Universidade Federal de Uberlândia
Faculdade de Matemática

Bacharelado em Matemática

Conjuntos algébricos: propriedades e resultados

Gabriela Gomes Gularte

Uberlândia-MG
2021

Gabriela Gomes Gularte

Conjuntos algébricos: propriedades e resultados

Trabalho de conclusão de curso apresentado à Coordenação do Curso de Bacharelado em Matemática como requisito parcial para obtenção do grau de Bacharel em Matemática.

Orientador: Prof. Dr. Luis Renato Gonçalves Dias

Uberlândia-MG
2021

Universidade Federal de Uberlândia
Faculdade de Matemática

Coordenação do Curso de Bacharelado em Matemática

A banca examinadora, conforme abaixo assinado, certifica a adequação deste trabalho de conclusão de curso para obtenção do grau de Bacharel em Matemática.

Uberlândia, 18 de junho de 2021.

BANCA EXAMINADORA

Prof. Dr. Luis Renato Gonçalves Dias

Profa. Dra. Laís Bássame Rodrigues

Profa. Dra. Adriana Rodrigues da Silva

Uberlândia-MG
2021

Agradecimentos

Agradeço à minha mãe Devanir, por ser incrível e por estar do meu lado em todos os momentos. Ao meu pai Renato, por ter feito de tudo para que eu chegasse até aqui. À minha irmã Giovanna e meu irmão Pedro Henrique, pela companhia e cumplicidade. À minha avó Dina, à Nina e a todos os familiares que contribuíram de alguma forma para a conclusão do meu curso. Minha família foi meu suporte e minha maior referência durante todo esse trajeto.

Ao Pedro Mendes, Dionathan, Leonardo Soria, Tiago, Vitor Marques, Marcelo, Jelir, Paulo Vitor, Matheus, Aline, Leonardo, Rafaela, Milvar, Mateus, Stefânia, Vitor, Fernanda, Gabriel, Alicia, Amanda e Maria Victoria, com quem eu estudei, chorei e me diverti, sem vocês eu não teria conseguido passar por esses 4 anos e meio. Agradeço também a todos os outros amigos e amigas que eu não mencionei aqui, mas que foram essenciais.

Aos professores e professoras que tive no decorrer da vida que me inspiraram e me deram uma base para construir novos aprendizados. Em especial à Cely, ao Borsatto e ao Gilson que me motivaram à entrar no curso. E ao Alonso, Cícero e Rosana que estiveram presentes na maior parte da minha graduação e por quem eu tenho grande admiração.

À portaria SESu-MEC pelo apoio financeiro e ao Programa de Educação Tutorial que foi, com toda certeza, a melhor parte da minha graduação. Sou imensamente grata por todos os aprendizados, experiências, viagens maravilhosas e, principalmente, por todas as pessoas que devido a esse programa eu conheci, trabalhei e festejei junto. Em particular, agradeço à professora Elisa que me aconselhou em diversas decisões e que me ensinou tanto sobre tanta coisa.

Agradeço às professoras Adriana e Laís por aceitarem o convite para participar da banca.

E, por fim, agradeço muito ao meu orientador Luis Renato, que esteve comigo desde o início, que sempre foi paciente e compreensivo, especialmente nessa reta final, e que se dispôs e buscou me auxiliar de todas as formas possíveis no decorrer da graduação, contribuindo intensamente para o meu crescimento acadêmico e pessoal.

À minha mãe, que me apoiou em cada escolha e cada jeito de ser.

Resumo

Este trabalho apresenta uma introdução elementar ao domínio da Geometria Algébrica, tendo como foco um dos principais objetos de estudo da área: conjuntos algébricos.

O trabalho visa descrever conceitos e propriedades de conjuntos algébricos do ponto de vista algébrico, geométrico e analítico. Teoremas clássicos, como o Teorema da Base de Hilbert e o Teorema de Zeros de Hilbert, são demonstrados. A Topologia de Zariski e as noções de variedade algébrica, anel de coordenadas, anel local, multiplicidade e dimensão são exploradas no decorrer do trabalho. Para esta construção foram estudados, previamente, conteúdos considerados pré-requisitos, como definições e resultados básicos de Álgebra Linear, Álgebra Abstrata e Topologia.

Palavras-chave: Geometria Algébrica, Conjuntos Algébricos, Variedades, Topologia de Zariski, Multiplicidade, Dimensão de Krull.

Abstract

This work presents an elementary introduction to the domain of Algebraic Geometry, focusing on one of the main study objects in the area: algebraic sets.

The paper aims to describe concepts and properties of algebraic sets from an algebraic, geometric and analytical point of view. Classical theorems, such as Hilbert's Basis Theorem and Hilbert's Nullstellensatz, the Zariski's Topology and the notions of algebraic variety, coordinate ring, local ring, multiplicity and dimension were explored throughout this work. For this construction, we have previously studied contents regarded as prerequisites, such as definitions and basic results of Linear Algebra, Abstract Algebra and Topology.

Keywords: Algebraic Geometry, Algebraic Sets, Varieties, Zariski's Topology, Multiplicity, Krull's Dimension.

Sumário

Introdução

Desde a Grécia Antiga, por volta de 400 a.C., a Geometria e a Álgebra são utilizadas em conjunto para resolver problemas. As dificuldades encontradas pelos gregos os levaram a criar a "Álgebra Geométrica", onde não era permitido somar áreas com volumes, a escrita era feita de forma mais homogênea e as equações eram interpretadas geometricamente, um claro exemplo disso é a utilização de construções geométricas simples para encontrar raízes de equações da forma "$x^2 = ab$". Posteriormente, a proximidade dessas duas áreas fica ainda mais explícita com a publicação do Livro II de "Os Elementos" de Euclides de Alexandria (século III a.C.) que apresenta dez proposições tratando de identidades algébricas descritas através de representações geométricas.

Com a introdução da Geometria Analítica no século XVI e os trabalhos de René Descartes, a relação entre a Álgebra e a Geometria foi além de dar significados à álgebra por meio de interpretações geométricas. No tratado *La Géométrie* de Descartes, ele buscou através de processos algébricos libertar a geometria de diagramas e usou métodos que utilizavam tanto geometria quanto álgebra como ferramentas para resolver problemas geométricos e algébricos. E assim, com essa mudança que acontece a partir da Álgebra Geométrica, chega-se às raízes da atual Geometria Algébrica, foco principal deste trabalho.

Hoje, a Geometria Algébrica ocupa um papel central na Matemática moderna e permite diversas abordagens, assim como variadas aplicações. Grandes áreas como Análise Complexa, Teoria dos Números e Topologia estão frequentemente relacionadas à tópicos estudados na Geometria Algébrica. Neste trabalho algumas dessas conexões vão ser apresentadas, por exemplo, ao trabalharmos com variedades algébricas sobre o corpo dos números complexos e ao apresentarmos caracterizações analíticas, fica evidente como a Análise Complexa está presente, assim como ao falarmos sobre a topologia de Zariski, é nítido a relação com a Topologia.

Dessa forma, o objetivo deste trabalho é fazer uma introdução à Geometria Algébrica, tendo como principal tema os conjuntos algébricos, isto é, manifestações geométricas das soluções de sistemas de equações polinomiais, e suas propriedades. Buscamos reunir resultados de algumas das diversas referências de Geometria Algébrica sobre este tema, entre elas estão *"Algebraic Geometry"* de Robin Hartshorne, *"The Red Book of Varieties"* de David Mumford, *"Algebraic Curves: An Introduction to Algebraic Geometry"* de William Fulton e *"Methods of Algebraic Geometry"* de Daniel Pedoe e William Vallance Douglas Hodge. Este estudo foi distribuído ao longo de 4 capítulos.

No Capítulo 1 apresentamos objetos iniciais desta teoria e pré-requisitos que serão utilizados no decorrer do trabalho. Neste capítulo relembramos e estudamos conceitos de Álgebra Linear, de Álgebra Abstrata e Topologia. As seções 1 e 3 são dedicadas à Álgebra Abstrata e nelas encontram-se os conceitos de anéis, corpos, ideais, homomorfismos, módulos, localizações, sequências exatas e diversos resultados relacionados. Na seção 2 é apresentado brevemente o conteúdo inicial de Álgebra Linear. E na última seção encontram-se os conceitos e resultados de topologia geral que serão utilizados, principalmente, ao estudarmos a Topologia de Zariski.

No Capítulo 2 são introduzidas as noções iniciais da Geometria Algébrica, como espaços afins e conjuntos algébricos, e são demonstrados alguns teoremas clássicos da área, entre eles o Teorema da Base de Hilbert e o Teorema dos Zeros de Hilbert. Fechamos o capítulo com a apresentação da Topologia de Zariski e alguns resultados relacionados, em especial, enunciamos uma relação entre a topologia usual e a Topologia de Zariski, este resultado é demonstrado posteriormente. O conteúdo deste capítulo é fundamental para o desenvolvimento dos próximos, visto que constrói uma base para os estudos seguintes e fornece ferramentas para as próximas demonstrações.

O Capítulo 3 refere-se ao estudo de variedades algébricas afins. A seção 1 é dedicada à definição e caracterização de conjuntos algébricos irredutíveis, isto é, variedades algébricas. Na seção 2 são apresentadas estruturas essenciais para este trabalho: anel de coordenadas, anel de funções regulares e anel local de uma variedade. Na seção 3 estudamos aplicações entre variedades algébricas e alguns resultados relacionados. As estruturas apresentadas neste capítulo são essenciais para as definições e caracterizações estudadas no Capítulo 4, principalmente nas seções 4.1 e 4.2.

No Capítulo 4 a interdisciplinaridade entre áreas da Matemática fica clara. Na seção 4.1 trazemos a noção de multiplicidade de conjuntos algébricos, inicialmente apresentamos tal noção para curvas planas e em seguida generalizamos para variedades algébricas. Na seção 4.2 estudamos e relacionamos conceitos de dimensões de conjuntos algébricos, neste momento vamos analisar a dimensão de três perspectivas, duas delas utilizam artifícios de Álgebra: dimensão de Krull e grau de transcendência de uma extensão. Já a terceira noção de dimensão apresentada neste trabalho trata-se de uma caracterização analítica em conjunto com uma interpretação geométrica. No decorrer do capítulo buscamos exibir e demonstrar as relações entre os conceitos trabalhados. O Capítulo é finalizado com uma seção dedicada à provar um resultado apresentado na seção 4.3, neste momento já construímos ferramentas suficientes para demonstrar tal resultado e justificar sua importância.

As informações e contextos históricos apresentados nesta introdução e no decorrer do trabalho têm como fonte o *MacTutor History of Mathematics archive* e a referência [2].

1. Conceitos básicos

Neste capítulo estamos interessados em reunir alguns pré-requisitos para o presente trabalho. Supomos que o (a) leitor (a) esteja familiarizado (a) com as noções básicas de Álgebra Comutativa, Álgebra Linear e Topologia, entretanto buscamos construir este trabalho tão autônomo quanto possível e, por isso, as próximas seções são dedicadas a revisões destes temas. Os conteúdos apresentados neste capítulo serão frequentemente utilizados ao longo do trabalho.

1.1 Estruturas algébricas

Nesta seção apresentaremos algumas estruturas algébricas e suas propriedades. Para um estudo detalhado de tais conceitos indicamos a referência [4].

1.1.1 Anéis, ideais e domínios

Muitos conjuntos possuem naturalmente duas operações binárias: soma e multiplicação. Exemplos que rapidamente vêm a nossa mente são: os números inteiros, os números reais, os polinômios e as matrizes. O conceito abstrato que assume essa possibilidade é justamente o de anel. Em meados do séculos XIX, Richard Dedekind introduziu este conceito, entretanto o termo anel (*Zahlring*) foi criado por David Hilbert em 1897 e a primeira definição axiomática de anéis foi dada por Adolf Fraenkel em um ensaio no *Journal für die reine und angewandte Mathematik* (A. L. Crelle), vol. 145, em 1914.

Definição 1.1 (Anel). *Um anel comutativo com unidade* $(A, +, \cdot)$ *é um conjunto* A *com pelo menos dois elementos, munido de uma operação denotada por* $+$*, chamada adição, e de uma operação denotada por* $\cdot$*, chamada multiplicação, que satisfazem as condições seguintes:*

A.1) *A adição é associativa, isto é,* $\forall x, y, z \in A,\ (x + y) + z = x + (y + z)$.

A.2) *Existe um elemento neutro com respeito à adição, isto é,* $\exists\, 0 \in A$ *tal que,* $\forall x \in A$, $0 + x = x$ *e* $x + 0 = x$.

A.3) *Todo elemento de* A *possui um inverso com respeito à adição, isto é,* $\forall\ x \in A$, $\exists z \in A$ *tal que* $x + z = 0$ *e* $z + x = 0$.

A.4) *A adição é comutativa, isto é,* $\forall\, x, y \in A,\ x + y = y + x$.

M.1) *A multiplicação é associativa, isto é,* $\forall x, y, z \in A,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M.2) *Existe um elemento neutro com respeito à multiplicação, isto é,* $\exists 1 \in A$ *tal que,* $\forall x \in A,\ 1 \cdot x = x \ \text{ e } \ x \cdot 1 = x.$

M.3) *A multiplicação é comutativa, isto é,* $\forall x, y \in A,\ \ x \cdot y = y \cdot x.$

AM) *A adição é distributiva relativamente à multiplicação, isto é,* $\forall x, y, z \in A,\ \ x \cdot (y + z) = x \cdot y + x \cdot z.$

Neste trabalho chamamos um anel comutativo com unidade apenas de anel.

Um conjunto G fechado em relação a operação $+$ que satisfaz as condições A.1, A.2 e A.3 é dito grupo. E, se também satisfaz a condição A.4, é dito grupo abeliano.

Definição 1.2 (Domínio e corpo)**.** *Um anel* $(D, +, \cdot)$ *é chamado domínio se ele satisfaz a seguinte condição:*

M.4) *O produto de quaisquer dois elementos não nulos de* D *é um elemento não nulo, isto é,* $\forall x, y \in D \setminus \{0\},\ x \cdot y \neq 0.$

Um anel $(K, +, \cdot)$ *é chamado de corpo se ele satisfaz a seguinte condição:*

M.4') *Todo elemento diferente de zero de* K *possui um inverso com respeito à multiplicação, isto é,* $\forall \in K \setminus \{0\},\ \exists y \in K$ *tal que* $x \cdot y = 1.$

Um corpo K *é dito algebricamente fechado se qualquer polinômio de uma variável com coeficientes em* K *possui uma raiz em* K*.*

Por exemplo, o corpo dos números reais $K = \mathbb{R}$ não é algebricamente fechado, visto que a equação polinomial $x^2+2 = 0$ em $\mathbb{R}[x]$ não possui raiz em $\mathbb{R}$. Por outro lado, o corpo dos números complexos $K = \mathbb{C}$ é algebricamente fechado e é exatamente isso que o Teorema Fundamental da Álgebra garante. A discussão sobre tal resultado ocorre desde o início do século XVII e dela participou diversos matemáticos, entre eles, Albert Girard, Descartes, Leibniz, Euler, Lagrange e Laplace. A primeira demonstração considerada sem falhas foi apresentada apenas no início do século XIX pelo suíço Argand.

Definição 1.3 (Ideal)**.** *Seja* $(A, +, \cdot)$ *um anel e* I *um subconjunto não vazio de* A*. Dizemos que* I *é um ideal de* A *se*

i) $x + y \in I,\ \ \forall x, y \in I;$

ii) $ax \in I,\ \ \forall x \in I, \forall a \in A.$

Se $I \neq A$ *então* I *é dito ideal próprio de* A*.*

Definição 1.4 (Ideal primo)**.** *Seja* A *um anel. Dizemos que um ideal* $I \subset A$ *é um ideal primo de* A *se para todo* $a, b \in A$ *tais que* $ab \in I$ *então* $a \in I$ *ou* $b \in I$*.*

Definição 1.5 (Ideal maximal)**.** *Seja* A *um anel. Dizemos que um ideal* $I \subset A$ *é um ideal maximal de* A *se:*

i) *$I \neq A$;*

ii) *$\forall$ ideal $J \subset A$, com $J \supset I \Rightarrow J = A$ ou $J = I$. Ou seja, não existe ideal intermediário entre I e A.*

Definição 1.6. *Seja S um subconjunto qualquer de um anel A. Definimos o ideal gerado por S como sendo a interseção de todos ideais que contém S. Denotamos por $\langle S \rangle$ o ideal gerado por S. Desta forma, todos os elementos $u \in \langle S \rangle$ são expressos como um somatório finito da forma:*

$$u = \sum_{j=1}^{n} a_j s_j, \ \text{com } a_j \in A \text{ e } s_j \in S. \tag{1.1}$$

Dado um anel A e elementos $a_1, \ldots, a_n \in A$, denotamos $\langle \{a_1, \ldots, a_n\} \rangle$ somente por $\langle a_1, \ldots, a_n \rangle$.

Definição 1.7 (Ideal principal)**.** *Seja A um anel. Dizemos que um ideal $I \subset A$ é um ideal principal de A se I pode ser gerado por um único elemento em A.*

Definição 1.8 (Domínio principal)**.** *Seja D um domínio. Dizemos que D é um domínio principal se cada ideal de D é um ideal principal.*

Um exemplo de um domínio principal é $\mathbb{R}[X]$.

Definição 1.9 (Anel quociente)**.** *Sejam A um anel e I um ideal de A. Definimos o anel quociente A/I como o anel de classes residuais módulo I, isto é, a relação de congruência módulo o ideal I. Temos que a seguinte relação ($a \equiv b \Leftrightarrow a - b \in I$) é uma relação de equivalência em A e a classe de equivalência de um elemento a é o conjunto $\overline{a} = \{a + b \mid b \in I\} = a + I$.*

Assim, o anel quociente A/I forma um anel em relação às operações

$$(a + I) + (b + I) \ := \ (a + b) + I, \tag{1.2}$$

$$(a + I)(b + I) \ := \ ab + I. \tag{1.3}$$

Definição 1.10. *Sejam D um domínio e a, b elementos de D. Dizemos que b divide a se existe $c \in D$ tal que $a = bc$. Denotamos por $b \mid a$ para dizer que b divide a.*

Definição 1.11. *Sejam D um domínio e $a \in D$. Dizemos que a é invertível em D se existe $b \in D$ tal que $ab = 1$.*

Definição 1.12. *Sejam D um domínio e $p \in D$ não nulo e não invertível. Dizemos que p é primo se sempre que $p \mid xy$, então $p \mid x$ ou $p \mid y$.*

A definição seguinte será utilizada em vários momentos deste trabalho.

Definição 1.13. *Sejam D um domínio e $p \in D$ um elemento não invertível e não nulo do anel. Dizemos que p é irredutível se $p = ab$ implicar que a ou b é invertível.*

1.1.2 ALGUNS RESULTADOS

Apresentamos agora resultados relacionados às definições dadas na seção anterior.

Teorema 1.14. *Sejam D um domínio principal e $p \in D$ um elemento irredutível. Então o ideal $I = \langle p \rangle$ é maximal.*

Demonstração. Suponha que existe J tal que $I \subsetneq J$. Como D é domínio principal $J = \langle a \rangle$ para algum $a \in D$. Temos que $p \in J$, então existe $c \in D$ tal que $p = ac$, como p é irredutível temos que a é invertível ou c é invertível. Se c é invertível, existe $d \in D$ tal que $cd = 1$, logo $pd = a$ e então $a \in I$, contradizendo a suposição de I contido propriamente em J. Então devemos ter que a é invertível e, assim, existe $b \in A$ tal que $ab = 1$, então $1 \in \langle a \rangle$. Logo $\langle a \rangle = D$, o que conclui a prova.

□

A seguir, apresentaremos o Lema de Zorn, necessário para demonstração de resultados posteriores.

Teorema 1.15 (Lema de Zorn). *Seja X um conjunto parcialmente ordenado tal que todo subconjunto $Y \subseteq X$ totalmente ordenado possui um limitante superior. Então X possui um elemento maximal.*

A demonstração do Lema de Zorn (Teorema 1.15) pode ser encontrada em [5], página 62.

Teorema 1.16. *Sejam A um anel e I um ideal próprio de A. Então I está contido em um ideal maximal m de A.*

Demonstração. Considere o conjunto

$$X = \{J \subseteq A \mid J \text{ é um ideal, onde } 1 \notin J \text{ e } I \subseteq J\}.$$

Como $I \in X$, temos que $X \neq \varnothing$ e X é um conjunto parcialmente ordenado com relação à inclusão "$\subseteq$". Seja $\{J_\lambda\}$ um subconjunto totalmente ordenado de X e $\mathcal{J} = \cup J_\lambda$. Assim, $\mathcal{J}$ é um ideal e $1 \notin \mathcal{J}$. Além disso, $J_\lambda \subseteq \mathcal{J}$, $\forall \lambda$. Assim, $\mathcal{J}$ é um limitante superior para o conjunto $\{J_\lambda\}$ em X e, portanto, todo subconjunto de X possui cota superior. Logo, pelo Lema de Zorn (Teorema 1.15), X possui elemento máximo m tal que $I \subseteq m$ e m é um ideal maximal, concluindo a demonstração. □

Os próximos resultados caracterizam ideais primos e maximais em termos de seus anéis quocientes.

Teorema 1.17. *Seja A um anel e I um ideal de A. Então, A/I é um domínio se, e somente se, I é um ideal primo.*

Demonstração. Suponha A/I domínio. Se $ab \in I$, então $(a + I)(b + I) = ab + I = I$. Como A/I é um domínio, devemos ter que $a + I = I$ ou $b + I = I$, logo $a \in I$ ou $b \in I$ e, portanto, I é ideal primo.

Por outro lado, o quociente A/I é um anel para qualquer ideal próprio I. Assim, devemos mostrar que se I é um ideal primo, então A/I não possui divisores de zero (veja Definição 1.2 M.4). Sejam a e b elementos não nulos de A e suponhamos que $(a+I)(b+I) = 0+I = I$, então temos que $ab \in I$. Como I é primo $a \in I$ ou $b \in I$ e portanto $a+I = I$ ou $b+I = I$. $\square$

Teorema 1.18. *Seja A um anel e m um ideal de A. Então, A/m é um corpo se, e somente se, m é um ideal maximal.*

Demonstração. Suponha que I é ideal maximal e provaremos que A/I é um corpo, isto é, que todo elemento não nulo de A/I possui inverso multiplicativo. Seja $b \in A$ tal que $b \notin I$, devemos mostrar que $b+I$ possui inverso multiplicativo. Considere o ideal $J = I + \langle b \rangle = \{a + br \mid a \in I,\ r \in A\}$. O ideal J contém propriamente I e como I é maximal, então devemos ter que $J = A$ logo, $1 \in J$. Portanto, existem $a \in I$ e $r \in A$ tais que $1 = a + br$. Então

$$1 + I = (a + br) + I = br + I = (b + I)(r + I), \tag{1.4}$$

logo A/m é um corpo. Por outro lado, suponha que A/I é um corpo e que J é um ideal de A que contém propriamente I. Seja $b \in J$ tal que $b \notin I$, então $b + I$ é um elemento não nulo de A/I e, portanto, possui inverso. Logo, existe $a + I$ não nulo tal que $(a + I)(b + I) = 1 + I$, disso segue que $1 - ab \in I \subset J$. Assim $1 = 1 - ab + (ab) \in J$ e, portanto, $J = A$ o que implica que I é maximal. $\square$

Dos Teoremas 1.17 e 1.18 segue o seguinte resultado:

Corolário 1.19. *Seja A um anel. Todo ideal maximal I de A é um ideal primo.*

Demonstração. Como I é maximal, A/I é um corpo e, em particular, um domínio. Logo I é primo. $\square$

1.1.3 Homomorfismos e extensões

Na Álgebra Abstrata, um homomorfismo é uma aplicação que preserva a estrutura entre duas estruturas algébricas. A seguir definimos homomorfismo entre anéis e apresentamos mais algumas noções e resultados.

Definição 1.20 (Homomorfismo). *Sejam $(A, +, \cdot)$ e $(B, \oplus, \odot)$ dois anéis. Uma aplicação $\varphi : A \to B$ é um homomorfismo se satisfaz as condições seguintes:*

i) $\varphi(a_1 + a_2) = \varphi(a_1) \oplus \varphi(a_2),\ \forall a_1, a_2 \in A$;

ii) $\varphi(a_1 \cdot a_2) = \varphi(a_1) \odot \varphi(a_2),\ \forall a_1, a_2 \in A$;

iii) $\varphi(1_A) = \varphi(1_B)$, *onde 1_A representa o elemento neutro da multiplicação de A e 1_B o elemento neutro da multiplicação de B.*

Proposição 1.21. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \odot)$ dois anéis e $\varphi : A \to B$ um homomorfismo.*

i) *Seja* $ker\,\varphi := \{a \in A \mid \varphi(a) = 0\}$. *Então* $ker\,\varphi$ *é um ideal de* A *chamado núcleo de* φ*;*

ii) *Seja* $Im\,\varphi := \{\varphi(a) \mid a \in A\} \subset B$. *Então* $(Im\,\varphi, \oplus, \odot)$ *é um anel chamado imagem de* φ*;*

iii) φ *é injetor se, e somente se,* $ker\,\varphi = 0$.

