y_1, \ldots, y_m]$, dado por $t_i \mapsto y_i$, ser um isomorfismo.

Prova. Provaremos este resultado utilizando indução sobre n. Seja $k[x_1, \ldots, x_n]$ o anel de polinômios sobre k em n variáveis, e seja

$$I := \ker(k[x_1, \ldots, x_n] \to k[a_1, \ldots, a_n] = A)$$

o núcleo do homomorfismo dado por $x_i \mapsto a_i$. Se $I = 0$ então podemos tomar $m = n$ e $y_1 = a_1, \ldots, y_n = a_n$, claramente (1) e (2) são válidos. Se este não é o caso, então existe um elemento não nulo $f \in I$. Se $n = 1$, então temos $f(a_1) = 0$, então o resultado segue do Lema 1 item (3), com $m = 0$, i.e., com o conjunto dos y_i sendo vazio. Assumimos agora que $n > 1$ e que o resultado é verdade para $n - 1$. O Lema 4 nos dá elementos $\alpha_1, \ldots, \alpha_{n-1} \in k$ tal que, definindo $a'_i := a_i - \alpha_i a_n$ e $A' := k[a'_1, \ldots, a'_{n-1}] \subset A$, temos que para uma constante não nula $c \in k$, o polinômio

$$F(x_n) := \frac{1}{c} f(a'_1 + \alpha_1 x_n, \ldots, a'_{n-1} + \alpha_{n-1} x_n, x_n)$$

é um polinômio mônico em $A'[x_n]$, e $F(a_n) = 0$. Pelo Lema 1 item (3) isto implica que a_n é integral sobre A'.

Pela hipótese de indução existem $y_1, \ldots, y_m \in A'$ com as seguintes propriedades:

(1) $y_1, \ldots, y_m$ são algebricamente independentes sobre k,

(2) A' é uma $k[y_1, \ldots, y_m]$-álgebra finita.

Pelo Lema 1 item (3) temos que $A = A'[a_n]$ é uma A'-álgebra finita, por (2) e pelo Lema 1 item (1) temos também que A é uma $k[y_1, \ldots, y_m]$-álgebra finita.

Observação 3. *Analisando a prova anterior, vemos que $y_1, \ldots, y_m$ podem ser tomados como uma escolha "geral" de formas lineares em $a_1, \ldots, a_n$, já que mudanças lineares sucessivas de coordenadas pelo Lema 4 podem ser tomadas deste jeito. O que se quer dizer por isso é, uma coleção de m-uplas de formas lineares em $a_1, \ldots, a_n$ forma um espaço afim $\mathbb{A}_k^{nm}$. Dizer que o conjunto de formas lineares é geral com respeito à alguma propriedade significa que existe um subconjunto aberto de Zariski de $\mathbb{A}_k^{nm}$ tal que para cada ponto neste conjunto, o conjunto correspondente de formas lineares satisfaz tal propriedade, i.e, a propriedade é verdadeira para um conjunto denso de formas lineares. O conceito de objetos "gerais" quer dizer objetos parametrizados pelos pontos de um conjunto denso e aberto de uma variedade, é frequentemente usado em geometria algébrica.*

Prova (Teorema 2.28)**.** Seja $A = k[a_1, \ldots, a_n]$ uma k-álgebra finitamente gerada, e suponha que A é um corpo. Pela normalização de Noether (Teorema 1) segue que $y_1, \ldots, y_m \in A$ para algum $m \leq n$ tal que, definindo $B = k[y_1, \ldots, y_m] \subset A$ temos que A é uma B-álgebra

finita. Pelo Lema 3, B é um corpo. Mas isso só pode acontecer se $m = 0$. Então A é uma extensão finita de k, e consequentemente algébrica sobre k. □.

APÊNDICE B – O significado Geométrico da normalização de Noether

Seja $A \subset \mathbb{A}_k^n$ uma variedade, que por simplicidade vamos assumir ser irredutível, i.e., assumimos que o ideal $I = I(X) \subset k[x_1, \ldots, x_n]$ é primo. Consideremos o anel

$$A = k[a_1, \ldots, a_n] = k[x_1, \ldots, x_n]/I,$$

onde $a_i := x_i \mod I$. (Mais tarde vamos nos referir a A como o *o anel de coordenadas de* X). A normalização de Noether nos diz que existem formas lineares algébricas independentes $y_1, \ldots, y_m$ em $a_1, \ldots, a_n$ tal que A é uma $k[y_1, \ldots, y_m]$-álgebra. Essas formas lineares se levantam (não unicamente) para as formas $\tilde{y_1}, \ldots, \tilde{y_m}$ em $x_1, \ldots, x_n$ onde $\tilde{y_i} \equiv y_i \mod I$. As formas $\tilde{y_1}, \ldots, \tilde{y_m}$ definem uma projeção linear

