Universidade Federal de Uberlândia - UFU
Faculdade de Matemática - FAMAT
Coordenação dos Cursos de Bacharelado e Licenciatura em Matemática

Trabalho de Conclusão de Curso

Elementos da Álgebra Comutativa e o teorema dos zeros de Hilbert

Aluno: Christopher Silva Aguiar

Orientador: Cícero Fernandes de Carvalho

Christopher Silva Aguiar

Elementos da Álgebra Comutativa e o teorema dos zeros de Hilbert

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de Bacharel em matemática

Universidade Federal de Uberlândia – UFU

Faculdade de Matemática

Orientador: Prof. Dr. Cícero Fernandes de Carvalho

Uberlândia-MG

2019

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, 11 de Julho de 2019

BANCA EXAMINADORA

Cícero Fernandes de Carvalho

Lúcia Resende Pereira

Victor Gonzalo Lopez Neumann

Uberlândia-MG

2019

Agradecimentos

Agradeço primeiramente a minha família, em especial, ao meu pai, padrinho e falecida avó que me deram muito apoio, tanto moral quanto financeiro, desde o momento que souberam que eu tinha conseguido uma vaga na universidade.

Agradeço também à Universidade Federal de Uberlândia pela minha formação acadêmica de qualidade. Juntamente com os professores que conseguiram me passar o que a matemática é, e o quão bela ela pode ser.

Agradeço ao meu orientador Cícero Fernandes de Carvalho por este projeto e por este ano de Iniciação Científica, no qual eu me dediquei. Obrigado por ser um orientador que compreenda as situações dos alunos, tanto academicamente quanto pessoalmente, e por ter tido paciência comigo no desenvolver deste trabalho.

Não menos importante, gostaria de agradecer ao meu primeiro orientador Germano Abud de Resende pois, mesmo que não tenha contribuído para este projeto diretamente, me ajudou a crescer muito, me ensinando várias coisas, como estudar, fazer apresentações, me ensinando ser a pessoa que sou hoje.

Não poderia deixar de agradecer à minha namorada Kauane por ter me ajudado muito durante estes 4 anos de luta. Muito obrigado por estar ao meu lado, por não me deixar desistir quando queria, por enxugar minhas lágrimas quando necessário, pelos risos e por tudo. Se não fosse por você eu não estaria onde estou também. Te amo muito meu amor!

Aos meus amigos que convivo, vocês tornaram estes 4 anos uma experiência única, tanto os presentes na faculdade, quanto os que me apoiaram de fora dela!

Também ao Programa de Educação Tutorial (PET), no qual contribuiu muito no meu crescimento acadêmico e pessoal, a qual tornou possível este trabalho.

Por fim, agradeço a todos que me ajudaram e apoiaram a chegar neste momento, este trabalho é o fruto dos nossos esforços.

A felicidade não é uma constante matemática,
mas pode alcançar o infinito em um dado momento.

Resumo

O objetivo deste trabalho é a compreensão do Teorema dos Zeros de Hilbert. Este é um resultado famoso na área de Álgebra, em particular, da Geometria Algébrica que relaciona três conceitos: ideais, variedades afins e radicais, no qual constrói uma correspondência entre ideais e o conjunto de zeros dos polinômios (variedades). Para este estudo, será necessário alguns conhecimentos sobre os três tópicos principais abordados e outras mais ferramentas, como os anéis Noetherianos.

Palavras-chaves: Álgebra. Ideais. Variedades.

Abstract

The objective of this work is the understanding of the Hilbert Zero Theorem. This is a famous result in the area of Algebra, in particular, Algebraic Geometry that relates three concepts: ideals, radical and affine varieties, in which it constructs a correspondence between ideals and the set of zeros of polynomials (varieties). For this study, you will need some knowledge about the three main topics covered and other more tools, such as Noetherian rings.

Keywords: Algebra. Ideals. Varieties.

Sumário

Introdução

Variedade afim é um conceito muito importante para a Geometria Algébrica, sendo este o seu principal foco de estudo. Uma variedade pode ser vista como o conjunto das soluções para um sistema de equações polinomiais sobre um corpo, ou seja, dados $p_1, \ldots, p_n \in \mathcal{P} = \mathbb{K}[x_1, \ldots, x_m]$ a variedade definida por estes polinômios é o conjunto:

$$V = \{(a_1, \ldots, a_m) \in \mathbb{K}^m \mid p_i(a_1, \ldots, a_m) = 0, \ \forall\, i = 1, \ldots, n\}.$$

Assim, baseando-se neste conceito, é possível construir uma relação entre álgebra e geometria que nos permite reformular alguns problemas algébricos em geométricos e vice-versa. Uma destas relações será feita neste trabalho, sendo este da seguinte forma:

Dado uma variedade $\mathbf{V} \subseteq \mathbb{K}^n$ definimos o ideal: $\mathbf{I}(V) \subseteq \mathcal{P}$ como sendo:

$$\mathbf{I}(V) = \{p \in \mathcal{P} \mid p(a_1, \ldots, a_k) = 0 \,\forall\, (a_1, \ldots, a_k) \in \mathbf{V}\}.$$

Assim, definimos a "aplicação":

$$\begin{array}{ccc} \text{Variedades Afins} & \longrightarrow & \text{Ideais} \\ \mathbf{V} & \longmapsto & \mathbf{I}(V) \end{array}$$

Agora, de maneira inversa, dado um conjunto $I \subseteq \mathcal{P}$, e considerando a variedade definida por ele, temos a seguinte aplicação:

$$\begin{array}{ccc} \text{Ideais} & \longrightarrow & \text{Variedades Afins} \\ I & \longmapsto & \mathbf{V}(I) \end{array}$$

Observe que não temos nenhuma informação à respeito de I, ou seja, ele é um conjunto qualquer. Porém o Teorema dos Zeros de Hilbert irá garantir que a aplicação acima está bem definida, isto é, I terá que ser um ideal, e mais ainda, será um ideal finitamente gerado.

A finalidade deste trabalho é demonstrar o Teorema dos Zeros de Hilbert para vermos que de fato, a relação abordada acima realmente é verdadeira. E este será feito em 3 etapas, partindo primeiramente de conceitos básicos vistos na graduação. Logo após, começaremos o estudo de variedades afins e radicais, para podermos então estudar o teorema principal.

1 Resultados preliminares

Começaremos este trabalho com algumas definições e resultados básicos envolvendo a estruturas de anéis, com ênfase na teoria de ideais, onde este estudo foi feito à partir da referência [1] .

1.1 Estruturas algébricas

Definição 1.1. Um *anel* é um conjunto R munido com duas operações (soma e produto) tal que as seguintes propriedades são respeitadas:

1. R é um grupo abeliano com a operação soma;
2. É associativo com a multiplicação $(\cdot)$, ou seja, se $a, b, c \in R$, então
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c;$$
3. A propriedade distributiva é satisfeita, isto é, dados $a, b, c \in R$, tem-se:
$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ e } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Se o anel satisfizer a propriedade:

$$\forall a, b \in R \Rightarrow a \cdot b = b \cdot a,$$

então o anel será chamado de comutativo.

Denotaremos por 0 e 1 os elementos unidades com respeito à soma e produto respectivamente. Assim, consideraremos que os anéis estudados neste trabalho são comutativos e contém estes elementos unidades.

Os exemplos mais conhecidos de anéis são os conjuntos: dos números inteiros $\mathbb{Z}$, dos números racionais $\mathbb{Q}$ e o conjunto dos números reais $\mathbb{R}$.

Vejamos agora que, no caso dos reais e dos racionais, eles respeitam também as propriedades de uma outra estrutura, a dos corpos.

Para definir o conceito dos corpos, precisa-se conhecer o que é um inverso multiplicativo ou unidade.

Definição 1.2. Sejam R um anel e $x \in R$. Dizemos que x é uma *unidade* em R se existir um elemento $y \in R$ tal que

$$x \cdot y = 1$$

Definição 1.3. Um conjunto $\mathbb{K}$ é dito ser um *corpo* se este for um anel comutativo e se todos os seus elementos não nulos forem unidades.

Como dito anteriormente, os exemplos mais comuns de corpos são os conjuntos $\mathbb{Q}$ e $\mathbb{R}$. Um outro exemplo de corpo, mas este não trivial, é o corpo de frações de um anel, denotado por $Frac(R)$, que possui a forma:

$$Frac(R) = \{x/y \mid x, y \in R\}.$$

Definição 1.4. Sejam R e S dois anéis. Um *homomorfismo* entre anéis é uma função $\phi : R \to S$ tal que para todos $x, y \in R$ as seguintes relações são satisfeitas:

1. $\phi(x + y) = \phi(x) + \phi(y)$;
2. $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

Observação 1.5. Observe que, usando esta definição, obtemos que $\phi(1)$ pode não precisa ser 1. Mas consideremos agora que um homomorfismo entre anéis leva elemento unidade em elemento unidade.

Assim, podemos listar e nomear alguns tipos de homomorfismo.

Definição 1.6. Seja $\phi : R \to S$ um homomorfismo entre anéis. Então:

i) Se ϕ for injetor então ele é dito *monomorfismo*;

ii) Se ϕ for sobrejetor então ele é dito *epimorfismo*;

iii) Se ϕ for bijetor, isto é, ser injetor e sobrejetor, então ϕ é dito *isomorfismo*;

iv) Se $R = S$ então ϕ é dito *endomorfismo*;

v) Se $R = S$ e ϕ for bijetora então ele é dito *automorfismo*.

Definição 1.7. Uma R-álgebra é um anel R' que está munido com um homomorfismo $\phi : R \longrightarrow R'$ chamada de homomorfismo de estrutura.

Definição 1.8. Seja R um anel. Dizemos que um elemento $a \in R$ é *idempotente* se $a^2 = a$.

Definição 1.9. Sejam R um anel e $e \in R$ um elemento idempotente. Então o conjunto

$$Re = \{xe; x \in R\}$$

é um anel que tem e como elemento identidade, ou seja, $(xe) \cdot e = xe^2 = xe$.

Observemos que Re não é um subanel de R, exceto quando $e = 1$, contudo Re é um ideal.

Lema 1.10. *Seja $e' = 1 - e$. Então e' é idempotente e $e \cdot e' = 0$.*

Demonstração. Temos que

$$(e')^2 = (1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e,$$

o que demonstra que e' é idempotente. Agora, para a segunda igualdade, basta observarmos que:

$$e \cdot e' = e \cdot (1-e) = e - e^2 = e - e = 0.$$

□

Definição 1.11. Chamamos e e e' definidos acima de *idempotentes complementares.*

De maneira inversa, se $e_1, e_2 \in R$ satisfazem $e_1 + e_2 = 1$ e $e_1.e_2 = 0$, então eles são idempotentes complementares, onde para cada i, temos:

$$e_i = e_i \cdot 1 = e_i(e_1 + e_2) = e_i^2,$$

onde $i = 1, 2$.

