José Antônio Santos Pimentel

Teorema dos Zeros de Hilbert

Itabaiana
2024

José Antônio Santos Pimentel

Teorema dos Zeros de Hilbert

Universidade Federal de Sergipe
Departamento de Matemática
Programa de Iniciação Científica Voluntária

Orientador: Prof. Me. Samuel Brito Silva

Itabaiana
2024

0.1 Introdução

Se pensarmos nos primórdios da interação entre geometria e álgebra, certamente iremos nos deparar com o brilhante matemático francês René Descartes ($1596 - 1650$). Sua ideia simples e genial consistiu em estabelecer coordenadas aos pontos de um plano bidimensional, isso estabeleceu uma relação intrínseca entre geometria e álgebra. Descartes observou que pontos, retas, círculos e planos, objetos já conhecidos da geometria euclidiana clássica poderiam ser representados usando equações. Assim surgia a geometria analítica, que possibilitou traduzir a geometria euclidiana em equações algébricas, e futuramente mostrou-se ser uma ferramenta fundamental para o desenvolvimento da física, química e biologia.

Com o avanço da geometria analítica, o desenvolvimento e generalização de um tipo especial de equações polinomiais de grau 1 (as equações lineares em n variáveis) passaram a ser sistematizadas em uma área específica da álgebra, a álgebra linear. Tal estudo consistiu em observar que equações lineares com n variáveis podem representar um objeto geométrico no $\mathbb{R}^n$, chamados de hiperplanos.

Os estudos de equações lineares da forma

$$a_{i1}x_1 + \cdots + a_{in}x_n = 0$$

foram bem desenvolvidos via álgebra linear. Entretanto, o questionamento sobre o comportamento de um sistema equações polinomiais de grau maior que 1 envolvendo um conjunto de pontos ainda era uma incógnita

$$\begin{cases} f_1(x_1, ..., x_n) = 0 \\ f_2(x_1, ..., x_n) = 0 \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases}$$

é baseado nisso que os estudos acerca da geometria algébrica são desenvolvidos.

Quando desenvolvemos os estudos da geometria algébrica, percebemos tal estrutura está diretamente ligada com os conceitos da álgebra comutativa. Os estudos iniciados nos anos de 1920 por B. L. van der Waerden ($1903 - 1996$), E. Noether($1882-1935$) e outros matemáticos, possibilitaram o avanço algébrico do conceito de variedades algébricas, que por sua vez viabilizou considerar variedades sobre um corpo arbitrário.

Generalizando ainda mais a relação entre geometria algébrica e álgebra comutativa, quando temos um corpo algebricamente fechado K, existe uma conexão forte entre o anel de polinômios $K[x_1, ..., x_n]$ e variedades algébricas em A_K^n. Essa relação entre as duas áreas foi construída através do Teorema dos zeros de Hilbert, tal teorema será alvo do nosso estudo neste trabalho.

0.2 Atividades Realizadas

De março à Julho de 2023 foram realizadas revisões bibliográficas. Nesse período, destacamos o estudo de anéis, ideais, anéis Noetherianos e teorema da base de Hilbert. Está foi a primeira etapa do trabalho.

De agosto à outubro de 2023 iniciou-se o estudo de variedades algébricas e ideal de definição de uma variedade algébrica. Com pausa nas atividades para dar início na disciplina de verão

De março à julho de 2024 retomamos os estudos com foco no teorema dos zeros de Hilbert.

0.3 Outras Atividades

Foi feito um estudo sobre o software LaTex, levando ao desenvolvimento e aperfeiçoamento das habilidades no manuseio do programa.

Fora cursado, de 15 de janeiro à 30 de fevereiro de 2024 a disciplina de Álgebra Linear, na modalidade de curso de verão. O curso foi ofertado pela XIII Escola de Verão em Matemática, organizado pelo Departamento de Matemática.

Além disso, foi feita uma pequena palestra sobre o tema em uma disciplina do campus em que estou inserido.

0.4 Metodologia

A metodologia para a execução deste projeto de pesquisa consistiu em encontros semanais, com as seguintes atividades realizadas: estudo direcionado, apresentação de seminários, seleção e leitura de referências bibliográficas, além de discussões sobre a manipulação do software LaTex.

0.5 Resumo

Neste trabalho serão apresentados conceitos de álgebra comutativa e geometria algébrica. Para isso, veremos o teorema da base de Hilbert, que usaremos como base para provar, o teorema dos zeros de Hilbert que por sua vez, permitirá estabelecer uma ligação entre os ideais dos anéis de polinômios e os subconjuntos do espaço afim. O texto foi dividido em 4 capítulos. Nestes capítulos, falaremos Anéis Noetherianos e conceitos básicos sobre geometria algébrica. Por último, apresentamos a demonstração do nullstellensats e suas consequências

Palavras-chave: Álgebra comutativa. Geometria algébrica. Teorema dos zeros de Hilbert.

Sumário

1 TEOREMA DA BASE DE HILBERT

O termo Noetheriano é uma homenagem à matemática alemã Emmy Noether cujas contribuições matemáticas revolucionaram a Algebra Abstrata. No presente capítulo definimos e caracterizamos os Anéis Noetherianos. E além disso, iremos conhecer o lema de Zorn, bastante usado em diversas áreas da matemática, principalmente na teoria dos anéis e ideais, e a partir do mesmo serão apresentados os anéis Noetherianos e o teorema da base de Hilbert.