Definição 1.22. *Um homomorfismo de anéis* $\varphi : A \to B$ *é um isomorfismo se* φ *é injetor e sobrejetor. Os anéis* A *e* B *são ditos isomorfos se existe um isomorfismo entre* A *e* B.

Teorema 1.23 (Teorema dos Isomorfismos)**.** *Sejam* $(A, +, \cdot)$ *e* $(B, \oplus, \odot)$ *dois anéis e* $\varphi : A \to B$ *um homomorfismo. Então a aplicação* $\overline{\varphi}$ *abaixo é um isomorfismo de anéis:*

$$\begin{array}{rrcl} \overline{\varphi}: & \dfrac{A}{ker\,\varphi} & \to & Im\,\varphi \\ & \overline{a} & \mapsto & \varphi(a). \end{array} \tag{1.5}$$

Demonstração. Sejam $a_1, a_2 \in A$ tais que $\overline{a_1} = \overline{a_2}$. Como $\overline{a_1} = \overline{a_2}$ segue que $\overline{a_1} - \overline{a_2} \in ker\,\varphi$ e como φ é um homomorfismo também segue que $\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2)$ e, assim, $\varphi(a_1) = \varphi(a_2)$, portanto $\overline{\varphi}(\overline{a_1}) = \overline{\varphi}(\overline{a_2})$. Logo, $\overline{\varphi}$ é uma função bem definida. Além disso, temos

$$\overline{\varphi}(\overline{a_1} + \overline{a_2}) = \overline{\varphi}(\overline{a_1 + a_2}) = \varphi(a_1 + a_2) = \varphi(a_1) \oplus \varphi(a_2) = \overline{\varphi}(\overline{a_1}) \oplus \overline{\varphi}(\overline{a_2}), \tag{1.6}$$

$$\overline{\varphi}(\overline{a_1} \cdot \overline{a_2}) = \overline{\varphi}(\overline{a_1 \cdot a_2}) = \varphi(a_1 \cdot a_2) = \varphi(a_1) \odot \varphi(a_2) = \overline{\varphi}(\overline{a_1}) \odot \overline{\varphi}(\overline{a_2}), \tag{1.7}$$

logo φ é um homomorfismo. Como $Im\ \overline{\varphi} = Im\ \varphi$, $\overline{\varphi}$ é sobrejetor. Por fim, temos que

$$ker\,\overline{\varphi} = \{\overline{a} \in A/ker\,\varphi \mid \overline{\varphi}(\overline{a}) = 0\} = \{\overline{a} \in A/ker\,\varphi \mid \varphi(a) = 0\} = \{\overline{a} \in A/ker\,\varphi \mid a \in ker\,\varphi\} = \{\overline{0}\}.$$

Portanto, $\overline{\varphi}$ é injetor, o que conclui a prova. □

Dado um anel A, denotamos por $A[x_1, \ldots, x_n]$ o anel de polinômios nas variáveis $x_1, \ldots, x_n$ com coeficientes em A.

Exemplo 1.24. *Sejam* A *um anel e* $a_1, \ldots, a_n$ *elementos de* A. *Temos que* $\frac{A[x_1,\ldots,x_n]}{\langle x_1 - a_1, \ldots, x_n - a_n\rangle} \simeq A$. *De fato, considere o homomorfismo*

$$\begin{array}{rrcl} \varphi: & A[x_1, \ldots, x_n] & \to & A \\ & f(x_1, \ldots, x_n) & \mapsto & f(a_1, \ldots, a_n). \end{array} \tag{1.8}$$

Temos que φ *é sobrejetor e* $\ker\,\varphi = \langle x_1 - a_1, \ldots, x_n - a_n\rangle$. *Assim, pelo Teorema dos Isomorfismos (Teorema 1.23),*

$$\frac{A[x_1, \ldots, x_n]}{\langle x_1 - a_1, \ldots, x_n - a_n\rangle} \simeq Im\ \varphi = A.$$

Se A *é um corpo, segue do Teorema 1.18, que o ideal* $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ *é maximal.*

Definição 1.25 (Corpo de frações). *Seja D um domínio com as operações $+$ e $\cdot$. Então existe um corpo K, chamado corpo de frações, tal que*

i) *$(K, \oplus, \odot)$ contém um subanel que é isomorfo à $(D, +, \cdot)$;*

ii) *Para todo $k \in K$, existem $a, b \in D$, $b \neq 0$ tais que $k = a \odot b^{-1}$.*

Demonstração. Seja $S = \{(a, b); a, b \in D \text{ e } b \neq 0\}$. Definimos a relação de equivalência $\sim$ em S por $(a, b) \sim (c, d)$ se $ad = bc$. Seja $K = S/\sim$ o conjunto das classes de equivalência e denote a classe de (a, b) por a/b, isto é, $a/b = \{(c, d) \in S; ad = bc\}$. Assim, definimos as operações de adição e multiplicação em K da seguinte forma:

$$a/b \oplus c/d = (ad + bc)/bd, \tag{1.9}$$
$$a/b \odot c/d = ac/bd. \tag{1.10}$$

Temos que $bd \neq 0$, pois $b \neq 0$, $d \neq 0$ e D é um domínio, logo K é fechado em relação às operações $\oplus$ e $\odot$. Mostraremos agora que as operações estão bem definidas. Sejam $a/b = a'/b'$ e $c/d = c'/d'$, temos que $ab' = a'b$ e $cd' = c'd$. Então

$$\begin{aligned}
(ad + bc)b'd' &= adb'd' + bcb'd' \\
&= (ab')dd' + (cd')bb' \\
&= (a'b)dd' + (c'd)bb' \\
&= a'd'bd + c'b'bd \\
&= (a'd' + c'b')bd.
\end{aligned}$$

Logo $a/b \oplus c/d = (ad + bc)/bd = (a'd' + b'c')/b'd' = a'/b' \oplus c'/d'$, isto é, a adição está bem definida em K. De forma análoga para a multiplicação temos que

$$(ac)b'd' = (ab')cd' = (a'b)c'd = (a'c')bd$$

e, portanto, $a/b \odot c/d = a'/b' \odot c'/d'$, isto é, a multiplicação também está bem definida em K.

Além disso, K é um corpo em que $0/1$ é a identidade da adição, $1/1$ é a identidade da multiplicação, $-a/b$ é o inverso aditivo de a/b e b/a é o inverso multiplicativo de um elemento não nulo a/b, onde 1 é o elemento neutro da multiplicação de D. As propriedades comutativa e associativa da adição e da multiplicação são facilmente mostradas, assim como a propriedade distributiva da adição em relação à multiplicação.

Por fim, considere a aplicação $\varphi : D \to K$ dada por $\phi(x) = x/1$. Para um elemento $a/b \in K$ temos que $a/b = a/1 \odot 1/b$, como $bb^{-1} = 1$, segue que $a/b = a/1 \odot b^{-1}/1$ e, portanto, φ é um isomorfismo sobre sua imagem. $\square$

Finalizamos a seção com a definição de extensão de corpos, alguns conceitos relacionados e um teorema que será utilizado posteriormente na demonstração do Teorema dos Zeros de Hilbert.

Definição 1.26 (Extensão)**.** *Um corpo K é dito uma extensão de F se K contém F como um subcorpo. Denotamos a extensão por $F \subset K$.*

Definição 1.27. *Seja $F \subset K$ uma extensão de corpos. Um elemento $a \in K$ é dito algébrico sobre F se existe um polinômio não nulo $f(x) \in F[x]$ tal que $f(a) = 0$.*

Por exemplo, considere $\mathbb{R} \subset \mathbb{C}$. Temos que i é algébrico sobre $\mathbb{R}$.

Definição 1.28 (Extensão Algébrica)**.** *Seja $F \subset K$ uma extensão de corpos. Se todos os elementos de K são algébricos sobre F, $F \subset K$ é dita uma extensão algébrica. Caso contrário a extensão é chamada extensão transcendental.*

Temos que $\mathbb{R} \subset \mathbb{C}$ é uma extensão algébrica.

Teorema 1.29. *Sejam F um corpo e K um domínio finitamente gerado sobre F, isto é, existem $\alpha_1, \ldots, \alpha_n \in K$ tais que $K = F[\alpha_1, \ldots, \alpha_n]$. Então K é algébrico sobre F.*

A demonstração do Teorema 1.29 pode ser encontrada em [12], página 7. Em [1], página 82 encontra-se a demonstração para o caso em que K é uma álgebra (Definição 1.47) finitamente gerada.

1.2 Álgebra Linear

Para realizar o estudo dos conceitos apresentados nesta seção utilizamos a referência [8].

Definição 1.30 (Espaço Vetorial)**.** *Dizemos que V tem uma estrutura de espaço vetorial sobre um corpo de escalares K com as operações de adição $+$ e de multiplicação por escalar $\cdot$ se as seguintes condições são satisfeitas:*

A.1) $\forall x, y, z \in V,\ (x + y) + z = x + (y + z)$.

A.2) $\exists 0 \in V$ *tal que* $\forall x \in V$, $0 + x = x$ *e* $x + 0 = x$.

A.3) $\forall x \in V$, $\exists z \in V$ *tal que* $x + z = 0$ *e* $z + x = 0$. *Este elemento z é denotado por $-x$.*

A.4) $\forall x, y \in V$, $x + y = y + x$.

M.1) $\forall x \in V$, $\forall \alpha,\ \beta \in K$, $(\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$.

M.2) $\forall x, y \in V$, $\forall \alpha,\ \beta \in K$, $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$ *e* $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$

M.3) $\forall x \in V$, $1 \cdot x = x$.

Definição 1.31 (Subespaço)**.** *Sejam V um espaço vetorial sobre K com as operações $+$ e $\cdot$ e W um subconjunto não vazio de V. Dizemos que W é um subespaço vetorial de V se, e somente se, as seguintes condições são satisfeitas*

i) *W é fechado em relação à operação adição sobre V. Isto é, se $x, y \in W$, então $x + y \in W$;*

ii) *W é fechado (estável) em relação à operação multiplicação por escalar sobre V. Isto é, se $x \in W$, então $\alpha \cdot x \in W$, $\forall \alpha \in K$.*

Definição 1.32 (Combinação Linear)**.** *Sejam V um espaço vetorial sobre K e $y \in V$. Dizemos que y é uma combinação linear de $x_1, \dots, x_n$ se, e somente se, existem $\alpha_1, \dots, \alpha_n \in K$ tais que $y = \alpha_1 x_1 + \cdots + \alpha_n x_n$.*

Definição 1.33. *Sejam V um espaço vetorial sobre K e S um subconjunto não vazio de V. Denotamos por $\langle S \rangle$ o conjunto de todas as combinações lineares de elementos de S. Temos que $\langle S \rangle$ é um subespaço e chamamos $\langle S \rangle$ de subespaço gerado por S.*

Definição 1.34. *Sejam V um espaço vetorial sobre K e $S \subset V$. Dizemos que S é um subconjunto linearmente dependente se, e somente se, existem vetores distintos $x_1, \dots, x_n \in S$ e escalares $\alpha_1, \dots, \alpha_n \in K$ não todos nulos tais que*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0. \tag{1.11}$$

Caso contrário, S é dito linearmente independente.

Definição 1.35 (Base)**.** *Seja V um espaço vetorial sobre K. Dizemos que um subconjunto $B \subset V$ é uma base de V se satisfaz*

i) *B gera V, isto é, $\langle B \rangle = V$;*

ii) *B é um conjunto linearmente independente.*

Dizemos que V é um espaço vetorial de dimensão finita se, e somente se, V admite uma base finita. Neste caso, definimos a dimensão de V como a quantidade de elementos em uma base B de V.

A definição de dimensão para um espaço vetorial de dimensão finita fica bem definida pelo seguinte resultado.

Teorema 1.36. *Seja V um espaço vetorial sobre K e o conjunto de vetores $x_1, x_2, \dots, x_m$ uma base de V. Então todo subconjunto linearmente independente de V é finito e contém no máximo m elementos.*

Demonstração. Para demonstrar o teorema basta mostrar que todo subconjunto S de V que contém mais de m vetores é linearmente dependente. Seja S tal conjunto, então existem vetores $y_1, \dots, y_n \in S$ distintos onde $n > m$. Como cada y_j com $j = 1, \dots, n$ está em V temos $y_j = \sum_{i=1}^{m} \alpha_{ij} x_i$, com $\alpha_{ij} \in K$ para $j = 1, \dots, n$. Se $\beta_1 y_1 + \cdots + \beta_n y_n = 0$, onde β_j são escalares, temos

$$\sum_{j=1}^{n} \beta_j y_j = \sum_{j=1}^{n} \beta_j \left(\sum_{i=1}^{m} \alpha_{ij} x_i \right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} \beta_j \right) x_i = 0. \tag{1.12}$$

Como $\{x_1, \dots, x_m\}$ é base de V, temos, para todo i, que

$$\sum_{j=1}^{n} \alpha_{ij} \beta_j = 0. \tag{1.13}$$

Isto representa um sistema de equações homogêneo com m linhas e n variáveis. Como $m < n$, existe solução não trivial, isto é, existem $(\beta_1, \ldots, \beta_n) \in K^n$ não todos nulos satisfazendo a equação (1.12). Portanto, S é um conjunto linearmente dependente.

□

Definição 1.37 (Transformação Linear)**.** *Sejam V e W espaços vetoriais sobre K. Uma transformação linear de V em W é uma função $T:\ V \to W$ tal que*

$$T(\alpha x + y) = \alpha T(x) + T(y) \tag{1.14}$$

para todo $x, y \in V$ e para todo escalar $\alpha \in K$.

Definição 1.38. *Sejam V e W espaços vetoriais sobre K e T uma transformação linear de V em W. O conjunto $ker\,(T) = \{x \in V \mid T(x) = 0\}$ é chamado núcleo de T. O conjunto $Im\,(T) = \{y \in W \mid \exists x \in V \text{ tal que } T(x) = y\}$ é chamado imagem de T.*

Temos que $Ker(T)$ e $Im(T)$ são subespaços vetoriais.

A seguir finalizamos a seção com um resultado que relaciona as dimensões de $Im\,(T)$ e $ker\,(T)$.

Teorema 1.39 (Teorema do Núcleo e da Imagem)**.** *Sejam V e W espaços vetoriais sobre K e T uma transformação linear de V em W. Se V é um espaço de dimensão finita, então*

$$dim\ Im\,(T) + dim\ ker\,(T) = dim\ V. \tag{1.15}$$

A demonstração do Teorema 1.39 pode ser encontrada na referência [8], página 71.

1.3 MÓDULOS E SEQUÊNCIAS

O conceito de módulo sobre um anel é a generalização da noção de espaço vetorial, em que, em vez de um corpo, temos um anel como o conjunto de escalares. Dessa forma, um módulo, como espaços vetoriais, é o produto entre elementos de um grupo abeliano com um anel. Nesta seção introduzimos a definição e propriedades elementares de módulos. Além disso, apresentamos brevemente a noção de sequência de A-módulos, de localização e de anéis (e módulos) graduados. Para a construção desta seção utilizamos a referência [1].

Definição 1.40 (Módulo)**.** *Seja A um anel. Um A-módulo é um par (M, μ) onde M é um grupo abeliano e $\mu : A \times M \to M$ que leva $(a, m) \mapsto am$ e satisfaz:*

i) $a(m + n) = am + an$*;*

ii) $(a + b)m = am + bm$*;*

iii) $(ab)m = a(bm)$*;*

iv) $1m = m$*;*

para todo $a, b \in A$ *e* $m, n \in M$*.*

Definição 1.41 (Submódulo)**.** *Sejam* A *um anel e* M *um* A*-módulo. Um submódulo* M' *de* M *é um subgrupo de* M *que é fechado em relação à multiplicação por elementos de* A*.*

O grupo abeliano M/M' herda uma estrutura de A-módulo de M, definida por $a(m+M') = am + M'$. Logo M/M' é definido como sendo o A-módulo quociente de M por M'.

Definição 1.42. *Sejam* M *um* A*-módulo e* $(M_i)_{i\in\mathbb{N}}$ *uma família de submódulos de* M*.*

i) *A soma direta* $\oplus M_i$ *será denotada por* $\sum M_i$ *e chamada de soma dos módulos* M_i*.*

ii) *Em geral não podemos definir o produto de dois submódulos, mas podemos definir o produto* IM *onde* I *é um ideal e* M *um* A*-módulo, como sendo o conjunto de todas as somas finitas* $\sum a_i m_i$ *com* $a_i \in I$ *e* $m_i \in M_i$*.*

A soma $\sum M_i$ é um submódulo de M e é o menor submódulo de M que contém todos os M_i. A interseção $\cap M_i$ e o produto IM também são submódulos de M.

Se um módulo $M = \sum Am_i$ dizemos que os m_i's formam um conjunto de geradores de M, isto significa que todo elemento de M pode ser expresso (não necessariamente de maneira única) como uma combinação linear finita dos m_i's com coeficientes em A. Um A-módulo é dito finitamente gerado se ele tem um conjunto finito de geradores.

Definição 1.43 (Aniquilador)**.** *Sejam* M *um módulo e* N *e* P *submódulos de* M*. Definimos* $(N : P)$ *como sendo o conjunto de todos os* $a \in A$ *tais que* $aP \subseteq N$*, logo* $(N : P)$ *é um ideal de* A*. Em particular,* $(0 : M)$ *é o conjunto de todos os* $a \in A$ *tais que* $aM = 0$*, este ideal é chamado aniquilador de* M *e é denotado por* $Ann(M)$*.*

Assim como definimos homomorfismo entre anéis (Definição 1.20), definimos agora homomorfismos entre A-módulos.

Definição 1.44. *Sejam* M *e* N A*-módulos. Uma função* $f : M \to N$ *é dita* A*-homomorfismo se para quaisquer* $m_1, m_2 \in M$ *e* $a \in A$*, valem as seguintes condições*

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$*;*

(ii) $f(am_1) = af(m_1)$*.*

A seguir apresentamos uma forma de representar uma relação entre homomorfismos de A-módulos por meio de diagramas: sequências exatas.

Definição 1.45 (Sequência exata)**.** *Sejam* $\{\ldots, M_{i-1}, M_i, M_{i+1}, \ldots\}$ *uma família de* A*-módulos e* $\{\ldots, f_{i+1} : M_i \to M_{i+1}, \ldots\}$ *uma família de* A*-homomorfismos. A sequência*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \tag{1.16}$$

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

Definição 1.46. *Uma sequência exata de A-módulos e A-homomorfismos do tipo*

$$0 \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow 0 \tag{1.17}$$

é dita sequência exata curta.

A seguir definimos mais uma estrutura algébrica.

Definição 1.47 (Álgebra)**.** *Sejam K um corpo e A um espaço vetorial sobre K equipado com uma operação binária $\cdot : A \times A \to A$ chamada de multiplicação. Então A é uma K-álgebra se para todo $x, y, z \in A$ e $a, b \in K$ valem as seguintes propriedades:*

(i) $(x + y) \cdot z = x \cdot z + y \cdot z$;

(ii) $z \cdot (x + y) = z \cdot x + z \cdot y$;

(iii) $(ax) \cdot (by) = (ab)(x \cdot y)$.

Os próximos conceitos serão fundamentais para a construção da seção 4.1.

Definição 1.48 (Anel graduado)**.** *Um anel graduado A é um anel com uma família $(A_n)_{n\in\mathbb{Z}}$ de subgrupos aditivos de A tais que $A = \bigoplus_{n\in\mathbb{Z}} A_n$ e $A_m A_n \subseteq A_{n+m}$ para todo $n, m \in \mathbb{Z}$.*

Definição 1.49. *Sejam A um anel graduado e M um A-módulo. Então M é dito graduado se existe uma família de subgrupos aditivos $(M_n)_{n\geq 0}$ de M tais que*

$$M = \oplus_{n=0}^{\infty} M_n \quad e \quad A_m M_n \subseteq M_{n+m} \; \forall \; m, n \geq 0.$$

Um elemento não nulo $x \in M$ é dito homogêneo de grau n se $x \in M_n$.

Definição 1.50. *Sejam A um anel graduado e I um ideal de A. O ideal I é dito homogêneo se é gerado por um conjunto de elementos homogêneos.*

Um módulo graduado que também é um anel graduado é dito álgebra graduada.

Exemplo 1.51. *O anel de polinômios $\mathbb{C}[x] = \oplus A_i$ é um anel graduado onde $A_i = \{ax^i\}$. O ideal $I = \langle x^2 \rangle$ é um ideal homogêneo em $\mathbb{C}[x]$. Analogamente $J = \langle x^2 + y^2 + z^2, xy, yz + zx, z^5 \rangle$ é um ideal homogêneo em $\mathbb{C}[x, y, z]$.*

Como uma generalização da forma em que construímos o corpo de frações de um domínio (Definição 1.25), podemos construir a localização em um subconjunto multiplicativo de um anel como sendo o anel obtido invertendo formalmente os elementos deste subconjunto.

Definição 1.52. *Seja A um anel. Um conjunto multiplicativo $S \subseteq A$ é um subconjunto que é fechado por produto, ou seja, se $s, t \in S$ então $st \in S$, e tal que $1 \in S$. Defina uma relação $\equiv$ em $A \times S$ como segue:*

$$(a, s) \equiv (a', s') \Leftrightarrow (as' - a's)u = 0 \text{ para algum } u \in S. \tag{1.18}$$

A relação $\equiv$ é uma relação de equivalência.

Denotemos por $\frac{a}{s}$ a classe de equivalência de (a, s) e seja $S^{-1}A = (A \times S)/\equiv$ o conjunto das classes de equivalências. Vamos colocar uma estrutura de anel $S^{-1}A$ definindo adição e multiplicação da maneira usual:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \quad \text{e} \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}. \tag{1.19}$$

Com estas operações de adição e multiplicação definimos o seguinte:

Definição 1.53 (Localização). *Seja $S^{-1}A$ o anel comutativo com elemento nulo $\frac{0}{1}$ e elemento identidade $\frac{1}{1}$. Este anel é dito de localização de A com respeito a S. Associado a $S^{-1}A$ temos um homomorfismo de anéis $\rho : A \to S^{-1}A$ dado por $a \mapsto \frac{a}{1}$ chamado de mapa de localização.*

Proposição 1.54 (Anel local). *Seja A um anel. As seguintes condições são equivalentes:*

i) *O conjunto de elementos não invertíveis de A forma um ideal.*

ii) *A possui um único ideal maximal que contém todo ideal próprio de A.*

Um anel que satisfaz tais condições é chamado anel local.

Demonstração. Suponha que A possui um único ideal maximal m que contém todo ideal próprio de A. Considere J o conjunto de elementos não invertíveis. Sejam $x, y \in J$ e $a \in A$. Temos que $x + y \in J$, pois $\langle x \rangle \subseteq m$ e $\langle y \rangle \subseteq m$ e portanto $\langle x + y \rangle \subseteq m$, o que mostra que $x + y \in J$. E suponha $ax \notin J$, logo $1 = rax = (ra)x$ para algum $r \in A$, ou seja, x é invertível, absurdo. Logo $ax \in J$ e, consequentemente, J é um ideal.

Por outro lado, suponha que o conjunto de elementos não invertíveis J de A é um ideal. Todo ideal próprio I de A não contém elementos invertíveis, logo $I \subset J$, $\forall I$, portanto, J é o único ideal maximal de A. $\square$

A seguir apresentamos um exemplo de anel local.

Exemplo 1.55. *Sejam A um domínio e $p \subseteq A$ um ideal primo. Então o conjunto $S = A \setminus p$ é multiplicativo. A localização de A por S é um anel denotado por A_p e dito localização de A por p. A extensão pA_p de p em A_p é o único ideal maximal em A_p, pois cada elemento fora dele é invertível.*

Desta forma, temos que o anel A_p é um anel local.

Se A é um anel graduado e p é um ideal homogêneo primo em A, então denotamos por $A_{(p)}$ o subanel de elementos de grau 0 na localização $T^{-1}A$ em respeito ao conjunto multiplicativo T formado pelos elementos homogêneos de A que não estão em p.