Denotemos o conjunto de todos os idempotentes por $Idem(R)$.

Exemplo 1.12. Seja $R := R' \times R''$ o produto cartesiano de dois anéis, com as operações feitas coordenada à coordenada. Temos que a identidade aditiva é $(0,0)$ e a identidade multiplicativa é $(1,1)$. Seja $e' = (0,1)$ e $e = (1,0)$. Então estes são idempotentes complementares.

Proposição 1.13. *Seja R um anel, e a, a' idempotentes complementares. Seja $R' = Ra'$ e $R'' = Ra''$. Defina $\phi : R \longrightarrow R' \times R''$ por $\phi(x) = (xa', xa'')$. Então ϕ é um isomorfismo entre anéis. Além disso, $R' \cong R/Ra''$ e $R'' \cong R/Ra'$.*

Demonstração. Vamos definir a sobrejeção $\phi' : R \to R'$ por $\phi'(x) = xe'$. Então ϕ' é um homomorfismo onde $xye' = xye'^2 = (xe')(ye')$. Além disso, $\ker(\phi') = Re''$, já que se $xe' = o$ então $x = x \cdot 1 = xe' + xe'' = xe''$. Assim pelo resultado que será visto mais adiante, vale que $R/Re'' = R'$.

Similarmente, definimos a sobrejeção $\phi'' : R \to R''$ por $\phi''(x) = xe''$. Então ϕ'' é um homomorfismo e $\ker(\phi'') = Re'$. Logo $R/Re' = R''$.

Assim, ϕ é um homomorfismo. Ele é sobrejetivo, já que $(xe', x'e'') = \phi(xe' + x'e'')$. Ele é injetivo pois se $xe' = 0$ e $xe'' = 0$, então $x = xe' + xe'' = 0$. Logo ϕ é um isomorfismo. □

1.2 Teoria de Ideais

Vejamos agora um dos conceitos mais importantes e utilizados como objeto de estudo desse trabalho, os ideais.

Definição 1.14. Seja R um anel. Dizemos que um subconjunto $I \subset R$ é um *ideal* se:

- $0 \in I$
- Sempre que $a, b \in I \Rightarrow a + b \in I$;
- Se $x \in R$ e $a \in I \Rightarrow xa \in I$.

Exemplo 1.15. Sejam R um anel e $A \subseteq R$ um subconjunto. Definimos o conjunto $\langle A \rangle$ formado por todas as combinações lineares dos elementos em A com coeficientes em R. Este conjunto é chamado de gerado por A. Não é difícil provar que $\langle A \rangle$ é um ideal.

Observação 1.16. O conjunto formado no exemplo anterior é o menor ideal que contém A. Além disso, os elementos de A são chamados de *geradores*.

Um resultado direto proveniente da Definição 1.14 é: dado um ideal I então $1 \in I \Leftrightarrow I = R$. Ou seja, se o ideal possuir o elemento unidade da multiplicação então o ideal é na verdade o anel inteiro.

Todo ideal I de R tal que $I \neq R$ é chamado de *ideal próprio*.

Definição 1.17. Diremos que um anel R é um *anel principal* se todos os seus ideais forem principais, isto é, todo ideal $I \subseteq R$ é da forma $\langle x \rangle$, onde $x \in R$.

Definição 1.18. Sejam I, J dois ideais de um anel R. Definimos o seguinte conjunto:

$$(I : J) = \{x \in R \mid (x \cdot b) \in I, \forall\, b \in J.\}$$

Este conjunto é dito condutor de J à I.

Lema 1.19. *Sejam I, J dois ideais de R. O conjunto $(I : J)$ é um ideal.*

Demonstração. Temos que $0 \in (I : J)$, pois $0 \cdot j = 0 \in I$ e isto ocorre para todo $j \in J$. Sejam $x, y \in (I : J)$. Então para todo $j \in J$ temos:

$$(x + y) \cdot j = x \cdot j + y \cdot j$$

Assim $(x \cdot j + y \cdot j) \in J$ pois $x \cdot j \in J$ e $y \cdot j \in J$. E como J é um ideal, segue que $(x + y) \in (I : J)$. Agora, se $a \in R$ e $x \in (I : J)$, temos que, para todo $j \in J$:

$$(a \cdot x) \cdot j = a \cdot (x \cdot j.)$$

Como $(x \cdot j) \in I$ e I é ideal então $a \cdot (x \cdot j) \in I$. Logo $a \cdot x \in (I : J)$. Portanto, $(I : J)$ é um ideal. □

Lema 1.20. *Sejam $\phi : R \to S$ um homomorfismo entre anéis e $J \subseteq S$ um ideal. Então $\phi^{-1}(J)$ é um ideal de R.*

Demonstração. Como $\phi(0) = 0$ temos que $0 \in \phi^{-1}(J)$. Sejam $x, y \in \phi^{-1}(J)$. Então $\phi(x), \phi(y) \in J$. Por hipótese J é um ideal, então $\phi(x)+\phi(y) \in J$. Mas $\phi(x)+\phi(y) = \phi(x+y)$. Logo $x + y \in \phi^{-1}(J)$. Agora sejam $r \in R$ e $x \in \phi^{-1}(J)$. Assim $\phi(x) \cdot \phi(r) \in J$. Por propriedade de homomorfismo, temos $\phi(x) \cdot \phi(r) = \phi(x \cdot r)$. Portanto $x \cdot r \in \phi^{-1}(J)$, o que completa a demonstração. □

Observação 1.21. O ideal $\phi^{-1}(J)$ é dito *contração* de J.

Definição 1.22. Sejam R um anel e $x \in R$. Dizemos que x é um *divisor de zero* se existe $y \in R$ não nulo tal que $x \cdot y = 0$. Caso contrário, ou seja, se $x \cdot y = 0$ implicar que $y = 0$ diremos que x é um *não divisor de zero*.

Observação 1.23. Denotaremos o conjunto de todos os não divisores por S_0.

Definição 1.24. Seja R um anel. Um subanel S é dito *multiplicativo* se:

1. $1 \in S$;
2. Se $x, y \in S$ então $xy \in S$.

Exemplo 1.25. S_0 é um conjunto multiplicativo. De fato, se $x \cdot 1 = 0 \Rightarrow x = 0$, pois $x \cdot 1 = x \; \forall x \in R$. Assim, $1 \in S_0$.

Agora se $x, y \in S_0$ então, para todo $z \in R, z \neq 0$, temos que

$$x \cdot z \neq 0 \text{ e } y \cdot z \neq 0.$$

Logo, se $(xy) \cdot z = 0$ então ou $x \cdot z = 0$ ou $y \cdot z = 0$, contradizendo o fato de pertencerem a S_0.

Definição 1.26. Um ideal P é chamado de ideal *primo* se seu complementar $R - P$ for multiplicativo, ou equivalentemente, se $1 \notin P$ e se $xy \in P$ então ou $x \in P$ ou $y \in P$.

Exemplo 1.27. O conjunto dos números pares $\langle 2 \rangle$ além de ideal é também um ideal primo no anel $\mathbb{Z}$, visto que $1 \notin \langle 2 \rangle$ e que o produto de números ímpares nunca dará um número par.

Definição 1.28. Um *domínio de integridade*, ou simplesmente *domínio*, é um anel R, não nulo, em que seus elementos são todos não divisores de zero, exceto o próprio 0.

Equivalentemente, um anel R é um domínio se $\langle 0 \rangle \subset R$ for primo.

Lema 1.29. *Qualquer subanel de um corpo $\mathbb{K}$ (incluindo o próprio $\mathbb{K}$) é um domínio.*

Demonstração. Ver em [3]. □

Outro resultado direto é que qualquer domínio R é um subanel de um corpo de frações, isto é, um corpo cujos elementos são da forma $\frac{x}{y}$, onde $x, y \in R$ e $y \neq 0$.

Definição 1.30. Sejam R um domínio e $p \in R$ não nulo tal que p não é uma unidade. Dizemos que p é *primo* se, sempre que, $p \mid x \cdot y$ então ou $p \mid x$ ou $p \mid y$.

Lema 1.31. *O ideal $\langle p \rangle$ é primo se, e somente se, p é um elemento primo.*

Demonstração. Ver em [3]. □

Definição 1.32. Sejam R um anel e $x, y \in R$. Dizemos que um elemento $d \in R$ é um *máximo divisor comum* de x e y se tivermos:

- $d \mid x$ e $d \mid y$;
- Se existir um elemento c tal que $c \mid x$ e $c \mid y$ então, temos que $c \mid d$.

Temos algumas observações a notar:

- O máximo divisor comum de x e y é denotado por $\text{mdc}(x, y)$;
- Quando R é um domínio de integridade, então o $\text{mdc}(x, y)$ é único além de unidades.

Definição 1.33. Seja $r \in R$ um elemento de um anel. Se $r = y \cdot z$ implicar que ou y ou z é uma unidade, então diremos que r é *irredutível*.

Definição 1.34. Diremos que um anel R é um *domínio de fatoração única*, denotado por D.F.U se:

1. Qualquer elemento não nulo que não é uma unidade possui fatoração como produto de irredutíveis.
2. Esta fatoração é única além de unidades.

Vejamos agora algumas observações que envolvem os itens (1) e (2) da definição acima.

Observação 1.35. i) Temos que (1) acontece $\Leftrightarrow$ qualquer cadeia de ideais principais $\langle x_1 \rangle \subset \langle x_2 \rangle \subset \ldots$ se estabiliza, ou seja, "possui um fim";

ii) Temos que (2) é válida $\Leftrightarrow$ qualquer elemento irredutível é primo;

iii) Se R é um D.F.U então o $\text{mdc}(x, y)$ sempre existe, para todos $x, y \in R$.

Exemplo 1.36. Os exemplos mais usuais de D.F.U são os inteiros $\mathbb{Z}$ e qualquer anel de polinômios $\mathcal{P} = R[x]$, onde R é um D.F.U.

Lema 1.37. *Sejam $\phi : R \to S$ um homomorfismo, $T \subset S$ um subconjunto. Se T for multiplicativo então $\phi^{-1}(T)$ é multiplicativo. A recíproca é válida se ϕ for sobrejetora.*

Demonstração. Seja $X = \phi^{-1}(T)$. Como T é multiplicativo então $1 \in T$, logo $1 \in X$ pois $\phi(1) = 1$. Se $x, y \in X$, então $\phi(x \cdot y) \in T$. Porém,

$$x, y \in X \Rightarrow \phi(x), \phi(y) \in T \Rightarrow \phi(x) \cdot \phi(y) \in T \Rightarrow \phi(x \cdot y) \in T \Rightarrow x \cdot y \in X,$$

concluindo que X é multiplicativo.

Como ϕ é sobrejetora, então

$$a, b \in T \Rightarrow \exists x, y \in R \ : \ \phi(x) = a, \ \phi(y) = b \Rightarrow x, y \in X$$

$$\Rightarrow x \cdot y \in X \Rightarrow \phi(x \cdot y) \in T \Rightarrow \phi(x) \cdot \phi(y) = a \cdot b \in T.$$

Portanto, T é multiplicativo. □

Agora, vejamos uma consequência direta do lema acima.