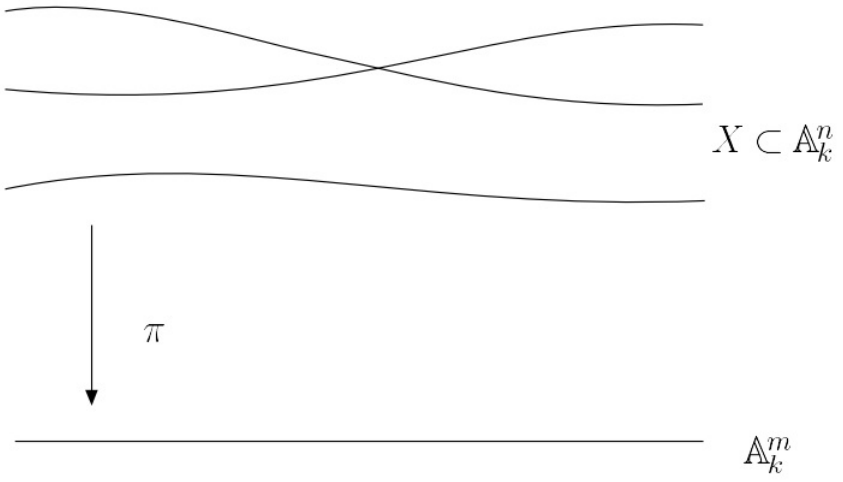
$$\pi := (\tilde{y_1}, \ldots, \tilde{y_m}) : \qquad \mathbb{A}_k^n \longrightarrow \mathbb{A}_k^m.$$

Restringindo $\tilde{y_1}, \ldots, \tilde{y_m}$ a X, obtemos o mapa

$$\phi := \pi|_X \ : \qquad X \longrightarrow \mathbb{A}_k^m.$$

Em X temos $y_i|_X = \tilde{y_i}|_X$, e então ϕ é independente da escolha do levantamento $\tilde{y_i}$. Vamos mostrar agora que as *fibras*[1] são finitas e não vazias, como na imagem a seguir.

Figura 31 – Significado geométrico da normalização de Noether: ϕ é sobrejetiva com fibras finitas.



Fonte: Ver (1) página 32. (2000)

Proposição 1. *Suponha que $k = \bar{k}$, e seja ϕ definido como anteriormente. Então para cada ponto $P \in \mathbb{A}_k^m$ a fibra $\phi^{-1}(P)$ é finita e não vazia.*

[1] Pode-se entender fibras aqui como a imagem inversa do mapa em questão.

Prova. Primeiro demonstraremos que $\phi^{-1}(P)$ é finita. Pelo Lema 1 item (2), temos que existem inteiros N e polinômios $f_0^i, \ldots, f_{N-1}^i$ para $1 \leq i \leq n$ tais que para $i = 1, \ldots, n$ temos

$$a_i^N + f_{N-1}^i(y_1, \ldots, y_m)a_i^{N-1} + \ldots + f_0^i(y_1, \ldots, y_m) = 0.$$

Isso significa que com $I = I(X)$ como anteriormente, temos

$$x_i^N + f_{N-1}^i(\tilde{y_1}, \ldots, \tilde{y_m})x_i^{N-1} + \ldots + f_0^i(\tilde{y_1}, \ldots, \tilde{y_m}) = g_i(x_1, \ldots, x_n)$$

para algum $g_i \in I$. Se $(x_1, \ldots, x_n) \in X$, então $g_i(x_1, \ldots, x_n) = 0$, logo x_i é uma solução da equação $f^i(x) = 0$, onde

$$f^i(x) := x^N + f_{N-1}^i(y_1, \ldots, y_m)x^{N-1} + \ldots + f_0^i(y_1, \ldots, y_m).$$