1.1 Anéis Noetherianos

Definição 1. *Seja R um conjunto parcialmente ordenado. Defina $\leq$ uma relação parcial de ordem. Um subconjunto $C \subset R$ é dito uma cadeia se para quaisquer $x, y \in C$ tivermos $x \leq y$ ou $y \leq x$.*

Definição 2. *Seja R um conjunto parcialmente ordenado e $C \subset R$ uma cadeia. Uma cota superior para C é um elemento $r \in R$ tal que $x \leq r$ para todo $x \in C$.*

Observação 1. *Pode acontecer de uma cota superior de C não pertencer a C.*

Definição 3. *Seja R um conjunto parcialmente ordenado. $m \in R$ é dito elemento maximal de R ae dado $x \in R$ tal que $m \leq x$, tivermos $m = x$.*

Lema 1. *(Lema de Zorn) Se $R \neq \varnothing$ é um conjunto parcialmente ordenado, tal que toda cadeia em R tem cota superior em R. Então, R possui elemento maximal.*

Demonstração. Queremos mostrar que R possui um elemento maximal. Seja então $C \subseteq R$ uma cadeia maximal de R. Por hipótese, existe $m \in R$ uma cota superior de C, vamos verificar que m é um elemento maximal de uma cadeia qualquer de R. Suponha por absurdo que existe $x \in R$ tal que $m < x$, como $m < x$, então $x \notin C$, note que $y \leq m \leq x$ para todo $y \in C$, pois $y \leq m$ e m é elemento maximal, por isso $y \in C$. Note que $C \cup \{x\}$ é uma cadeia, pois C já é uma cadeia por definição e anteriormente comparamos x com m. Por isso, a união é uma cadeia. Observe $C \subseteq R$ é uma cadeia maximal de R e como $C \cup \{x\}$ é uma cadeia de R gera um absurdo, já que não deveria existir nenhuma outra cadeia de R contendo estritamente C pelo fato de C

ter característica de uma cadeia maximal. conclui-se que R possui elemento maximal.

□

Teorema 1. *Todo anel $A \neq \varnothing$ possui algum ideal maximal.*

Demonstração. Defina S como o conjunto de todos os ideias próprios. Ou seja, são ideais que não contem 1_A, note que $S \neq \varnothing$, pois $\{0\} \in S$, observe que S é parcialmente ordenado com relação a inclusão usual. Cada cadeia $C = \{I_\lambda\}_{\lambda \in L}$, como $I_\lambda \neq A$. Cada cadeia C tem uma relação de inclusão e dado $\alpha, \beta \in L$, então $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$. Seja então $I = \bigcup_{\lambda \in L} I_\lambda$. Note que I é ideal próprio do anel A, devido ao fato de C ser uma cadeia de ideais próprios de A e I é a cota superior, pois I é a junção de todos I_λ: $I_1 \subseteq I_2 \subseteq \cdots \subseteq I$ de $C \in S$. Pelo lema de Zorn S possui um elemento maximal, no caso L possui ideal maximal.

□

Definição 4. *(Anel Noetheriano) Um anel A é Noetheriano se toda cadeia ascendente de ideia de A*

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

é estacionária, isto é, $m \geq 0$ tal que $I_m = I_j$, para todo $j \geq m$.

Definição 5. *Um ideal I é dito finitamente gerado, se existir $a_1, a_2, ..., a_n$ em A tal que qualquer elemente de I pode ser escrito na forma*

$$x_1 a_1 + x_2 a_2 + \cdots + x_n a_n$$

com $x_1, x_2, ..., x_n \in I$.

Teorema 2. *Um anel A é Noetheriano se, e somente se, todo ideal de A é finitamente gerado.*

Demonstração. Seja A um anel Noetheriano. Ou seja, toda cadeia ascendente de ideais de A é estacionária. Vamos mostrar que um ideal I de A é finitamente gerado. Para isso, defina como λ o conjunto de todos os ideais finitamente gerados de A. Note que λ não é vazio, pois $\{0\} \in \lambda$, e pelo teorema anterior, λ possui um elemento maximal I_0. Se $I \neq I_0$ então existe $n \in I$ tal que $n \notin I_0$. Considere $J = I_0 + (n)$, temos que J é finitamente

gerado, pois todos os seus elementos são formados de ideias finitamente gerados, e além disso J contém estritamente I_0, o que é um absurdo, pois I_0 é maximal e não deveria ter outro conjunto contendo I_0.

Reciprocamente, queremos mostrar que a cadeia de ideias do anel A é estacionária. Dada uma cadeia ascendente de ideais $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$, então $M = \bigcup_{n=1}^{\infty} I_n$ é um ideal de A. é importante observar que já mostramos que nem sempre a união de ideias de um anel A é um ideal, mas nesse caso, será pois todos elementos operados em qualquer ideal estará em M. Sejam $x_1, x_2, ..., x_r$ os geradores de M tais que $x_i \in I_{n_i}$ e seja $n = max\{n_1, n_2, ..., n_r\}$, daí segue que cada x_i pertence a I_n, logo $J = I_n$ e portanto a cadeia é estacionária.

□

Seja A um anel e $A[x]$ o anel de polinômios numa variável sobre A. De fato $f(x) \in A[x]$, escrevemos f como $f(x) = ax^r + a_r(x)$ (onde $a_r(x)$ é o polinômio que representa o termo de grau menor que r em $f(x)$).

Para indicar que a é o coeficiente líder de $f(x)$ e que $f(x) - ax^r$ representa o polinômio de grau menor, ou até mesmo o polinômio de grau nulo. Par cada ideal J de $A[x]$, temos um recurso que permite associa-lo a alguns ideais do anel A. defina:

O conjunto de todos os coeficientes líderes dos polinômio pertencentes a J, união zero.

$$C(J) = \{a \in A; \exists\ n \in \mathbb{N}, f(x) \in J\ /\ f(x) = ax^n + a_0(x)\} \cup \{0\}$$

ou seja, $C(J)$ é o conjunto de todos os coeficientes líderes dos polinômios de grau $n \in J$ união com o zero, onde $a_0(x)$ tem grau menor que n.