Proposição 1.38. *Sejam $\phi : R \to S$ um homomorfismo e $J \subset S$ um ideal. Seja $I = \phi^{-1}(J)$. Assim, se J é um ideal primo então I também é. A recíproca ocorre se ϕ for sobrejetora.*

Demonstração. Se J é um ideal primo então $S - J$ é multiplicativo. Assim pelo Lema 1.37, $\phi^{-1}(S - J)$ é multiplicativo. Porém, $\phi^{-1}(S - J) = R - I$. Logo I é um ideal primo.

A volta é análoga, pois como ϕ é sobrejetora, e novamente pelo Lema 1.37, o complementar dos ideais são multiplicativos. □

Corolário 1.39. *Sejam R um anel e $I \subset R$ um ideal. Então I é um ideal primo se, e somente se, R/I é um domínio.*

Demonstração. Por definição, um conjunto X é um domínio se $\langle 0 \rangle \subset X$ é um ideal primo. Como I é primo, então $\langle 0 \rangle \subset R/I$ é primo. Logo R/I é um domínio. □

Definição 1.40. Seja R um anel. Um ideal $J \subset R$ é dito *maximal* se existir um ideal M tal que $J \subset M \subset R$ então, obrigatoriamente, $J = M$ ou $M = R$.

Proposição 1.41. *Seja R um anel. Então R é um corpo se, e somente se, $\langle 0 \rangle$ é maximal em R*

Demonstração. $\Rightarrow$) Seja I um ideal não nulo de R, ou seja, existe $a \in I$. Como R é um corpo, temos que a é uma unidade. Logo, existe um elemento $a^{-1} \in R$ tal que $1 = a \cdot a^{-1} \in I$, pois I é um ideal. Logo $I = R$ e portanto, $\langle 0 \rangle$ é maximal.

$\Leftarrow$) Suponhamos que $\langle 0 \rangle$ é um ideal maximal. Seja $x \in R$ tal que $x \neq 0$. Logo os ideais gerados por ambos são distintos. Como por hipótese, $\langle 0 \rangle$ é maximal, então $\langle x \rangle = R$. Logo x é uma unidade e como este raciocínio foi para qualquer $x \in R$ não nulo, temos que R é um corpo. □

Corolário 1.42. *Sejam R um anel e $J \subset R$ um ideal. Então J é um ideal maximal se, e somente se, R/I for um corpo.*

Demonstração. Esta demonstração é direta, visto que J é um ideal maximal em R se, e somente se, o ideal $\langle 0 \rangle$ é maximal em R/J se, e somente se, R/J é um corpo. Esta última equivalência se dá pela Proposição 1.41. □

Corolário 1.43. *Em um anel R qualquer ideal maximal I é também um ideal primo.*

Demonstração. Pelo Corolário 1.42, temos que como I é um ideal maximal, então R/I é um corpo. Pelo Lema 1.29 R/I é um domínio de integridade. E logo, pelo Corolário 1.39, I é um ideal primo. □

Definição 1.44. Diremos que dois ideais I, J de um anel R são *comaximais* se todo elemento de R pode ser escrito como a soma de um elemento de I com outro em J, ou seja,

$$\forall\, x \in R,\ \exists a, b\ :\ a \in I,\ b \in J,\ x = a + b.$$

Definição 1.45. Sejam R um anel e dois elementos $x, y \in R$. Diremos que x e y são *estritamente coprimos* se os ideais gerados por eles $\langle x \rangle$ e $\langle y \rangle$ são comaximais.

Definição 1.46. Sejam R um anel e dois elementos $x, y \in R$. Se estes não compartilharem nenhum fator primo em comum, então diremos que x e y são *relativamente primos*.

Definição 1.47. Seja um domínio R. Diremos que R é um *domínio de ideal principal*, denotado por D.I.P, se acontecer de todos os ideais de R forem principais.

Exemplo 1.48. Os D.I.P mais usuais são: o conjunto dos números inteiros $\mathbb{Z}$, qualquer corpo $\mathbb{K}$, o conjunto dos polinômios com coeficiente em um corpo $\mathcal{P}$.

Proposição 1.49. *Todo domínio de ideal principal é um D.F.U.*

Demonstração. Ver em [1]. □

Observação 1.50. Sejam R um D.I.P, I um ideal primo não vazio. Suponhamos que $I = \langle p \rangle$, para algum $p \in R$. Assim, pelo Lema 1.31 p é primo. Logo pela Observação 1.35 (ii), temos que p é irredutível.

Lema 1.51. *Sejam R um D.I.P e $p \in R$ um elemento irredutível. Então o ideal $I = \langle p \rangle$ é maximal.*

Demonstração. Suponha que $I \subsetneq J = \langle x \rangle$, com $x \in R$. Então, $p = x \cdot y$, para alguma não unidade $y \in R$. Como p é irredutível, então x tem que ser uma unidade, implicando que $J = R$. □

Uma conclusão imediata usando o Lema 1.51 é: R/J é um corpo, onde $J = \langle p \rangle$, com $p \in R$ irredutível. Além disso, J é um ideal primo, implicando que p é um elemento primo.

Conclusão: Em um D.I.P qualquer elemento irredutível é primo e qualquer ideal primo não vazio é também um ideal maximal.

Proposição 1.52. *Sejam R um D.I.P e $x, y \in R$ dois elementos. Então x e y são relativamente primos se, e somente se, eles são coprimos.*

Demonstração. Ver em [1]. □

Para a demonstração do próximo teorema, precisaremos do Lema de Zorn ([7]), para isto citaremos o próprio a seguir.

Teorema 1.53 (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 máximo.*

Teorema 1.54. *Em um anel R qualquer ideal próprio $I \subseteq R$ está contido em um ideal J maximal.*

Demonstração. Defina o seguinte conjunto:

$$S = \{\kappa \subseteq R \mid \kappa \text{ é um ideal, onde } 1 \notin \kappa \text{ e } I \subseteq \kappa\}.$$

Observe que este conjunto é não vazio pois $I \in S$ e S é um conjunto parcialmente ordenado com a operação " $\subset$ ". Sejam $\{\kappa_\lambda\}$ um subconjunto totalmente ordenado de S e $\kappa = \cup\kappa_\lambda$. Temos que κ é um ideal e $1 \notin \kappa$. Observe que $\kappa_\lambda \subseteq \kappa$, $\forall\, \lambda$. Assim, κ é um limitante superior para $\{\kappa_\lambda\}$ em S. Assim, como o conjunto tomado κ_λ foi qualquer, segue que todo subconjunto de S possui cota superior. Portanto, pelo Lema de Zorn (Teorema 1.53), S possui um elemento máximo J, ou seja, $I \subseteq J$ e J é maximal, concluido a demonstração. □

Corolário 1.55. *Sejam R um anel e um elemento $x \in R$. Então x é uma unidade se, e somente se, x não é elemento de nenhum ideal maximal.*

Demonstração. A demonstração se conclui usando as seguintes equivalências:

x é uma unidade $\Leftrightarrow \langle x\rangle$ não é um ideal próprio $\Leftrightarrow \langle x\rangle$ não está contido em nenhum ideal maximal (isto se dá negando o Teorema 1.54).

□

1.3 Anéis Residuais

Definição 1.56. Seja $\phi : R \to R'$ um homomorfismo de anéis. Relembremos que o *núcleo* $\ker(\phi)$ é o ideal:

$$\ker(\phi) = \{x \in R \mid \phi(x) = 0.\}$$

Definição 1.57. Sejam $\phi : R \to R'$ um homomorfismo de anéis e I um ideal. Chamamos de *anel de resíduos* ou *anel quociente* o seguinte conjunto:

$$R/I = \{x + I | x \in R\}$$

Assim, com a definição acima, conseguimos construir um homomorfismo quociente:

$$\kappa : R \to R/I,$$

onde $\kappa(x) = x + I$. O elemento $\kappa(x)$ é chamado de resíduo de x. Observemos que κ é sobrejetivo, e κ possui núcleo I. Logo qualquer ideal pode ser um núcleo.

Analisemos a seguinte situação agora:

Dados $\phi : R \to R'$ e I um ideal, temos que existe um homomorfismo sobrejetor $\kappa : R \to R/I$. Agora se $I \subset \ker(\phi)$ então existe um outro homomorfismo de anéis $\psi : R/I \to R'$, com $\psi(\kappa(x)) = \phi(x)$. (Ver [1]).

Observação 1.58. Observem as seguintes implicações:

1. De maneira inversa, se ψ existir então $I \subset \ker(\phi)$, desde que $\kappa(I) = 0$;
2. Podemos ir mais além, onde se ψ existe então ele é único pois κ é sobrejetivo;
3. Agora, por κ ser sobrejetivo, temos que se ψ existir então ψ é sobrejetivo se, e somente se, ϕ for também;
4. Temos que ψ é injetor se, e somente se $\ker(\phi) = I$.

Assim, concluímos que ψ é um isomorfismo se, e somente se, ϕ é sobrejetiva e $ker(\phi) = I$, ou seja, sempre $R/\ker(\phi) \simeq Im(\phi)$.

Definição 1.59. Sejam R um anel, I um ideal e $\kappa : R \longrightarrow R/I$ um homomorfismo quociente. Dado outro ideal J tal que $I \subset J$, definimos o seguinte conjunto:

$$J/I := \{j + I; j \in J\} = \kappa(J).$$

Temos que J/I é um ideal de R/I. Claramente, as operações $J \longmapsto J/I$ e $J' \longmapsto \kappa^{-1}(J')$ são inversos entre si, e estabelecem uma relação bijetora entre o conjunto dos ideais J de R que contem o ideal I e o conjunto de todos os ideais $J' \subseteq R/I$.

Dado um ideal $I \subset J$, formamos a composição de homomorfismos quocientes:

$$\phi : R \to R/I \to (R/I)/(J/I).$$

Claramente ϕ é sobrejetiva e $\ker(\phi) = J$.

1.4 Anéis de Polinômios

Iniciaremos agora o estudo sobre os polinômios de várias variáveis, este anel com coeficientes em um corpo, modificando logo após para um domínio qualquer.

Definição 1.60. Seja um corpo $\mathbb{K}$. O conjunto de polinômios em n variáveis $\mathcal{P} = \mathbb{K}[x_1, \ldots, x_n]$ é a coleção dos elementos da forma:

$$p = \sum_{\alpha} a_\alpha x^\alpha,$$

onde $a_\alpha \in \mathbb{K}$ e $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$.

Exemplo 1.61. Seja $R = \mathbb{R}$, definimos $\mathcal{P} := R[X, Y]$. Onde os elementos de P são da forma $y = \sum aX^{e_1}Y^{e_2}$, como por exemplo: $3X^2Y^1 + 5XY$, $3X^3Y^4$.