O conjunto $T^{-1}A$ tem uma graduação natural dada por

$$grau(f/g) = grau(f) - grau(g), \tag{1.20}$$

para f homogêneo em A e $g \in T$. Assim, $A_{(p)}$ é um anel local e o único ideal maximal é a interseção $(p \cdot T^{-1}A) \cap A_{(p)}$. Em particular, se A é um domínio, então para $p = \langle 0 \rangle$ obtemos o corpo $A_{(\langle 0\rangle)}$. Analogamente, se $f \in A$ é um elemento homogêneo, denotamos por $A_{(f)}$ o subanel de elementos de grau 0 no anel localizado S.

Proposição 1.56 (Propriedade Universal da Localização)**.** *Seja $g: A \to B$ um homomorfismo de anéis tal que todos os elementos $g(s) \in B$, $s \in S$ são invertíveis. Então existe um único homomorfismo $h: S^{-1}A \to B$ tal que $g = h \circ \rho$.*

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "\rho"'] & B \\ S^{-1}A \arrow[ur, "h"'] & \end{tikzcd}$$

A demonstração da Proposição 1.56 pode ser encontrada em [1], página 37.

Assim, temos o seguinte fato:

Proposição 1.57. *Se A é um domínio, o conjunto $S = A \setminus \{0\}$ é multiplicativo e a localização por S é somente o corpo de frações de A.*

Proposição 1.58. *Sejam $S_1 \subseteq S_2$ conjuntos multiplicativos e $\rho: A \to S_1^{-1}A$ o homomorfismo canônico dado na Definição 1.53. Então a localização dupla $(\rho(S_2))^{-1}S_1^{-1}A$ é isomorfa à $S_2^{-1}A$.*

Juntando a Proposição 1.57, o Exemplo 1.55 e a transitividade de localização para um domínio A, temos o seguinte resultado:

Proposição 1.59. *Sejam A um domínio e $\mathfrak{p}$ um ideal primo de A. Então o corpo de frações de A é igual ao corpo de frações da localização de A por $\mathfrak{p}$. Isto é, considere a transitividade de localização com dois conjuntos multiplicativos $A \setminus \mathfrak{p} \subseteq A \setminus \{0\}$.*

1.4 Topologia Geral

Topologia geral é um ramo da Matemática que preocupa-se com o estudo da generalização dos conceitos de distância, continuidade e convergência. Nesta seção trazemos alguns conceitos básicos desta área. Para a construção desta seção utilizamos a referência [10].

Definição 1.60 (Topologia)**.** *Seja X um conjunto. Uma coleção τ de subconjuntos de X é dita topologia se satisfaz as seguintes condições:*

i) *O conjunto vazio $\varnothing$ e o conjunto todo X pertencem à τ;*

ii) *A união dos elementos de qualquer subcoleção de τ pertence à τ;*

iii) *A interseção dos elementos de qualquer subcoleção finita de τ pertence à τ.*

Espaço topológico é o par ordenado (X, τ), onde X é um conjunto e τ é uma topologia em X.

Definição 1.61. *Sejam τ e τ' topologias em um conjunto X. Se $\tau \subseteq \tau'$, dizemos que τ' é mais fina que τ.*

Dados (X, τ) e $Y \subseteq X$, definimos $\tilde{\tau} = \{Y \cap A; A \in \tau\}$. Temos que $(Y, \tilde{\tau})$ é um espaço topológico. Neste caso, dizemos que Y é um subespaço de X.

Definição 1.62 (Aberto). *Seja X um espaço topológico com uma topologia τ , um subconjunto $A \subseteq X$ é um conjunto aberto de X se $A \in \tau$.*

Com a Definição 1.62 podemos reescrever a noção de "mais fina". Se τ e τ' são topologias em um conjunto X, tais que todo aberto de τ é um aberto de τ', então τ' é mais fina que τ.

Definição 1.63 (Fechado). *Seja X um espaço topológico e F um subconjunto de X. Dizemos que F é fechado se o conjunto $X - F$ for aberto.*

Definição 1.64 (Interior). *Seja X um espaço topológico e Z um subconjunto de X. O interior de Z é a união de todos os conjuntos abertos contidos em Z.*

Definição 1.65 (Fecho). *Seja X um espaço topológico e Z um subconjunto de X. O fecho de Z é a interseção de todos os conjuntos fechados que contêm Z. Equivalentemente, o fecho de Z é o menor fechado que contém Z.*

Denotamos o fecho de Z por $\overline{Z}$.

Definição 1.66. *Seja X um espaço topológico. O subconjunto Z de X é dito denso em X se o fecho de Z é igual a X. Equivalentemente, Z é denso em X se qualquer vizinhança de um ponto $x \in X$ possui um elemento $a \in Z$.*

Por exemplo, com a topologia usual de $\mathbb{R}$, temos que $\mathbb{Q}$ é denso em $\mathbb{R}$.

Segue da Definição 1.66 o seguinte resultado:

Proposição 1.67. *Sejam τ e τ' topologias em um conjunto X tal que τ' é mais fina que τ. Então o fecho de um conjunto Z em τ' está contido no fecho de Z em τ.*

Teorema 1.68. *Seja X um espaço topológico. Então as seguintes condições valem:*

i) *$\varnothing$ e X são fechados;*

ii) *Interseção arbitrária de conjuntos fechados é um conjunto fechado;*

iii) *União finita de conjuntos fechados é um conjunto fechado.*

Veja demonstração do Teorema 1.68 em [10], página 94.

Os seguintes resultados serão utilizados na comparação da Topologia de Zariski com a topologia usual em $\mathbb{C}^n$.

Teorema 1.69. *Seja X um espaço topológico e Y um subespaço de X. Então um conjunto Z é fechado em Y se, e somente se, Z é igual a interseção de um conjunto fechado de X com Y.*

Veja demonstração do Teorema 1.69 em [10], página 94.

Definição 1.70. *Seja X um espaço topológico e Y um subespaço de X. Dizemos que Y é localmente fechado se para todo $a \in Y$, existe um aberto U em X tal que $U \cap Y$ é fechado em U.*

Teorema 1.71. *Seja X um espaço topológico, Y um subespaço de X e Z um subconjunto de Y. Então o fecho de Z em Y é $\overline{Z} \cap Y$. Onde $\overline{Z}$ denota o fecho de Z em X.*

Demonstração. Seja $\overline{Z}^Y$ o fecho que Z em Y. O fecho $\overline{Z}$ é fechado em X, então, pelo Teorema 1.69, $\overline{Z} \cap Y$ é fechado em Y. Como $\overline{Z}$ contém Z e Y contém Z temos que $\overline{Z} \cap Y$ contém Z. E como $\overline{Z}^Y$ é, por definição, a interseção de todos os conjuntos fechados de Y que contêm Z, temos $\overline{Z}^Y \subset (\overline{Z} \cap Y)$.

Por outro lado, sabemos que $\overline{Z}^Y$ é fechado em Y, então, pelo Teorema 1.69, $\overline{Z}^Y = F \cap Y$ para algum conjunto fechado F em X. Logo F é um conjunto fechado de X que contém Z e como $\overline{Z}$ é a interseção de todos os conjuntos fechados de X que contêm Z, temos que $\overline{Z} \subset F$. Portanto, $(\overline{Z} \cap Y) \subset (F \cap Y) = \overline{Z}^Y$, ou seja, $\overline{Z}^Y = \overline{Z} \cap Y$. □

Teorema 1.72. *Seja X um espaço topológico e Y um subconjunto localmente fechado de X. Então Y é aberto em $\overline{Y}$.*

Demonstração. Como Y é localmente fechado, dado $a \in Y$ existe um aberto U em X tal que $U \cap Y$ é fechado em U. Temos que $U \cap \overline{Y}$ é aberto em $\overline{Y}$. Como $U \cap Y$ fechado em U temos que $\overline{U \cap Y}^U = U \cap Y$, então, pelo Teorema 1.71, $U \cap \overline{Y} = U \cap Y$.

Dessa forma, como a é um ponto arbitrário e como $U \cap \overline{Y} = U \cap Y \subset Y$ é aberto em $\overline{Y}$, segue que Y é aberto em $\overline{Y}$. □

2. Alguns teoremas clássicos

Neste capítulo enunciamos e demonstramos alguns teoremas clássicos. Em particular, demonstramos o Teorema da Base Hilbert e o Teorema de Zeros de Hilbert.

Além disso, apresentamos os conjuntos algébricos e como estes objetos são definidos em termos de ideais, exibimos propriedades básicas de conjuntos algébricos e consequências do Teorema de Zeros de Hilbert. Por fim, mostramos a possibilidade de induzir uma topologia, chamada de Topologia de Zariski sobre essas estruturas. Utilizamos como referência [12], [9] e [6].

2.1 Anéis noetherianos e Teorema da Base de Hilbert

Emmy Noether foi uma matemática alemã que contribuiu de maneira significativa nos campos de Física Teórica e Álgebra Abstrata, considerada uma das mulheres mais importantes da história da matemática, ela revolucionou as teorias sobre anéis, corpos e álgebra. Em 1921, no artigo "*Idealtheorie in Ringbereichen*" ela utilizou de forma elegante a Condição da Cadeia Ascendente e, por isso, objetos que satisfazem esta condição são ditos noetherianos em homenagem à Emmy Noether. A seguir, apresentamos alguns destes conceitos.

Definição 2.1 (Anel noetheriano)**.** *Dizemos que um anel A é um anel noetheriano se qualquer ideal I de A for finitamente gerado, isto é, existem $r_1, \ldots, r_k \in A$ tais que $I = \langle r_1, \ldots, r_k \rangle$.*

Apresentamos a seguir resultados que caracterizam a definição acima.

Teorema 2.2. *Seja A um anel. Temos que A é um anel noetheriano se, e somente se, A satisfaz a condição de cadeia ascendente, isto é, para a cadeia de ideais encaixados $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots$, existe $k \in \mathbb{N}$ tal que $I_k = I_j$ para todo $j \geq k$.*

Demonstração. Primeiramente, provaremos que se A um anel noetheriano, então A satisfaz a condição de cadeia ascendente. De fato, dada uma cadeia arbitrária

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots \tag{2.1}$$

Considere $I := \bigcup\limits_{i \in \mathbb{N}} I_i$. Temos que I é um ideal de A pois é a união de ideais encaixados de A.

Como A é um anel noetheriano (Definição 2.1), segue que I é finitamente gerado, ou seja, $I = \langle r_1, \ldots, r_t \rangle$. Provaremos agora que $I = I_j$ para algum $j \in \mathbb{N}$.

Pela definição de I, segue que para todo $i \in \{1, \ldots, t\}$, existem $j_i \in \mathbb{N}$ tais que $r_i \in I_{j_i}$. Desta forma, seja $j := \max\{j_1, \ldots, j_t\}$. Temos então

$$I_j \supseteq \{r_1, \ldots, r_t\}. \tag{2.2}$$

Logo, $I_j \supset I$. Por outro lado, como $I_j \subseteq I_{j+1} \subseteq \cdots \subseteq \cup I_i = I$, segue, portanto, que $I_j = I_{j+1} = \cdots = I$. Assim, concluímos que a cadeia (2.1) satisfaz a condição de cadeia ascendente e, como a cadeia é arbitrária, temos que A satisfaz a condição de cadeia ascendente.

Seja A um anel que satisfaz a condição de cadeia ascendente, mostraremos que A é um anel noetheriano.

A prova será por absurdo. Tome I um ideal de A e suponha que I não é finitamente gerado. Considere $i_1 \in I$ e defina $I_1 := \langle i_1 \rangle$. Seja $i_2 \in I \setminus I_1$ e considere $I_2 := \langle i_1, i_2 \rangle$. De modo análogo, tomemos $i_n \in I \setminus I_{n-1}$ e definimos $I_n := \langle i_1, i_2, \ldots, i_n \rangle$. Sempre é possível encontrar i_j visto que I não é finitamente gerado. Por construção, obtemos a seguinte cadeia:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_n \subsetneq \ldots. \tag{2.3}$$

Por hipótese A satisfaz a condição de cadeia ascendente, então existe $k \in \mathbb{N}$ tal que $I_k = I_j$ para todo $j \geq k$, o que implica que I é finitamente gerado, o que é absurdo. Logo, todo ideal I de A é finitamente gerado, o que prova que A é um anel noetheriano. □

Teorema 2.3. *Seja A um anel. Temos que A é um anel noetheriano se, e somente se, A satisfaz a condição maximal, isto é, toda família não-vazia de ideais admite elemento maximal na família.*

Demonstração. Seja A um anel noetheriano, mostraremos que A satisfaz a condição maximal. Seja $\mathcal{F}$ uma família de ideais de A não vazia tal que $\mathcal{F}$ não tem elemento maximal. Assim, seja $I_1 \in \mathcal{F}$, então existe $I_2 \in \mathcal{F}$ tal que $I_1 \subsetneq I_2$. Segue que, existe $I_3 \in \mathcal{F}$ tal que $I_2 \subsetneq I_3$. Assim, obtemos a seguinte cadeia de ideais

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq I_n \subsetneq \ldots. \tag{2.4}$$

que não estabiliza, absurdo. Pois, pelo Teorema 2.2, toda cadeia de ideais encaixados de A estabiliza. Logo $\mathcal{F}$ tem um elemento maximal.

Por outro lado, seja A um anel que satisfaz a condição maximal, suponhamos por contradição que A não é noetheriano. Então, pelo Teorema 2.2, existe pelo menos uma cadeia de ideais em A que não estabiliza, que denotaremos por

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \ldots \tag{2.5}$$

Considere a família $\mathcal{F} = \{I_i \mid i \in \mathbb{N}\}$, temos que $\mathcal{F}$ não tem elemento maximal, o que contraria a hipótese. Portanto, A é noetheriano. $\square$

Teorema 2.4 (Teorema da Base de Hilbert). *Seja A um anel noetheriano. Então o anel de polinômios $A[x]$ também é noetheriano.*

Demonstração. Suponha que $A[x]$ não é noetheriano, então existe um ideal $\mathcal{J} \subset A[x]$ tal que $\mathcal{J}$ não é finitamente gerado. Seja $f_1(x) \in \mathcal{J}$ um polinômio não constante de menor grau possível. Seja $f_2(x)$ um polinômio não constante de menor grau possível em $\mathcal{J} \setminus \langle f_1 \rangle$. De modo análogo, seja

$$f_n(x) \in \mathcal{J} \setminus \langle f_1, \dots, f_{n-1} \rangle$$

de menor grau possível. Notemos que, as escolhas dos f_i sempre é possível devido ao Princípio da Boa Ordem e pelo fato de $\mathcal{J}$ não ser finitamente gerado. Para cada i, considere $gr(f_i) := m_i \neq 0$. Temos que $m_{i+1} > m_i$, $\forall i$. Podemos escrever $f_i = a_i x^{m_i} + \dots$ e tomemos a seguinte cadeia de ideais de A:

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \cdots \subset \langle a_1, a_2, a_3, \dots, a_n \rangle \subset \dots \tag{2.6}$$

Como A é um anel noetheriano, segue que A satisfaz a condição de cadeia ascendente e portanto existe $n \in \mathbb{N}$ tal que:

$$\langle a_1, a_2, a_3, \dots, a_n \rangle = \langle a_1, a_2, a_3, \dots, a_n, a_{n+1} \rangle = \langle a_1, a_2, a_3, \dots, a_n, a_{n+1}, a_{n+2} \rangle = \dots \tag{2.7}$$

Assim $a_{n+1} \in \langle a_1, a_2, a_3, \dots, a_n \rangle$. Logo, existem $\alpha_i \in A$ tais que $a_{n+1} = \sum_{i=1}^{n} \alpha_i a_i$. Tomemos

$$g(x) := f_{n+1}(x) - \sum_{i=1}^{n} \alpha_i x^{m_{n+1} - m_i} f_i(x). \tag{2.8}$$

Por construção, g satisfaz as seguintes propriedades:

i) $g(x) \neq 0$;

ii) $g(x) \notin \langle f_1, \dots, f_n \rangle$;

iii) $gr(g(x)) < gr(f_{n+1}(x))$.

Logo, f_{n+1} não é o polinômio de menor grau possível em $\mathcal{J} \setminus \langle f_1, \dots, f_n \rangle$, o que é um absurdo pela escolha de f_{n+1}. Portanto, obtemos que $A[x]$ é noetheriano. $\square$

O Teorema 2.4 admite uma generalização natural como se segue.

Corolário 2.5. *Sejam A um anel noetheriano e $x_1, \dots, x_n$ variáveis. Então o anel de polinômios $A[x_1, \dots, x_n]$ é noetheriano.*

Demonstração. Utilizaremos indução sobre n.
i) O caso $n = 1$, segue pelo Teorema 2.4;

ii) Suponhamos que $A[x_1, \ldots, x_n]$ é noetheriano. Verificaremos que $A[x_1, \ldots, x_{n+1}]$ é noetheriano. De fato, considere $A' = A[x_1, \ldots, x_n]$, aplicando o Teorema 2.4, temos que $A'[x_{n+1}]$ é noetheriano. Como

$$A'[x_{n+1}] = A[x_1, \ldots, x_n][x_{n+1}] = A[x_1, \ldots, x_n, x_{n+1}],$$

temos que $A[x_1, \ldots, x_{n+1}]$ é noetheriano, o que termina a prova. □

2.2 Conjuntos algébricos

Um dos estudos em Geometria Algébrica é a geometria das formas determinadas por equações algébricas. De forma simplificada, é o estudo geométrico do conjunto de zeros de uma família de polinômios. Assim, nesta seção, apresentamos os conjuntos algébricos buscando constituir uma relação entre a Álgebra e a Geometria.

Definição 2.6 (Espaço Afim)**.** *Seja K um corpo algebricamente fechado. O conjunto de todas as n-uplas $(a_1, \ldots, a_n)$ de elementos de K é denotado por K^n e será chamado de n-espaço afim sobre K.*

Definição 2.7 (Conjunto Algébrico)**.** *Denotamos o conjunto de todas as soluções em K^n de um sistema de equações*

$$f_\alpha(x_1, \ldots, x_n) = 0, \quad \alpha = 1, \ldots, l,$$

onde cada f_α é um polinômio do anel de polinômios $K[x_1, \ldots, x_n]$, por $V(f_1, \ldots, f_l)$ e chamamos de conjunto algébrico. Ou seja,

$$V(f_1, \ldots, f_l) = \{(a_1, \ldots, a_n) \in K^n \mid f_\alpha(a_1, \ldots, a_n) = 0,\ \alpha = 1, \ldots, l\}. \tag{2.9}$$

Definição 2.8. *Para um ideal I em um anel de polinômios $K[x_1, \ldots, x_n]$, definimos*

$$V(I) = \{(b_1, \ldots, b_n) \in K^n \,|\, \forall\, g \in I,\ g(b_1, \ldots, b_n) = 0\}. \tag{2.10}$$

$V(I)$ é dito o conjunto algébrico determinado pelo ideal I.

Lema 2.9. *Quando $I = \langle f_1, \ldots, f_l \rangle$, temos $V(I) = V(f_1, \ldots, f_l)$.*

Demonstração. Por um lado, para um elemento arbitrário f do ideal I gerado por $f_1, \ldots, f_l$ no anel de polinômios $K[x_1, \ldots, x_n]$ de n variáveis, existem $g_\alpha \in K[x_1, \ldots, x_n]$, $\alpha = 1, \ldots, l$, tais que

$$f(x_1, \ldots, x_n) = \sum_{\alpha=1}^{l} g_\alpha(x_1, \ldots, x_n) f_\alpha(x_1, \ldots, x_n). \tag{2.11}$$

Assim, se $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_l)$ segue que $f_1(a_1, \ldots, a_n) = \ldots = f_l(a_1, \ldots, a_n) = 0$, o que implica $f(a_1, \ldots, a_n) = 0$. Logo, $V(f_1, \ldots, f_l) \subset V(I)$. Mostraremos agora que $V(I) \subset V(f_1, \ldots, f_l)$. Seja $(b_1, \ldots, b_n) \in V(I)$, como $f_\alpha \in I$, temos $f_\alpha(b_1, \ldots, b_n) = 0$, para todo $\alpha = 1, \ldots, l$. Assim, $V(I) \subset V(f_1, \ldots, f_l)$, o que termina a prova. □

O Teorema da Base de Hilbert (Teorema 2.4) garante que todo ideal do anel de polinômios $K[x_1, \ldots, x_n]$ é da forma $I = \langle f_1, \ldots, f_l \rangle$. Então, pelo Lema 2.9, o conjunto algébrico determinado por um ideal é, de fato, o conjunto algébrico de um sistema de equações. E mais, o conjunto algébrico $V(f_1, \ldots, f_l)$, determinado pelo sistema de equações

$$f_\alpha = 0, \quad \alpha = 1, \ldots, l$$

é precisamente o conjunto algébrico determinado pelo ideal $I = \langle f_1, \ldots, f_l \rangle$ no anel de polinômios $K[x_1, \ldots, x_n]$ gerado por $f_1, \ldots, f_l$. No decorrer deste trabalho estudaremos mais o conjunto algébrico $V(I)$ determinado pelo ideal I do que o sistema de equações.

Para o ideal nulo $\langle 0 \rangle$, temos que $V(\langle 0 \rangle) = K^n$. Dessa forma, os n-espaços afins sobre K não são apenas espaços vetoriais n-dimensionais, mas também são conjuntos algébricos e quando considerados como tal, denotaremos por $\mathbb{A}^n$ ou $\mathbb{A}^n_K$.

O próximo resultado caracteriza todos os conjuntos algébricos de $\mathbb{A}^1_K$.

Lema 2.10. *Os conjuntos algébricos próprios e não vazios de $\mathbb{A}^1_K$ são conjuntos finitos de pontos.*

Demonstração. Seja $V \subsetneq \mathbb{A}^1_K$ um conjunto algébrico, isto é, $V = V(S)$ para algum subconjunto de polinômios $S \subset K[x]$. Assim, $V = \{a \in K^1 \mid f(a) = 0, \forall f \in S\}$. Se V for infinito, um polinômio de uma variável f admitirá infinitas raízes, absurdo. Logo V é finito. $\square$

A seguir, apresentamos resultados fundamentais para a correspondência entre ideais e conjuntos algébricos.

Proposição 2.11. *Para ideais I, J e $\{I_\lambda\}_{\lambda \in \Lambda}$ no anel de polinômios $K[x_1, \ldots, x_n]$ sobre um corpo K, $\lambda \in \Lambda$, onde Λ pode ser um conjunto infinito, temos:*

i) $V(I) \cup V(J) = V(I \cap J)$;

ii) $\cap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$;

iii) $V(I) \supset V(J)$, *para* $\sqrt{I} \subset \sqrt{J}$,

onde $\sum_{\lambda \in \Lambda} I_\lambda$ *denota o ideal de* $K[x_1, \ldots, x_n]$ *gerado por* $\{I_\lambda\}_{\lambda \in \Lambda}$ *e* $\sqrt{I} = \{f \in K[x_1, \ldots, x_n] | f^m \in I$ *para algum inteiro* $m\}$, $\sqrt{I}$ *é dito radical de* I.

Demonstração. **i)** Direto da definição de conjunto algébrico, temos que $V(I) \supset V(J)$ para $I \subset J$. De fato, se $(a_1, \ldots, a_n) \in V(J)$, um zero de todos os polinômios em J é, certamente, zero de todos os polinômios em I. Logo, temos $V(I \cap J) \supset V(I)$ e $V(I \cap J) \supset V(J)$. Assim, $V(I) \cup V(J) \subset V(I \cap J)$.