Para cada $r \in \mathbb{N}$, fixo tome

$$C_r(J) = \{a \in A, \exists\ f(x) \in J\ /\ f(x) = ax^r + a_r(x)\} \cup \{0\}$$

ou seja, $C_r(J)$ é o conjunto de todos os coeficientes líderes dos polinômios de grau igual a $r \in J$ união com o zero.

Proposição 1. *O conjunto* $C(J) = \bigcup_{r=o}^{\infty} C_r(J)$ *é um ideal do anel* A.

Demonstração. Para isso, vamos verificar que o conjunto $C(J)$ satisfaz três condições.

1. Queremos mostrar que $0 \in C(J)$. Segue de como o conjunto foi definido.

2. Dado $a, b \in C(J)$, queremos mostrar que $a + b \in C(J)$. Dado $a, b \in C(J)$ existem polinômios $f, g \in J$ tal que $f(x) = ax^n + o_n(n)$ e $g(x) = bx^n + k_n(x)$, fazendo a soma entre f e g $(f+g)(x) = (a+b)^n + (o+k)(x)$, então $a + b \in C(J)$.

3. Queremos mostrar que dado $\lambda \in A$ e $b \in C(J)$ $\lambda b \in C(J)$. Seja $b \in C(J)$,então existe um polinômio $g \in J$ tal que $g(x) = bx^n + k_n(x)$, como $A \subset A[x]$ $\lambda g(x) = (\lambda b)x^n + \lambda k_n(x)$ e $\lambda b \in C(J)$. E consequentemente, $C(J)$ é um ideal do anel A. De forma análoga, pode-se verificar que $C_r(J)$ é um ideal do anel A.

□

Esses conceitos sobre os ideais de uma anel A que representam os coeficientes líderes dos polinômios de um determinado ideal pertencente a $A[x]$ serão muito úteis para a demonstração do teorema da base de Hilbert.

1.2 Teorema da Base de Hilbert

Teorema 3. *(Teorema da base de Hilbert) Se A é um anel Noetheriano, então o anel de polinômios $A[x]$ é Noetheriano.*

Demonstração. Queremos mostrar que $A[x]$ é Noetheirano, para isso, vamos tomar um ideal I qualquer em $A[x]$ e mostrar que esse ideal I é finitamente gerado.

Seja I um ideal qualquer em $A[x]$, se I for o ideal nulo, temos que I é finitamente gerado, ou seja,$I = \langle 0 \rangle$. Suponha que $I \neq \{0\}$, vamos mostrar que I é finitamente gerado.

Seja $d \in \mathbb{Z}^+$, onde $C_d = C_d(I)$, já sabemos pela demonstração anterior que e C_d é um ideal. E além disso, mostramos que C_d forma uma cadeia acendente, onde $C_d \subseteq C_{d+1}$. Assim, $\{C_d\}_{d \in \mathbb{Z}^+}$ é uma cadeia ascendente de ideais de A, e como A é Noetheriano então existe $D \geq 0$ tal que $C_d = C_D$. Essa informação nos diz que essa cadeia é estacionária, justamente por ser uma cadeia de ideais do anel A.

Observe que D estabelece uma quantidade, usaremos o fato de A ser um anel Neotheriano e em A temos os seguintes ideais: $C_0, ..., C_D$, como eles são ideais do anel A cada um deles é finitamente gerado. O conjunto de elementos formam C_i, são elementos que são coeficientes líderes de uma quantidade de polinômios.

Se C_i são gerados por $S_i = \{b_{i1}, ..., b_{ili}\}$ cada elemento de S_i é coeficiente líder de um polinômio, então cada elemento de S_i determina uma quantidade finita de polinômios cujo os coeficientes líderes são geradores de cada C_i. Por isso, é importante a quantidade finita de termos C_D.

Para cada $i \in \{0, ..., D\}$ o ideal C_i é um ideal de A, então existe um conjunto finito de polinômios, onde denotaremos de $B_i \subseteq A[x]$ tais que os coeficientes líderes dos polinômios B_i geram C_i. Logo, A união de todos os B_{is} é finita, pois todos B_i são finitos. Escreva a união de todos os B_{is} como $\{P_1, ..., P_n\}$.

É importante observar que cada polinômio desses P_i está no ideal I, pois B_i são coeficientes líderes de polinômios que estão no ideal I. Os polinômios P_i estão na união B_i, mas cada B_i é formado por polinômios cujo o coeficiente líder é coeficiente líder de um polinômio que está em I, observe que o B_i é um polinômio cujo o coeficiente líder está em C_i Claramente,

$$\{P_1, ..., P_n\} \subseteq I \Rightarrow A[x]P_1 + \cdots + A[x]P_n \subseteq I$$

mostraremos agora que a outra inclusão é verdadeira. Ou seja,

$$I \subseteq A[x]P_1 + \cdots + A[x]P_n$$

assim mostraremos que o ideal I, um ideal arbitrário de $A[x]$ é finitamente gerado. Seja $f \in I$, suponha que $f \neq 0$. Vamos mostrar pelo segundo princípio de indução matemática sobre o grau de f.

Suponha que $\partial(f) = 0$. Logo existe $c \in A$ onde c é uma constante, tal que $f = c \neq 0$. É importante observar que, $c \in C_0$, sabemos também que B_0 gera C_0. Logo, $f = c \in C_0$ que é gerado por coeficientes líderes de polinômios em $B_0 \subseteq \{P_1, ..., P_n\}$.

Assim, existem

$$P_{i1}, ..., P_{ir} \in \{P_1, ..., P_n\}$$

de grau 0, cujo os coeficientes líderes são eles mesmos que geram $f = c$, portanto f é combinação de $\{P_1, ..., P_n\}$. isso nos dá o fato de que para um caso inicial

$$f \in A[x]P_1 + \cdots + A[x]P_n$$

.