Observação 1.62. Observemos que um polinômio é uma soma finita de parcelas compostas pelas variáveis e sua constante. Estas parcelas são chamadas de monômios.

Definição 1.63. Seja R um anel e $\mathcal{P}$ um anel de polinômios em qualquer número de variáveis. Dado $f \in P$ definimos o *grau* de f, denotado por $gr(f)$ como sendo:

1. Se f é um monômio, então $Gr(f)$ é a soma dos expoentes;
2. Se f é qualquer, então $Gr(f)$ é o maior $Gr(m)$, para todo monômio m que compõe f.

Exemplo 1.64. Seja $R = \mathbb{R}$, definimos $\mathcal{P} := R[X, Y]$. Então se $y = X^5Y^3, z = 3$ e $w = 3X^3Y + 4X^3 + 2Y^3$, temos que $Gr(y) = 5 + 3 = 8, Gr(z) = 0$ e $Gr(w) = 3 + 3 = 6$.

Observação 1.65. O termo constante que acompanha a variável de maior grau é chamado *coeficiente líder* do polinômio.

Proposição 1.66. *Sejam R um anel, $\mathcal{P} = R[X]$ um anel de polinômios em uma variável, $a \in R$ e $\pi : \mathcal{P} \longrightarrow R$ um homomorfismo de $R-$álgebra definido por $\pi(X) = a$. Então:*

- $\ker(\pi) = \{F(X) \in \mathcal{P}; F(a) = 0\} = \langle X - a\rangle$;
- $P/\langle X - a\rangle \cong R$(*são isomorfos*).

Demonstração. Mostremos o primeiro item. Seja $G = X - a$. Dado $f \in \mathcal{P}$, vamos mostrar que $F = GH + r$, onde $H \in \mathcal{P}$ e $r \in R$. Por linearidade, vamos assumir que $F = X^n$. Se $n \geq 1$, então $F = (G + a)X^{n-1}$. Logo $F = GH + aX^{n-1}$, com $H = X^{n-1}$. Se $n - 1 \geq 1$, repetimos este processo com F sendo X^{n-1}. Temos que este processo é finito pois $n \in \mathbb{N}$. Então, $\pi(F) = \pi(G)\pi(H) + \pi(r) = r$. Assim, $F \in \ker(\pi) \iff F = GH \Rightarrow F \in \langle X - a\rangle$. Mas $F(a) = \pi(F) = 0$. Agora o segundo item é direto pelo resultado acima obtido pelas observações. □

Dados $p, q \in \mathcal{P}$, notemos que:

$$Gr(F \cdot G) \leq Gr(F) + Gr(G).$$

Temos que a igualdade nem sempre ocorre! De fato seja $R = \mathbb{Z}_6$ e $\mathcal{P} = \mathbb{Z}_2[x]$. Tomemos $p(x) = 2x + 1$ e $q(x) = 3x + 1$. Observe que $Gr(p(x)) = 1$ e $Gr(q(x)) = 1$ em $\mathcal{P}$. Logo:

$$Gr(p(x) \cdot q(x)) = Gr(5x + 1) = 1 < Gr(p(x)) + Gr(q(x)) = 1 + 1 = 2.$$

Definição 1.67. Seja R um domínio. Então definimos o conjunto dos polinômios em qualquer número finito de variáveis como o conjunto $\mathcal{P} = R[x_1, \ldots, x_n]$.

Lema 1.68. *Se R é um domínio então $\mathcal{P}$ é um domínio também.*

Demonstração. A demonstração deste lema é imediata, visto que, como R é um domínio então este não possui divisores de zero. Logo o produto de dois polinômios em $\mathcal{P}$ não é nulo pois o coeficiente líder de um polinômio cujo grau é maior ou igual a 1 é sempre não nulo. E quando for um polinômio constante, temos que estes estão em R e logo não se anulam também. □

Observação 1.69. Quando R for um domínio, então dados dois polinômios $p, q \in \mathcal{P}$, temos a igualdade:

$$Gr(F \cdot G) = Gr(F) + Gr(G).$$

Teorema 1.70. *Sejam R um D.I.P, $\mathcal{P} = R[x]$ o anel de polinômios em uma variável e $J \subset P$ um ideal primo não nulo. Então valem as seguintes afirmações:*

1. *Alguma das alternativas é válida:*

i) $J = \langle p \rangle$, *onde* $p \in \mathcal{P}$ *é um elemento primo;*

ii) J *é um ideal maximal.*

2. *Assumindo que* J *é um ideal maximal, temos que acontece alguma das possibilidades:*

   i) $J = \langle p \rangle$, *onde* $p \in \mathcal{P}$ *é um elemento primo,*

   ii) $J = \langle f, q \rangle$ *onde* $f \in R$ *é um elemento primo,* $\mathcal{P} \cap R = fR = \{f \cdot x \mid x \in R\}$. *Além disso,* $q \in \mathcal{P}$ *é um elemento primo, cuja imagem* $Q \in R/fR[x]$ *é também um primo.*

Demonstração. Primeiramente relembraremos que, pelo Lema 1.55, se R é um D.F.U então $\mathcal{P}$ também é. Se $J = \langle p \rangle$, com $p \in \mathcal{P}$. Então como J é um ideal primo, tem-se que p é primo. Agora vamos assumir que J não seja um ideal principal. Tomemos $p_1 \in J$, não nulo. Como J é primo, então J contém um fator primo t_1 de p_1. Substituamos p_1 por t_1. Como J não é principal então $J \neq \langle p_1 \rangle$. Assim existe um elemento primo $p_2 \in J - \langle p_1 \rangle$. Defina $\mathbb{K} = Frac(R)$. Pelo lema de Gauss, estes primos em $\mathcal{P}$ também são primos em $\mathbb{K}[x]$. Assim, p_1 e p_2 são relativamente primos em $\mathbb{K}[x]$. Assim pela Definição 1.46 e pela Proposição 1.52, tem-se que p_1 e p_2 são relativamente coprimos. Logo existem $q_1, q_2 \in \mathcal{P}$ tal que:

$$\frac{q_1}{c} \cdot p_1 + \frac{q_2}{c} \cdot p_2 = 1 \Rightarrow q_1 \cdot p_1 + q_2 \cdot p_2 = c \in R \cap J.$$

Logo, $R \cap J$ é não vazio. Porém $R \cap J$ é primo e R é um D.I.P. Logo $R \cap J = f \cdot R$, com $f \in R$ primo.

Além disso, $f \cdot R$ é maximal pois f é primo. Seja $L = R/f \cdot R$. Então L é um corpo. Defina $T = J/f \cdot R \subset L[x]$. Então $L[x]/T = \mathcal{P}/J$. Agora, como J é primo, temos que $\mathcal{P}/J$ é um domínio de integridade, implicando que $L[x]/T$ também é. Assim, T é primo e logo maximal. Mas se T é maximal, então J também é, o que demonstra o item (1).

Como $L[x]$ é um D.I.P e que T é um ideal primo, então $T = \langle Q \rangle$, com Q sendo um elemento primo em $L[x]$. Tome $q \in J$, com imagem Q. Então $J = \langle f, q \rangle$, pois $J/\langle f \rangle = \langle Q \rangle$. Suponha que $q = \prod h_i$, onde $h_i \in \mathcal{P}$ são elementos primos. Então $Q = \prod h_i$, com h_i sendo a imagem de q_i em $L[x]$ para todo i. Contudo, Q é primo, assim $\langle Q \rangle = \langle h_j \rangle$, para algun j. Portanto, substitua Q por h_j e q por q_j, concluindo que q é primo.

Finalmente, $J = \langle p \rangle$ e $J = \langle f, q \rangle$ não podem acontecer simultaneamente, pois se acontecesse, teríamos que $p \mid f$, e logo $Gr(p) = 0$, implicando que $\langle p \rangle = \langle f \rangle$ e logo $J = \langle f \rangle$. Assim, $Q = 0$, que é um absurdo! Logo concluímos a demonstração do item (2). □

2 Variedades

Neste capítulo introduziremos um dos conceitos mais importantes deste trabalho, as variedades. Veremos algumas definições e propriedades que elas possuem, iniciando também o estudo sobre as relações que elas possuem com os ideais de polinômios.

Definição 2.1. Sejam $\mathbb{K}$ um corpo, $\mathcal{P}$ o conjunto de polinômios em n variáveis sobre $\mathbb{K}$ e $p_1, \ldots, p_k \in \mathcal{P}$. A *variedade afim* definida por $p_1, \ldots, p_k$ é o conjunto:

$$\mathbf{V}(p_1, \ldots, p_k) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid p_i(a_1, \ldots, a_n) = 0,$$

$$\forall \text{ i} = 1, \ldots, k\}.$$

Por convenção, vamos denotar variedades apenas por $\mathbf{V}$ e $\mathbf{W}$

Exemplo 2.2. Tome $\mathbb{K} = \mathbb{R}$ e $P = \mathbb{R}[x, y]$. Então $\mathbf{V}(x^2 + y^2 - 1) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 = 0\}$, ou seja, este conjunto define a circunferência centrada na origem e de raio 1.

Lema 2.3. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ variedades. Então $\boldsymbol{V} \cup \boldsymbol{W}$ e $\boldsymbol{V} \cap \boldsymbol{W}$ são variedades também.*

Demonstração. Suponhamos que $\mathbf{V} = \mathbf{V}(p_1, \ldots, p_s)$ e $\mathbf{W} = \mathbf{V}(q_1, \ldots, q_t)$, onde $p_1, \ldots, p_s, q_1, \ldots, q_t \in \mathcal{P}$. Para mostrar que os conjuntos $\mathbf{V} \cap \mathbf{W}$ e $\mathbf{V} \cup \mathbf{W}$ são variedades vamos demonstrar as seguintes igualdades:

$$\begin{aligned} \mathbf{V} \cap \mathbf{W} &= \mathbf{V}(p_1, \ldots, p_s, q_1, \ldots, q_t) \\ \mathbf{V} \cup \mathbf{W} &= \mathbf{V}(p_i q_j \,, 1 \leq i \leq t, 1 \leq j \leq s). \end{aligned}$$

A primeira igualdade é trivial. De fato, seja $(a_1, \ldots, a_n) \in \mathbf{V} \cap \mathbf{W}$. Assim, para todo i e para todo j, temos que

$$p_i(a_1, \ldots, a_n) = 0 \text{ e } q_j(a_1, \ldots, a_n) = 0.$$

Isto nos diz que $(a_1, \ldots, a_n) \in \mathbf{V}(p_1, \ldots, p_s, q_1, \ldots, q_t)$ e logo $\mathbf{V} \cap \mathbf{W} \subseteq \mathbf{V}(p_1, \ldots, p_s, q_1, \ldots, q_t)$. Agora suponha que $(a_1, \ldots, a_n) \in \mathbf{V}(p_1, \ldots, p_s, q_1, \ldots, q_t)$. Assim, pela definição de variedade temos que todos os polinômios p_i e q_j se anulam em $(a_1, \ldots, a_n)$. Logo $(a_1, \ldots, a_n) \in \mathbf{V}$ e $(a_1, \ldots, a_n) \in \mathbf{W}$ e assim pertencendo também a $\mathbf{V} \cap \mathbf{W}$, provando a primeira igualdade.