Por outro lado, tome $(a_1, \ldots, a_n) \in V(I \cap J)$. Se $(a_1, \ldots, a_n) \notin V(I)$ então existe um polinômio $f \in I$ tal que $f(a_1, \ldots, a_n) \neq 0$. Então, para um elemento arbitrário $g(x_1, \ldots, x_n) \in J$, temos $h = f \cdot g \in I \cap J$. Logo,

$$h(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) g(a_1, \ldots, a_n) = 0. \tag{2.12}$$

Consequentemente $g(a_1,\ldots,a_n)=0$, o que implica que $(a_1,\ldots,a_n)\in V(J)$, assim, $V(I\cap J)\subset V(I)\cup V(J)$. Portanto, $V(I\cap J)=V(I)\cup V(J)$.
ii) Como $I_\mu \subset \sum_{\lambda\in\Lambda} I_\lambda$ para todo $\mu\in\Lambda$, temos

$$V(I_\mu)\supset V(\sum_{\lambda\in\Lambda} I_\lambda) \Rightarrow \bigcap_{\mu\in\Lambda} V(I_\mu)\supset V(\sum_{\lambda\in\Lambda} I_\lambda).$$

Para cada λ, escreva I_λ em termos de geradores $I_\lambda=\langle h_{\lambda 1},\ldots,h_{\lambda m_\lambda}\rangle$. Para $(a_1,\ldots,a_n)\in \cap_{\lambda\in\Lambda}V(I_\lambda)$, temos $h_{\lambda j}(a_1,\ldots,a_n)=0$, $j=1,\ldots,m_\lambda$. Por outro lado, $\{h_{\lambda j}\}_{\lambda\in\Lambda,\,1\le j\le m_\lambda}$ gera o ideal $\sum_{\lambda\in\Lambda} I_\lambda$. Assim, $(a_1,\ldots,a_n)\in V(\sum_{\lambda\in\Lambda} I_\lambda)$. Portanto, $\cap_{\lambda\in\Lambda}V(I_\lambda)=V(\sum_{\lambda\in\Lambda} I_\lambda)$.
iii) Basta mostrarmos que $V(\sqrt{I})=V(I)$. Seja $f\in\sqrt{I}$, então $f^m\in I$ para algum inteiro m. Para $(a_1,\ldots,a_n)\in V(I)$, temos $f^m(a_1,\ldots,a_n)=0$. Consequentemente, $f(a_1,\ldots,a_n)=0$, isto é, $(a_1,\ldots,a_n)\in V(\sqrt{I})$, o que mostra que $V(I)\subset V(\sqrt{I})$. A inclusão $V(\sqrt{I})\subset V(I)$, segue pelo fato de que $I\subset\sqrt{I}$. Portanto, $V(I)=V(\sqrt{I})$, o que termina a prova.

□

Corolário 2.12. *Para um quantidade finita de ideais $I_1,\ldots,I_s$ em $K[x_1,\ldots,x_n]$, temos*

$$\bigcup_{j=1}^{s} V(I_j)=V\left(\bigcap_{j=1}^{s} I_j\right).$$

Demonstração. A prova segue por indução sobre s e pela Proposição 2.11, item (i).

□

Na Proposição 2.11 item ii), Λ não precisa ser finito. Já o Corolário 2.12 vale apenas para uma quantidade finita de ideais. A seguir, apresentamos um contraexemplo com um caso em que $K=\mathbb{C}$.

Exemplo 2.13. *Seja $\{c_i\}_{i\in\mathbb{N}}\subset\mathbb{C}$ uma coleção enumerável e infinita de elementos distintos do corpo dos complexos $\mathbb{C}$. Considere os ideais*

$$I_j=\langle x-c_j\rangle,\qquad j\in\mathbb{N}$$

em $\mathbb{C}[x]$. Temos que

$$I_{j_1}\cap\cdots\cap I_{j_s}=\prod_{i=1}^{s}\langle x-c_{j_i}\rangle.$$

Assim, a igualdade

$$\bigcap_{j=1}^{\infty} I_j=\langle 0\rangle$$

vale. Por outro lado, temos

$$\bigcup_{j=1}^{\infty} V(I_j)=\{c_1,c_2,\ldots\},$$

e $V(\langle 0\rangle) = \mathbb{C}^1$. *Podem ser escolhidos* $c_1, c_2, \ldots$ *tais que* $\mathbb{C}^1 \supsetneqq \{c_1, c_2, \ldots\}$. *Então*

$$\bigcup_{j=1}^{\infty} V(I_j) \subsetneqq V\left(\bigcap_{j=1}^{\infty} I_j\right).$$

2.3 Ideal de um conjunto

Apresentamos mais algumas notações.

Definição 2.14. *Dado um conjunto* V *no espaço afim* n*-dimensional* K^n *sobre um corpo algebricamente fechado* K*, definimos o ideal* $I(V)$ *determinado por* V *da seguinte forma*

$$I(V) = \{f \in K[x_1, \ldots, x_n] \mid f(b_1, \ldots, b_n) = 0, \text{ para todo } (b_1, \ldots, b_n) \in V\}.$$

As seguintes propriedades mostram algumas das relações entre ideais e conjuntos algébricos.

Proposição 2.15. *Para* X, Y *subconjuntos de* K^n *e* S *subconjunto de* $K[x_1, \ldots, x_n]$ *temos:*

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

ii) $I(X \cup Y) = I(X) \cap I(Y)$*;*

iii) $I(V(S)) \supset S$ *e* $V(I(X)) \supset X$*;*

iv) $I(V(I(X))) = I(X)$*. Então se* I *é o ideal de um conjunto algébrico* W*,* $I = I(V(I))$*.*

Demonstração. **i)** Tome $f \in I(Y)$, temos $f(P) = 0$ para todo $P \in Y$, Em particular, como $X \subset Y$, $f(P) = 0$ vale para todo $P \in X$. Portanto $f \in I(X)$ e $I(Y) \subset I(X)$.

ii) Como $X \cup Y \supset X$ e $X \cup Y \supset Y$, pelo item (i) temos que $I(X \cup Y) \subset I(X)$ e $I(X \cup Y) \subset I(Y)$, consequentemente, $I(X \cup Y) \subset I(X) \cap I(Y)$.

Por outro lado, tome $f \in I(X) \cap I(Y)$, temos que $f \in I(X)$ e $f \in I(Y)$. Então, $f(P) = 0$, $\forall P \in X$, e $f(P) = 0$, $\forall P \in Y$. Logo $f(P) = 0$, $\forall P \in X \cup Y$. Portanto $f \in I(X \cup Y)$, assim $I(X \cup Y) \supset I(X) \cap I(Y)$. Logo $I(X \cup Y) = I(X) \cap I(Y)$.

iii) Se $f \in S$, então $f(P) = 0$ para todo $P \in V(S)$, pela definição de $V(S)$. Logo $f \in I(V(S))$. Analogamente, se $P \in X$, temos que $g(P) = 0$ para todo $g \in I(X)$. Assim, $P \in V(I(X))$.

iv) Pela segunda afirmação do item (iii) temos que $V(I(X)) \supset X$, assim, pelo item (ii) segue que $I(V(I(X))) \subset I(X)$. E pela primeira afirmação do item (iii), com $S = I(X)$, segue que $I(V(I(X))) \supset I(X)$, o que concluí a prova. □

2.4 O Teorema dos Zeros de Hilbert

É necessário ter $V(I) \neq \varnothing$ para que um conjunto algébrico $V(I)$ em K^n tenha um significado geométrico. O teorema chamado Versão Fraca do Teorema de Zeros de Hilbert garante esta condição.

Lema 2.16. *Um ideal maximal no anel de polinômios $K[x_1, \ldots, x_n]$ sobre um corpo algebricamente fechado K tem a seguinte forma:*

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle, \qquad a_j \in K, \ j = 1, \ldots, n.$$

Demonstração. Seja m um ideal maximal de $K[x_1, \ldots, x_n]$. Vamos definir $J = K[x_1, \ldots, x_n]/m$. Temos pelo Teorema 1.18 que J é um corpo. Temos também que J é finitamente gerado com coeficientes em K, ou seja, $J = K[\overline{x_1}, \ldots, \overline{x_n}]$. Assim, pelo Teorema 1.29, temos que J é algébrico sobre K e portanto, como K é algebricamente fechado, concluímos que $J = K$.

Assim, para cada x_i, existe $a_i \in K$ tal que a_i é resíduo de x_i assim, $x_i - a_i \in m$ para todo $i = 1, \ldots, n$. Logo, $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset m$. Pelo Exemplo 1.24 $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ é um ideal maximal e, então, $m = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. $\square$

Teorema 2.17 (Versão Fraca do Teorema de Zeros de Hilbert)**.** *Sejam K um corpo algebricamente fechado e I um ideal de $K[x_1, \ldots, x_n]$ que não contém a identidade (isto é, $I \neq K[x_1, \ldots, x_n]$). Então $V(I) \neq \varnothing$.*

Demonstração. Seja I um ideal qualquer de $K[x_1, \ldots, x_n]$. Pelo Teorema 1.16 sabemos que existe um ideal maximal m tal que $I \subset m$. Assim, $V(m) \subset V(I)$, então basta provarmos que $V(m) \neq \varnothing$. Pelo Lema 2.16 segue que $m = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, então $V(m) = \{(a_1, \ldots, a_n)\} \neq \varnothing$.

$\square$

O Lema 2.16 também é comumente chamado de Versão Fraca do Teorema de Zeros de Hilbert. Além disso, perceba que é crucial que K seja um corpo algebricamente fechado no Lema 2.16 e no Teorema 2.17. Pois, por exemplo, sabemos que se $K = \mathbb{R}$ tais resultados não valeriam. Pelo Teorema 1.14, os ideais maximais do anel de polinômios $\mathbb{R}[x]$ de uma variável são da forma $\langle x - a \rangle$, $a \in \mathbb{R}$ e da forma $\langle x^2 + ax + b \rangle$, $a, b \in \mathbb{R}$, $a^2 - 4b < 0$, visto que estes são os elementos irredutíveis em $\mathbb{R}[x]$. Um exemplo explícito seria $V(x^2 + 1) = \varnothing$ que mostra que o Teorema 2.17 não vale em $\mathbb{R}$.

Para $V := V(J)$, com J um ideal de $K[x_1, \ldots, x_n]$, temos

$$J \subset I(V(J)).$$

Entretanto, $V(f^2) = V(f)$ para f em $K[x_1, \ldots, x_n]$. Mais ainda, $V(J) = V(\sqrt{J})$, veja a prova do item (iii) da Proposição 2.11. Assim, a igualdade $I(V(J)) = J$ pode não ser válida, veja Exemplo 2.18.

Exemplo 2.18. *Considere o ideal $J = \langle y^4 \rangle$ em $\mathbb{C}[x, y]$. Temos que*

$$V(J) = \{(a, 0) \in \mathbb{C}^2\}.$$

Como $f(a, 0) = 0$ para todo polinômio da forma $f(x, y) = g(x, y).y$ com $g \in \mathbb{C}[x, y]$ segue que

$$I(V(J)) = \langle y \rangle.$$

Logo $I(V(J)) \neq J$.

O próximo teorema, conhecido como o Teorema de Zeros de Hilbert, originalmente *Hilbert's Nullstellensatz*, explica melhor a relação entre J e $I(V(J))$. O Teorema de Zeros de Hilbert estabelece uma relação fundamental entre Álgebra e Geometria, considerada uma das bases da Geometria Algébrica. Esta relação foi descoberta e demonstrada em *Ueber die Theorie der algebraischen Formen* (1893) por David Hilbert.

Teorema 2.19 (Teorema dos Zeros de Hilbert)**.** *Para um ideal J no anel de polinômios $K[x_1, \ldots, x_n]$ sobre um corpo algebricamente fechado K, temos*

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

Demonstração. Pela Definição 2.14, temos que $\sqrt{J} \subset I(V(J))$. De fato, se $g \in \sqrt{J}$, então $g^m \in J$ para algum inteiro m. Assim,

$$g^m(a_1, \ldots, a_n) = 0 \;\; \forall (a_1, \ldots, a_n) \in V(J),$$

consequentemente, $g(a_1, \ldots, a_n) = 0 \; \forall (a_1, \ldots, a_n) \in V(J)$. Logo $g \in I(V(J))$, o que mostra a inclusão $\sqrt{J} \subset I(V(J))$.

Então, é suficiente provar que para $f \in I(V(J))$ vale que $f \in \sqrt{J}$.

Seja x_0 uma nova variável e seja $\tilde{J}$ o ideal gerado por $1 - x_0 f(x_1, \ldots, x_n)$ e por J, sendo J considerado como um ideal no anel de polinômios $K[x_0, \ldots, x_n]$ com $n+1$ variáveis.

Primeiramente, suponha $V(\tilde{J}) \neq \varnothing$. Seja $(a_0, \ldots, a_n) \in V(\tilde{J})$, temos que $(a_1, \ldots, a_n) \in V(J)$ pois $J \subset \tilde{J}$.

Então $f(a_1, \ldots, a_n) = 0$, pois $(a_1, \ldots, a_n) \in V(J)$ e por hipótese $f \in I(V(J))$. Entretanto, como $1 - x_0 f \in \tilde{J}$ e $(a_0, \ldots, a_n) \in V(\tilde{J})$, obtemos a contradição

$$0 = 1 - a_0 f(a_1, \ldots, a_n) = 1. \tag{2.13}$$

Logo, devemos ter $V(\tilde{J}) = \varnothing$. Portanto, pelo Teorema 2.17, $\tilde{J} = K[x_0, \ldots, x_n]$, então $\tilde{J}$ contém a identidade 1. Logo, podemos escrever

$$1 = h(x_0, \ldots, x_n)(1 - x_0 f(x_1, \ldots, x_n)) + \sum_{j=1}^{l} g_j(x_0, \ldots, x_n) f_j(x_1, \ldots, x_n), \tag{2.14}$$

$h, g_j \in K[x_0, \ldots, x_n]$, $f_j \in J$. Substituindo x_0 por $1/f$ na equação acima e multiplicando dos dois lados por uma certa potência m de f obtemos

$$f^m = \sum_{j=1}^{l} \tilde{g}_j(x_1, \ldots, x_n) f_j(x_1 \ldots, x_n), \qquad \tilde{g}_j \in K[x_1, \ldots, x_n]. \tag{2.15}$$

Consequentemente, $f^m \in J$, o que termina a prova. $\square$

Devido a este teorema, para estudar conjuntos algébricos $V(J)$ podemos focar apenas nos ideais que satisfazem $J = \sqrt{J}$. Ideais com esta propriedade são chamados de ideais reduzidos.

2.5 Topologia de Zariski e consequências do Teorema dos Zeros

Nesta seção apresentamos consequências do Teorema de Zeros de Hilbert e exibimos uma topologia que pode ser induzida sobre conjuntos algébricos. Nesta seção K é um corpo algebricamente fechado.

Lembrando que um ideal é radical se $I = \sqrt{I}$.

Corolário 2.20. *Se I é um ideal radical em $K[x_1, \ldots, x_n]$, então $I(V(I)) = I$. Portanto, existe uma correspondência bijetora entre ideais radicais e conjuntos algébricos.*

Teorema 2.21. *Seja I um ideal em $K[x_1, \ldots, x_n]$. Então $K[x_1, \ldots, x_n]/I$ é um espaço vetorial de dimensão finita sobre K se, e somente se, $V(I)$ é um conjunto finito. Se isso acontece, o número de pontos em $V(I)$ é no máximo $dim_K(K[x_1, \ldots, x_n]/I)$.*

Demonstração. Suponha $K[x_1, \ldots, x_n]/I$ um espaço vetorial de dimensão finita sobre K. Sejam $P_1, \ldots, P_r \in V(I)$ pontos distintos. Tome $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ tais que $f_i(P_j) = 0$ se $i \neq j$ e $f_i(P_i) = 1$, com $i,\ j = 1, \ldots, r$.

Seja $\overline{f_i}$ o I-resíduo de f_i. Se $\sum_i \lambda_i \overline{f_i} = 0$, $\lambda_i \in K$ então $\sum \lambda_i f_i \in I$. Logo $\lambda_j = (\sum \lambda_i f_i)(P_j) = 0$. Consequentemente, os $\overline{f_i}$ são linearmente independentes sobre K, então, pelo Teorema 1.36, segue que

$$r \leq dim_K(K[x_1, \ldots, x_n]/I). \tag{2.16}$$

Por outro lado, suponha $V(I)$ finito, isto é, $V(I) = \{P_1, \ldots, P_r\}$. Seja $P_i = (p_{i1}, \ldots, p_{in})$, e defina F_j por $F_j = \prod_{i=1}^r (x_j - p_{ij})$, $j = 1, \ldots, n$. Então $F_j \in I(V(I))$, logo, pelo Teorema dos Zeros de Hilbert (Teorema 2.19), $F_j^N \in I$ para algum $N > 0$. Considere N grande o suficiente para funcionar para todos os F_j.

Tomando I-resíduos, $\overline{F}_j^N = 0$, então $\overline{x_j}^{rN}$ é uma combinação linear sobre K de $\overline{1}, \overline{x_j}, \ldots, \overline{x_j}^{rN-1}$. Segue por indução que $\overline{x_j}^s$ é uma combinação linear sobre K de $\overline{1}, \overline{x_j}, \ldots, \overline{x_j}^{rN-1}$ para todo s. De fato, já temos que esta afirmação vale para $\overline{x_j}^{rN}$, supomos que vale para $\overline{x_j}^s$ com $s > rN$ e mostraremos para $\overline{x_j}^{s+1}$. Temos que

$$\overline{x_j}^{s+1} = \overline{x_j}^s . \overline{x_j} = \sum_{k=0}^{rN-1} (a_k \overline{x_j}^k) . \overline{x_j} = \sum_{k=0}^{rN-1} (a_k \overline{x_j}^{k+1}) = \sum_{k=0}^{rN-2} (a_k \overline{x_j}^{k+1}) + a_{rN-1} \overline{x_j}^{rN}.$$

Mas temos também que $\overline{x_j}^{rN} = \sum\limits_{k=0}^{rN-1}(b_k\overline{x_j}^k)$. Então podemos escrever

$$\overline{x_j}^{s+1} = \sum_{k=0}^{rN-2} a_{rN-1}b_0 + (a_{rN-1}b_{k+1} + a_k)\overline{x_j}^{k+1}, \tag{2.17}$$

com a_k, $b_k \in K$, para $k = 0, \ldots, rN-2$, concluindo a indução.

Além disso, um elemento $Q \in K[x_1, \ldots, x_n]/I$ é uma combinação linear do conjunto $\{\overline{x_1}^{s_1} \cdot \ldots \cdot \overline{x_n}^{s_n} \mid s_i \in \mathbb{N}\}$. Assim, como cada $\overline{x_j}^{s_j}$ é combinação linear de $\overline{1}, \overline{x_j}, \ldots, \overline{x_j}^{rN-1}$, o conjunto $\{\overline{x_1}^{m_1} \cdot \ldots \cdot \overline{x_n}^{m_n} \mid m_i < rN\}$ gera $K[x_1, \ldots, x_n]/I$ como um K-espaço vetorial. □

A seguir apresentamos um exemplo do Teorema 2.21.

Exemplo 2.22. *Considere $f(x,y) \in \mathbb{C}[x,y]$. Temos que $f(x,y)$ possui um número finito de singularidades, isto é,*

$$\left\{(x,y);\ \frac{\partial f}{\partial x}(x,y) = \frac{\partial f}{\partial y}(x,y) = 0\right\}$$

é finito, se, e somente se, $\dfrac{\mathbb{C}[x,y]}{\left(\frac{\partial f}{\partial x}; \frac{\partial f}{\partial y}\right)}$ *tem dimensão finita sobre $\mathbb{C}$.*

Corolário 2.23. *Sejam $V = V(J_1)$ e $W = V(J_2)$ conjuntos algébricos em K^n que satisfazem $V \supsetneq W$ então temos que*

$$\sqrt{J_1} \subsetneq \sqrt{J_2}. \tag{2.18}$$

Demonstração. Pela Proposição 2.15 i) temos que se $V \supset W$, então $I(V(J_1)) \subset I(V(J_2))$. Então o Teorema 2.19 implica que

$$\sqrt{J_1} \subset \sqrt{J_2}.$$

Suponha $\sqrt{J_1} = \sqrt{J_2}$, então $V = W$. Logo para $V \supsetneqq W$ obtemos $\sqrt{J_1} \subsetneqq \sqrt{J_2}$. □

Corolário 2.24. *Quando um conjunto algébrico $V(I)$ é não vazio e diferente de $\mathbb{A}^n_K$, o complemento*

$$V(I)^C = \mathbb{A}^n_K \setminus V(I) = \{(a_1, \ldots, a_n) \in K^n \,|\, \exists f \in I \ \textit{tal que}\ f(a_1, \ldots, a_n) \neq 0\}$$

não é um conjunto algébrico.

Demonstração. Suponha que exista um ideal J em $K[x_1, \ldots, x_n]$ satisfazendo $V(I)^C = V(J)$. Então, como $V(I) \cup V(J) = \mathbb{A}^n_K$, pela Proposição 2.11(i), temos

$$V(I \cap J) = V(I) \cup V(J) = \mathbb{A}^n_K.$$

Pelo Teorema de Zeros de Hilbert (Teorema 2.19) temos que $\sqrt{I \cap J} = (0)$. Logo, pela definição de radical, $I \cap J = (0)$. Se $(I) \neq (0)$ e $(J) \neq (0)$, existem polinômios f e g tais que $f \in I$ e $g \in J$, com f, g não nulos. Assim, $f \cdot g \neq 0$ e $f \cdot g \in I \cap J$, o que contradiz $I \cap J = (0)$. Logo ou $I = (0)$ ou $J = (0)$, o que implica que $V(I) = \mathbb{A}^n_K$ ou $V(I) = \varnothing$, contradizendo nossa hipótese. Isto é, não existe um ideal J que satisfaça $V(I)^C = V(J)$. □

Proposição 2.25. *O conjunto de todos os complementos de conjuntos algébricos*

$$\mathcal{O} = \{V(I)^C | I \text{ é um ideal de } K[x_1, \ldots, x_n]\}$$

tem as seguintes propriedades:

i) $\varnothing \in \mathcal{O}$ *e* $\mathbb{A}^n_K \in \mathcal{O}$.

ii) *Se* $O_1, O_2 \in \mathcal{O}$, *então* $O_1 \cap O_2 \in \mathcal{O}$.

iii) $\bigcup_{\lambda \in \Lambda} O_\lambda \in \mathcal{O}$, *para* $O_\lambda \in \mathcal{O}$ *e* $\lambda \in \Lambda$, *onde* Λ *pode ser infinito.*

Definindo um subconjunto O como conjunto aberto se $O \in \mathcal{O}$, induzimos uma topologia sobre K^n, onde os fechados serão os conjuntos algébricos. Esta topologia é chamada de *Topologia de Zariski* em K^n.

Tomando $K = \mathbb{C}$ e considerando a topologia usual em $\mathbb{C}^n$ sendo a topologia proveniente da métrica euclidiana em $\mathbb{C}^n$, finalizamos esta seção com a noção de construtibilidade e alguns resultados que relacionam a topologia usual com a topologia de Zariski.

Definição 2.26 (Construtibilidade)**.** *Seja* V *um conjunto algébrico. Um subconjunto* A *de* V *é construtível se* A *é uma união finita de subconjuntos de* V *localmente fechados.*

Teorema 2.27. *Se* Z *é um subconjunto construtível de* $\mathbb{C}^n$, *então o fecho de* Z *na topologia de Zariski é igual ao fecho de* Z *na topologia usual.*

Do teorema acima segue que se X é fechado na topologia de Zariski então X é fechado na topologia usual. Entretanto, a recíproca vale apenas se X for construtível, ou seja: Se X é construtível e é fechado na topologia usual então X é fechado na topologia de Zariski.

Além disso, se Z é construtível então o fecho $\overline{Z}$ na topologia usual é algébrico. Temos que se $f : \mathbb{C}^n \to \mathbb{C}^m$ é uma aplicação polinomial, $X \subseteq \mathbb{C}^n$ conjunto construtível, então $f(X)$ é um conjunto construtível; veja seção 4.3. Por outro lado, a imagem de um conjunto algébrico não é, necessariamente, algébrico. Veja Exemplo 2.28

Exemplo 2.28. *Seja* X *um conjunto algébrico definido como*

$$X = \{xy - 1 = 0\} \subset \mathbb{C}^2,$$

e π *a aplicação*

$$\begin{array}{rccc} \pi : & \mathbb{C}^2 & \to & \mathbb{C} \\ & (x, y) & \mapsto & x. \end{array}$$

Não é difícil ver que $\pi(X) = \mathbb{C}^*$ *e que* $\overline{\mathbb{C}^*} = \mathbb{C}$. *Assim, temos que* $\mathbb{C}^*$ *é construtível mas não é algébrico e o fecho* $\overline{\mathbb{C}^*}$ *é algébrico.*

As demonstrações do Teorema 2.27 e das consequências dele exigem ferramentas que ainda não apresentamos e, por isso, serão feitas posteriormente na seção 4.3. A referência utilizada para o estudo de tais resultados é a [9].

3. Variedades algébricas afins

3.1 Variedades algébricas

Abordamos agora os conjuntos algébricos irredutíveis e apresentamos mais algumas notações e resultados. Em particular, provaremos que todo conjunto algébrico se decompõe em componentes irredutíveis. Utilizamos para o estudo deste tópicos as referências [12] e [3]. Nesta seção K é um corpo algebricamente fechado.

Definição 3.1 (Variedade Algébrica)**.** *Um conjunto algébrico V no espaço afim K^n sobre um corpo K é dito redutível quando V é a união de conjuntos algébricos V_1 e V_2,*

$$V = V_1 \cup V_2, \qquad V \neq V_1 \text{ e } V \neq V_2.$$

Quando um conjunto algébrico não é redutível, ele é dito irredutível. Um conjunto algébrico irredutível é chamado variedade algébrica.