Vamos supor que $\partial(f) > 0$, e que $g \in A[x]P_1 + \cdots + A[x]P_n$ desde que $g \in I - \{0\}$, onde $\partial(g) < \partial(f)$. Nosso objetivo é mostrar que $f \in A[x]P_1 + \cdots + A[x]P_n$.

Antes de constatar o que foi dito acima, vamos precisar mostrar a seguinte afirmação: existe $h \in A[x]P_1 + \cdots + A[x]P_n$, tal que $\partial(h) = \partial(f)$ e além disso, f e h possuem o mesmo coeficiente líder.

Iremos mostrar tal afirmação, pois se conseguimos um h nessas condições, então $(f - h)$ vai cair o grau, já que ambos têm grau d e mesmo coeficiente líder. Com isso, $\partial(f - h) < \partial(f)$ e podemos aplicar a hipótese de indução, já que $f \in I$ e $h \in A[x]P_1 + \cdots + A[x]P_n$ que pela primeira inclusão está contido em I.

Portanto, $f - h \in I - \{0\}$, pela hipótese de indução

$$f - h \in A[x]P_1 + \cdots + A[x]P_n$$

o que nos permite fazer a seguinte operação

$$(f - h) + h \in A[x]P_1 + ... + A[x]P_n$$

concluiremos então que

$$f \in A[x]P_1 + \cdots + A[x]P_n.$$

Para mostrar que h existe nestas condições, vamos dividir em 2 casos. Primeiro

1. Suponha que $\partial(f) \leq D$.

Tome $i = \partial(f) \leq D$ e seja $c_f \in A$ o coeficiente líder de f. Logo, $c_f \subseteq C_0$. Isso acontece, pois c_f é coeficiente líder de um polinômio f que está em $I - \{0\}$ de grau i. C_f é gerado por coeficientes líderes de polinômios que estão em B_i.

Vamos fixar a notação C_h para o conjunto de coeficientes líderes de grau h já mencionado acima e c_h, com "c"(minúsculo) será é o coeficiente líder do polinômio h.

Daí existem $\alpha_1, ..., \alpha_r \in A$ tais que

$$c_f = \alpha_1 C_{P_{i1}} + \cdots + \alpha_r C_{P_{ir}}$$

onde $P_{i1}, .., P_{ir}$ possuem grau i Tome

$$h = \alpha_1 P_{i1} + \cdots + \alpha_r P_{ir} \in A[x]P_1 + \cdots + A[x]P_n$$

e o termo de grau i de h é

$$\alpha_1 c_{P_{i1}} + \cdots + \alpha_r c_{P_{ir}} = c_f \neq 0$$

isso implica que

$$\partial(h) = i = \partial(f)$$

e, f e h possuem o mesmo coeficiente líder. Assim, para $\partial(f) \leq D$, encontramos h nas condições desejadas.

2. Suponha que $\partial(f) > D$.

Seja $\partial(f) = d$. Como $d > D$ e a cadeia é estacionária, temos que $C_d = C_D$. Chamando $c_f \in A$ o coeficiente líder de f, então $c_f \in C_d = C_D$. Observe que os coeficientes líderes que geram C_D estão em B_D, vamos aplicar uma ideia parecida com a do primeiro caso.

Assim, existem $\beta_1, ..., \beta_s \in A$ e $P_{J1}, ..., P_{js} \in B_D$ tais que

$$c_f = \beta_1 c_{P_{j1}} + \cdots + \beta_s c_{P_{js}}$$

vamos tomar espertamente

$$h = \beta X^{d-D} P_{j1} + \cdots + \beta_s X^{d-D} P_{js} \in A[x]P_1 + \cdots + A[x]P_n$$

logo, o termo de grau d de h é

$$\beta_1 c_{P_{j1}} + \cdots + \beta_s c_{P_{js}} = c_f \neq 0$$

e isso vai implicar em $h \neq 0$

$$\partial(h) = d = \partial(f)$$

e $c_h = c_f$. Para $\partial(f) \geqslant D$. Portanto, a afirmação está mostrada.

Vamos então analisar as possibilidades para f e h. Se

$$f = h \Rightarrow f \in A[x]P_1 + \cdots + A[x]P_n$$

suponha que $f \neq h$. Como nesse caso, f e h possuem o mesmo grau e mesmo coeficiente líder, então

$$\partial(f-h) < \partial(f)$$

como f e $h \in I$, segue que

$$(f-h) \in I - \{0\}$$

e pela hipótese de indução matemática qualquer polinômio com grau menor que f está em $A[x]P_1 + \cdots + A[x]P_n$. Temos então que

$$(f-h) \in A[x]P_1 + \cdots + A[x]P_n$$

e como sabemos, $h \in A[x]P_1 + \cdots + A[x]P_n$, podemos operar da seguinte forma,

$$(f-h) + h = f \in A[x]P_1 + \cdots + A[x]P_n$$

temos então que

$$I \subseteq A[x]P_1 + \cdots + A[x]P_n$$

como a inclusão contrária já era conhecida podemos concluir que $A[x]$ é um anel Noetheriano, pois tomamos um ideal qualquer em $A[x]$ e mostramos que ele é finitamente gerado. Isso é garantido pelo fato de A ser Noetheriano.

□

Corolário 1. *Se A é um anel Noetheriano, então $A[x_1, ..., x_n]$ é Noetheriano.*

Demonstração. Por indução sobre n. Para $n = 1$, é especificamente o Teorema da Base de Hilbert. Se $n = 2$, temos $(A[x_1])[x_2]$, como $(A[x_1])$ é Noetheriano, então $(A[x_1])[x_2]$ também é. Pelo segundo princípio de indução matemática, temos que $A[x_1, ..., x_{n-1}]$ é Noetheriano.