Agora para demonstrarmos a segunda igualdade, suponhamos que $(a_1, \ldots, a_n) \in \mathbf{V}$. Assim,

$$p_i(a_1, \ldots, a_n) = 0 \Rightarrow p_i q_j(a_1, \ldots, a_n) = 0$$

para todo $i = 1, \ldots, t$ e para todo $j = 1, \ldots, s$. Logo $(a_1, \ldots, a_n) \in \mathbf{V}(p_i q_j \, , 1 \leq i \leq t, 1 \leq j \leq s)$, obtendo a primeira inclusão. Suponhamos então que $(a_1, \ldots, a_n) \in \mathbf{V}(p_i q_j \, , 1 \leq i \leq t, 1 \leq j \leq s)$. Temos que, se $(a_1, \ldots, a_n) \in \mathbf{V}$ terminamos a demonstração. Agora, se $(a_1, \ldots, a_n) \notin \mathbf{V}$, temos que existe um índice $i_0 \in \mathbb{N}$ tal que

$$p_{i_0}(a_1, \ldots, a_n) \neq 0.$$

Mas por hipótese, temos que

$$p_{i_0} q_j(a_1, \ldots, a_n) = 0,$$

para todo $j = 1, \ldots, s$. Então $(a_1, \ldots, a_n)$ deve pertencer a $\mathbf{W}$. Assim, $(a_1, \ldots, a_n) \in \mathbf{V} \cup \mathbf{W}$, o que conclui a segunda inclusão e a demonstração. □

2.1 Relacionando Variedades e Ideais

Agora, tendo visto alguns conceitos, começaremos a teoria principal deste tópico, começando com um lema já envolvendo as duas definições estudadas neste trabalho.

Lema 2.4. *Sejam $p_1, \ldots, p_t \in \mathcal{P}$. Então $\boldsymbol{V}(p_1, \ldots, p_t) = \boldsymbol{V}(\langle p_1, \ldots, p_t \rangle)$.*

Demonstração. E claro que se $p_i(a_1, \ldots, a_n) = 0$, $\forall\, i = 1, \ldots, t$. Então qualquer combinação linear formada por todos os p_i se anula em $(a_1, \ldots, a_n)$. Logo $\mathbf{V}(p_1, \ldots, p_t) \subset \mathbf{V}(\langle p_1, \ldots, p_t \rangle)$. Temos que qualquer $(a_1, \ldots, a_n) \in \mathbf{V}(\langle p_1, \ldots, p_t \rangle)$ se anula qualquer polinômio de $\langle p_1, \ldots, p_t \rangle$. Em particular, os próprios $p_i \in \langle p_1, \ldots, p_t \rangle$, para todo i. Logo, $\mathbf{V}(p_1, \ldots, p_t) \supset \mathbf{V}(\langle p_1, \ldots, p_t \rangle)$, concluindo a igualdade almejada. □

Com o lema anterior, temos uma proposição direta com a primeira relação.

Proposição 2.5. *Sejam $p_1, \ldots, p_s$ e $q_1, \ldots, q_t$ duas bases para o mesmo ideal em P, isto é, $\langle p_1, \ldots, p_s \rangle = \langle q_1, \ldots, q_t \rangle$. Então suas variedades são iguais, ou seja, $\boldsymbol{V}(p_1, \ldots, p_s) = \boldsymbol{V}(q_1, \ldots, q_t)$.*

Demonstração. Esta demonstração é direta. Se usarmos o Lema anterior, a nossa hipótese e novamente o Lema, nesta mesma ordem, temos

$$\mathbf{V}(p_1, \ldots, p_s) = \mathbf{V}(\langle p_1, \ldots, p_s \rangle) = \mathbf{V}(\langle q_1, \ldots, q_t \rangle) = \mathbf{V}(q_1, \ldots, q_t),$$

o que conclui a demonstração.

□

Uma dúvida recorrente é se vale a recíproca desta proposição, ou seja, se $\mathbf{V}(p_1, \ldots, p_s) = \mathbf{V}(q_1, \ldots, q_t)$ então $\langle p_1, \ldots, p_s \rangle = \langle q_1, \ldots, q_t \rangle$.

A resposta é NÃO! De fato, seja $p = x,$ e $q = x^2$. Ambos pertencem a $\mathbb{R}[x]$. Temos que $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. Mas $\langle x \rangle \neq \langle x^2 \rangle$ pois, por exemplo, $x \notin \langle x^2 \rangle$.

Sejam $q_1, \ldots, q_t \in P$. Nós temos a variedade afim $\mathbf{V}(q_1, \ldots, q_t) \subseteq \mathbb{K}^n$ definida por estes polinômios. Ou seja, todos os q_i se anulam em todos os pontos de V. Como achar todos os polinômios que se anulam em todos os pontos de V? Esta pergunta será respondida a seguir.

Definição 2.6. Seja $V \subseteq \mathbb{K}^n$ uma variedade afim. Então definimos o seguinte conjunto:

$$\mathbf{I}(V) = \{p \in P \mid p(a_1, \ldots, a_n) = 0, \forall (a_1, \ldots, a_n) \in V.\}$$

Lema 2.7. *Se $\boldsymbol{V} \subseteq \mathbb{K}^n$ for uma variedade então $\boldsymbol{I}(V)$ definido acima é um ideal.*

Demonstração. Mostremos que $\mathbf{I}(V)$ possui as características de um ideal. Sejam $p, q \in \mathbf{I}(V)$, $(a_1, \ldots, a_n) \in V$ e $h \in \mathcal{P}$. Temos que:

1. Claramente $0 \in \mathbf{I}(V)$;
2. Soma:
$$(p + q)(a_1, \ldots, a_n) = p(a_1, \ldots, a_n) + q(a_1, \ldots, a_n) = 0 + 0 = 0;$$
3. Produto:
$$(h \cdot p)(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot p(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0$$

Por tanto $\mathbf{I}(V)$ é um ideal. □

Exemplo 2.8. Seja a variedade $\mathbf{V} = \{(0, 0)\} \subseteq \mathbb{R}^2$. Então $\mathbf{I}(V) = \langle x, y \rangle \subseteq \mathbb{R}[x, y]$ é um ideal.

Lema 2.9. *Sejam $p_1, \ldots, p_t \in P$. Então $\langle p_1, \ldots, p_t \rangle \subseteq \boldsymbol{I}(V(p_1, \ldots, p_t))$*

Demonstração. Seja $p \in \langle p_1, \ldots, p_t \rangle$. Então p é uma combinação linear destes p_i's. Então se, para todo $i = 1, \ldots, t$ os p_i's se anulam nos pontos de $V(p_1, \ldots, p_t)$ temos que p também, se aplicado em todos os pontos $V(p_1, \ldots, p_t)$. Logo, $p \in \mathbf{I}(V(p_1, \ldots, p_t))$, obtendo então a inclusão. □

Observação 2.10. Observe que a inclusão é própria, e não ocorre a inclusão contrária. Por exemplo, temos que $\mathbf{V}(x^2) = 0$, mas $\mathbf{I}(V(0)) = \langle x \rangle$. Então temos que $\langle x^2 \rangle \subsetneq \langle x \rangle$.

Lema 2.11. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ duas variedades em $\mathbb{K}^n$. Então valem as seguintes afirmações:*

i) $\boldsymbol{V} \subseteq \boldsymbol{W} \iff \boldsymbol{I}(W) \subseteq \boldsymbol{I}(V)$;

ii) $\boldsymbol{V = W \iff I(W) = I(V)}$.

Demonstração. Provemos o primeiro item. Primeiramente suponhamos que $\mathbf{V} \subseteq \mathbf{W}$. Então qualquer polinômio que se anula nos pontos de $\mathbf{W}$ também se anulará nos elementos de $\mathbf{V}$. Assim, $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. Por outro lado, suponha que $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. Sabemos que $\mathbf{W}$ é uma variedade definida por um conjunto de polinômios $p_1, \ldots, p_k \in \mathcal{P}$. Assim, $p_1, \ldots, p_k \in \mathbf{I}(W) \subseteq \mathbf{I}(V)$. Portanto, $p_1, \ldots, p_k$ se anulam nos pontos de $\mathbf{V}$ também. Isso mostra que $\mathbf{V} \subseteq \mathbf{W}$.

Para demonstrarmos a segunda afirmação, basta notarmos que se dois conjuntos A e B são iguais, então $A \subseteq B$ e $B \subseteq A$. Logo, basta aplicarmos o item (i) duas vezes para demonstrar o item (ii). □

3 Radicais

Neste capítulo será estudado a definição do Ideal de Jacobson, afim de demonstrar um resultado que caracterisa o conjunto das não unidades de um anel. Veremos também o conceito de radicais, tendo como objetivo principal o Teorema dos Zeros de Hilbert.

Definição 3.1. Seja R um anel. O *Ideal de Jacobson* é um ideal $I \subseteq R$ tal que I é a interseção de todos os ideais maximais em R.

Este ideal é denotado por $J(R)$.

Proposição 3.2. *Sejam R um anel, $I \subseteq R$ um ideal, $x \in R$ um elemento do anel e $u \in R^x$ uma unidade. Então $x \in J(R)$ se, e somente se, $u - xy \in R^x$, $\forall\, y \in R$. Em particular, a soma entre um elemento do radical e uma unidade resulta em uma unidade e $I \subset J(R)$ se $1 - z \in R^x$, $\forall\, z \in I$.*

Demonstração. Vamos assumir que $x \in J(R)$. Dado um ideal maximal $M \in R$, suponha $u - xy \in M$. Se $x \in M$ então $u \in M$, que é uma contradição pelo Corolário 1.55. Logo, novamente pelo Corolário 1.55, $u - xy$ é uma unidade. Em particular, tomando $y = -1$, temos que $u + x \in R^x$.