Como I é primo, $A = k[a_1, \ldots, a_n]$ é um domínio de integridade e portanto tem um corpo de frações $k(a_1, \ldots, a_n)$, podemos considerar $f^i(x) \in k(a_1, \ldots, a_n)[x]$. Pelo teorema fundamental da álgebra existe um número finito de soluções x_i^0 para $f^i(x) = 0$. Então, para qualquer ponto $\mathbf{Y} = (y_1, \ldots, y_m) \in \mathbb{A}_k^m$ temos somente um número finito de pontos $\mathbf{X} = (x_1^0, \ldots, x_n^0) \in X$ com $\phi(\mathbf{X}) = \mathbf{Y}$. Para mostrar que $\phi^{-1}(P)$ é sempre não vazio, é suficiente mostrar que para cada ponto $P = (b_1, \ldots, b_m) \in \mathbb{A}_k^m$ nós teremos

$$I_P := I + (y_1 - b_1, \ldots, y_m - b_m) \neq k[x_1, \ldots, x_n]. \tag{.1}$$

Utilizando o Nullstellensatz de Hillbert, temos que $\phi^{-1}(P) = V(I_P) \neq \emptyset$. A equação (.1) é equivalente a $(y_1 - b_1, \ldots, y_m - b_m) \neq k[a_1, \ldots, a_n]$. Já que $(y_1 - b_1, \ldots, y_m - b_m)$ é um ideal maximal em $k[y_1, \ldots, y_m]$ (c.f Nullstellensatz de Hillbert), em particular é um ideal próprio, (.1) segue do Lema de Nakayama (Lema 2) com $B = k[y_1, \ldots, y_m]$, $A = k[a_1, \ldots, a_n]$ e $m = (y_1 - b_1, \ldots, y_m - b_m)$. □

Exemplo 1. *Seja $f := x_1x_2 + x_2x_3 + x_3x_1 \in k[x_1, x_2, x_3]$. Para a hipersuperfície quádrica $S := V(f) \subset \mathbb{A}_k^3$, temos $A = k[x_1, x_2, x_3]/(f)$, e como anteriormente, usamos a notação $a_i = x_i \mod (f)$ para $i = 1, 2, 3$. Na prova do Teorema 1, já que f não contém nenhum termo da forma x_i^m, podemos fazer uma mudança de variável. Por exemplo, seja $z = x_2 + x_1$. Então $f = z(x_1 + x_3) - x_1^2$. Agora A é algébrica sobre $k[a_1 + a_2, a_3]$, e o mapa ϕ correspondente é dado por*

$$\begin{aligned} \phi : \quad & S \longrightarrow \mathbb{A}_k^2, \\ & (x_1, z, x_3) \longmapsto (z, x_3). \end{aligned}$$

A fibra $\phi^{-1}(a, b) = \{(x, a, b) \mid x^2 - ax - ab = 0\}$ consiste de pelo menos dois pontos.

Note que S contém o eixo coordenado, então para qualquer escolha de $1 \leq i < j \leq 3$, a projeção para o plano x_i, x_j,

$$\begin{aligned} S &\longrightarrow \mathbb{A}_k^2, \\ (x_1, x_2, x_3) &\longmapsto (x_i, x_j), \end{aligned}$$

tem uma fibra infinita sobre $(0,0)$. De modo similar, se $(a,b,c) \in S$, então S contém a reta $L := \{(\lambda a, \lambda b, \lambda c) \mid \lambda \in k\}$, e a projeção $(x_1, x_2, x_3) \mapsto (bx_1 - ax_2, cx_1 - ax_3)$ leva L para $(0,0)$. No entanto, existe um conjunto denso de hiperplanos tal que a projeção correspondente tem um número finito de fibras.

Observação 4. *O inteiro m dado na normalização de Noether é o* grau de transcendência *do corpo de frações da k-álgebra K. Na Proposição 1 vimos que quando K é o anel coordenado de uma variedade afim X, existe um mapa sobrejetivo para $\mathbb{A}_k^m$ com fibras finitas. Já que $\mathbb{A}_k^m$ deveria ter dimensão m, seria razoável esperar que X tenha dimensão m. Mais à frente daremos uma definição rigorosa de dimensão e veremos que essa ideia intuitiva faz sentido. Vamos mostrar também que isso é verdade num caso mais geral, que a dimensão de uma variedade afim é igual ao grau de transcendência do seu corpo de funções (Teorema 4.21).*

APÊNDICE C – Corpos de característica positiva

Como mencionado anteriormente, a normalização de Noether (Teorema 1) tem consequências relevantes, queremos garantir que essas consequências também são válidas no caso de corpos com característica positivas. Primeiro, lembremos que a **a característica de um corpo** k, char (k), é o menor primo p tal que

$$p \cdot 1 = \underbrace{1 + \cdots + 1}_{\text{p vezes}} = 0,$$

e a característica é dita zero quando tal primo não existe. Por exemplo para qualquer primo p o corpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ e seu fecho algébrico têm ambos característica p. O corpo $\mathbb{C}$ e seus subcorpos têm todos característica 0.