Como

$$A[x_1, ..., x_n] = (A[x_1, ..., x_{n-1}])[x_n]$$

concluímos que $A[x_1, ..., x_n]$ é Noetheriano.

□

2 VARIEDADES ALGÉBRICAS

Neste capítulo iremos conhecer o que é o espaço afim, uma variedade algébrica e suas propriedades. Para isso, vamos trabalhar com conjuntos de pontos e ideais de uma anel de polinômios $K[x_1, ..., x_n]$. Tais conceitos são fundamentais para introdução de estudo acerca da geometria algébrica. Além disso, são fundamentais para enunciar o teorema dos zeros de Hilbert.

2.1 Espaço Afim

Definição 6. *(Espaço afim) Seja K um corpo O espaço afim $n-$dimensional sobre K é definido por*

$$A_k^n = \{(a_1, ..., a_n); a_i \in K, i \in \{1, ..., n\}\}$$

Normalmente, chamamos os elementos deste conjunto de pontos Note que A_k^n é o conjunto $K^n = \underbrace{K \times ... \times k}_{n-vezes}$.Observe os seguintes casos

1. $n = 1$, o conjunto A_k^1: Reta afim sobre k;
2. $n = 2$, o conjunto A_k^2:Plano afim sobre k;
3. $n = 3$, o conjunto A_k^3: Espaço afim tridimensional k.

Definição 7. *Sejam $f \in K[x_1, ..., x_n]$ um polinômio e $P = (a_1, ..., a_n) \in A_k^n$ um ponto. Dizemos que P é um zero de f, se $f(P) = 0$.*

Observação 2. *A ideia da Geometria Algébrica é basicamente estudar conjuntos que são obtidos através de zeros de equações polinomiais.*

Definição 8. *Uma hipersuperfície afim em A_K^n é um conjunto de pontos $P \in A_K^n$ que são zeros de um único polinômio $f \in K[x_1, ..., x_n]$. Denotaremos tal conjunto como $\mathcal{V}(f)$.*

Exemplo 1. *Círculo: Considere $f : x^2 + y^2 - 1$ Note que o conjunto de zeros de f, ou seja $\mathcal{V}(f)$ é o representado graficamente por um círculo centrado na origem de raio 1.*

Exemplo 2. *Parábola: No caso $f : y - x^2$ tem como representação gráfica no plano uma parábola.*

2.2 Variedades Algébricas

Definição 9. *(Variedade algébrica) Seja K um corpo. Um subconjunto $X \subseteq A_K^n$ é dito uma variedade algébrica afim, ou simplesmente variedade algébrica se for o conjunto-solução de um sistema de equações:*

$$\begin{cases} f_1(x_1, ..., x_n) = 0 \\ f_2(x_1, ..., x_n) = 0 \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases}$$

onde $f_1, f_2, ..., f_m$ *são polinômios no anel* $K[x_1, ...x_n]$.

Seja $S = \{f_1, ..., f_m\}$, podemos escrever o conjunto X da definição acima como

$$X = \mathcal{V}(S) = \{(a_1, ..., a_n) \in A_K^n; f(a_1, ..., a_n) = 0 \ \forall \ f \in S\}.$$

É notável que uma variedade algébrica é simplesmente a interseção dos conjunto de zeros definidos por cada polinômio do sistema dado.

Exemplo 3. *Vamos determinar a variedade algébrica de*

$$S = \{y^2 - x^3, y - x^2\}$$

determinar a variedade de S *é determinar os pontos que zeram todos os polinômios de* S.

$$\begin{cases} y^2 - x^3 = 0 \\ y - x^2 = 0 \end{cases}$$

resolvendo o sistema, teremos que se $x = 0$ *então* $y = 0$ *e se* $x = 1$ *então* $y = 1$. *Portanto,* $\mathcal{V}(S) = \{(0, 0), (1, 1)\}$. *Neste caso, temos um conjunto finito de pontos.*

Observação 3. *Vamos tomar* $I = \langle S \rangle$ *o ideal gerado pelos polinômios pertencentes a* S.

Proposição 2. *Seja $I = \langle S \rangle$, então $\mathcal{V}(\langle S \rangle) = \mathcal{V}(S)$.*

Demonstração. Seja $P \in \mathcal{V}(\langle S \rangle)$, temos então que P é anulado por todos os polinômios no ideal gerado por S. Para mostrar que $P \in \mathcal{V}(S)$, vamos pegar um polinômio em S e mostrar que tal polinômio anula P. Tomando $f \in S$, em particular f está no ideal gerado por S, basta escrever $f = 1.f$, claramente P é anulado por f, pois $f \in \langle S \rangle$, concluímos que $P \in \mathcal{V}(S)$. Reciprocamente, vamos mostrar que $\mathcal{V}(S) \subseteq \mathcal{V}(\langle S \rangle)$ Para isso, tome $P \in \mathcal{V}(S)$, onde $f \in \langle S \rangle$, temos então que $f = h_1 g_1 + \cdots + h_n g_n$, onde $h_i \in K[x_1, ..., x_n]$ e $g_1, ..., g_n \in S$ com $i \in \{1, ..., n\}$ Como $P \in \mathcal{V}(S)$, então P anula todo $g_i, i \in \{1, ..., n\}$ Logo, aplicando

$$\begin{aligned} f(P) &= (h_1 g_1 + \cdots + h_n g_n)(P) \\ &= h_1(P) g_1(P) + \cdots + h_n(P) g_n(P) \\ &= h_1(P) \cdot 0 + \cdots + h_n(P) \cdot 0 = 0 \end{aligned}$$

logo, $P \in \mathcal{V}(\langle S \rangle)$, já que encontramos um polinômio em $f \in \langle S \rangle$ que anula P. Obtemos então igualdade deseja.