Agora mostremos a recíproca desta proposição. Para isso iremos demonstrar a contra positiva, ou seja, assuma que $x \notin J(R)$. Então, pelo Corolário 1.55 existe um ideal maximal M tal que $x \notin M$. Então $\langle x \rangle + M = R$. Assim, todo elemento $u \in R$ é escrito da forma $yx + m$, onde $y \in R, m \in M$. Então $u - xy = m \in M$ e, novamente pelo Corolário 1.55, $u - xy$ não é uma unidade. Tome $z \in I$ e defina $b = u^{-1}zy$. Queremos provar que se $1 - z \in R^x$ então $z \in J(R)$. Temos que

$$u - zy = u(1 - b) \in R^x, \text{ se } 1 - b \in R^x.$$

Além disso, $b \in I$ pois $z \in I$, e usando o item demonstrado acima, temos que $z \in J(R)$, provando o último item do teorema. □

Corolário 3.3. *Sejam R um anel, $I \subset R$ um ideal e $\phi : R \to R/I$ um homomorfismo quociente. Assuma que $I \subset J(R)$. Então o homomorfismo $Idem(\phi) : IdemR \to Idem(R/I)$ é injetor.*

Demonstração. Sejam $e, e' \in Idem(R)$ com $\phi(e) = \phi(e')$. Defina $x = e - e'$. Então:

$$x^3 = e^3 - 3e^2 \cdot e' + 3e \cdot (e')^2 - (e')^3 = e - e' = x.$$

Logo

$$x^3 = x \Leftrightarrow x \cdot (1 - x^2) = 0.$$

Observe que como $x = e - e'$ temos que

$$\phi(x) = \phi(e) - \phi(e') = 0 \Rightarrow x \in I.$$

Contudo, $I \subset J(R)$, concluindo que $1 - x^2$ é uma unidade pela Proposição 3.2. Portanto $x = 0 \Rightarrow e = e'$, implicando na injetividade de $Idem(\phi)$ □

Definição 3.4. Um anel R é chamado *local* se ele possuir apenas 1 ideal maximal. E será chamado *semilocal* se este possuir uma quantidade finita de ideais maximais.

Definição 3.5. Seja R um anel local. Chamaremos de *corpo residual* o corpo R/I, onde I é o único ideal maximal de R.

Lema 3.6 (Critério das não unidades)**.** *Seja R um anel e $B \subset R$ o conjunto das não unidades de R. Então R é local se, e somente se, B for um ideal e logo, B é o ideal maximal de R.*

Demonstração. Assumindo que R é local, temos que ele possui apenas um ideal maximal. Denotemos este ideal por M. Logo $R - M = R - B$, pois pelo Corolário 1.55, todos os elementos de $R - B$ são unidades, que não pertencem a nenhum ideal maximal. Portanto, $M = B$, concluindo que B é um ideal e maximal.

De maneira inversa, temos que qualquer ideal próprio P está contido em B pois este só possui não unidades. Logo, se B é um ideal, então pelo Teorema 1.54 B é maximal e ele é único. □

Proposição 3.7. *Sejam R um anel, $S \subset R$ um subconjunto multiplicativo e $I \subset R$ um ideal tal que $I \cap S = \emptyset$. Definamos o seguinte conjunto:*

$$\mathcal{S} = \{\beta \subset R \mid I \subset \beta \text{ e } \beta \cap S = \emptyset.\}$$

Então $\mathcal{S}$ possui um elemento maximal B que, será também um ideal primo.

Demonstração. Primeiramente observemos que $\mathcal{S}$ é não vazio pois $I \subset \mathcal{S}$. Agora, temos que $\mathcal{S}$ é parcialmente ordenado usando a relação " $\subset$ ". Dado um conjunto totalmente ordenado $\{B_i\}$ de $\mathcal{S}$ seja $B = \bigcup B_i$. Então temos que B é um limite superior para $\{B_i\}$ em $\mathcal{S}$. Logo, pelo Lema de Zorn (1.53) $\mathcal{S}$ possui um elemento maximal P. Provemos agora que este é um ideal primo. Sejam $x, y \in R - P$. Então os conjuntos:

$$P + \langle x \rangle = \{p + ax \mid p \in P,\ a \in R\} \text{ e } P + \langle y \rangle = \{q + by \mid p \in P,\ b \in R\}$$

são estritamente maiores que o conjunto P. Logo existem $c, d \in R$ e $r, s \in P$ tais que

$$z = r + cx \in S \text{ e } t = s + dy \in S$$

pois $S \cap P = \emptyset$. Logo

$$t \cdot z \in S \Rightarrow sr + rdy + cxs + cxdy \in S.$$

Contudo, $sr + rdy + cxs \in P$. Portanto

$$cxdy \notin P \Rightarrow xy \notin P,$$

concluindo o que queríamos, a primalidade do ideal P. □

Definição 3.8. Seja $S \subset R$ um subconjunto multiplicativo de um anel. Diremos que S é *saturado* se, dados $a, b \in R$ onde $a \cdot b \in S$ então $a, b \in S$ obrigatoriamente.

Exemplo 3.9. Os conjuntos das unidades de um anel R^x e o conjunto dos não divisores de zero S_0 são subconjuntos multiplicativos e saturados. De fato, provemos primeiramente que R^x é saturado. Sejam $a, b \in R$ onde $a \cdot b \in R^x$. Então existe um elemento $z \in \mathbb{R}$ tal que:

$$(ab) \cdot z = 1 \Rightarrow a \cdot (bz) = 1.$$

Portanto, $a \in R^x$. Pelo mesmo raciocínio se mostra que $b \in R^x$ também, concluindo que R^x é multiplicativo saturado.

Agora mostremos o mesmo em S_0. Seja $z = (ab) \in S_0$. Suponha por absurdo que $a \notin S_0$. Então existe $a' \in R$ tal que $a' \neq 0$ e $a \cdot a' = 0$. Assim,

$$0 = (a' \cdot (a)) \cdot b = a' \cdot (ab) = a' \cdot z,$$

que é um absurdo! Portanto $a \in S_0$. Analogamente se mostra que $b \in S_0$.

Lema 3.10. *Dados R, R' dois anéis e $\phi : R \to R'$ um homomorfismo, temos que se um subconjunto $T \subset R'$ é saturado então $\phi^{-1}(T)$ é saturado também. A recíproca só é verdadeira se ϕ for sobrejetor.*

Demonstração. Pelo Lema 1.37 temos que $\phi^{-1}(T)$ é multiplicativo. Mostremos que este é saturado. Sejam $a, b \in R$ tais que $a \cdot b \in \phi^{-1}(T)$. Por definição temos que $\phi(a \cdot b) = \phi(a) \cdot \phi(b) \in T$. Como T é saturado, temos que $\phi(a) \in T$ e $\phi(b) \in T$. E portanto, $a, b \in \phi^{-1}(T)$. Para demonstrar a volta, usa-se um raciocínio análogo, utilizando a recíproca do Lema 1.37. □

Lema 3.11. *Sejam R um anel, $I \subset R$ um subconjunto que respeita as operações de soma e multiplicação, e $P_1, \ldots, P_n$ ideais tal que para todo índice $i \geq 3$, P_i é um ideal primo. Se $I \not\subset P_j$, para todo $j = 1, \ldots n$ então existe um elemento $a \in I$ tal que $a \notin P_j$ para todo j, ou seja, se $I \subset \bigcup_{j=1}^{n} P_j$ então $I \subset P_j$ para algum $j = 1, \ldots, n$.*

Demonstração. Esta demonstração é por indução em n.

Se $n = 1$, a inclusão é trivial, logo provaremos para $n \geq 2$.

Se $n = 2$, segue que, como $I \not\subset P_1$ e $I \not\subset P_2$, então existem $x_1, x_2 \in I$ tais que $x_1 \notin P_2$ e $x_2 \notin P_1$. Vamos assumir que $x_i \in P_i$, com $i = 1, 2$, pois caso contrário, acabamos. Temos que $x_1 + x_2 \notin P_1$ e $x_1 + x_2 \notin P_2$, caso não aconteça, como P_i é um ideal, teríamos que $x_i \in P_j$, para $j \neq i$, contradizendo o fato assumido acima, provando este caso.

Agora, supondo $n \geq 3$ temos que, se $x_i \in P_i$ e $x_i \notin P_j$ para $i \neq j$, então $(x_1 \cdot \ldots \cdot x_{n-1}) + x_n \notin P_j$, para todo $j = 1, \ldots, n$. Se não teríamos dois casos:

1. Se $j = n$, teríamos que $(x_1 \cdot \ldots \cdot x_{n-1}) + x_n \in P_n$. Como P_n é um ideal primo, implicaria que $x_j \in P_n$ para algum $j < n$ gerando um absurdo;

2. Se $j < n$, teríamos que $(x_1 \cdot \ldots \cdot x_{n-1}) + x_n \in P_j$, implicando que $x_n \in P_j$ gerando outro absurdo.

Logo, $(x_1 \cdot \ldots \cdot x_{n-1}) + x_n \notin P_j$, para todo j, demonstrando o lema. □

Definição 3.12. Sejam A um anel e $I \subseteq A$ um subconjunto. Definimos o radical $\sqrt{I}$ como sendo o conjunto:

$$\sqrt{I} = \{x \in A \mid x^n \in I, \text{ para algum } n \in \mathbb{N}\}$$

Observação 3.13. Sejam I, J dois subconjuntos de um anel R. Então valem as seguintes propriedades de radical:

1. $I \subset \sqrt{I}$;
2. $\sqrt{\sqrt{I}} = \sqrt{I}$;
3. Se $J \subset I$ então $\sqrt{J} \subset \sqrt{I}$.

Definição 3.14. Se I é um ideal de um anel R e $I = \sqrt{I}$ diremos que I é um *radical*.

Chamaremos também o radical $\sqrt{\langle 0 \rangle}$ de *nilradical*.

Definição 3.15. Dizemos que $a \in R$ é um elemento *nilpotente* se $a \in \sqrt{\langle 0 \rangle}$, ou seja, $a^n = 0$, para algum $n \geq 1$.

Também chamaremos um ideal I de nilpotente se todos os seus elementos forem nilpotentes.

Lema 3.16. *Para todo anel R vale que $\sqrt{J(R)} = J(R)$, onde $J(R)$ é como segue a Definição 3.1.*

Demonstração. De fato, como visto pela definição, $J(R) \subset \sqrt{J(R)}$. Por outro lado, se $x \in \sqrt{J(R)}$ então $x^n \in J(R)$ e, portanto, $x^n \in M$, com M sendo um ideal maximal. Pelo Corolário 1.43, segue que M é primo também. Portanto $x \in M$, e logo $x \in J(R)$, provando a igualdade. □

Uma implicação direta que provém destas definições é que o nilradical de um anel está contido na interseção de todos os ideais maximais deste, ou seja, se $x \in \sqrt{\langle 0 \rangle}$ então $x \in J(R)$. Este fato é demonstrado a partir de que $\langle 0 \rangle \subset J(R)$ e utilizando o item 3 da Observação 3.13.

Definição 3.17. Diremos que um anel R é *reduzido* se seus elementos nilpotentes são os que pertencem ao ideal $\langle 0 \rangle$, ou seja, se R não possui elementos nilpotentes não nulos.

Teorema 3.18 (Schein nullstellensatz)**.** *Sejam R um anel e I um ideal. Então:*

$$\sqrt{I} = \bigcap_{I \subset P} P$$

onde P são todos os ideais primos que contém I. (Por convenção, consideraremos a interceção nula como sendo o anel inteiro.)