Proposição 3.2. *Um conjunto algébrico V é irredutível se, e somente se, o ideal $I(V)$ associado a V é um ideal primo.*

Demonstração. As provas serão por absurdo. Tome V um conjunto algébrico irredutível e suponha que $I(V)$ não é um ideal primo, isto é, existem $f_1,\ f_2 \notin I(V)$ tais que $f_1 f_2 \in I(V)$. Logo $V(f_1 f_2) \supset V(I(V)) = V$, então segue que

$$V = V \cap V(f_1 f_2) = V \cap (V(f_1) \cup V(f_2)) = (V \cap V(f_1)) \cup (V \cap V(f_2)). \tag{3.1}$$

temos que $V \cap V(f_i) \subsetneq V$ pois, caso contrário, $V \subset V(f_i)$ e $I(V) \supset I(V(f_i))$ e, então, teríamos $f_i \in I(V)$ para $i = 1,\ 2$. Logo V é redutível, absurdo.

Por outro lado, temos $I(V)$ primo. Suponha $V = V_1 \cup V_2$ com $V_i \subsetneq V$, então $I(V_i) \supsetneq I(V)$. Seja $f_i \in I(V_i)$, $f_i \notin I(V)$, $i = 1,\ 2$. Como $I(V) = I(V_1 \cup V_2)$, temos que para todo $P \in V$, $P \in V_1$ ou $P \in V_2$. Assim $f_1 f_2(P) = f_1(P).f_2(P) = 0$ e, portanto, $f_1 f_2 \in I(V)$. Logo $I(V)$ não é primo, absurdo. $\square$

Como consequência do Teorema 2.19 e da Proposição 3.2 temos o seguinte resultado.

Corolário 3.3. *Se I é um ideal primo, então $V(I)$ é irredutível. Existe uma correspondência bijetora entre ideais primos e conjuntos algébricos irredutíveis. Os ideais maximais correspondem à pontos.*

Proposição 3.4. *Um ideal m de $K[x_1,\dots,x_n]$ é maximal se, e somente se, $m = I(P)$ para algum $P \in K^n$.*

Demonstração. ($\Rightarrow$) Como m é maximal, então m é um ideal primo de $K[x_1,\dots,x_n]$ (Corolário 1.19). Assim, $V = V(m)$ é uma variedade algébrica. Por definição V é não vazio, então podemos tomar um ponto $P \in V$ e, pela Proposição 2.15, temos que $m = I(V) \subseteq I(P)$ mas como m é maximal e $I(P) \neq K[x_1,\dots,x_n]$ segue que $m = I(P)$.

($\Leftarrow$) Suponha $m = I(P)$ para algum $P \in K^n$. Vamos que mostrar que se um ideal J de $K[x_1,\dots,x_n]$ contém m então $J = m$ ou $J = K[x_1,\dots,x_n]$. De fato se $J \supset m$ temos $V(J) \subset V(m) = \{P\}$, logo $V(J) = \{P\}$ ou $V(J) = \varnothing$. No primeiro caso, $\sqrt{J} = I(V(J)) = I(P) = m$ então $J \subseteq m$, mas como supomos $m \subseteq J$, temos $J = m$. No segundo caso, $\sqrt{J} = I(V(J)) = I(\varnothing) = K[x_1,\dots,x_n]$ então $J = K[x_1,\dots,x_n]$. Logo m é um ideal maximal. □

O próximo lema será utilizado na demonstração do Teorema 3.6. No Teorema 2.3 vimos que uma coleção qualquer não vazia de ideias em um anel noetheriano tem elemento maximal. Como consequência deste teorema temos o seguinte resultado:

Lema 3.5. *Uma coleção qualquer não vazia de conjuntos algébricos em K^n tem um elemento minimal.*

Demonstração. Seja $\{V_i\}$ uma coleção não vazia de conjuntos algébricos em K^n. Considere a coleção de ideais $\{I(V_i)\}$. Pelo Teorema 2.3 a coleção $\{I(V_i)\}$ possui um elemento maximal $I(V_m)$. Como $I(V_m) \supset I(V_i)$ para todo $i \in \mathbb{N}$, temos $V_m = V(I(V_m)) \subset V(I(V_i)) = V_i$. Portanto V_m é um elemento minimal da coleção $\{V_i\}$. □

A decomposição de um conjunto algébrico em conjuntos algébricos irredutíveis é única e finita, conforme o resultado a seguir.

Teorema 3.6. *Seja V um conjunto algébrico em K^n. Então existem $V_1,\dots,V_n$ conjuntos algébricos irredutíveis tais que $V = V_1 \cup \cdots \cup V_n$ e $V_i \nsubseteq V_j$ para $i \neq j$. Os conjuntos algébricos $V_1,\dots,V_n$ são únicos.*

Demonstração. Seja S o conjunto de todos os conjuntos algébricos V em K^n tais que V não é a união de conjuntos algébricos irredutíveis. Queremos mostrar que S é vazio. Suponhamos S não vazio e tomemos V um elemento minimal de S. Como $V \in S$, existem V_1, $V_2 \in K^n$ tais que $V = V_1 \cup V_2$ com $V_i \subsetneq V$ para $i = 1$ ou 2. Como $V_i \subset V$ e V é elemento minimal de S, temos $V_i \notin S$. Então V_i é redutível, isto é, $V_i = V_{i1} \cup \cdots \cup V_{im}$ com V_{ij} irredutível para todo j. Dessa forma, concluímos que $V = \cup_{ij} V_{ij}$ contradizendo a suposição de $V \in S$. Portanto, qualquer conjunto algébrico V pode ser escrito como $V = V_1 \cup \cdots \cup V_n$, V_i irredutível para $i = 1,\dots,n$. Para obter $V_i \nsubseteq V_j$ para $i \neq j$, descartamos V_i tal que $V_i \subset V_j$ para $i \neq j$.

Mostraremos agora a unicidade de $V_1,\dots,V_n$. Seja $V = W_1 \cup \cdots \cup W_m$ outra decomposição, então

$$V_i = V \cap V_i = \left(\bigcup_{j=1}^{m} W_j\right) \cap V_i = \bigcup_{j=1}^{m} (W_j \cap V_i). \tag{3.2}$$

Logo $V_i \subset W_{j(i)}$ para algum $j(i)$ e $W_{j(i)} \subset V_k$ para algum k. Mas $V_i \subset V_k$ implica $i = k$ e, portanto, $V_i = W_{j(i)}$. Analogamente, cada W_i é igual a algum $V_{i(j)}$. □

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

3.2 Estruturas associadas a uma variedade algébrica

Apresentamos mais algumas notações e resultados algébricos que são utilizados no estudo de variedades algébricas, como anel de coordenadas, anel local e corpo de funções de V.

Definição 3.7 (Anel de coordenadas). *Para uma variedade algébrica V no espaço afim n-dimensional K^n, o anel quociente*

$$A(V) := K[x_1, \dots, x_n]/I(V)$$

é chamado anel de coordenadas de V.

Assim, a Proposição 3.2 pode ser reescrita da seguinte forma:

Proposição 3.8. *Um conjunto algébrico V em K^n é irredutível se, e somente se, seu anel de coordenadas $A(V)$ é um domínio.*

O anel de coordenadas $A(V)$ pode ser visto como o conjunto de funções polinomiais definidas em V.

Definição 3.9 (Corpo de frações). *Se V é uma variedade algébrica, então o corpo dos quocientes f/g com f e g no domínio $A(V)$ é chamado de corpo de frações sobre V e é denotado por $K[V]$. Um elemento de $K[V]$ é uma função racional em V.*

Definição 3.10. *Seja V uma variedade algébrica em K^n. Se f é uma função racional em V e $P \in V$, dizemos que f está definida em P se existe algum par $a, b \in A(V)$, tal que $f = a/b$, temos $b(P) \neq 0$.*

Apresentamos mais alguns conceitos de natureza algébrica.

Proposição 3.11 (Domínio de valorização discreta). *Seja D um domínio que não é corpo. As seguintes condições são equivalentes:*

i) *D é um anel noetheriano e local, e o ideal maximal m de D é principal.*

ii) *Existe um elemento irredutível $t \in D$ tal que todo $z \in D$ diferente de zero pode ser escrito de maneira única na forma $z = ut^n$, u elemento invertível em D e n um número inteiro não negativo.*

Um anel que satisfaz tais condições é chamado anel de valorização discreta. Um elemento t como em (ii) é dito parâmetro de uniformização de D.

Demonstração. $(i) \Rightarrow (ii)$: Seja m o ideal maximal de D e t um gerador de m. Suponha $ut^n = vt^m$, u e v elementos invertíveis e $n \geq m$. Então $ut^{n-m} = v$ é um elemento invertível e como t não pode ser um elemento invertível, segue que $n = m$ e $u = v$. Assim, a expressão de qualquer $z = ut^n$ é única. Para mostrar que qualquer z pode ser expresso dessa forma, podemos assumir que z não é invertível (para z invertível basta tomar $z = zt^0$). Então $z = z_1 t$ para algum $z_1 \in A$. Se z_1 é um elemento invertível acabamos, caso contrário assuma $z_1 = z_2 t$ para algum $z_2 \in A$. Continuando este processo encontra-se uma sequência infinita $z_1, z_2, \ldots$, com $z_i = z_{i+1}t$. Afirmamos que para algum m, z_m é invertível, o que termina a prova. Caso contrário, como A é noetheriano, a cadeia de ideais $\langle z_1 \rangle \subset \langle z_2 \rangle \subset \ldots$ tem um elemento maximal (Teorema 2.3), então $\langle z_n \rangle = \langle z_{n+1} \rangle$ para algum n. Logo $z_{n+1} = vz_n$ para algum $v \in A$ e, então, $z_n = vtz_n$ e $vt = 1$. Absurdo, pois t não pode ser unidade. Portanto, todo $z \in D$ se escreve como $z = ut^n$.

$(ii) \Rightarrow (i)$: Temos que $m = \langle t \rangle$ é um conjunto de elementos não invertíveis. E os únicos ideais de A são ideais principais $\langle t^n \rangle$, n inteiro não negativo. Logo A é um domínio de ideais principais e, consequentemente, é um anel noetheriano. Além disso, A é um anel local cujo ideal maximal é $m = \langle t \rangle$. □

Sugerimos ao (à) leitor (a) relembrar a definição de anel local dada na Proposição 1.54.

Definimos a seguinte estrutura:

Definição 3.12 (Anel local de uma variedade)**.** *Seja V uma variedade algébrica em K^n e $P \in V$. Definimos $\mathcal{O}_P(V)$ como o conjunto de funções racionais em V que estão definidas em P. O anel $\mathcal{O}_P(V)$ é chamado anel local de V em P.*

Provaremos que $\mathcal{O}_P(V)$ é um domínio, noetheriano e local, veja Proposição 3.19.

Explicamos agora a noção de uma função regular em uma variedade algébrica V.

Definição 3.13. *Uma função $f : V \to K$ é regular em um ponto $P \in V$ se existe uma vizinhança aberta U, tal que $P \in U \subseteq V$, e existem polinômios $g, h \in K[x_1, \ldots, x_n]$ tais que h nunca é zero em U e $f = g/h$ em U. Dizemos que f é regular em V se é regular em cada ponto de V.*

Definição 3.14. *Seja V uma variedade algébrica. Denotamos por $\mathcal{O}(V)$ o anel das funções regulares em V.*

Proposição 3.15. *O conjunto $\mathcal{O}(V)$ das funções regulares na variedade algébrica V é um anel (K-álgebra) munido das operações*

$$(f+g)(y) := f(y) + g(y), \quad (\lambda f)(y) := \lambda(f(y)), \quad (fg)(y) := f(y)g(y). \tag{3.3}$$

Definição 3.16. *Considere a relação de equivalência $\sim$ definida por*

$$f \sim g \Leftrightarrow \exists U \text{ um aberto, com } 0 \in U \text{ tal que } f_{|U} = g_{|U}.$$

As classes de equivalência são chamadas de germes da função f.

Lema 3.17. *Sejam V uma variedade algébrica, $f, g \in \mathcal{O}(V)$ e U um aberto não vazio de V. Se $f_{|U} = g_{|U}$ então $f(x) = g(x)$ para todo $x \in V$.*

Veja demonstração do Lema 3.17 em [6], página 15.

Reescrevendo a definição 3.12 utilizando a noção de função regular, temos o seguinte:

Definição 3.18 (Anel Local)**.** *Se $P \in V$, definimos o anel local $\mathcal{O}_P$ de P em V como o anel de germes de funções regulares em V ao redor de P. Ou seja, um elemento de $\mathcal{O}_P$ é um par $\langle U, f\rangle$ onde U é uma vizinhança de V contendo P e f uma função regular em U e identificamos dois pares $\langle U, f\rangle$ e $\langle W, g\rangle$ se $f = g$ em $U \cap W$.*

$\mathcal{O}_P$ possui um ideal maximal de germes de funções que se anulam em P e, por isso, o nome "anel local de P" é justificado. O próximo resultado mostra exatamente isso.

Proposição 3.19. *Sejam V uma variedade algébrica e $P \in V$.*

i) O conjunto $\mathcal{O}_P$ munido das operações

$$\langle U, f\rangle + \langle W, g\rangle := \langle U \cap W, f + g\rangle \quad e \quad \langle U, f\rangle \cdot \langle V, g\rangle := \langle U \cap W, fg\rangle \tag{3.4}$$

é um anel.

ii) O conjunto $m_P := \{\langle U, f\rangle \in \mathcal{O}_P \mid f(P) = 0\}$ é o único ideal maximal de $\mathcal{O}_P$. Consequentemente, $\mathcal{O}_P$ é um anel local.

Demonstração. Provaremos somente o item (ii).

ii) Primeiro, mostraremos que o subconjunto m_P é um ideal próprio de $\mathcal{O}_P$. Como $0(P) = 0$ temos $\langle V, 0\rangle \in m_P$, então m_P é não vazio. Considere $\langle U, f\rangle$, $\langle W, g\rangle \in m_P$ e $\langle Y, h\rangle \in \mathcal{O}_P$, temos que $\langle U \cap W, f - g\rangle \in m_P$, pois como $f(P) = g(P) = 0$ tem-se $(f - g)(P) = f(P) - g(P) = 0$. Além disso, $(fh)(P) = f(P)h(P) = 0.h(P) = 0$ e, consequentemente, $\langle U \cap Y, fh\rangle \in m_P$. Logo m_P é um ideal. E para $\langle V, 1\rangle \in \mathcal{O}_P$, temos $1(P) = 1$ e, portanto, $\langle V, 1\rangle \notin m_P$, isto é, m_P é um ideal próprio de $\mathcal{O}_P$.

Agora mostraremos que m_P é o único ideal maximal de $\mathcal{O}_P$, para isso, mostremos que todo elemento $\mathcal{O}_P \setminus m_P$ é invertível. Dado $\langle U, f\rangle \in \mathcal{O}_P \setminus m_P$, existem polinômios $f_1, f_2 \in K[x_1, \ldots, x_n]$ tais que $f(u) = \frac{f_1(u)}{f_2(u)}$ e $f_2(u) \neq 0$ para todo $u \in U$. Considere o subconjunto fechado $Z(f_1) = \{Q \in V \mid f_1(Q) = 0\}$, temos que $Z(f_1) \not\supseteq U$, pois caso contrário teríamos $f_1(U) = 0$, consequentemente, pelo Lema 3.17, $f_1(V) = 0$, o que contradiz a hipótese de $f \notin m_P$. Dessa forma, temos que $Z(f_1) \cap U$ é um subconjunto fechado próprio de U. Então o complementar $W = U \setminus (U \cap Z(f_1))$ é um aberto próprio de U. Além disso, $P \in W$ pois $f(P) \neq 0$ já que $\langle U, f\rangle \notin m_P$. Como $f_1(w) \neq 0$ para todo $w \in W$, então $\langle W, \frac{f_2}{f_1}\rangle \in \mathcal{O}_P$ e $\langle U, f\rangle\langle W, \frac{f_2}{f_1}\rangle = \langle U \cap W, \frac{f_1}{f_2}\frac{f_2}{f_1}\rangle = \langle W, 1\rangle = \langle V, 1\rangle$, ou seja, $\langle U, f\rangle$ é um elemento invertível de $\mathcal{O}_P$. E como tomamos $\langle U, f\rangle$ um elemento qualquer, mostramos que todo elemento de $\mathcal{O}_P \setminus m_P$ é invertível. Assim, pela Proposição 1.54 a prova segue.

□

Definição 3.20 (Corpo de Funções). *Seja V uma variedade algébrica. Definimos o corpo de funções $K(V)$ de V da seguinte maneira: um elemento de $K(V)$ é uma classe de equivalência de pares $\langle U, f\rangle$, onde U é um subconjunto aberto não vazio (na topologia de Zariski) de V, f é uma função regular em U e identificamos dois pares $\langle U, f\rangle$ e $\langle W, g\rangle$ se $f = g$ em $U \cap W$.*

Os elementos de $K(V)$ são chamadas as funções regulares em V.

Proposição 3.21. *Seja V uma variedade algébrica. O corpo de funções $K(V)$ quando munido das operações*

$$\langle U, f\rangle + \langle W, g\rangle := \langle U \cap W, f + g\rangle \quad e \quad \langle U, f\rangle \cdot \langle V, g\rangle := \langle U \cap W, fg\rangle \tag{3.5}$$

é um corpo.

Na próxima seção veremos que $\mathcal{O}(V)$ se identifica em $\mathcal{O}_P$ que, por sua vez, se identifica em $K(V)$. E, por fim, apresentamos um exemplo que motivará os estudos da próxima seção.

Exemplo 3.22. *O anel de coordenadas de um curva quadrática*

$$C = V(x^2 + y^2 - 1)$$

no plano afim K^2 quando $K = \mathbb{C}$ é dada por

$$A(C) = K[x, y]/\langle x^2 + y^2 - 1\rangle$$

Tome $u = x + iy$ e $v = x - iy$. Então o anel de coordenadas $A(C)$ torna-se

$$A(C) = K[u, v]/\langle uv - 1\rangle.$$

Perceba que este anel de coordenadas é isomorfo a $K[u, 1/u]$. A mudança de coordenadas acima pode ser formulada em termos da teoria dos anéis comutativos como um isomorfismo:

$$\begin{array}{rcl} \varphi :\ K[x, y]/\langle x^2 + y^2 - 1\rangle & \tilde{\to} & K[u, 1/u], \\ x & \mapsto & \dfrac{1}{2}(u + 1/u), \\ y & \mapsto & \dfrac{1}{2i}(u - 1/u). \end{array}$$

Pode ser observado que a inversa deste isomorfismo é dado por

$$\begin{array}{rcl} \varphi^{-1} :\ K[u, 1/u] & \tilde{\to} & K[x, y]/\langle x^2 + y^2 - 1\rangle, \\ u & \mapsto & x + iy. \end{array}$$

3.3 Morfismo entre variedades e algumas relações

Generalizando o conceito de mudança de coordenadas como no Exemplo 3.22, pode-se definir um morfismo entre conjuntos algébricos V e W. O termo morfismo é uma terminologia utilizada para aplicações na Geometria Algébrica.

Definição 3.23 (Morfismo)**.** *Sejam $V \subset K^n$ e $W \subset K^m$ conjuntos algébricos e $\varphi : V \to W$ uma aplicação de conjuntos. A aplicação φ é dita morfismo de V em W se pode ser expressa em termos de polinômios. Isto é, existem polinômios $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ tais que para todo $P = (a_1, \ldots, a_n) \in V$ vale que*

$$\varphi(P) = (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)). \tag{3.6}$$

Proposição 3.24. *Sejam V e W variedades algébricas e $\varphi : V \to W$ um morfismo. Então φ induz um homomorfismo φ^* entre os anéis de coordenadas $A(V)$ e $A(W)$:*

$$\begin{array}{rccc} \varphi^* : & A(W) & \to & A(V) \\ & f & \mapsto & f \circ \varphi. \end{array} \tag{3.7}$$

Isto é, se $f \in A(W)$ é o $I(W)$-resíduo de um polinômio F, então $\varphi^*(f) = f \circ \varphi$ é o $I(V)$-resíduo do polinômio $F(f_1, \ldots, f_m)$.

Definição 3.25 (Isomorfismo)**.** *Sejam V e W variedades algébricas e $\varphi : V \to W$ um morfismo. Então φ é dito isomorfismo se existe um morfismo $\psi : W \to V$ tal que $\psi \circ \varphi = I_V$ $\varphi \circ \psi = I_W$, onde I_V representa a função identidade em V e I_W a função identidade em W.*

Conjuntos algébricos isomorfos podem ser considerados algebricamente e geometricamente iguais. Neste sentido, é desejável obter uma definição de um morfismo em termos de um conjunto algébrico e seu anel de coordenadas.

Proposição 3.26. *Sejam $V \subset K^n$ e $W \subset K^m$ variedades algébricas. Existe uma correspondência bijetora natural entre os morfismos $\varphi : V \to W$ e os homomorfismos $\varphi^* : A(W) \to A(V)$. Qualquer morfismo φ é uma restrição de um morfismo de K^n em K^m.*

Demonstração. Seja $\psi : A(W) \to A(V)$ um homomorfismo. Escolhemos $T_i \in K[x_1, \ldots, x_n]$ tais que $\psi(x_i + I(W)) = T_i + I(V)$, $i = 1, \ldots, m$. Então $T = (T_1, \ldots, T_m)$ é um morfismo de K^n em K^m e induz $\overline{T} : A(\mathbb{A}^m_K) \to A(\mathbb{A}^n_K)$, onde $A(\mathbb{A}^m_K) = K[x_1, \ldots, x_m]$ e $A(\mathbb{A}^n_K) = K[x_1, \ldots, x_n]$.

Temos que $T(V) \subset W$. De fato, tomando $F \in I(W)$ segue para todo $a \in V$ temos

$$\overline{T}(F)(a) = F \circ T(a) = F(T_1, \ldots, T_m)(a). \tag{3.8}$$

Como $F(T_1, \ldots, T_m) \in I(W)(a) = \overline{F(T_1, \ldots, T_m)}(a)$ se $a \in V$, então

$$F \circ T(a) = \overline{F}(\overline{T_1}, \ldots, \overline{T_m})(a) = \psi(F(x_1, \ldots, x_m))(a) = \psi(0_{A(W)})(a), \tag{3.9}$$

pois $F \in I(W)$. Uma vez que ψ é homomorfismo, $\psi(0_{A(W)})(a) = 0_{A(V)}(a) = 0$. Com isso, obtemos $T(a) \in V(I(W))$. Mas W é uma variedade algébrica, garantindo que $V(I(W)) = W$ e, assim, $T(V) \subset W$. Logo a restrição $\varphi = T_{|V} : V \to W$ é um morfismo.

A Proposição 3.24 garante que, a partir de φ, obtemos um homomorfismo $\varphi^* : A(W) \to A(V)$ tal que $\varphi^*(F + I(W)) = F(T_1, \ldots, T_m) + I(V)$. Portanto $\varphi^* = \psi$.

Portanto, dado um homomorfismo entre os anéis de coordenadas, construímos um morfismo entre as variedades. E, pela Proposição 3.24, dada um morfismo entre variedades, construímos um homomorfismo entre anéis de coordenadas. $\square$

O resultado a seguir segue diretamente da Proposição 3.26.

Corolário 3.27. *Sejam V e W variedades algébricas. Então V e W são isomorfas se, e somente se, os anéis de coordenadas $A(V)$ e $A(W)$ são isomorfos sobre K.*

Definição 3.28 (Mudança de Coordenadas)**.** *Uma mudança afim de coordenadas em K^n é um morfismo $T = (T_1, \ldots, T_n) : K^n \to K^n$ tal que cada T_i é um polinômio de grau 1 e tal que T é bijetor.*

Estudamos agora a conexão entre os pontos de um conjunto algébrico V e os ideais maximais do anel de coordenadas $A(V)$ de V.

Definição 3.29 (Espectro Maximal)**.** *Seja A um anel. Denotamos a totalidade de ideais maximais de A por Spm A e chamamos de espectro maximal de A.*

Proposição 3.30. *Para um conjunto algébrico V, existe uma correspondência um-a-um entre os pontos de V e o espectro maximal Spm $A(V)$. Para o anel de coordenadas*

$$A(V) = K[x_1, \ldots, x_n]/I(V),$$

o ponto $(a_1, \ldots, a_n)$ em V corresponde ao ideal maximal de $A(V)$ determinado por $\langle \overline{x_1} - a_1, \ldots, \overline{x_n} - a_n \rangle$.