Definição 2. *Um polinômio irredutível não constante*

$$f = a_n x^n + \ldots + a_1 x + a_0 \in k[x]$$

é chamado ***separável*** *se a derivada formal é diferente de 0, i.e.,*

$$f' = n a_n x^{n-1} + \ldots + a_1 \neq 0.$$

Do contrário f é dito ***inseparável****. Um polinômio arbitrário é dito separável se cada fator é separável. Um polinômio irredutível $f \in k[x_1, \ldots, x_n]$ é chamado de separável com respeito à variável x_i se a derivada formal com respeito a essa variável é diferente de zero.*

Observação 5. *Pode-se ver que todos os polinômios não constantes sobre um corpo de característica 0 são separáveis, e um polinômio irredutível $f \in k[x]$ sobre um corpo de característica p é separável se, e somente se, $f(x) = g(x^p)$ para algum $g \in k[x]$. Por exemplo, $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$ é um polinômio inseparável irredutível em característica p. Em característica p a identidade de Frobenius $a^p + b^p = (a + b)^p$ implica que se k é algebricamente fechado então podemos escrever $f(x) = g(x^p) = h(x)^p$, onde $h(x)$ é obtido de $g(x)$ substituindo todos os coeficientes pela sua p-ésima raiz.*

Definição 3. *Se K/k é uma uma extensão de corpos e $x \in K$ é algébrica sobre k, então x é chamado de* ***separável*** *sobre k, se o polinômio mínimo de x é separável sobre k. Caso contrário, x é inseparável.*

Definição 4. *Uma extensão algébrica K/k é chamada de* ***separável*** *se, todos os elementos de K são separáveis sobre k*

Agora faremos uma extensão para a normalização de Noether, que é necessária para o caso de corpos com característica positiva.

Proposição 2. *Seja k um corpo algebricamente fechado, e seja $A = k[a_1, \ldots, a_n]$ um domínio de integridade com corpo de frações K. Então existem $y_1, \ldots, y_m \in A$ tal que* (1) *e* (2) *do Teorema 1 são válidos, e ainda mais*

(3) *K é um extensão separável de $k(y_1, \ldots, y_m)$.*

Prova. Em característica 0 todas as extensões algébrica são separáveis, podemos assumir então que a característica de p é positiva. Seja x_i algebricamente independente sobre k e seja o mapa

$$\pi \ : \ k[x_1, \ldots, x_n] \longrightarrow k[a_1, \ldots, a_n]$$

definido como $\pi(x_i) = a_i$. O fato de que A é um **domínio de integridade** é equivalente ao ideal

$$I := \ker(\pi)$$

ser primo. Em particular, podemos escolher um elemento irredutível $f \in I$. Suponha que f tem grau d. Pelo Lema 4, existe uma mudança de variáveis da forma $\tilde{x}_i = x_i + \alpha_i x_n$ tal que $\tilde{f}(\tilde{x}_1, \tilde{x}_2, \ldots) = f(x_1, \ldots, x_n)$ tem um termo da forma $c(\tilde{x}_n)^d$. Note que se f tem um termo da forma cx_i^d então $\tilde{f}$ tem um termo da forma $c(\tilde{x}_n)^d$, logo, mudando o papel de x_n com x_j para $j = 1, \ldots, n-1$, podemos fazer uma sequência de mudanças de variáveis para obter um polinômio $\tilde{x}_1, \ldots, \tilde{x}_n$, onde $\tilde{x}_i = x_i + \sum_{j \neq i, j=1}^{n} \beta_{ij} x_j$, para algumas constantes β_{ij}, $1 \leq i, j \leq n$, $i \neq j$, tal que para cada i, como um polinômio em $\tilde{x}_i$ sobre $k[\{x_j \mid j \neq i\}]$, o termo líder é da forma $c_i(\tilde{x}_i)^d$ para algum termo $c_i \in k$. Já que f é irredutível, $k[x_1, \ldots, x_n]/(f)$ é um domínio de integridade. As mudanças de variáveis induzem um isomorfismo entre o anel e o anel $k[\tilde{x}_1, \ldots, \tilde{x}_n]/(\tilde{f})$, que é também um domínio de integridade. Logo $(\tilde{f})$ também é irredutível. Já que $k[\tilde{x}_1, \ldots, \tilde{x}_n]$, podemos substituir x_i por $\tilde{x}_i$ e f por $\tilde{f}$, logo podemos assumir que f é irredutível e tem um termo líder da forma $c_i(x_i)^d$, para algum $c_i \in k$, com respeito a cada variável.