Demonstração. Vamos provar a igualdade de conjuntos da forma usual ($A = B \iff A \subset B$ e $B \subset A$). Provemos primeiramente que $\sqrt{I} \supset \bigcap_{I \subset P} P$. Pela contrapositiva, tome um elemento $a \notin \sqrt{I}$. Temos que o conjunto

$$N = \{1, a, a^2, a^3, \ldots\}$$

é multiplicativo e sua intercessão com o ideal I é vazia. Assim pela Proposição 3.7, existe um ideal primo B que contém o ideal I e que $a \notin B$. Assim $a \notin \bigcap_{I \subset P} P$, provando a inclusão pretendida.

Por outro lado, tome $x \in \sqrt{I}$. Assim, $x^n \in I$ para algum $n \geq 1$. Então $x^n \in P$, pois $I \subset P$. Então, por P ser primo, temos que $x \in P$ e logo $x \in \bigcap_{I \subset P} P$, demonstrando a inclusão contrária e também o teorema. □

Proposição 3.19. *Se I é um ideal de R então $\sqrt{I}$ é um ideal também.*

Demonstração. Tome $x, y \in \sqrt{I}$. Então $x^n, y^m \in I$, para algum $m, n \in \mathbb{N}$. Assim, pelo Binômio de Newton, conseguimos expandir a expressão $(x+y)^{m+n-1}$ da seguinte forma:

$$(x+y)^{m+n-1} = \sum_{i+j=m+n-1} \binom{n+m-1}{j} x^i y^j.$$

Observe que esta soma pertence a I pois, em cada parcela da soma, x^i ou y^j estão em I, para $n \leq i \leq m+n-1$ e $m \leq j \leq m+n-1$, mas não simultaneamente, pois $i + j = m + n - 1$, logo se $j = m$ então $y^j \in I$. Neste caso, $i = n - 1$, ou seja, $x^i \notin I$. Agora, sejam $x \in \sqrt{I}$ e $y \in R$. Queremos provar que $xy \in \sqrt{I}$. Observe que:

1. Como $x \in \sqrt{I}$ então $x^n \in I$, para algum $n \in \mathbb{N}$;

2. Temos que:
$$(xy)^n = x^n y^n \in I,$$
pois $y^n \in R$ e I é um ideal.

Logo $\sqrt{I}$ é um ideal. □

Observação 3.20. Uma demonstração alternativa para a proposição anterior seria utilizando o Teorema 3.18.

4 Teoremas de Hilbert

Neste capítulo veremos o principal resultado deste trabalho, Teorema dos Zeros de Hilbert. Para isso, vejamos alguns conceitos adicionais que nos ajudarão a demonstrar este resultado importante, como o famoso Teorema das Bases de Hilbert.

Definição 4.1. Diremos que um anel R é um *anel Noetheriano* se qualquer ideal $I \subseteq R$ é finitamente gerado.

Exemplo 4.2. Seja $\mathbb{K}$ um corpo. Temos que qualquer ideal $I \subseteq \mathbb{K}$ é finitamente gerado pois todo ideal de um corpo (ou o corpo inteiro) é, na verdade, o próprio corpo, e logo, finitamente gerado pelo elemento 1 (exceto quando $\mathbb{K} = \{0\}$, que é gerado pelo 0). Assim, qualquer corpo é um anel Noetheriano.

Um outro exemplo de anel Noetheriano, devido ao teorema que demonstraremos à seguir, é $R[x_1, \ldots, x_n]$, quando R também for Noetheriano.

Teorema 4.3 (Teorema das Bases de Hilbert)**.** *Se R é um anel Noetheriano então $R[x_1, \ldots, x_n]$ é Noetheriano também.*

Demonstração. Observemos inicialmente que

$$R[x_1, \ldots, x_n] \cong R[x_1, \ldots, x_{n-1}][x_n].$$

Assim, se demonstrarmos que $R[x]$ é Noetheriano, concluiremos a demonstração deste teorema, pois podemos considerar $R[x_1, x_2] = R[x_1][x_2]$ e aplicar novamente o teorema, pois $R[x_1]$ será Noetheriano.

Então demonstremos que $R[x]$ é Noetheriano. Seja $I \subseteq R[x]$ um ideal. Queremos achar um conjunto finito de geradores para I. Defina J como sendo o conjunto de todos os coeficientes líderes dos polinômios pertencentes a I. Como I é um ideal, segue que $J \subseteq R$ é um ideal também. Assim, por R ser Noetheriano por hipótese, temos que:

$$J = \langle a_1, \ldots, a_t \rangle,$$

onde $a_1, \ldots, a_t \in R$. Como $a_j \in J$ então existe $P_j \in I$ tal que a_j é o coeficiente líder de P_j. Então sejam $P_1, \ldots, P_t \in I$ os polinômios cujos coeficientes líderes são os a_i definidos acima. Agora tome $N \in \mathbb{N}$ tal que:

$$N \geq gr(P_i),\ \forall\, i = 1, \ldots, t.$$

Depois, para cada $m \in \mathbb{N}$, onde $m \leq N$ defina J_m como sendo o conjunto de todos os coeficientes líderes dos polinômios de I com grau menor ou igual a m. Feito isso, defina

o conjunto:

$$Z = \{P \in I \mid \ gr(P) \leq m \text{ e os coeficientes líderes destes polinômios geram } J_m.\}$$

Temos que Z é finito pois J_m é gerado por uma quantidade finita de elementos.

Por fim, defina

$$I' = \langle P_1, \ldots, P_t, Z \rangle.$$

Iremos mostrar que $I = I'$ e concluir que I é gerado por uma quantidade finita de geradores. Observe que construímos I' apenas com polinômios de I. Logo I' não pode possuir mais elementos que I.

Assim, suponha por absurdo que I seja estritamente maior que I'. Assim, existe um polinômio $G \in R$, cujo grau seja o menor possível, tal que $G \in I$ mas $G \notin I'$. Assim temos dois casos:

1. Se $gr(G) > N$, então existem $Q_j \in R$ tais que o polinômio $Y = \sum Q_i P_i$ possui o mesmo grau e o mesmo coeficiente líder que G. Assim, como $gr(G - Y) < gr(G)$ e tomamos G com o menor grau possível, temos que $G - Y \in I'$ e logo $G \in I'$, gerando o primeiro absurdo.

2. Se $gr(G) = m \leq N$, então usaremos o mesmo raciocínio do item acima, diminuindo o grau de G por uma combinação linear dos elementos de Z e concluindo que $G \in I'$, gerando o segundo absurdo.

Portanto, $I = I'$, o que demonstra o teorema. □

Exemplo 4.4. Se $\mathbb{K}$ é um corpo, então pelo teorema anterior $\mathcal{P} = \mathbb{K}[x_1, \ldots, x_m]$ é um anel Noetheriano.

Começaremos agora um estudo breve sobre extensão de corpos pois necessitamos de um resultado muito importante para a demonstração do Teorema principal deste trabalho.

Definição 4.5. Seja $\mathbb{K}$ um corpo. Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$ quando $\mathbb{K} \subset \mathbb{L}$ e as operações que tornam $\mathbb{K}$ e $\mathbb{L}$ corpos são as mesmas quando aplicadas a elementos de $\mathbb{K}$.

Exemplo 4.6. Temos que $\mathbb{C}$ é uma extensão de $\mathbb{R}$.

Definição 4.7. Sejam $\mathbb{L} \supset \mathbb{K}$ uma extensão de corpo e um elemento $a \in \mathbb{L}$. Definimos o conjunto $\mathbb{K}(a)$ como sendo a interseção de todos os subcorpos de $\mathbb{L}$ que contenham $\mathbb{K}$ e a.

O próximo resultado nós não demonstraremos neste trabalho porém a demonstração está presente na referência [3].

Lema 4.8 (Forma Explícita de $\mathbb{K}(a)$)**.** *Temos que $\mathbb{K}(a)$ é um subcorpo de $\mathbb{L}$. Além disso temos que*

$$\mathbb{K}(a) = \left\{ \frac{P(a)}{Q(a)} \ : \ P(x), Q(x) \in \mathbb{K}[x] \ e \ Q(a) \neq 0 \right\}$$

Definição 4.9. Dizemos que um elemento $a \in \mathbb{K}$ é algébrico sobre um corpo $\mathbb{F}$ se existir coeficientes $b_0, \ldots, b_n \in F$ tais que

$$b_0 + b_1 a + \ldots + b_n a^n = 0,$$

ou seja, existe um polinômio $q(x) \in F[x] \backslash 0$ tal que $q(a) = 0$. Caso a não seja algébrico, diremos que ele é um elemento transcendente.

Definição 4.10. Uma extensão de corpos $\mathbb{L} \supset \mathbb{K}$ é dita ser uma extensão algébrica se todos os elementos de $\mathbb{L}$ são algébricos sobre $\mathbb{K}$. Caso contrário será dito que esta extensão é transcendental.

Definição 4.11. Um subconjunto $A \subset \mathbb{L}$ é chamado de algebricamente independente sobre $\mathbb{K}$ se não existe qualquer relação polinomial não-trivial com coeficientes em $\mathbb{K}$ entre os elementos de A.

A maior cardinalidade de um conjunto algebricamente independente é chamada de grau de transcendência de $\mathbb{L}$ sobre $\mathbb{K}$. Pode-se mostrar que, se $\mathbb{L} \,|\, \mathbb{K}$ é extensão transcendente então existe um conjunto algebricamente independente $A \subset \mathbb{L}$ sobre $\mathbb{K}$ tal que $\mathbb{L}$ é algébrico sobre $\mathbb{K}(A)$. Um tal conjunto é chamado de base de transcendência, temos que duas bases de transcendência têm a mesma cardinalidade (v. [4, Thm. 1.1, pag. 356]).

Enfim, vamos agora ao teorema!

Teorema 4.12. *Sejam $\mathbb{K}$ um corpo infinito e suponha que $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$ é corpo. Então $\mathbb{L}$ é algébrico sobre $\mathbb{K}$.*

Demonstração. A demonstração será por absurdo. Suporemos que $\mathbb{L}$ é transcendental sobre $\mathbb{K}$ e vamos concluir que ele não pode ser finitamente gerado, ou seja, sempre existirá um elemento de $\mathbb{L}$ que não está em $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$.

Inicialmente suponha que $\mathbb{L}$ possui grau de transcendência 1 sobre $\mathbb{K}$. Logo vai existir um subcorpo $\mathbb{K}(x)$ tal que $x \in \mathbb{L}$ é transcendente sobre $\mathbb{K}$ e $\mathbb{L}$ é algébrico sobre $\mathbb{K}(x)$. Assim α_i é algébrico sobre $\mathbb{K}(x)$ para todo $i = 1, \ldots, n$ e logo $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$ possui dimensão finita quando visto como um $\mathbb{K}(x)$-espaço vetorial. Seja $\{e_1, \ldots, e_m\} \subset \mathbb{L}$ uma base para $\mathbb{L}$, dados $i, j \in \{1, \ldots, n\}$ temos

$$e_i \cdot e_j = \sum_k \frac{p_{ijk}(x)}{q_{ijk}(x)} e_k,$$

onde $p_{ijk}(x), q_{ijk}(x) \in \mathbb{K}[x]$, para todos i, j e k.