Demonstração. Um ponto $(a_1, \ldots, a_n)$ em um conjunto algébrico $V \subset K^n$ corresponde a um ideal maximal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ de $K[x_1, \ldots, x_n]$. Denotaremos a classe residual de x_j por $\overline{x_j}$ no anel de coordenadas $A(V) = K[x_1, \ldots, x_n]/I(V)$. Então $\langle \overline{x_1} - a_1, \ldots, \overline{x_n} - a_n \rangle$ é um ideal maximal de $A(V)$. Por outro lado, para um ideal maximal m de $A(V)$, a imagem inversa $\psi^{-1}(\mathrm{m})$ de m sob o homomorfismo sobrejetor canônico

$$\psi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/I(V)$$

é um ideal maximal do anel de polinômios $K[x_1, \ldots, x_n]$. Utilizando o Corolário 2.16, podemos escrever

$$\psi^{-1}(\mathrm{m}) = \langle x_1 - b_1, \ldots, x_n - b_n \rangle.$$

Mostraremos que $(b_1, \ldots, b_n) \in V$. É suficiente mostrar que

$$\langle x_1 - b_1, \ldots, x_n - b_n \rangle \supset I(V).$$

Como $\overline{0} \in \mathrm{m}$ e $\psi^{-1}(\overline{0}) = I(V)$, obtemos $\psi^{-1}(\mathrm{m}) \supset \psi^{-1}(\overline{0}) = I(V)$.

□

Mostraremos agora como um homomorfismo de anéis é induzido por um morfismo entre conjuntos algébricos.

Proposição 3.31. *Sejam A e B anéis e $\phi : A \to B$ um homomorfismo sobrejetivo de anéis com núcleo ker $\phi = N$.*

i) Um ideal $I \subseteq B$ é primo se, e somente se, $\phi^{-1}(I)$ é um ideal primo de A tal que $N \subseteq \phi^{-1}(I)$.

ii) Um ideal $I \subseteq B$ é maximal se, e somente se, $\phi^{-1}(I)$ é um ideal maximal de A tal que $N \subseteq \phi^{-1}(I)$.

Demonstração. **i)** ($\Rightarrow$) Como I é um ideal, $0 \in I$ e, portanto, $N = \phi^{-1}(0) \subseteq \phi^{-1}(I)$. Considere $x, y \in A$ tais que $xy \in \phi^{-1}(I)$. Como $\phi(xy) \in I$, então $\phi(xy) = \phi(x)\phi(y) \in I$, logo, $\phi(x) \in I$ ou $\phi(y) \in I$, pois I é um ideal primo. Logo, $x \in \phi^{-1}(I)$ ou $y \in \phi^{-1}(I)$, ou seja, $\phi^{-1}(I)$ é um ideal primo de A.

($\Leftarrow$) Suponha que $\phi^{-1}(I)$ é um ideal primo de A tal que $N \subseteq \phi^{-1}(I)$. Considere $a, b \in B$ tais que $ab \in I$. Como ϕ é sobrejetor, então existem $x, y \in A$, $z \in \phi^{-1}(I)$, tais que $a = \phi(x)$, $b = \phi(y)$ e $ab = \phi(z)$. Assim, $\phi(xy - z) = \phi(x)\phi(y) - \phi(z) = ab - ab = 0$, isto é, $xy - z \in N$. Como $N \subseteq \phi^{-1}(I)$ e $z \in \phi^{-1}(I)$, temos que $xy \in \phi^{-1}(I)$. Além disso, $x \in \phi^{-1}(I)$ ou $y \in \phi^{-1}(I)$, pois $\phi^{-1}(I)$ é um ideal primo. Disso segue que $\phi(x) = a \in I$ ou $\phi(y) = b \in I$, portanto, I é um ideal primo.

ii) ($\Rightarrow$) Como I é um ideal, $0 \in I$ e, portanto, $N = \phi^{-1}(0) \subseteq \phi^{-1}(I)$. Suponha que $J \subseteq A$ é um ideal contendo $\phi^{-1}(I)$. Como ϕ é sobrejetora, temos que $I \subseteq \phi(J)$ mas como I é maximal, temos $\phi(J) = I$ ou $\phi(J) = B$. Se $\phi(J) = I$, então $J \subseteq \phi^{-1}(I)$ e com isso $J = \phi^{-1}(I)$. Se $\phi(J) = B$, então $J = A$, pois como $\phi(J) = B$, dado $x \in A$, existe $j \in J$ tal que $\phi(j) = \phi(x)$, assim $x - j \in N \subseteq J$, logo $a \in J$, isto é, $A \subseteq J$. Portanto, $\phi^{-1}(I)$ é maximal.

($\Leftarrow$) Suponha que $\phi^{-1}(I)$ é um ideal maximal de A tal que $N \subseteq \phi^{-1}(I)$. Considere um ideal $J \subseteq B$ contendo I, então $\phi^{-1}(I) \subseteq \phi^{-1}(J)$. Como $\phi^{-1}(I)$ é um ideal maximal, então $\phi^{-1}(J) = \phi^{-1}(I)$ ou $\phi^{-1}(J) = A$. Mas como ϕ é sobrejetor temos que $J = \phi(\phi^{-1}(J))$. Logo, $J = \phi(\phi^{-1}(J)) = \phi(\phi^{-1}(I)) = I$ ou $J = \phi(A) = B$. Portanto, I é um ideal maximal.

□

A seguir apresentamos alguns resultados relacionados ao anel de funções regulares, anel local e corpo de funções regulares.

Definição 3.32. *Sejam V uma variedade e $P \in V$ um ponto. O corpo de resíduos de P é definido como $K_P := \mathcal{O}_P/m_P$, onde $m_P := \{\langle U, f\rangle \mid f(P) = 0\}$.*

Proposição 3.33. *Seja V uma variedade. Para todo ponto $P \in V$ existe um isomorfismo de corpos $K_P \simeq K$.*

Demonstração. Considere a função

$$\begin{aligned} \varepsilon: \mathcal{O}_P &\rightarrow K \\ \langle U, f\rangle &\mapsto f(P). \end{aligned} \tag{3.10}$$

Mostraremos que ε é um homomorfismo sobrejetor de anéis cujo núcleo é m_P.

Sejam $\langle U, f\rangle = \langle W, g\rangle \in \mathcal{O}_P$. Logo $P \in U \cap W$ e $f_{|U\cap W} = g_{|U\cap W}$ e, então, $\varepsilon(f) = f(P) = g(P) = \varepsilon(g)$. Portanto, ε está bem definida. Além disso, dados $\langle U, f\rangle, \langle W, g\rangle \in \mathcal{O}_P$ temos que

$$\begin{aligned} \varepsilon(\langle U, f\rangle + \langle W, g\rangle) = \varepsilon(\langle U \cap W, f+g\rangle) &= (f+g)(P) \qquad (3.11) \\ &= f(P) + g(P) = \varepsilon(\langle U, f\rangle) + \varepsilon(\langle W, g\rangle), \\ \varepsilon(\langle U, f\rangle\langle W, g\rangle) = \varepsilon(\langle U \cap W, fg\rangle) &= (fg)(P) \qquad (3.12) \\ &= f(P)g(P) = \varepsilon(\langle U, f\rangle)\varepsilon(\langle W, g\rangle). \end{aligned}$$

Logo ε é um homomorfismo de anéis e, por definição de núcleo, temos $ker\, \varepsilon = \{\langle U, f\rangle \in \mathcal{O}_P \mid f(P) = 0\} = m_P$. Além disso, para cada $c \in K$, considere a função constante $f_c : V \rightarrow K$ dada por $f_c(v) = c$ para todo $v \in V$, então f_c é regular em V e $\varepsilon(\langle V, f_c\rangle) = f_c(P) = c$, ou seja, ε é sobrejetor. Assim, pelo Teorema dos Isomorfismos (Teorema 1.23), temos que $K_P \simeq K$. □

Proposição 3.34. *Seja V uma variedade. Para todo ponto $P \in V$, existem homomorfismos injetores de anéis $\mathcal{O}(V) \rightarrow \mathcal{O}_P \rightarrow K(V)$.*

Demonstração. **i)** $\mathcal{O}(V) \rightarrow \mathcal{O}_P$. Dada $f \in \mathcal{O}(V)$, por definição f é regular em todo V. Como V é um aberto de V que contém P, podemos definir a função

$$\begin{aligned} \varphi_P: \mathcal{O}(V) &\rightarrow \mathcal{O}_P \\ f &\mapsto \langle V, f\rangle \end{aligned} \tag{3.13}$$

Dados $f, g \in \mathcal{O}(V)$, temos

$$\begin{aligned} \varphi_P(f+g) = \langle V, f+g\rangle &= \langle V, f\rangle + \langle V, g\rangle = \varphi_P(f) + \varphi_P(g), \qquad (3.14) \\ \varphi_P(fg) = \langle V, fg\rangle &= \langle V, f\rangle\langle V, g\rangle = \varphi_P(f)\varphi_P(g). \end{aligned}$$

Logo φ_P é um homomorfismo. Além disso, φ_P é injetor, pois se $\varphi_P(f) = \langle V, 0\rangle$, $f = 0$ em todo V.

ii) $\mathcal{O}_P \rightarrow K(V)$. Dada $\langle U, f\rangle \in \mathcal{O}_P$, por definição U é aberto em V, $P \in V$ e $f \in O(U)$. E se $\langle U, f\rangle = \langle W, g\rangle \in \mathcal{O}_P$, então $U \cap W$ é um aberto de V, $p \in U \cap w$ e $f_{|U\cap w} = g_{|U\cap w}$. Assim, podemos definir a função

$$\begin{aligned} \psi_P : \mathcal{O}_P &\rightarrow K(V) \\ \langle U, f\rangle &\mapsto \langle U, f\rangle \end{aligned} \tag{3.15}$$

Pelas Proposições 3.19 e 3.21, ψ_P é um homomorfismo de anéis. Além disso, ψ_P é injetor. De fato, se $\langle U, f\rangle \in \mathcal{O}_P$ é tal que $\psi_P(\langle U, f\rangle) = \langle V, 0\rangle$, então $f = 0$ em U. Como $\langle U, 0\rangle = \langle V, 0\rangle$ em $\mathcal{O}_P$, então $\langle U, f\rangle = \langle V, 0\rangle$ em $\mathcal{O}_P$.

□

No próximo exemplo esta relação se mostra clara.

Exemplo 3.35. *Considere a variedade algébrica $V = V(f) \subset \mathbb{C}^2$ onde $f : x = 0$. E sejam $\mathcal{O}(V)$ o anel de funções regulares em V, $\mathcal{O}_P(V)$ o anel local de V em um ponto $P \in V$ e $K(V)$ o corpo de funções regulares em V.*

Temos que a função

$$g = \frac{1}{y^2+1} \notin \mathcal{O}(V),$$

de fato g não é regular em $(0, i)$, por exemplo.

Além disso, $g \in \mathcal{O}_P(V)$ quando $P = (0, 0)$ mas $g \notin \mathcal{O}_P(V)$ quando $P = (0, i)$.

Agora, considere $Z(q)$ o conjunto de zeros de $q = y^2+1$. Temos que V é fechado na topologia de Zariski e, consequentemente $V - Z(q)$ é um aberto. Em $V - Z(q)$ a função

$$g = \frac{1}{y^2+1}$$

é regular e, portanto, $g \in K(V)$.

4. Multiplicidade e dimensões

4.1 Multiplicidade

No decorrer desta seção noções de módulos e sequências serão utilizados frequentemente, sugerimos ao (à) leitor (a) relembrar tais conceitos na seção 1.3, se necessário.

4.1.1 Multiplicidade local de curvas planas

Nesta seção definimos e apresentamos uma forma de calcular a multiplicidade local de curvas planas a fim de motivar e possibilitar a generalização deste conceito para variedades algébricas. Para as demonstrações deste conteúdo são necessárias as definições de retas tangentes, pontos singulares, translações e resultados relacionados a módulos e sequências exatas, a seguir apresentamos estas noções. Para este estudo foi utilizada a referência [3].

O espaço afim (veja Definição 2.6) K^1 de dimensão 1 é dito reta afim, assim como K^2 é dito plano afim.

Definição 4.1 (Hipersuperfície)**.** *Seja $F \in K[x_1, ..., x_n]$. Se F não for uma constante, o conjunto de zeros de F é chamado de hipersuperfície definido por F e é denotado por $V(F)$.*

Em K^n o conjunto $V(F)$ é chamado de hiperplano quando F é um polinômio de grau um. Uma hipersuperfície em K^2 é chamada de curva plana afim e se F é um polinômio de grau um, essa curva será uma reta. Nesta seção apresentamos resultados para curvas planas afins, isto é, vamos trabalhar em K^2.

Temos que as curvas do plano afim correspondem a polinômios não constantes $F \in K[X, Y]$ sem múltiplos fatores, onde F é determinado até a multiplicação por uma constante diferente de zero. Para alguns propósitos, é útil permitir que F tenha vários fatores, modificando ligeiramente esta definição, temos o seguinte:

Definição 4.2. *Sejam $F, G \in K[X, Y]$ polinômios. Dizemos que F e G são equivalentes se $F = \lambda G$ para algum $\lambda \in K$ diferente de zero.*

Definição 4.3 (Curva)**.** *Definimos uma curva do plano afim como uma classe de equivalência de polinômios não constantes sob essa relação de equivalência.*

Frequentemente, distorcemos essa distinção de equivalência e dizemos, por exemplo, "a curva plana $Y^2 - X^3$" ou mesmo "a curva plana $Y^2 = X^3$".

Definição 4.4 (Grau de curva)**.** *O grau de uma curva é o grau do polinômio que a define.*

Uma curva de grau um é uma reta, então falamos da "reta $aX + bY + c$" ou "da reta $aX + bY + c = 0$".

Definição 4.5. *Seja F uma curva. Se $F = \prod F_i^{e_i}$, onde F_i são os fatores irredutíveis de F, dizemos que os F_i's são as componentes de F e e_i é a multiplicidade da componente F_i.*

A componente F_i é simples se $e_i = 1$ e múltipla caso contrário. Observe que as componentes F_i de F podem ser recuperados (mesmo a equivalência) de $V(F)$, mas as multiplicidades dos componentes não podem.

Definição 4.6 (Ponto Singular)**.** *Sejam F uma curva e $P = (a, b) \in F$. O ponto P é dito ponto simples de F se uma das derivadas parciais é não nula, isto é, $F_X(P) \neq 0$ ou $F_Y(P) \neq 0$. Um ponto que não é simples é dito múltiplo ou singular.*

Uma curva formada por pontos simples é dita curva não singular.

Definição 4.7 (Reta tangente)**.** *Sejam F uma curva e $P = (a, b) \in F$ um ponto simples. Neste caso a reta $F_X(P)(X - a) + F_Y(P)(Y - b) = 0$ é chamada de tangente de F em P.*

Proposição 4.8. *Sejam P e P' pontos em $\mathbb{A}^2_K$, L_1, L_2 retas distintas que passam por P e L'_1, L'_2 retas distintas que passam por P'. Então existe uma mudança de coordenadas afim T de $\mathbb{A}^2_K$ tal que $T(P) = P'$ e $T(L_i) = L'_i$, $i = 1, 2$.*

Demonstração. Considere as equações vetoriais

$$L_1 = P + \lambda v_1, \quad L_2 = P + \lambda v_2, \quad L'_1 = P' + \lambda v'_1 \quad \text{e} \quad L'_2 = P' + \lambda v'_2$$

das retas L_1, L_2, L'_1 e L'_2, onde $\lambda \in K$ e $v_1, v_2, v'_1, v'_2 \in K^2$.

Como L_1 e L_2 são distintas e ambas passam pelo ponto P então as retas L_1 e L_2 não são paralelas e, assim, o conjunto $B = \{v_1, v_2\}$ é linearmente independente. Dessa forma o conjunto B forma uma base para o espaço K^2. Definimos então a aplicação linear $h : \; K^2 \to K^2$ tal que

$$h(v_1) = v'_1 \quad \text{e} \quad h(v_2) = v'_2$$

que está bem definida pois está definida em uma base B de K^2. Considere então a transformação

$$\begin{array}{rccl} T: & K^2 & \to & K^2 \\ & Q & \mapsto & h(Q) + (P' - h(P)). \end{array}$$

Temos que $T(P) = P'$ e $T(L_i) = T(P+\lambda v_i) = h(P+\lambda v_i)+P'-h(P) = P'+\lambda v'_1$ para $i \in \{1, 2\}$ como queríamos demonstrar. □

Definição 4.9 (Multiplicidade de Curva)**.** *Seja F uma curva qualquer, $P = (0, 0)$. Escreva $F = F_m + F_{m+1} + \cdots + F_n$, onde F_i é um polinômio homogêneo em $K[X, Y]$ de grau i, $F_m \neq 0$. Definimos m como a multiplicidade de F em $P = (0, 0)$ e denotamos $m = \mu_P(F)$.*

Proposição 4.10. *Seja F uma curva. O ponto $P = (0,0)$ é simples em F se, e somente se, $\mu_P(F) = 1$ e neste caso F_1 é exatamente a reta tangente de F em P.*

Demonstração. Como $P \in F$ temos que $m > 0$, pois caso contrário $F_0 = c \neq 0$ e, consequentemente, $F(P) = F_0(P) + F_1(P) + \cdots + F_n(P) = c + 0 = c \neq 0$, o que implicaria que $P \notin F$.

($\Rightarrow$) Se $P = (0,0)$ é um ponto simples, então $F_X(0,0) \neq 0$ ou $F_Y(0,0) \neq 0$. Mas como a derivada parcial de todo polinômio homogêneo F_i com $i \geq 2$ é um polinômio homogêneo de grau $i - 1 \geq 1$, então $F_{iX}(0,0) = 0$ e $F_{iY}(0,0) = 0$ para todo $i \geq 2$. Portanto, F tem um termo $F_1 = aX + bY$ com a ou b não nulo, isto é, $F = F_1 +$ termos de maior grau. Logo, $\mu_P(F) = 1$.

($\Leftarrow$) Suponha $\mu_P(F) = 1$ e $F_1 = aX + bY$ com $a \neq 0$ ou $b \neq 0$. Então $F_X = a +$ termos de maior grau e $F_Y = b +$ termos de maior grau. Como cada F_i é um polinômio homogêneo, temos que $F_X(0,0) = a$ e $F_Y(0,0) = b$, logo $F_X \neq 0$ ou $F_Y \neq 0$, ou seja, P é um ponto simples.

E nesse caso a reta tangente é justamente F_1, de fato $t = F_X(P)(X-0) + F_Y(P)(Y-0) = aX + bY = F_1$. □

Se $P = (a,b)$ é um ponto arbitrário de F, nós estendemos a definição da multiplicidade $\mu_P(F)$ transladando $(0,0)$ para P. Seja T a mudança de coordenadas afim tal que $T(X,Y) = (X + a, Y + b)$, então $T(0,0) = P$ e $T \circ F$ é uma curva contendo $(0,0)$. Definimos então $\mu_P(F) = \mu_{(0,0)}(T(F))$. A Proposição 4.10 vale para P um ponto qualquer. Se $m = 2$, P é chamado ponto duplo, se $m = 3$, ponto triplo, e assim segue.

Se F é uma curva irredutível, $V(F)$ é uma variedade algébrica em K^2. Usualmente escrevemos $A(F)$, $K(F)$ e $\mathcal{O}_P(F)$ invés de $A(V(F))$, $K(V(F))$, e $\mathcal{O}_P(V(F))$. Relembramos que escrevemos K^n para nos referir ao espaço afim de dimensão n e $\mathbb{A}^n_K$ quando identificamos K^n como uma variedade algébrica.

Proposição 4.11. *Sejam P, $Q \in K^n$ e $T : K^n \to K^n$ uma mudança de coordenadas afim T tal que $T(P) = Q$. Então $\tilde{T} : \mathcal{O}_Q(\mathbb{A}^n_K) \to \mathcal{O}_P(\mathbb{A}^n_K)$ é um isomorfismo. Além disso, se $V \subseteq K^n$ é uma variedade algébrica e $P \in T^{-1}(V)$, então $\tilde{T}$ induz um isomorfismo de $\mathcal{O}_Q(V)$ em $\mathcal{O}_P(T^{-1}(V))$.*

Lema 4.12. *Seja $P = (0,\ldots,0) \in K^n$, $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n_K)$, $m = m_P(\mathbb{A}^n_K)$. Seja $I \subset K[x_1,\ldots,x_n]$ o ideal gerado por $x_1,\ldots,x_n$. Então se $I\mathcal{O} = m$ temos $I^r\mathcal{O} = m^r$ para todo r.*

A Proposição 4.11 e o Lema 4.12 são, respectivamente, os exercícios 2.22 e 2.43 da referência [3].

Lema 4.13. *Seja $I = \langle X,Y \rangle \subset K[X,Y]$. Então $dim_K(K[X,Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.*

Demonstração. Considere $K[X,Y]$ um K-espaço vetorial que tem como base o conjunto $\{X^iY^j \mid i + j \geq 0\}$, da mesma forma o ideal $I = \langle X,Y \rangle$ tem como base o conjunto $\{X^iY^j \mid i + j \geq 1\}$. Então a base do ideal I^n enquanto K-espaço vetorial é $\{X^iY^j \mid i + j \geq n\}$.

Logo

$$\frac{K[X,Y]}{I^n} = \langle \{X^iY^j \mid i+j<n\}\rangle \Rightarrow dim_K \frac{K[X,Y]}{I^n} = 1+2+\cdots+n = \frac{n(n+1)}{2}. \quad (4.1)$$

□

Lema 4.14. *Se $V(I)=\{P\}$, então $K[x_1,\ldots,x_n]/I$ é isomorfo à $\mathcal{O}_P(\mathbb{A}^n_K)/I\mathcal{O}_P(\mathbb{A}^n_K)$.*

O Lema 4.14 é consequência direta de um resultado (*"Proposition 6"*) apresentado na referência [3], página 27.

Proposição 4.15. i) *Seja $0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\varphi} V'' \longrightarrow 0$ uma sequência exata de espaços vetoriais de dimensão finita sobre K. Então $dim\, V' + dim\, V'' = dim\, V$.*

ii) *Seja $0 \longrightarrow V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \longrightarrow 0$ uma sequência exata de espaços vetoriais de dimensão finita sobre K.Então $dim\, V_4 = dim\, V_3 - dim\, V_2 + dim\, V_1$.*

Demonstração. **i)** Pelo o Teorema do Núcleo e da Imagem (Teorema 1.39) nas aplicações $\psi: V' \to V$ e $\varphi: V \to V''$ vale que

$$dim\ V = dim\ ker(\varphi) + dim\ Im(\varphi)$$

e

$$dim\ V' = dim\ ker(\psi) + dim\ Im(\psi).$$

Como a sequência é exata temos que $Im\,(\psi) = ker\,(\varphi)$, $ker\,(\psi) = 0$ e $dim\, Im(\varphi) = dim\, V''$. Logo $dim\, V = dim\, V' + dim\, V''$.

ii) A aplicação φ_1 é injetora e aplicação φ_3 é sobrejetora, então $dim\, ker(\varphi_1) = 0$ e $dim\, Im(\varphi_3) = dim\, V_4$. E como a sequência é exata vale $dim\, Im(\varphi_2) = dim\, ker(\varphi_3)$ e $dim\, Im(\varphi_1) = dim\, ker(\varphi_2)$. Assim, utilizando o Teorema do Núcleo e da Imagem (Teorema 1.39) em φ_1, φ_2 e φ_3 temos que

$$dim\, V_3 = dim\, ker(\varphi_3) + dim\, Im(\varphi_3) = dim\, ker(\varphi_3) + dim\, V_4, \quad (4.2)$$

$$dim\, V_2 = dim\, ker(\varphi_2) + dim\, Im(\varphi_2) = dim\, ker(\varphi_2) + dim\, ker(\varphi_3), \quad (4.3)$$

$$dim\, V_1 = dim\, ker(\varphi_1) + dim\, Im(\varphi_1) = dim\, ker(\varphi_2) \quad (4.4)$$

Logo

$$\begin{aligned} dim\, V_4 &\overset{4.2}{=} dim\, V_3 - dim\, ker(\varphi_3) \\ &\overset{4.3}{=} dim\, V_3 - (dim\, V_2 - dim\, ker(\varphi_2)) \\ &\overset{4.4}{=} dim\, V_3 - dim\, V_2 + dim\, V_1 \end{aligned}$$

□

Proposição 4.16. *Se $\mathcal{O}$ é um anel local com um ideal maximal m, então existe uma sequência exata natural de $\mathcal{O}$-módulos*

$$0 \longrightarrow m^n/m^{n+1} \longrightarrow \mathcal{O}/m^{n+1} \longrightarrow \mathcal{O}/m^n \longrightarrow 0. \tag{4.5}$$

Lema 4.17. *Sejam A um anel de valorização discreta com um ideal maximal m. Suponha que o corpo K é um subanel de A e que a composição $K \longrightarrow A \longrightarrow A/m$ é um isomorfismo de K com A/m. Se $K \subseteq A$ e m^n/m^{n+1} é um A-módulo, então m^n/m^{n+1} é um K-espaço vetorial e $dim_K(m^n/m^{n+1}) = 1$ para todo $n \geq 0$.*

A Proposição 4.16 e o Lema 4.17 são, respectivamente, os exercícios 2.49(e) e 2.50 da referência [3].