Afirmamos que f é separável com respeito a ao menos uma variável x_i. Caso contrário poderíamos ter $f \in k[x_1, \ldots, x_i^p, \ldots, x_n]$ para todo i, e existiriam polinômios g e h com

$$f = g(x_1^p, \ldots, x_n^p) = h(x_1, \ldots, x_n)^p,$$

contradizendo a irredutibilidade de f. Logo podemos assumir que f é separável com respeito a x_n. Agora, como na prova do Teorema 2.28, podemos ver a equação

$$f(a_1, \ldots, a_{n-1}, a_n) = 0$$

como uma equação separável para a_n sobre o corpo de frações de $A' = k[a_1, \ldots, a_{n-1}]$. Novamente, aplicamos um argumento indutivo, e usamos o fato de que a composição de duas extensões separáveis é também uma extensão separável. □

APÊNDICE D – Redução ao caso de uma hipersuperfície

Finalizamos esta seção com uma outra consequência de Normalização de Noether.

Teorema 2 (**Teorema do Elemento Primitivo**). *Seja K um corpo com infinitos elementos, e $L \supset K$ uma extensão finita e separável. Então existe um elemento $x \in L$ com $L = K(x)$. Mais ainda, se L é gerado sobre K por um conjunto finito de elementos $z_1, \ldots, z_n$, então x pode ser escolhido para ser um elemento da forma $x = \sum \alpha_i z_i$, com $\alpha_i \in K$.*

Prova. Seja $K \subset M$ o fecho normal de L sobre K. Então $K \subset M$ é uma extensão Galoisiana finita. Pelo teorema fundamental da teoria de Galois existem somente um número finito de corpos entre K e M. Os corpos $\{K_i\}$ entre K e L formam um número finito de K-subespaços do espaço vetorial L. Se K tem infinitos elementos, então existe $x \in L$ que não estariam na união dos K_i. Portanto $L = K(x)$. Se $z_1, \ldots, z_n$ gerassem L, eles não poderiam estar todos contidos em um único K_i, logo existe alguma combinação linear $x = \sum \alpha_i z_i$ que não está contida em nenhum K_i, portanto $L = K(x)$. □

Podemos agora fazer uma extensão da normalização de Noether:

Corolário 1. *Utilizando a mesma notação e condições da Proposição 2, podemos escolher $y_1, \ldots, y_{m+1} \in A$ tal que $y_1, \ldots, y_m$ satisfaz $(1) - (3)$ da Proposição 2 e o Teorema 1, tal que o corpo de frações K de A é gerado sobre k por $y_1, \ldots, y_{m+1}$.*

Prova. Pela Proposição 2 podemos assumir que K é uma extensão de corpos separável de $k(y_1, \ldots, y_m)$. Já que $A = k[a_1, \ldots, a_n]$, os a_i geram K como uma extensão de corpos de $k(y_1, \ldots, y_m)$. Podemos então escrever y_{m+1} como uma combinação linear dos a_i com coeficientes em $k(y_1, \ldots, y_m)$. Depois de multiplicar pelo denominador comum, podemos escrever y_{m+1} como uma combinação linear dos a_i com coeficientes em $k[y_1, \ldots, y_m]$. □

Este corolário nos diz que que a extensão $k \subset K$ pode ser decomposta como

$$k \subset K_o = k(y_1, \ldots, y_m) \subset K = K_0(y_{m+1}), \tag{.1}$$

onde a primeira extensão é puramente transcendental, a segunda é uma extensão primitiva algébrica, i.e., uma extensão algébrica gerada por um elemento. Em outras palavras, $K = k(y_1, \ldots, y_{m+1})$, onde existe apenas uma relação algébrica entre os y_i. Isto significa geometricamente que se y_i são as coordenadas de $\mathbb{A}^{n+1}$, então essa relação descreve uma hipersuperfície em $\mathbb{A}^{n+1}$, geometricamente, a equação (.1) nos diz que toda variedade irredutível é "quase" isomorfa a uma hipersuperfície. Isto será discutido com mais atenção posteriormente.