Queremos mostrar que para quaisquer $\beta_1, \ldots, \beta_l$, temos que $\mathbb{K}[\beta_1, \ldots, \beta_l]$ será estritamente menor que $\mathbb{L}$. Como estes elementos estão em $\mathbb{L}$, vamos escreve-los em relação à sua base, ou seja,

$$\beta_i = \sum_j \frac{r_{ij}(x)}{s_{ij}(x)} e_j,$$

com $r_{ij}, s_{ij} \in \mathbb{K}[x]$. Das expressões para os β_i's acima vemos que um produto $\mathcal{P}$ desses elementos pode ser escrito, inicialmente, como um produtos dos e_i's com coeficientes em $\mathbb{K}(x)$, sendo que o denominador desses coeficientes é um produto de polinômios s_{ij}. Escrevendo agora o produto dos e_i's como combinação linear de $\{e_1, \ldots, e_n\}$ com coeficientes em $\mathbb{K}(x)$, vemos que o produto $\mathcal{P}$ acima considerado pode ser escrito como uma combinação linear de $\{e_1, \ldots, e_n\}$ com coeficientes em $\mathbb{K}(x)$, de modo que os denominadores dos coeficientes são produtos de polinômios s_{ij} vezes produtos de polinômios q_{ijk}. É claro que qualquer elemento em $\mathbb{K}[\beta_1, \ldots, \beta_l]$ também se escreve como uma tal combinação linear, pois é uma combinação de produtos dos β_i's com coeficientes em $\mathbb{K}$. Como $\mathbb{K}$ é um corpo infinito, existem infinitos polinômios irredutíveis da forma $x - c$ com $c \in \mathbb{K}$. Assim, existe $a \in \mathbb{K}$ tal que $x - a$ não é fator irredutível de nenhum s_{ij} e de nenhum q_{ijk}. Nesse caso, claramente $\dfrac{1}{x-a} e_1$ não pertence a $\mathbb{K}[\beta_1, \ldots, \beta_l]$. Isso mostra que $\mathbb{L}$ não pode ser finitamente gerado como $\mathbb{K}$-álgebra, contrariando a hipótese.

Agora suponha que $\mathbb{L}$ possua grau de transcendência sobre $\mathbb{K}$ igual a $\ell > 1$. Então existem $x_1, \ldots, x_l \in \mathbb{L}$, transcendentes sobre $\mathbb{K}$ e tais que a extensão $\mathbb{L} \,|\, \mathbb{K}(x_1, \ldots, x_l)$ é algébrica. Observe também que a extensão $\mathbb{L} \,|\, \mathbb{K}(x_1, \ldots, x_{l-1})$ tem grau de transcendência igual a 1, então podemos aplicar o que foi feito acima e concluir que $\mathbb{L}$ não é uma $\mathbb{K}(x_1, \ldots, x_{l-1})$-álgebra finitamente gerada. Como consequência, temos que $\mathbb{L}$ não é uma $\mathbb{K}$-álgebra finitamente gerada. Isso conclui a prova do teorema. □

Definição 4.13. Um corpo $\mathbb{K}$ é dito algebricamente fechado se todo polinômio $p \in \mathbb{K}[x]$ possuir pelo menos uma raiz em K.

Para demonstrar o Teorema dos Zeros de Hilbert, precisaremos de dois lemas que veremos a seguir:

Lema 4.14. *Para qualquer ideal $J \subseteq \mathcal{P}$, valem as seguintes afirmações:*

i) $\boldsymbol{V}(J) = \boldsymbol{V}(\sqrt{J})$;

ii) $\sqrt{J} \subseteq \boldsymbol{I}(V(J))$

Demonstração. i) Como $J \subseteq \sqrt{J}$ temos que $\mathbf{V}(J) \supseteq \mathbf{V}(\sqrt{J})$. Seja $(a_1, \ldots, a_n) \in V(J)$ e seja $P \in \sqrt{J}$, então $P^m \in J$ para algum inteiro positivo m. Assim $P^m(a_1, \ldots, a_n) = 0$ e logo $P(a_1, \ldots, a_n) = 0$, donde $(a_1, \ldots, a_n) \in \mathbf{V}(\sqrt{J})$.
ii) Seja $P \in \sqrt{J}$, então $P^m \in J$ para algum inteiro positivo m. Seja $(a_1, \ldots, a_n) \in V(J)$, como acima temos $P(a_1, \ldots, a_n) = 0$ e logo $P \in \mathbf{I}(V(J))$. □

Lema 4.15. *Qualquer ideal maximal de* $\mathcal{P} = \mathbb{K}[x_1, \ldots, x_n]$ *é da forma* $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, *onde* $a_1, \ldots, a_n \in \mathbb{K}$

Demonstração. Seja $J \subset \mathcal{P}$ um ideal maximal. Vamos definir $\mathcal{L} = \mathcal{P}/J$. Temos pelo Corolário 1.42 que $\mathcal{L}$ é um corpo. Temos também que $\mathcal{L}$ é finitamente gerado com coeficientes em $\mathbb{K}$, ou seja, $\mathcal{L} = \mathbb{K}[\overline{x_1}, \ldots, \overline{x_n}]$. Assim, pelo Teorema 4.12, temos que $\mathcal{L}$ é algébrico sobre $\mathbb{K}$ e portanto, como $\mathbb{K}$ é algebricamente fechado, concluímos que $\mathcal{L} = \mathbb{K}$. Então, para cada x_i, existe $a_i \in \mathbb{K}$ tal que a_i é o resíduo de x_i, ou seja, $x_i - a_i \in J$ e isto ocorre para todo $i = 1, \ldots, n$. Assim, temos que $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset J$ e como $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ é um ideal maximal, temos que $J = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. E como este raciocínio foi feito para um ideal maximal qualquer, o resultado segue. □

Teorema 4.16 (Zeros de Hilbert)**.** *Suponha que o corpo* $\mathbb{K}$ *seja algebricamente fechado. Então valem as seguintes propriedades:*

I) Se I *é um ideal de* $\mathcal{P}$ *tal que* $I \neq \langle 1 \rangle$ *então* $V(I)$ *é não-vazio*

II) Para qualquer ideal $Z \subseteq \mathcal{P}$, *tem-se que* $\boldsymbol{I}(V(Z)) = \sqrt{Z}$

Demonstração. Demonstremos cada item separadamente.

I) Vamos considerar que I é um ideal maximal pois, usando o Teorema (1.51), existe um ideal maximal J tal que $I \subseteq J$. Como $\mathbf{V}(J) \subseteq \mathbf{V}(I)$, então basta mostrarmos que $\mathbf{V}(J) \neq \emptyset$. Pelo Lema 4.15, segue que $J = \langle x_1 - b_1, \ldots, x_n - b_n \rangle$ e portanto $\mathbf{V}(J) = \{(b_1, \ldots, b_n)\} \neq \emptyset$.

II) Pelo Teorema 4.3 temos que Z é finitamente gerado. Então tome $P_1, \ldots, P_n \in \mathcal{P}$ tais que

$$Z = \langle P_1, \ldots, P_n \rangle.$$

Temos que pelo Lema 4.14 a inclusão $\mathbf{I}(V(Z)) \supseteq \sqrt{Z}$ acontece. Agora tome $f \in \mathbf{I}(V(P_1, \ldots, P_n))$. Defina

$$J = \langle P_1, \ldots, P_n, (x_{n+1} \cdot f) - 1 \rangle \subset \mathbb{K}[x_1, \ldots, x_n, x_{n+1}].$$

Temos que

$$\mathbf{V}(J) = \emptyset,$$

pois f se anula apenas nos pontos onde os P_i's se anulam ao mesmo tempo, ou seja, $(x_{n+1} \cdot f) - 1$ não se anula nos pontos de $\mathbf{V}(P_1, \ldots, P_n)$. Logo, pelo item (I) deste teorema, como $\mathbf{V}(J) = \emptyset$ então J não é um ideal próprio e portanto, $1 \in J$. Assim, temos que

$$1 = \left(\sum Q_i(x_1, \ldots, x_{n+1}) \cdot P_i\right) + R((x_1, \ldots, x_{n+1}) \cdot ((x_{n+1} \cdot f) - 1).$$

Sejam $y = \frac{1}{x_{n+1}}$ e $N > 0$ a maior potência de x_{n+1} que aparece na equação acima. Assim $y^N \in \mathbb{K}[x_1, \ldots, x_n, y]$ e logo,

$$y^N = \left(\sum C_i(x_1, \ldots, x_n, y) \cdot P_i\right) + D(x_1, \ldots, x_n, y) \cdot (f - y).$$

Se fizermos $y = f$, temos que

$$f^N = \left(\sum C_i(x_1, \ldots, x_n, f) \cdot P_i\right).$$

Assim concluímos nossa demonstração pois conseguimos uma potência de f que está em $\mathcal{P}$. Logo $f \in \sqrt{Z}$.

□

Observação 4.17. A demonstração do item (II) foi feita desta forma pois o problema envolvido pode ser visto da seguinte maneira: Se $f_1, \ldots, f_r, P \in \mathcal{P}$ onde P se anula apenas nos pontos de $\mathbf{V}(f_1, \ldots, f_r)$ então a seguinte equação é satisfeita:

$$P^k = G_1 f_1 + \ldots + G_r f_r,$$

para algum $k > 0$ e $G_i \in \mathcal{P}$.

5 Conclusão

Neste trabalho, foram apresentadas algumas relações entre os Ideais e as Variedades, sendo uma delas, o importante Nullstelensatz (ou Teorema dos Zeros de Hilbert), que nos fornece uma caracterização dos polinômios que se anulam em uma variedade qualquer.

Cumprimos com o cronograma que havia sido preparado e estudamos todos os tópicos programados, compreendendo detalhadamente cada um deles. Embora este projeto tenha se encerrado, temos uma base muito satisfatória para estudos futuros em Geometria Algébrica.

Referências

[1] ALTMAN, Allen; KLEIMAN, Steven. A Term of Commutative Algebra. Worldwide Center of Mathematics, LCC 2012.

[2] COX, David; LITTLE, John; O'SHEA, Donal. *Ideals, Varieties, and Algorithms : An Introduction to Computacional Algebraic Geometry and Commutative Algebra*. 3a. ed. Springer-Verlag, 2010.

[3] HERSTEIN, I. N. *Tópicos de álgebra*. Editora Polígono.

[4] LANG, S. *Algebra, 3rd. ed.*. Springer, 2002.

[5] FULTON, W. *Algebraic Curves : An Introduction to Algebraic Geometry*. 2008.

[6] ALLCOCK, D. *Hilberts Nullstellensatz*. Department of Mathematics - University of Texas, Austin, 2005.

[7] ROSARIO, E.C. **Lema de Zorn, suas Equivalências e Aplicações**. 2016. 27 f. Trabalho (Trabalho de Conclusão de Curso) – Universidade Federal do Amapá, Amapá, 2016.