Seja F uma curva plana irredutível e $P \in F$. Os próximos resultados nos dão uma forma de encontrar a multiplicidade de P em F em termos do anel local $\mathcal{O}_P(F)$.

Teorema 4.18. *P é um ponto simples de F se, e somente se, $\mathcal{O}_P(F)$ é um anel de valorização discreta. Neste caso, se $L = aX + bY + c$ é uma reta qualquer que passa por P e não é a reta tangente à F em P, então a imagem de L em $\mathcal{O}_P(F)$ é um parâmetro de uniformização.*

Demonstração. ($\Rightarrow$) Seja $V = V(F)$. Suponha $P = (a, b)$ um ponto simples em F, $t = f_X(P)(X - a) + f_Y(P)(Y - b)$ a reta tangente à F em P e L a reta que passa por P e não é tangente à F em P. Então, existe uma mudança de coordenadas $T : K^2 \to K^2$ tal que $T(0) = P$ e T induz um isomorfismo $\tilde{T} : K[X, Y] \to K[X, Y]$ dado por $\tilde{T}(X) = L$ e $\tilde{T}(Y) = t$. Assim, podemos assumir $P = (0, 0)$, em que $Y = 0$ é a reta tangente à F em P (veja Proposições 4.8 e 4.11). Pela Proposição 3.11 basta mostrar que $m_P(F)$ é gerado por x.

A sequência

$$0 \longrightarrow \langle F \rangle \longrightarrow K[X, Y] \longrightarrow A(V) \to 0 \tag{4.6}$$

é exata. Como $F \in I(P) = I = \langle X, Y \rangle$, existe um isomorfismo de anéis locais

$$\frac{K[X, Y]_I}{\langle F \rangle} \simeq A(V)_I \simeq \mathcal{O}_P(V) \tag{4.7}$$

e $m_P(V)$ é gerado pelas imagens de X e Y.

Dessa forma, temos $F = Y + F_m + F_{m+1} + \cdots + F_n$, onde F_i são polinômios homogêneos em $K[X, Y]$ de grau $i \in \{m, \ldots, n\}$. Seja $F(X, 0) = Q(X)$ os termos de F que não dependem de Y. Então X^2 divide $Q(X)$ e, assim, podemos escrever $F = YG + X^2H$ com $G \in K[X, Y]$ e $H \in K[X]$. Em $A(V)$, $YG = -X^2H \in \langle X \rangle$. Mas $G(0, 0) \neq 0$, logo, $G \notin \langle X, Y \rangle$ e G é um elemento invertível em $\mathcal{O}_P(V)$. Então,

$$Y = -X^2HG^{-1} \tag{4.8}$$

e, portanto, $Y \in \langle X \rangle$, como queríamos.

($\Leftarrow$) Suponhamos que $\mathcal{O}_P(F)$ é um anel de valorização discreta. Então, $m_P(F)$ é um ideal principal e, pelo Lema 4.17, temos que $dim_K\, m_P(F)^n/m_P(F)^{n+1} = 1$. Pelo Teorema 4.19

(próximo resultado), $\mu_P(F) = 1$, isto é, P é um ponto simples. $\square$

Finalizamos com o principal resultado desta seção.

Teorema 4.19. *Seja P um ponto em uma curva irredutível F. Então para todo n suficientemente grande*

$$\mu_P(F) = dim_K(m_P(F)^n/m_P(F)^{n+1}).$$

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

Demonstração. No decorrer dessa demonstração escreveremos m no lugar de $m_P(F)$. Considere a sequência exata de $\mathcal{O}_P(F)$-módulos (que existe pela Proposição 4.16):

$$0 \longrightarrow \frac{m^n}{m^{n+1}} \longrightarrow \frac{\mathcal{O}_P(F)}{m^{n+1}} \longrightarrow \frac{\mathcal{O}_P(F)}{m^n} \longrightarrow 0. \tag{4.9}$$

É suficiente mostrar que $dim_K \, \mathcal{O}_P(F)/m^n = n\mu_P(F) + c$ para alguma constante c e para todo $n \geq \mu_P(F)$ (veja Proposição 4.15). Desta forma, obteremos que

$$(n+1)\mu_P(F) + c = dim_K \, m^n/m^n + n\mu_P(F) + c. \tag{4.10}$$

Tome $P = (0,0)$, logo, $m^n = I^n\mathcal{O}_P(F)$, onde $I = \langle X, Y\rangle \subseteq K[X,Y]$ (veja Lema 4.12). Então, $V(I^n) = P$ e pelo Lema 4.14

$$\frac{K[X,Y]}{I^n} = \frac{\mathcal{O}_P(\mathbb{A}^2)}{I^n\mathcal{O}_P(\mathbb{A}^2)}. \tag{4.11}$$

Logo,

$$\frac{K[X,Y]}{\langle I^n, F\rangle} = \frac{\mathcal{O}_P(\mathbb{A}^2)}{\langle I^n, F\rangle\mathcal{O}_P(\mathbb{A}^2)} = \frac{\mathcal{O}_P(F)}{I^n\mathcal{O}_P(F)} = \frac{\mathcal{O}_P(F)}{m^n}. \tag{4.12}$$

Denotando $\mu_P(F)$ por μ e escrevendo F como a soma de polinômios homogêneos, temos $F = F_\mu +$ termos de maior grau. Assim, $F \in I^\mu$ e se $G \in I^{n-\mu}$, então $FG \in I^n$. Seja ϕ o homomorfismo natural sobrejetor

$$\phi : \frac{K[X,Y]}{I^n} \to \frac{K[X,Y]}{\langle I^n, F\rangle}.$$

E seja ψ a aplicação linear sobre K dada por

$$\begin{array}{rccc} \psi : & \dfrac{K[X,Y]}{I^{n-\mu}} & \to & \dfrac{K[X,Y]}{I^n} \\ & G & \mapsto & FG. \end{array}$$

Temos então que $\ker \phi = \langle F\rangle = Im\,\psi$ e ψ é injetora.A sequência de K-espaços vetoriais

$$0 \longrightarrow \frac{K[X,Y]}{I^{n-\mu}} \xrightarrow{\psi} \frac{K[X,Y]}{I^n} \xrightarrow{\phi} \frac{K[X,Y]}{\langle I^n, F\rangle} \longrightarrow 0 \tag{4.13}$$

é exata. Considerando a sequência (4.13), a Proposição 4.13 e a Proposição 4.15 segue que

$$dim_K \frac{K[X,Y]}{\langle I^n, F\rangle} = \frac{n(n+1)}{2} - \frac{(n-\mu)((n-\mu)+1)}{2} = n\mu - \frac{\mu(\mu-1)}{2}. \tag{4.14}$$

Definindo $c = \mu(1-\mu)/2$ e considerando a relação dada na equação (4.12) acabamos a prova. □

4.1.2 Multiplicidade de variedades algébricas

Generalizando a noção apresentada na seção anterior, apresentamos uma forma de calcular a multiplicidade de uma variedade algébrica. Para realizar este estudo foi utilizada a referência [6].

Proposição 4.20. *Seja M um módulo graduado finitamente gerado sobre um anel noetheriano S. Então existe uma filtração $0 = M^0 \subseteq M^1 \subseteq \cdots \subseteq M' = M$ de submódulos graduados tal que para cada i, $M^i/M^{i-1} \simeq (S/p_i)(l_i)$, onde p_i é um ideal homogêneo primo de S e $l_i \in \mathbb{Z}$. A filtração não é única e para uma filtração qualquer temos que:*

i) *Se p é um ideal homogêneo primo de S, então $p \supseteq Ann\, M \Leftrightarrow p \supseteq p_i$ para algum i. Em particular, os elementos minimais do conjunto $\{p_1, \ldots, p_r\}$ são apenas os primos minimais de M, ou seja, os primos que são minimais e contém $Ann\; M$.*

ii) *Para cada primo de M, o número de vezes que p aparece no conjunto $\{p_1, \ldots, p_r\}$ é igual ao comprimento de M_p sobre o anel local S_p independente da filtração.*

Demonstração. Para provar a existência da filtração, considere τ o conjunto de submódulos graduados de M que admitem tal filtração. Claramente, o módulo 0 admite tal filtração, logo τ não é vazio. M é um módulo noetheriano, logo existe um submódulo maximal $M' \subset M$. Considere então $M'' = M/M'$. Se $M'' = 0$ a prova está concluída. Caso contrário, considere o conjunto de ideais $\mathcal{J} = \{I_m = Ann(m)\,;\, m \in M''$ é um elemento homogêneo não nulo$\}$. Cada I_m é um ideal homogêneo e $I_m \neq S$. Como S é um anel noetheriano, existe um elemento $m \in M''$, $m \neq 0$, tal que I_m é um elemento maximal do conjunto $\mathcal{J}$. Provaremos que I_m é um ideal primo. Suponha $ab \in I_m$, mas $b \notin I_m$. Queremos mostrar que $a \in I_m$. Decompondo em componentes homogêneas, podemos assumir que a, b são elementos homogêneos. Agora considere o elemento $bm \in M''$. Como $b \notin I_m$, $bm \neq 0$. Então, temos que $I_m \subset I_{bm}$, mas como I_m é maximal $I_m = I_{bm}$. Mas $ab \in I_m$, então $abm = 0$, logo $a \in I_{bm} = I_m$ como queríamos demonstrar. Assim I_m é um ideal homogêneo primo de S. Chamando $I_m = p$. Tome m com grau l. Então o módulo $N \subset M''$ gerado por m é isomorfo à $(S/p)(-l)$. Seja $N' \subset M$ a imagem inversa de N em M. Então $M' \subset N'$ e $N'/M' \simeq (S/p)(-l)$. Logo N' também tem uma filtração como queríamos. Isso contradiz a maximalidade de M'. Concluímos então que M' é igual a M, o que prova a existência da filtração.

i) Suponha a filtração dada de M. Temos que $p \supset Ann\, M \Leftrightarrow p \supset Ann\,(M^i/M^{i-1})$ para algum i. Mas $Ann\,(S/p_i)/(l)) = p_i$, portanto, está provado (i).

ii) Para provar (ii) calculamos a localização no ideal primo minimal p. Como p é minimal no conjunto $\{p_1, \ldots, p_r\}$, após a localização segue que $M_p^i = M_p^{i-1}$ exceto nos casos em que $p = p_i$. Nestes casos temos $M_p^i / M_p^{i-1} \simeq (S/p)_p = k(p)$. O corpo quociente de S/p, esquecendo a graduação. Isso mostra que M_p é um S_p-módulo de comprimento finito igual ao número que p ocorre no conjunto $\{p_1, \ldots, p_r\}$. □

Definição 4.21 (Multiplicidade de módulo)**.** *Seja M um S-módulo graduado e p um primo minimal de M. Definimos a multiplicidade de M em p, denotada por $\mu_p(M)$, como o comprimento de M_p sobre S_p.*

Visto a noção de multiplicidade para um módulo graduado finitamente gerado qualquer, olharemos para o anel local $\mathcal{O}_P(V)$ como um módulo graduado e esta será a multiplicidade da variedade algébrica V.

4.2 Dimensão de variedades algébricas

Nesta seção abordaremos de maneira algébrica e geométrica o conceito de dimensão de conjuntos algébricos e mostramos a equivalência das dimensões algébrica e geométrica de uma variedade algébrica, ou seja, de um conjunto algébrico irredutível. Para tais estudos foram utilizadas as referências [12], [13], [7]. Além disso, apresentamos a noção de dimensão de Krull para conjuntos algébricos e mostramos algumas equivalências. Para este estudo foram utilizadas as referências [11], [1], [6].

4.2.1 Dimensão algébrica

Relembramos que notação utilizada para a extensão de corpos (Definição 1.26) $F \subset K$ é F/K.

Definição 4.22. *Dado $\mathrm{B} = \{X_1, \ldots, X_n\} \subseteq K$, B é dito algebricamente independente sobre F se não existem polinômios com coeficientes em F zerados por B. Ou seja,*

$$\nexists\, f \in F[y_1, \ldots, y_n]; f(X_1, \ldots, X_n) = 0$$

Definição 4.23. *Um subconjunto B de K é dito base de transcendência de F/K se*

i) B *é algebricamente independente sobre F.*

ii) $\mathrm{B} \subseteq \mathrm{B}'$ *e B' é um subconjunto algebricamente independente sobre F então* $\mathrm{B} = \mathrm{B}'$.

A cardinalidade de uma base de transcendência de F/K é chamado grau de transcendência de F/K e será denotado por $tr.deg_K F$.

Definição 4.24. *Se V é um conjunto algébrico irredutível, então o corpo dos quocientes f/g com f e g no domínio*

$$K[V] = K[x_1, \ldots, x_n]/I(V)$$

é chamado de corpo de frações sobre V e é denotado por $(K[V])$.

Perceba que $K \subset (K[V])$, dessa forma $(K[V])$ é dito extensão de K e assim a seguinte definição pode ser feita.

Definição 4.25. *O grau de transcendência de $(K[V])$ sobre K é chamado de dimensão algébrica de V sobre K.*

4.2.2 Dimensão geométrica

Seja V um conjunto algébrico não vazio qualquer em $\mathbb{C}^n$. Pelo Teorema da Base de Hilbert sabemos que existem polinômios $f_1, \dots, f_k$ que são geradores do ideal $I(V)$. Para cada $x \in V$, considere a matriz $\partial f_i/\partial x_j$ de tamanho $k \times n$ avaliado em x. Seja ρ o maior posto que esta matriz atinge em pontos de V.

Definição 4.26. *Um ponto $x \in V$ é dito não-singular se a matriz $(\partial f_i/\partial x_j)$ atinge seu posto máximo ρ em x, e singular se*

$$posto(\partial f_i/\partial x_j)(x) < \rho.$$

A definição acima não depende da escolha dos polinômios geradores de $I(V)$.

Teorema 4.27. *Seja V uma variedade algébrica. Consideramos $M_1 \subset V$ o conjunto de pontos p em que o posto de V é o máximo ρ. E sendo $V_1 := V - M_1$, então*

i) *M_1 é uma variedade analítica diferenciável de dimensão $n - \rho$;*

ii) *V_1 é vazio ou é um conjunto algébrico próprio de V;*

iii) *$Dim(V) = n - \rho$.*

A dimensão de M_1 é dita dimensão geométrica de V. Dessa forma, o item (iii) nos permite concluir que as dimensões algébrica e geométrica de uma variedade algébrica são equivalentes.

A demonstração do item 4.27.i pode ser encontrada em [13] e as demonstrações dos itens 4.27.ii e 4.27.iii podem ser encontradas em [7], Capítulo X, seção 5.

Exemplo 4.28. *Considere V a variedade algébrica em $\mathbb{C}^3$ definida pelo ideal de polinômios gerado por $f(x, y, z) = x^3 - y^2 + z^4$. Calculando a matriz das derivadas parciais temos:*

$$\nabla f(x, y, z) = (3x^2 \ , \quad -2y \ , \quad 4z^3).$$

O posto desta matriz é máximo e igual à 1 exceto no ponto $(0, 0, 0)$. Dessa forma, se escrevermos $V = M_1 \cup V_1$, onde $V_1 = \{(0, 0, 0)\}$ e $M_1 = V - \{(0, 0, 0)\}$, pelo item (i) temos que $dimM_1 = 3 - 1 = 2$, consequentemente,

$$dim\ V = 2.$$

4.2.3 Dimensão de Krull

Wolfgang Krull foi um matemático alemão que fez contribuições fundamentais para a álgebra comutativa, uma delas foi a definição de dimensão de Krull, essa noção pode ser trabalhada em espaços topológicos, anéis e conjuntos algébricos. Nesta seção exploramos este conceito e buscamos relacionar o conteúdo estudado neste capítulo.

As próximas definições e resultados relacionados à elas podem ser encontrados em [6], Capítulo 1. Apresentamos, inicialmente, algumas definições essenciais.

Definição 4.29 (Espaço noetheriano). *Um espaço topológico X é dito espaço noetheriano se satisfaz a condição de cadeia descendente para subconjuntos fechados, isto é, para qualquer sequência de subconjuntos fechados $V_1 \supseteq V_2 \supseteq \cdots \supseteq V_n \supseteq \ldots$, existe $k \in \mathbb{N}$ tal que $V_k = V_j$ para todo $j \geq k$.*

Definição 4.30 (Ideal primário). *Um ideal $q \subsetneq A$ é chamado um ideal primário se qualquer divisor de zero em A/q é um elemento nilpotente. Em outras palavras, se $x,\ y \in A$ e $xy \in q$, então $x \in q$ ou $y^n \in q$ para algum $n > 0$.*

Definição 4.31 (Decomposição Primária). *Seja A um anel e I um ideal de A. Uma decomposição primária de I é a representação de I como interseção finita de ideais primários*

$$I = \bigcap_{i=1}^{n} q_i.$$

Se, além disso, todos os ideais $\sqrt{q_i}$ são distintos e temos $q_i \not\supseteq \bigcap_{j \neq i} q_j$ para todo i, a decomposição é chamada decomposição minimal.

Definição 4.32 (Extensão Integral de Anéis). *Seja $A \subseteq B$ uma extensão de aneis. Um elemento $b \in B$ é chamado um elemento integral (ou algébrico, se A e B são corpos) se b satisfaz uma equação polinomial com coeficientes em A, isto é, existem $a_0,\ a_1, \ldots, a_{n-1} \in A$, $n \in \mathbb{N}$, tais que*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0. \tag{4.15}$$

Se cada elemento de B é integral sobre A, então B é dita uma extensão integral de A (extensão algébrica no caso de extensão de corpos).

Vamos apresentar a definição de dimensão de Krull de um anel e algumas noções relacionadas.

Definição 4.33. *Seja A um anel e $p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n$ uma cadeia de ideais primos de A. Dizemos que esta cadeia tem comprimento n.*

Definição 4.34 (Dimensão de Krull para Anéis). *Seja A um anel. O supremo de comprimentos de todas as cadeias de ideais primos em A é dito a dimensão de Krull de A.*

Exemplo 4.35. *Considere $\mathbb{Z}$ o anel dos inteiros. Veja que como $\mathbb{Z}$ é um domínio de fatoração única, cada ideal primo não nulo é maximal. Logo a dimensão de Krull de $\mathbb{Z}$ é 1.*

Definição 4.36 (Altura de ideal primo)**.** *Seja A um anel e $p \subseteq A$ um ideal primo. A altura de p é o supremo de comprimentos de todas as cadeias de ideais primos contidos em p, isto é, o supremo das cadeias da forma*

$$p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n = p. \tag{4.16}$$

Em outras palavras, é a dimensão de localização de A por p. Denotamos a altura de p por $ht(p)$

Temos que a dimensão de A é o supremo das alturas de seus ideais primos. Apresentamos agora a noção de altura para ideais arbitrários:

Definição 4.37. *Seja A um anel e I um ideal de A. A altura q de I é o ínfimo de alturas de ideais primos contendo I.*

Proposição 4.38. *Seja A um anel. Para todo ideal I de A vale que*

$$ht(I) + dim(A/I) \leq dimA. \tag{4.17}$$

Veremos que esta desigualdade vira igualdade quando A é um domínio e I é um ideal primo.

As demonstrações da Proposição 4.38 e dos próximos resultados podem ser encontradas em [1].

Teorema 4.39. *Seja A um anel noetheriano. Então $dim\, A[x] = dim\, A + 1$.*

Observe que a dimensão de Krull de qualquer corpo K é 0.

Utilizando Teorema 4.39 e o Teorema da Base de Hilbert (Teorema 2.4) temos o resultado a seguir.

Teorema 4.40. *Seja K um corpo e $K[x_1, \ldots, x_n]$ o anel de polinômios em n variáveis sobre K. Então*

$$dim\, K[x_1, \ldots, x_n] = n. \tag{4.18}$$

Lema 4.41. *Seja K um corpo. A altura do ideal $\langle x_1, \ldots, x_i \rangle \subseteq K[x_1, \ldots, x_i]$ é exatamente i.*

Lema 4.42. *Seja $A \subseteq B$ uma extensão integral, $I \subseteq B$ um ideal e $S \subseteq A$ um conjunto multiplicativo. Então:*

i) *B/I é integral sobre $A/(A \cap I)$;*

ii) *$S^{-1}B$ é integral sobre $S^{-1}A$.*

Teorema 4.43 (Teorema de Going-Up)**.** *Seja $A \subseteq B$ um extensão integral de anéis. Considere uma cadeia de ideais primos $p_1 \subseteq \cdots \subseteq p_n$ em A e uma cadeia de primos $q_1 \subseteq \cdots \subseteq q_m$ de B, com $m < n$, tais que $q_i \cap A = p_i$ para todo $1 \leq i \leq m$. Então existem $q_m \subseteq q_{m+1} \subseteq \cdots \subseteq q_n$ para qual $q_i \cap A = p_i$ para todo $1 \leq i \leq n$. Além disso, se a primeira cadeia tem inclusões estritas, a segunda também tem.*

Corolário 4.44. *Seja $A \subseteq B$ uma extensão integral. Então $dim\, A = dim\, B$.*

Teorema 4.45 (Teorema de Normalização de Noether (forte))**.** *Seja $A = K[x_1, \ldots, x_n]$ uma álgebra polinomial sobre o corpo K e seja I um ideal de A tal que $ht(I) = r$. Então existem n elementos $y_1, \ldots, y_n \in A$ algebricamente independentes tais que*

1. *A é uma extensão integral de $K[y_1, \ldots, y_n]$;*

2. *$I \cap K[y_1, \ldots, y_n] = \langle y_1, \ldots, y_r \rangle$.*

Teorema 4.46 (Teorema de Normalização de Noether)**.** *Seja A uma álgebra finitamente gerada sobre um corpo K. Então existem $z_1, \ldots, z_r \in A$ algebricamente independentes sobre K e A é uma extensão integral de $K[z_1, \ldots, z_r]$. Além disso, $dim\, A = r$.*

Teorema 4.47. *Seja A um domínio finitamente gerado sobre o corpo K. Então $dim\, A = tr.deg_K Frac\, A$, onde $Frac\, A$ é o corpo de frações de A.*

Demonstração. Pelo Teorema de Normalização de Noether (Teorema 4.46), existem $z_1, \ldots, z_r \in A$ algebricamente independentes sobre K tais que A é uma extensão integral de $K[z_1, \ldots, z_r]$. Seja $F = Frac\, A$ e $L = K(z_1, \ldots, z_r)$. Então $L \subseteq F$ é uma extensão algébrica e $tr.deg_K F = tr.deg_K L + tr.deg_L F = r + 0 = dim\, A$. □

Teorema 4.48. *Seja A um domínio finitamente gerado sobre o corpo K e p um ideal primo de A. Então*

$$ht\, p + dim\, (A/p) = dim\, A. \tag{4.19}$$

Demonstração. Pelo Teorema de Normalização de Noether (Teorema 4.46), existem $z_1, \ldots, z_r \in A$ algebricamente independentes sobre K tais que A é uma extensão integral de $K[z_1, \ldots, z_r]$ e, além disso, $dim\, A = r$. Denote $p' = p \cap K[z_1, \ldots, z_r]$. Pelo Lema 4.42 e pelo Corolário 4.44 temos $dim\, A/p = dim\, K[z_1, \ldots, z_k]/p'$ e pelo Teorema de Going-Up (Teorema 4.43) segue que $ht(p) = ht(p')$. Dessa forma, podemos supor que A é um álgebra polinomial e aplicar o Teorema de Normalização de Noether Forte (Teorema 4.45) para $K[z_1, \ldots, z_r]$ e p', isto é, existem $y_1, \ldots, y_n \in K[z_1, \ldots, z_r]$ algebricamente independentes tais que $K[z_1, \ldots, z_r]$ é integral sobre $K[y_1, \ldots, y_r]$ e $p' \cap K[y_1, \ldots, y_r] = (y_1, \ldots, y_{ht(p)})$. Pelo Teorema 4.40 e novamente pelo Lema 4.42 e Corolário 4.44 temos

$$dim\, K[z_1, \ldots, z_r]/p' = dim\, K[y_1, \ldots, y_r]/K[y_1, \ldots, y_{ht(p)}] = r - ht(p). \tag{4.20}$$

E do Lema 4.41 obtemos

$$ht(p') = ht(K[y_1, \ldots, y_{ht(p)}]) = ht(p), \tag{4.21}$$

por fim, pelo Teorema 4.40 segue que

$$ht(p') = dim\, (K[z_1, \ldots, z_r]) = dim\, A. \tag{4.22}$$

□

Podemos generalizar o resultado visto no Teorema 3.6 para espaços noetherianos com a proposição a seguir.