APÊNDICE E – Conceitos básicos de categoria

Faremos agora uma análise do que foi feito utilizando a linguagem da teoria de categorias, para isso vamos introduzir alguns conceitos.

Definição 5. *Uma* ***categoria*** $\mathcal{C}$ *consiste dos seguintes dados:*

(1) *Uma classe de* ***objetos*** $Ob\,\mathcal{C}$.

(2) *Para quaisquer dois objetos* $A, B \in Ob\,\mathcal{C}$, *existe o conjunto* $Mor_{\mathcal{C}}(A, B)$. *Os elementos deste conjunto são chamados de* ***morfismos.***

(3) *Para cada três objetos* $A, B, C \in Ob\,\mathcal{C}$ *existe o mapa*

$$\begin{aligned} \circ \ : \ Mor_{\mathcal{C}}(A,B) \times Mor_{\mathcal{C}}(B,C) &\longrightarrow Mor_{\mathcal{C}}(A,C) \\ (f,g) &\longmapsto g \circ f, \end{aligned}$$

tal que as seguintes afirmações são válidas:

(a) $\circ$ *é associativo, i.e.,* $(g \circ f) \circ h = g \circ (f \circ h)$, *e*

(b) *para todo* $A \in Ob\ \mathcal{C}$ *existe um morfismo* $id_A \in Mor_{\mathcal{C}}(A, A)$, *chamado de* ***identidade de A****, tal que para todo* $B \in Ob\,\mathcal{C}$ *e para todo* $f \in Mor_{\mathcal{C}}(A, B)$ *e* $g \in Mor_{\mathcal{C}}(B, A)$ *temos*

$$f \circ id_A = f \ \text{ e } id_A \circ g = g.$$

Exemplo 2. *Segue alguns exemplos de categorias:*

(1) *A categoria de conjuntos e mapas.*

(2) *A categoria de espaços topológicos e mapas contínuos.*

(3) *A categoria de grupos e homomorfismos de grupos.*

Definição 6. *Para categorias* $\mathcal{C}$ *e* $\mathcal{D}$, *um* ***funtor*** $F : \mathcal{C} \longrightarrow \mathcal{D}$, *que pode ser covariante ou contravariante, é dado por*

(1) *um mapa* $F : Ob\,\mathcal{C} \longrightarrow Ob\,\mathcal{D}$, *e*

(2) *uma coleção de mapas*

$$\begin{aligned} Mor_{\mathcal{C}}(A,B) &\longrightarrow Mor_{\mathcal{D}}(F(A),F(B)), \ \textit{no caso covariante,} \\ Mor_{\mathcal{C}}(A,B) &\longrightarrow Mor_{\mathcal{D}}(F(B),F(A)), \ \textit{no caso contravariante,} \end{aligned}$$

tendo as seguintes propriedades:

(1) $F(id_A) = id_{F(A)}$.

(2) $F(f \circ g) = \begin{cases} F(f) \circ F(g), & \text{no caso covariante,} \\ F(g) \circ F(f), & \text{no caso contravariante.} \end{cases}$

Exemplo 3. *Para toda categoria $\mathcal{C}$ existe o funtor $id_{\mathcal{C}}$ dado pela identidade.*

Exemplo 4. *Para várias categorias existe um funtor "esquecimento", que simplesmente "esquece" alguma estrutura dos objetos do domínio do funtor. Um exemplo é dado pelo seguinte funtor:*

$$F : \{\textit{grupos, homomorfismos}\} \longrightarrow \{\ \textit{conjuntos, mapas}\}$$

que leva um grupo no seu conjunto subjacente.