□

Exemplo 4. *Se tomarmos o espaço afim $A^2_{\mathbb{R}}$ Dado o ideal*

$$I = \langle xy - 1 \rangle \subseteq \mathbb{R}[x, y]$$

temos que $\mathcal{V}(I) \subseteq A^2_{\mathbb{R}}$ representa uma hipérbole no plano bidimensional sobre $\mathbb{R}$.

Proposição 3. *Seja A^n_k um espaço afim qualquer, então são satisfeitas as seguintes propriedades:*

1. *Os conjuntos $\varnothing$ e A^n_K são variedades algébricas;*
2. *Seja $I \subseteq J \subset K[x_1, ..., x_n]$, então $\mathcal{V}(J) \subseteq \mathcal{V}(I)$;*
3. *Seja P um ponto de A^n_k, então o conjunto $\{P\}$ é uma variedade algébrica;*
4. *Seja $\{I\}_{\alpha \in L}$ uma coleção arbitrária de ideais de $K[x_1, ..., x_n]$. Então*

$$\bigcap_{\alpha \in L} \mathcal{V}(I_\alpha) = \mathcal{V}\left(\bigcup_{\alpha \in L} I_\alpha \right) = \mathcal{V}\left(\sum_{\alpha \in L} I_\alpha \right);$$

5. $\mathcal{V}(I \cdot J) = \mathcal{V}(I) \cup \mathcal{V}(J)$. *Em particular, a união finita de variedades algébricas ainda é uma variedade algébrica.*

Demonstração. Queremos mostrar que os 5 itens acima são verdadeiros.

1. Para mostrar que $\varnothing$ é uma variedade, precisamos encontrar um ideal em $k[x_1, ..., x_n]$ tal que $\mathcal{V}(I) = \varnothing$. Considere então $I = \langle 1 \rangle$, note que nenhum ponto no espaço afim pode zerar qualquer polinômio constante. Logo, $\mathcal{V}(I) = \varnothing$. Analogamente, para mostrar que A_k^n é um variedade, considere $J = \langle 0 \rangle$, note que qualquer ponto no espaço afim zera o polinômio identicamente. Portanto, $\mathcal{V}(J) = A_K^n$.

2. Por definição, temos que

$$\mathcal{V}(J) = \{(a_1, ..., a_n) \in A_K^n / f(a_1, ..., a_n) = 0 \ \forall \ f \in J\}$$

, mas temos que $I \subseteq J$, logo teremos que $f \in I$. Assim, todos os pontos $\mathcal{V}(J)$ são zeros de $f \in I$. Ou seja, $\mathcal{V}(J) \subseteq \mathcal{V}(I)$

3. Considere um ponto P qualquer de A_k^n, temos que $P = (a_1, ..., a_n)$. Seja $M = \langle x_1 - a_1, ..., x_n - a_n \rangle$, note que o único ponto que é zero de qualquer polinômio em M é P, pois se $f \in M$, temos que

$$f = h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n)$$

tal que $h_i \in \{1, ..., n\}$ em $K[x_1, ..., x_n]$, note que

$$\begin{aligned} f(P) &= (h_1(x_1 - a_1) + \cdots + h_n(x_n - a_n))(P) \\ &= h_1(P)(a_1 - a_1) + \cdots + h_n(P)(a_n - a_n) \\ &= h_1(P) \cdot 0 + \cdots + h_n(P) \cdot 0 = 0 \end{aligned}$$

ou seja, $\mathcal{V}(M) = \{P\}$.

4. Vamos mostrar inicialmente que $\bigcap_{\alpha \in L} \mathcal{V}(I_\alpha) \subseteq \mathcal{V}(\bigcup_{\alpha \in L} I_\alpha)$. Seja $P \in \bigcap_{\alpha \in L} \mathcal{V}(I_\alpha)$. Dado $f \in \bigcup_{\alpha \in L} I_\alpha$ arbitrário, existe $\beta \in L$ tal que $f \in I_\beta$ e como $P \in \mathcal{V}(I_\beta)$, então $f(P) = 0$. Logo $P \in \mathcal{V}(\bigcup_{\alpha \in L} I_\alpha)$. Reciprocamente, como $I_\alpha \subseteq \bigcup_{\lambda \in L}$ então pelo item dois temos que $\mathcal{V}(\bigcup_{\lambda \in L} I_\lambda) \subseteq \mathcal{V}(I_\alpha), \forall \ \alpha \in L$ e portanto $\mathcal{V}(\bigcup_{\alpha \in L} I_\alpha) \subseteq \bigcap_{\alpha \in L} \mathcal{V}(I_\alpha)$. Portanto,

$$\bigcap_{\alpha \in L} \mathcal{V}(I_\alpha) = \mathcal{V}\left(\bigcup_{\alpha \in L} I_\alpha\right)$$

Além disso, como o ideal gerado por $\bigcup_{\alpha\in L} I_\alpha$ é $\sum_{\alpha\in l} I_\alpha$ pela proposição em que diz que $\mathcal{V}(\langle I\rangle) = \mathcal{V}(I)$. temos que

$$\mathcal{V}\left(\bigcup_{\alpha\in L} I_\alpha\right) = \mathcal{V}\left(\sum_{\alpha\in L} I_\alpha\right)$$