Proposição 4.49. *Em um espaço noetheriano X, cada subconjunto fechado V pode ser expresso como união finita $V = V_1 \cup \cdots \cup V_r$ de conjuntos irredutíveis V_i. Se requeremos que $V_i \nsubseteq V_j$ para $i \neq j$, então os conjuntos V_i são determinados unicamente. Chamamos eles as componentes irredutíveis de V.*

Demonstração. Suponha agora que $V = V_1' \cup \ldots V_s'$ é uma outra representação de V como união de conjuntos irredutíveis. Então, $V_1' = V_1' \cap V = \cup_{i=1}^{r}(V_1' \cap V_i)$. Mas V_1' é irredutível, por isso $V_1' = V_1' \cap V_i$ para algum i e $V_1' \subseteq V_i$. Pela mesma argumentação, $V_i \subseteq V_j'$ para algum j. Logo $V_1' \subseteq V_j'$ e $j = 1$, consequentemente $V_1' = V_i$. Aplicando indução sobre o conjunto $V \setminus V_1 = \cup_{j\neq 1} V_j' = \cap_{j \neq i} V_j$ concluímos a prova. □

Definimos agora a dimensão de um conjunto algébrico enquanto espaço topológico e noetheriano e estudamos algumas formas de se calcular tal dimensão.

Definição 4.50 (Dimensão de conjunto algébrico)**.** *Seja X um espaço topológico. A dimensão de X é o supremo de comprimentos de cadeias $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ de subconjuntos irredutíveis fechados distintos. A dimensão topológica de um conjunto algébrico V é a dimensão de V como espaço topológico na topologia de Zariski.*

Teorema 4.51. *Seja V um conjunto algébrico. Então a dimensão topológica de V é igual à dimensão de seu anel de coordenadas $A(V)$.*

Demonstração. Se V é um conjunto algébrico de K^n, então os subconjuntos irredutíveis em V correspondem aos ideais primos de $K[x_1, \ldots, x_n]$ contendo $I(V)$ (veja Proposição 3.2) que correspondem aos ideais primos de $A(V) = K[x_1, \ldots, x_n]/I(V)$. Então *dim* V é o supremo de comprimentos das cadeias de ideais primos em $A(V)$, que é a dimensão de Krull do anel $A(V)$. □

Proposição 4.52. *Seja $V = V_1 \cup \cdots \cup V_r$ a decomposição de um espaço topológico V em união de componentes irredutíveis. Então $dim\ V = max_i dim\, V_i$.*

Demonstração. A dimensão de V é o supremo de cadeias $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ de subconjuntos irredutíveis, então para todo V_i em alguma cadeia vale que $Z_j = V_i$ para algum j. Logo $dim\, V \geq max_i dim\, V_i$.

Por outro lado, seja $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ uma cadeia de conjuntos irredutíveis fechados com comprimento maximal. Temos que

$$Z_n = Z_n \cap V = Z_n \cap (V_1 \cup \cdots \cup V_r) = \bigcup_{i=1}^{r} (Z_n \cap V_i)$$

é uma representação de Z_n como uma união de conjuntos fechados em Z_n. Como Z_n é irredutível $Z_n = Z_n \cap V_i$, para algum i. Por isso, $Z_n \subseteq V_i$. Mas por construção Z_n é um conjunto irredutível maximal, por isso $Z_n = V_i$. Assim, $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n = V_i$ então $dim\ V_i \geq n = dim\, V$. Portanto, $dim\, V = max_i dim\, V_i$. □

Exemplo 4.53. *Seja $X \subseteq K^2$ uma curva plana $X = V(\langle f \rangle)$, onde $f(x,y) = x - y$. Como f é um polinômio irredutível, o ideal gerado por f, $\langle f \rangle$, é um ideal primo e, então, $X \subseteq K^2$ é um conjunto algébrico irredutível. Além disso, $A(X) = K[x,y]/\langle f \rangle \simeq K[x]$ tem dimensão 1, logo X também tem dimensão 1.*

Proposição 4.54. *Todo subconjunto aberto e não vazio de um espaço topológico irredutível é irredutível e denso.*

Demonstração. Sejam X um espaço topológico irredutível e Y um subconjunto aberto não vazio de X. Suponha, por contradição, que Y não seja irredutível. Então existem Y_1 e Y_2 subconjuntos fechados próprios de Y tais que $Y = Y_1 \cup Y_2$. Como Y_1 e Y_2 são fechados em Y, existem X_1 e X_2 subconjuntos fechados de X, tais que $Y_1 = Y \cap X_1$ e $Y_2 = Y \cap X_2$. Tome $Y' = Y_2 \cup (X \setminus Y)$. Como Y é aberto em X, então $X \setminus Y$ é fechado e, portanto, Y' também é fechado em X. Além disso, como Y_1, Y_2 são subconjuntos próprios de Y por hipótese, então $Y' \neq X$. De fato, $(Y')^C = (Y_2 \cup (X \setminus Y))^C = Y_2^C \cap Y = Y_2^C \cap (Y_1 \cup Y_2) = Y_2^C \cap Y_1 = Y_1 \setminus Y_2$ é não vazio. Assim, $X = Y_1 \cup Y'$, o que contradiz a hipótese de X ser irredutível. Logo Y é irredutível.

Além disso, Y é denso em X. De fato, se $\overline{Y} \neq X$, então $X = (X \setminus Y) \cup \overline{Y}$. Como $(X \setminus Y)$ é um fechado próprio de X pois, por hipótese, Y é aberto e não vazio e $\overline{Y}$ é um fechado próprio de X, pois $\overline{Y} \neq X$, isso contradiz a hipótese de X ser irredutível. □

Lema 4.55. *Seja A um anel e $Spm(A)$ o espectro de ideais maximais de A. Se A é um domínio, então $A = \bigcap_{m \in Spm(A)} A_m$.*

Demonstração. Denote o corpo de frações de A por $K(A)$. Tome $m \in Spm\,(A)$, como m é um ideal maximal $1 \notin m$. Logo para todo $x \in A$ temos que $x = \frac{x}{1} \in A_m$, portanto $A \subseteq A_m$. Como $A \subseteq A_m$ para cada $m \in Spm\,(A)$, então $A \subseteq \bigcap_{m \in Spm(A)} A_m$.

Agora, tome $r \in K(A)$ e defina $I_r := \{a \in A \mid ar \in A\}$. Dados $x, y \in I_r$ e $z \in A$ temos que $(x-y)r = xr - yr \in A$, pois como $a \in A$ e $xr \in R$, segue que $xr, yr \in A$ e $(ax)r = a(xr) \in A$, portanto, I_r é um ideal de A. Além disso, temos que $I_r = A$ se, e somente se, $r \in A$. De fato, se $r \in A$, então $xr \in A$ para todo $x \in A$, ou seja, $A = I_r$. Por outro lado, se $I_r = A$ temos $r = 1r \in A$.

Assim, para mostrar $\bigcap_{m \in Spm(A)} A_m \subseteq A$ basta mostrar que: se $r \in K(A)$ é tal que $I_r \neq R$ então existe $m \in Spm\,(A)$ tal que $r \notin A_m$. Com efeito, se $I_r \neq A$ existe $m \in Spm\,(A)$ tal que $I_r \subseteq m$. Por contradição, se $r \in A_m$ existem $p \in A$ e $q \in A \setminus m$ tais que $r = \frac{p}{q}$. Logo $qr = p \in A$ e então $q \in I_r \subseteq m$, absurdo! □

Por fim, o próximo teorema mostra a relação entre conceitos apresentados anteriormente. Veremos que a dimensão de V é igual à dimensão do anel de funções regulares $\mathcal{O}(V)$ (Veja definição 3.12). A vantagem desta abordagem é que a dimensão de $\mathcal{O}(V)$ pode ser calculada localmente. Isto é, para cada ponto $P \in V$ definimos o anel local $\mathcal{O}_P$ de P em V tal que $dim\,\mathcal{O}_P = dim\,V$.

Teorema 4.56. *Seja $V \subseteq K^n$ uma variedade algébrica, $A(V)$ o anel de coordenadas de V, $\mathcal{O}(V)$ o anel de funções regulares em V e $K(V)$ o corpo de funções regulares em V. Então*

i) $\mathcal{O}(V) \simeq A(V)$;

ii) *Para cada ponto $P \in V$ seja $m_P \subsetneq A(V)$ o ideal das funções que se anulam em P. Então $P \leftrightarrow m_P$ é uma correspondência $1-1$ entre os pontos de V e os ideais maximais de $A(V)$;*

iii) *Para cada ponto $P \in V$, existe um isomorfismo de anéis $A(V)_{m_P} \simeq \mathcal{O}_P$ e $\dim \mathcal{O}_P = \dim V$;*

iv) *O corpo de frações de $A(V)$ é isomorfo a $K(V)$ e, consequentemente, $K(V)$ é uma extensão finitamente gerada de K e $tr.deg_K K(V) = \dim V$.*

Demonstração. Lembre que todo polinômio $f \in K[x_1, \ldots, x_n]$ induz uma função $f: V \to K$. Assim, considere o homomorfismo

$$\begin{aligned} \tilde{\alpha}: K[x_1,\ldots,x_n] &\to \mathcal{O}(V) \\ f &\mapsto f_{|V}, \end{aligned} \tag{4.23}$$

como $\tilde{\alpha}(f) = 0 \Leftrightarrow f \in I(V)$, temos que $ker\,\tilde{\alpha} = I(V)$. Então $\tilde{\alpha}$ induz um homomorfismo injetor $\alpha : A(V) \to \mathcal{O}(V)$. Mostraremos agora os itens (ii), (iii) e (iv) e, posteriormente, retornaremos à demonstração do item (i).

ii) Segue da Proposição 3.30.

iii) Fixe $P \in V$ e considere o homomorfismo injetor (veja Proposição 3.34) de anéis

$$\begin{aligned} \varphi_P = \varphi: \mathcal{O}(V) &\to \mathcal{O}_P \\ f &\mapsto \langle V, f\rangle. \end{aligned} \tag{4.24}$$

E considere também o homomorfismo $\varphi \circ \alpha: A(V) \to \mathcal{O}_P$. Observe que se $g(P) \neq 0$, isto é, $g \in A(V) \setminus m_P$, então $P \in V \setminus Z(\alpha(g))$ e, consequentemente, $V \setminus Z(g)$ é um aberto não vazio de V. Isso implica que $\varphi \circ \alpha(g)$ é um elemento invertível em $\mathcal{O}_P$. Pela Propriedade Universal da Localização (Proposição 1.56) existe (um único) homomorfismo

$$\begin{aligned} \alpha_P: A(V)_{m_P} &\to \mathcal{O}_P \\ \frac{f}{g} &\mapsto \left\langle U, \frac{f}{g}\right\rangle, \quad \text{onde } U = V \setminus Z(g). \end{aligned} \tag{4.25}$$

Como α e φ são injetores, α_P é injetor. Além disso, para todo $\langle W, h\rangle \in \mathcal{O}_P$ existe $h \in A(V)_{m_P}$ tal que $\alpha_P(h) = \langle W, h\rangle$, isto é, α_P é sobrejetor.

Logo os anéis $A(V)_{m_P}$ e $\mathcal{O}_P$ são isomorfos.

Além disso, temos que todo elemento $A(V)_{m_P} \setminus m_P$ é invertível, logo $A(V)_{m_P}$ é um anel local e seu ideal maximal é m_P. E como $A(V)_{m_P} \simeq \mathcal{O}_P$, segue da Proposição 3.31 que

$\alpha_P(m_P) = \mathrm{m}$ é um ideal maximal e pela definição de Anel Local (Proposição 1.54) que todo ideal próprio de $\mathcal{O}_P$ está contido em m. E pela Proposição 3.33, Proposição 4.51, Teorema 4.47 e Teorema 4.48 temos que

$$dim\, V \overset{4.51}{=} dim\, A(V) \overset{4.48}{=} ht(m_P) + dim\, A(V)/m_P = ht(\mathrm{m}) + dim\, K_P = dim\, \mathcal{O}_P. \quad (4.26)$$

iv) Pela Proposição 1.59 o corpo de frações de $A(V)$ é isomorfo ao corpo de frações de $A(V)_{m_P}$ e pelo item (iii) temos que $\mathcal{O}_P \simeq A(V)_{m_P}$, logo o corpo de frações de $A(V)_{m_P}$ é isomorfo ao corpo de frações de $\mathcal{O}_P$, o qual denotaremos por $\mathcal{K}_P$. Então para mostrar que o corpo de frações de $A(V)$ é isomorfo à $K(V)$, mostraremos que $\mathcal{K}_P$ é isomorfo à $K(V)$.

Considere agora a função injetora $\psi_P = \psi : \mathcal{O}_P \to K(V)$ definida na Proposição 3.34. Temos que se $\langle U, f\rangle \neq \langle V, 0\rangle \in \mathcal{O}_P$ então $\psi(\langle U, f\rangle) \neq \langle V, 0\rangle \in K(V)$. Logo, pela Propriedade Universal da Localização (veja Proposição 1.56), ψ induz o seguinte homomorfismo (as operações estão bem definidas e a prova pode ser consultada na Proposição 3.21):

$$\begin{array}{rccl} \phi_P = \phi : & \mathcal{K}_P & \to & K(V) \\ & \left(\dfrac{\langle U, f\rangle}{\langle W, g\rangle}\right) & \mapsto & \langle U, f\rangle \cdot \langle W, g\rangle^{-1}. \end{array} \quad (4.27)$$

Primeiramente, temos que ϕ é não nula, basta tomar $\phi(\langle V, c\rangle) = \langle V, c\rangle \neq 0$ para c uma função constante não nula. Pela própria definição da função, ϕ é injetora. Temos que ϕ é sobrejetora. E, portanto, $K(V)$ é isomorfo à $\mathcal{K}_p$ (corpo de frações de $\mathcal{O}_P$).

Além disso, temos que $A(V)$ é um domínio finitamente gerado, então pelo Teorema 4.47 segue que

$$dim\, V = dim\, A(V) = tr.deg_K Frac(A(V)) = tr.deg_K K(V), \quad (4.28)$$

o que conclui a prova do item.

i) Pelas definições temos $A(V) \subseteq \mathcal{O}(V)$. E pelo Lema 4.55, Proposição 3.30 e itens (ii) e (iii), temos que

$$A(V) \subseteq \mathcal{O}(V) \subseteq \cap_{P\in V}\mathcal{O}_P \simeq \cap_P A(V)_{m_P}.$$

Logo $A(V) \subseteq \mathcal{O}(V) \subseteq \cap_{P\in V} A(V)_{m_P}$. Portanto $A(V) \simeq \mathcal{O}(V)$.

□

4.3 TOPOLOGIA DE ZARISKI E TOPOLOGIA USUAL

Oscar Zariski foi um matemático nascido no Império Russo, atual Bielorrússia, em 1899, conhecido pelo seu trabalho com as fundações da Geometria Algébrica utilizando métodos algébricos, além disso, Zariski é conhecido por ter introduzido a topologia de Zariski na década de 1950. Exibimos esta topologia na seção 2.5 e, agora, estamos interessados em demonstrar o Teorema 2.27 apresentado anteriormente e em explorar alguns outros resultados relacionados.

Ao escrever "fechado" e "aberto" nesta seção, nos referimos a fechados e abertos na topologia de Zariski, denotamos o fecho de um conjunto X em relação à esta topologia por $\overline{X}^Z$. Quando nos referirmos a fechados e abertos da topologia proveniente da métrica euclidiana em $\mathbb{C}^n$ estará indicado, denotamos o fecho de um conjunto X em relação à esta topologia por $\overline{X}$. No decorrer desta seção chamamos a topologia proveniente da métrica euclidiana em $\mathbb{C}^n$ de "topologia usual".

Considere a caracterização de dimensão dada no Teorema 4.56, isto é $dim\, V = tr.deg_K K(V)$.

Proposição 4.57. *Seja Y uma subvariedade fechada própria de V. Então $dim\, Y < dim\, V$.*

A demonstração da Proposição 4.57 pode ser encontrada em [9], página 40.

Definição 4.58 (Codimensão)**.** *Seja Y uma subvariedade fechada própria de V. Então $dim\, V - dim\, Y$ é dito codimensão de V em Y. Denotamos a codimensão de V em Y por $codim\,(V \text{ em } Y)$.*

Definição 4.59. *Um morfismo $f : X \to Y$ de variedades algébricas afim é dito dominante se a imagem de f é densa em Y, isto é, $Y = \overline{f(X)}^Z$.*

Teorema 4.60. *Seja $f : X \to Y$ um morfismo dominante de variedades algébricas e seja $r = dim\, X - dim\, Y$. Então existe um aberto não vazio $U \subset Y$ tal que*

i) *$U \subset f(X)$;*

ii) *Para todo subconjunto fechado irredutível $W \subset Y$, tal que $W \cap U \neq \varnothing$, e para toda componente Z de $f^{-1}(W)$ tal que $Z \cap f^{-1}(U) \neq \varnothing$,*

$$dim\, Z = dim\, W + r \tag{4.29}$$

ou

$$codim\,(Z \text{ em } X) = codim\,(W \text{ em } Y). \tag{4.30}$$

A demonstração do Teorema 4.60 pode ser encontrada em [9], página 49.

Álgebras boolianas são estruturas algébricas caracterizadas por serem fechadas sobre uniões finitas e complementos, o nome "booliana" é uma homenagem ao matemático inglês George Boole que introduziu este sistema algébrico em 1847. Conjuntos construtíveis (veja Definição 2.26) formam uma álgebra booliana de subconjuntos de X. Na verdade, conjuntos construtíveis são precisamente a álgebra booliana gerada por conjuntos abertos e conjuntos fechados, formando, assim, a menor álgebra booliana contendo todos conjuntos abertos, o nome construtível segue deste fato. A seguir, apresentamos um resultado sobre morfismos e conjuntos construtíveis.

Corolário 4.61 (Chevalley)**.** *Sejam X e Y variedades algébricas e $f : X \to Y$ um morfismo qualquer. Então a imagem de f é um conjunto construtível em Y. De forma geral, f leva conjuntos construtíveis de X em conjuntos construtíveis de Y.*

Demonstração. Dividiremos essa prova em dois casos:

i) Se f é dominante, seja $U \subseteq Y$ um aberto não vazio como no Teorema 4.60. Aplicaremos indução sobre $dim\, Y$. Temos que a imagem de f é um conjunto construtível para $dim\, Y = 0$, pois a imagem será um conjunto finito de pontos e um conjunto finito de pontos é construtível. Suponha que o resultado vale para $dim\, Y < k$, mostraremos que também vale para $dim\, Y = k+1$. Sejam $Z_1, \dots, Z_t$ as componentes de $Y - U$ e sejam $W_{i1}, \dots, W_{is_i}$ as componentes de $f^{-1}(Z_i)$. Considere $g_{ij} : W_{ij} \to Z_i$ a restrição de f. Como $dim\, Z_i < dimY$, pela hipótese de indução temos que $g_{ij}(W_{ij})$ é construtível. E como

$$f(X) = U \cup \bigcup_{i,j} g_{ij}(W_{ij}),$$

$f(X)$ também é construtível.

ii) Se f é não dominante, seja $Z = \overline{f(X)}^Z$. Então $f(X) \subseteq Z = \overline{f(X)}^Z \subseteq Y$ e, portanto, $dimZ < dimY$. Assim, o fato da imagem de f ser construtível em Y segue do caso anterior.

□

A partir deste momento tomamos $K = \mathbb{C}$.

Teorema 4.62. *Seja X uma variedade algébrica e $U \subseteq X$ um aberto não vazio. Então U é denso (em relação à topologia usual) em X, isto é, $\overline{U} = X$.*

Do Teorema 4.62 segue o Teorema 2.27 enunciado na Seção 4.3. A seguir enunciamos este resultado novamente e apresentamos uma demonstração.

Corolário 4.63. *Se $Y \subseteq X$ é um subconjunto construtível de uma variedade algébrica X, então o fecho de Y na topologia de Zariski e o fecho de Y na topologia usual são os mesmos.*

Demonstração. Como a topologia de Zariski é mais fina que a topologia usual, temos que $\overline{Y} \subseteq \overline{Y}^Z$ (veja Proposição 1.67). Como Y é uma união finita de conjuntos localmente fechados, então Y é localmente fechado em X. Assim, pelo Teorema 1.72, temos que Y é aberto em $\overline{Y}^Z$. E pelo Teorema 4.62 segue que $\overline{Y} = \overline{Y}^Z$. □

Considere $f : \mathbb{C}^2 \to \mathbb{C}^2$ uma aplicação polinomial tal que a diferencial df_a possui inversa diferenciável em um ponto $a \in \mathbb{C}^2$. Então o Teorema da Função Inversa implica que existe um aberto (na topologia usual) V que está contido na imagem $f(\mathbb{C}^2)$ e que contém $f(a)$. Como o conjunto $\mathbb{C}^2$ é construtível, $f(\mathbb{C}^2)$ é construtível, pelo Teorema 4.61. Além disso, segue do Teorema 4.63 que $\overline{f(\mathbb{C}^2)} = \overline{f(\mathbb{C}^2)}^Z \supseteq f(\mathbb{C}^2)$. Dessa forma, garantimos que existe um aberto V em $\overline{f(\mathbb{C}^2)}^Z$ e V tem exatamente dimensão 2, mas como $\overline{f(\mathbb{C}^2)}^Z$ é uma variedade algébrica, teremos que a dimensão de $\overline{f(\mathbb{C}^2)}^Z$ também é 2 e, portanto, $\overline{f(\mathbb{C}^2)} = \overline{f(\mathbb{C}^2)}^Z = \mathbb{C}^2$. Isto é, a imagem de f é densa em $\mathbb{C}^2$ tanto na topologia de Zariski como na topologia usual.

Mostrar que a imagem de uma função é densa (em relação a topologia a usual) e encontrar o fecho de um conjunto na topologia de Zariski nem sempre são trabalhos fáceis, mas, em geral, mostrar que um conjunto é construtível e encontrar o fecho (na topologia usual) de um conjunto é uma tarefa mais simples.

Referências Bibliográficas

[1] ATIYAH, M. F. e MACDONALD, I. G.: *Introduction To Commutative Algebra*. Series in Mathematics. Addison-Wesley, 1969.

[2] DIEUDONNE, J. A.: *History of Algebraic Geometry*. Wadsworth Mathematics Series. Springer, 1ª ed., 1985.

[3] FULTON, W.: *Algebraic Curves: An Introduction to Algebraic Geometry*. Redwood City: Addison-Wesley, 1989.

[4] GARCIA, A. e LEQUAIN, Y.: *Elementos de Álgebra*. Rio de Janeiro: IMPA, 4ª ed., 2006.

[5] HALMOS, P. R.: *Naive Set Theory*. Undergraduate texts in mathematics. New York: Springer-Verlag, 1ª ed., 1998.

[6] HARTSHORNE, R.: *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977.

[7] HODGE, W. V. D. e PEDOE, D.: *Methods of Algebraic Geometry*, vol. 2 de *Cambridge Mathematical Library*. New Delhi: Press Syndicate of the University of Cambridge, 1994.

[8] HOFFMAN, K. e KUNZE, R.: *Álgebra Linear*. Rio de Janeiro: LTC, 2ª ed., 1961.

[9] MUMFORD, D.: *The Red Book of Varieties and Schemes*. Lecture Notes in Mathematics 1358. Springer-Berlin Heidelberg, 2ª ed., 1999.

[10] MUNKRES, J. R.: *Topology*. Upper Saddle River: Prentice Hall, 2ª ed., 2000.

[11] POPOV, Y.: *Teoria de dimensão de anéis e variedades*. Monografia, 2017. Universidade de Campinas.

[12] UENO, K.: *Algebraic Geometry 1: From Algebraic Varieties to Schemes*, vol. 185 de *Translations of Mathematical Monographs*. Providence: American Mathematical Society, 1999.

[13] WHITNEY, H.: *Elementary Structure of Real Algebraic Varieties*. Annals of Mathematics, 66(3), 1957.