Exemplo 5. *A relação que vem sendo discutida entre variedades e ideias pode agora ser expressa utilizando o seguinte funtor contravariante:*

$$F : \left\{ \begin{array}{c} \textit{variedades afins} \\ e \\ \textit{mapas polinomiais} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} k\textit{-álgebras reduzidas} \\ \textit{finitamente geradas e} \\ \textit{homomorfismos de } k\textit{-álgebras} \end{array} \right\}$$

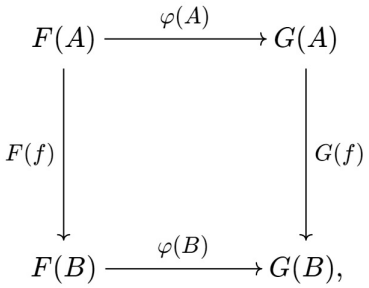
$$V \longmapsto k[V],$$
$$(f : V \longrightarrow W) \longmapsto (f^* : k[W] \to k[V]).$$

Vamos nos referir à categoria da esquerda como **categoria das variedades afins**, e a categoria da direita como **categoria das k-álgebras reduzidas finitamente geradas**. Frequentemente vamos nos referir à categoria pelos seus objetos, os morfismos sendo entendidos como os morfismos usuais entre os objetos em questão.

Para dar uma descrição mais precisa das propriedade do funtor do Exemplo 5, vamos introduzir algumas notações a mais.

Definição 7. *Para dois funtores $F, G : \mathcal{C} \longrightarrow \mathcal{D}$, que são ambos covariantes ou contravariantes, um **morfismo funtorial** $\varphi : F \longrightarrow G$ é uma família de morfismos $\{\varphi(A) : F(A) \longrightarrow G(A) \mid A \in Ob\ \mathcal{C}\}$ tal que para cada morfismo $f : A \longrightarrow B$ com $A, B \in Ob\,\mathcal{C}$, no caso covariante, temos o seguinte diagrama comutativo*

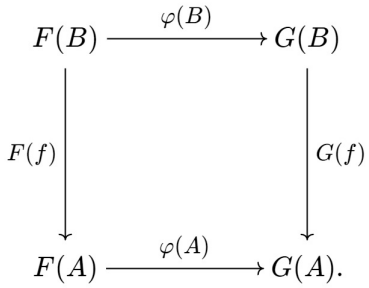
Figura 32 – Diagrama.



Fonte: Ver (1) página 46.
(2000)

enquanto que no caso contravariante temos o seguinte diagrama comutativo

Figura 33 – Diagrama.



Fonte: Ver (1) página 46.
(2000)

Definição 8. *O morfismo funtorial φ define um* ***isomorfismo funtorial*** *$\varphi : F \cong G$, se existe um morfismo funtorial $\psi : G \longrightarrow F$ com $\psi \circ \varphi = id_F$ e $\varphi \circ \psi = id_G$.*

Definição 9. *Um funtor $F : \mathcal{C} \longrightarrow \mathcal{D}$ define uma* ***equivalência de categorias*** *se existe um funtor $G : \mathcal{D} \longrightarrow \mathcal{C}$ com $G \circ F \cong id_C$ e $F \circ G \cong id_{\mathcal{D}}$.*

Proposição 3. *O funtor definido por*

$$V \longmapsto k[V],$$
$$(f : V \longrightarrow W) \longmapsto (f^* : k[W] \longrightarrow k[V]),$$

induz as seguintes equivalências de funtores contravariantes:

$$\left\{\begin{array}{c} \textit{categoria das} \\ \textit{variedades afins} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \textit{categoria das } k-\textit{álgebras reduzidas} \\ \textit{finitamente geradas} \end{array}\right\}$$

$$\left\{\begin{array}{c} \textit{categoria das} \\ \textit{variedades afins} \\ \textit{irredutíveis} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \textit{categoria das } k-\textit{álgebras} \\ \textit{finitamente geradas} \\ \textit{que são domínio de integridade} \end{array}\right\}$$

Prova. Para construir um funtor inverso G, procederemos como se segue. Para uma $k-$álgebra finitamente gerada A escolhemos geradores $a_1, \ldots, a_n$ de A e consideramos o homomorfismo

$$\pi : k[x_1, \ldots, x_n] \longrightarrow A = k[a_1, \ldots, a_n],$$

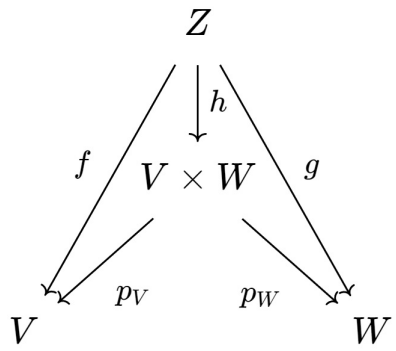
dado por $\pi(x_i) = a_i$. O ideal $I = \ker \pi$ é um ideal radical e define uma variedade $V = V(I)$, que é irredutível se, e somente se, I é um ideal primo, i.e., se A é um domínio de integridade. Definimos $G(A) = V$.