5. Como $I\cdot J \subseteq I$ e $I\cdot J \subseteq J$ então pelo item dois segue que $\mathcal{V}(I) \subseteq \mathcal{V}(I\cdot J)$, analogamente $\mathcal{V}(j) \subseteq \mathcal{V}(I\cdot J)$, concluímos que $\mathcal{V}(I)\cup\mathcal{V}(J) \subseteq \mathcal{V}(I\cdot J)$. Reciprocamente,vamos mostrar que $\mathcal{V}(I\cdot J) \subseteq \mathcal{V}(I)\cup\mathcal{V}(J)$. Para isso, considere $P \in \mathcal{V}(I\cdot J)$. Se $P \in \mathcal{V}(I)$ então nada a provar. Suponha $P \notin \mathcal{V}(I)$. Então existe $h \in I$ tal que $h(P) \neq 0$. Dado $g \in J$, com $h\cdot g \in I\cdot J$ e $P \in \mathcal{V}(I\cdot J)$ então

$$(hg)(P) = h(P)g(P) = 0$$

como $h(P) \neq 0$, segue que $g(P) = 0$. Logo, $P \in \mathcal{V}(J)$ e portanto $p \in \mathcal{V}(I)\cup\mathcal{V}(J)$.

□

Corolário 2. *Se $X = \{P_1, ..., P_n\} \subset A_K^n$ é um subconjunto finito de pontos, então X é uma variedade algébrica.*

Demonstração. Podemos escrever $X = X_1 \cup X_2 \cup \cdots \cup X_n$, onde $X_i = \{P_i\},\ i \in \{1, ..., n\}$. De acordo com uma das propriedades acima, sabemos que cada X_i é uma variedade algébrica. Além disso, vimos que a união finita de variedades é uma variedade, logo $X = \bigcup_{i=1}^n X_i$ é uma variedade. Concluímos que $X = \{P_1, ..., P_n\} \subset A_K^n$ é uma variedade algébrica.

□

Proposição 4. *Seja K um corpo qualquer, e sejam $a_1, ..., a_n \in K$. Então $M = \langle x_1 - a_1, ..., x_n - a_n\rangle$ é maximal.*

Demonstração. Para mostrar que M é ideal maximal, vamos usar o teorema do isomorfismo. Considere então a aplicação

$$\psi : K[x_1, ..., x_n] \longrightarrow K$$

$$f(x_1, ..., x_n) \longmapsto f(a_1, ..., a_n)$$

claramente é um homomorfismo sobrejetor e temos que

$$ker(\psi) = \langle x_1 - a_1, ..., x_n - a_n \rangle.$$

Pelo teorema do isomorfismo

$$\frac{K[x_1, ..., x_n]}{Ker(\psi)} = \frac{K[x_1, ..., x_n]}{M} \cong k$$

isso nos diz que o quociente $\frac{K[x_1,...,x_n]}{M}$ é um corpo. E já vimos que isso só ocorre se $M = \langle x_1 - a_1, ..., x_n - a_n \rangle$ for ideal maximal.

□

Em geometria analítica, aprende-se que curvas contidas no espaço bidimensional ou superficies no espaço tridimensional, definidas por $\mathbb{R}$ podem ser parametrizadas. De forma geral, o mesmo ocorre em variedades algébricas, é comum que elas venham "camufladas", isto é parametrizadas.

Exemplo 5. *Seja C uma curva algébrica, tal que*

$$C = \{(cost, sent) \in A^2_{\mathbb{R}}; t \in \mathbb{R}\}$$

normalmente representamos a primeira e segunda coordenada dos pontos $A^2_{\mathbb{R}}$ por x e y respectivamente, logo

$$\begin{cases} x = cost \\ y = sent \end{cases}$$

A relação fundamental de trigonometria diz que $sen^2t + cos^2t = 1$. Portanto, um ponto qualquer da curvar C, satisfaz a equação $x^2 + y^2 - 1 = 0$, e assim, $\mathcal{V}(x^2 + y^2 - 1)$, onde sua representação geométrica é simplesmente uma circunferência centrada na origem de raio unitário.

Podemos ver as variedades algébricas como uma espécie de função $\mathcal{V}$, que associa cada ideal I de um anel de polinômios $K[x_1, ..., x_n]$ (onde K é um corpo), ao seu conjunto de zeros $\mathcal{V}(I)$. Neste capítulo, vamos definir o ideal de definição de uma variedade algébrica, iremos construir e observar que sob condições especiais, iremos ter um mecanismo onde esse ideal irá se comportar como uma função inversa de $\mathcal{V}$.

2.3 Ideal de Definição

Definição 10. *(Ideal de definição) Seja K um corpo e $X \subseteq A_K^n$ uma variedade algébrica afim. O ideal de definição de X é o conjunto*

$$\mathcal{L}(X) = \{f \in k[x_1, ..., x_n]; f(P) = 0, \ \forall \ P \in X\}.$$

Proposição 5. *$\mathcal{L}(X)$ é um ideal de $k[x_1, ..., x_n]$.*

Demonstração. Para mostrar que $\mathcal{L}(X)$ é um ideal de $k[x_1, ..., x_n]$, vamos verificar três condições. Primeiro, que o polinômio identicamente nulo está em $\mathcal{L}(X)$, e de fato, pois $0(P) = 0$ para todo P em X
Dados $f, g \in \mathcal{L}(X)$, sabemos que

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

ou seja, $f + g \in \mathcal{L}(X)$.

Por último, considere $h \in \mathcal{L}(X)$ e $g \in k[x_1, ..., x_n]$, sabemos que

$$(f \cdot g)(P) = h(P) \cdot g(P) = 0 \cdot g(P) = 0$$

Concluímos que $h \cdot g \in \mathcal{L}(X)$ e $\mathcal{L}(X)$ é um ideal de $k[x_1, ..., x_n]$.