A Proposição 2.42 implica que todo homomorfismo $\varphi : A \longrightarrow B$ de $k-$álgebras reduzidas finitamente geradas dão origem a um único morfismo $f : G(B) \longrightarrow G(A)$ com $\varphi = F(f)$, então definimos $G(\varphi) = f$. É possível verificar que F e G definem uma equivalência de categorias. □

APÊNDICE F – O produto de duas variedades

Um **produto categórico** é definido puramente em termos da existência de certos morfismos na categoria com que se trabalha, na categoria das variedades afins, dizer que $V \times W$ é um produto categórico de variedades V e W significa que $V \times W$ é uma variedade afim. E que existem mapas polinomiais $p_V : V \times W \longrightarrow V$ e $p_W : V \times W \longrightarrow W$, as projeções, tais que para qualquer variedade afim Z, que é levada para V e W via mapas polinomiais $f : Z \longrightarrow V$, e $g : Z \longrightarrow W$, existe um único mapa polinomial $h : Z \to V \times W$ tal que o seguinte diagrama comuta:

Figura 34 – Diagrama.



Fonte: Ver (1) página 48.
(2000)

Para variedades afins V e W, o produto categórico de V e W é dado pelo "produto cartesiano teórico[1]" $V \times W$: no diagrama acima tome $V \times W$ como sendo esse produto, tome p_V e p_W como sendo as restrições das projeções no espaço afim envolvido, e tome $h = (f, g)$. Resta mostrar que esse produto $V \times W$ é de fato uma variedade afim.

Proposição 4. *Para variedades $V \subset \mathbb{A}_k^n$ e $W \subset \mathbb{A}_k^m$ temos:*

(1) *O produto cartesiano teórico $V \times W \subset \mathbb{A}_k^n \times \mathbb{A}_k^m = \mathbb{A}_k^{n+m}$ é uma variedade;*

(2) *Se V e W são irredutíveis, então $V \times W$ também é irredutível.*

Prova. (1) Se $f_1, \ldots, f_l \in k[x_1, \ldots, x_n]$ e $g_1, \ldots, g_r \in k[y_1, \ldots, y_m]$ são polinômios tais que

$$V = \{f_1 = \ldots = f_l = 0\} \text{ e } W = \{g_1 = \ldots = g_r = 0\},$$

então

$$V \times W = \{f_1 = \ldots = f_l = g_l = \ldots = g_r = 0\}$$

portanto é de fato uma variedade.

[1] Tradução livre de "set-theoretic product".

(2) Primeiro notemos que para todo $w \in W$ a projeção no primeiro fator define um isomorfismo entre $V \times \{w\}$ e V. Similarmente $\{v\} \times W$ é isomorfo a W para todo $v \in V$. Suponha que exista uma decomposição $V \times W = Z_1 \cup Z_2$. Isto induz a decomposição

$$V \times \{w\} = (V \times \{w\} \cap Z_1) \cup (V \times \{w\} \cap Z_2).$$

Já que $V \times \{w\}$ é isomorfo a V e dessa forma irredutível, ou $V \times \{w\} \cap Z_1 = V \times \{w\}$ ou $V \times \{w\} \cap Z_2 = V \times \{w\}$, i.e., $V \times \{w\} \subset Z_1$ ou $Z \times \{w\} \subset Z_2$. Podemos agora definir

$$W_i := \{w \in W \mid V \times \{w\} \subset Z_i\} \qquad (i = 1, 2).$$

Então $W_1 \cup W_2 = W$. Se mostrarmos que W_i são fechados, então segue da irredutibilidade de W que $W_1 = W$ ou $W_2 = W$. No primeiro caso temos $V \times W = Z_1$, e no segundo caso $V \times W = Z_2$. Para cada ponto $v \in V$, seja

$$W_i^v := \{w \in W \mid (v, w) \in Z_i\} \qquad (i = 1, 2).$$

Segue que esses conjuntos W_i^v são fechados, já que $\{v\} \times W_i^v = (\{v\} \times W) \cap Z_i$. Já que $W_i = \bigcap_{v \in V} W_i^v$, portanto os conjuntos W_i são também fechados. □

Observação 6. *Note que a topologia de Zariski em $V \times W$ não é a topologia produto.*