□

Proposição 6. *Seja $X \subseteq A_K^n$ uma variedade algébrica afim. $\mathcal{L}(X)$ é um ideal radical do anel $k[x_1, ..., x_n]$.*

Demonstração. Já vimos que $\mathcal{L}(X)$ é um ideal, basta mostrar que também é ideal radical. Isto é, $\mathcal{L}(X) = \sqrt{\mathcal{L}(X)}$.

Tome f em $\mathcal{L}(X)$, note que $f^1 \in \mathcal{L}(X)$, logo $\mathcal{L}(X) \subseteq \sqrt{\mathcal{L}(X)}$. Reciprocamente, seja $h \in \sqrt{\mathcal{L}(X)}$, então existe $n \in \mathbb{N} - \{0\}$ tal que $h^n \in \mathcal{L}(X)$, isto nos diz que $h^n(P) = 0$ para todo $P \in X$, segue:

$$h^n(P) = (h^{n-1} \cdot h)(P) = h^{n-1}(P)h(P)$$

$$= \underbrace{h(P) \cdot h(P) \cdot \cdots \cdot h(P)}_{n-vezes} = (h(P))^n = 0$$

Como $k[x_1, ..., x_n]$ é um domínio de integridade, temos que $h(P) = 0$. O que nos garante que $h \in \mathcal{L}(X)$.Concluímos que $\mathcal{L}(X) = \sqrt{\mathcal{L}(X)}$, como desejado.

□

2.4 Anel de Coordenadas

Definição 11. *O anel de Coordenadas de uma variedade algébrica $X \subseteq A_k^n$ é dado por*

$$A(X) = \frac{k[x_1, ..., x_n]}{\mathcal{L}(X)}.$$

Proposição 7. *Seja A um anel e $I \subseteq A$ um ideal radical, então o anel quociente $\frac{A}{I}$ é reduzido.*

Demonstração. Nosso objetivo é mostrar que o único elemento nilpotente do quociente $\frac{A}{I}$ é o $\bar{0}$.

Seja $\bar{x} \in \frac{A}{I}$, tal que $\bar{x}^n = \bar{0}$, para algum $n \in \mathbb{N} - \{0\}$. Segue que

$$x^n - 0 \in I \Rightarrow x^n \in I \Rightarrow x \in \sqrt{I}$$

mas sabemos que $\sqrt{I} = I$, ou seja $x \in I \Rightarrow x - 0 \in I$. concluímos que $\bar{x} = \bar{0}$. Ou seja, dado um elemento $\bar{x}$ nilpotente no quociente $\frac{A}{I}$ onde $\bar{x}^n = \bar{0}$ implica que $\bar{x} = \bar{0}$.

□

Corolário 3. *Seja $X \subseteq A_K^n$ uma variedade algébrica, então o anel de coordenadas de X é reduzido.*

Demonstração. De fato, pois $k[x_1, ..., x_n]$ é um anel e $\mathcal{L}(X)$ é um ideal radical, logo $A(X) = \frac{k[x_1,...,x_n]}{\mathcal{L}(X)}$, é reduzido.

□

Proposição 8. *Seja A_K^n um espaço afim qualquer com relação ao ideal de definição das variedades algébricas contidos em A_K^n, são válidas as seguintes propriedades:*

1. *Se $X \subseteq Y$ então $\mathcal{L}(Y) \subseteq \mathcal{L}(X)$;*
2. *$\mathcal{L}(\varnothing) = k[x_1, ..., x_n]$;*
3. *Se K é um corpo infinito, então $\mathcal{L}(A_K^n) = \langle 0 \rangle$;*
4. *$\mathcal{L}(X \cup Y) = \mathcal{L}(X) \cap \mathcal{L}(Y)$;*
5. *$\mathcal{L}(Y) \cdot \mathcal{L}(W) \subseteq \mathcal{L}(Y \cup W)$;*

6. $\mathcal{V}(\mathcal{L}(X)) = X$ *e* $\mathcal{L}(\mathcal{V}(\mathcal{L}(X))) = \mathcal{L}(X)$.

Demonstração. Queremos mostrar que os 6 itens acima são válidos.

1. Seja $f \in \mathcal{L}(Y)$, temos que $f(P) = 0$ para todo P em Y, mas como $X \subseteq Y$, $f(P') = 0$, para todo P' em X. Ou seja, $f \in \mathcal{L}(X)$, logo $\mathcal{L}(Y) \subseteq \mathcal{L}(x)$

2. Note que $\mathcal{L}(\varnothing) \subseteq k[x_1, ..., x_n]$, por definição. Reciprocamente, basta tomar $f \in k[x_1, ..., x_n]$ e mostrar que $f \in \mathcal{L}(\varnothing)$. tome $f \in k[x_1, ..., x_n]$ e $P \in \varnothing$. Afirmação: $f(P) = 0$ Suponha por absurdo que $f(P) \neq 0$. ou seja, existe $P \in \varnothing$ tal que $f(P) \neq 0$.Mas isso é um absurdo, ou seja, conseguimos provar por vacuidade.

3. O polinômio identicamente nulo é o único que anula todos os pontos $P \in A_K^n$ isto nos diz que $\mathcal{L}(A_K^n) = \langle 0 \rangle$.

4. considere $f \in \mathcal{L}(X \cup Y)$, isso significa que $f(P) = 0$ para qualquer que seja $P \in X \cup Y$, em particular $f(P) = 0$ para todo $P \in X$, o que nos garante que $f \in \mathcal{L}(X)$, analogamente temos que $f(P') = 0$ para todo $P' \in Y$ ou seja, $f \in \mathcal{L}(Y)$. Como temos que f está nos dois ideias de definição, temos a garantia que $f \in \mathcal{L}(X) \cap \mathcal{L}(Y)$.
   Agora, se $f \in \mathcal{L}(X) \cap \mathcal{L}(Y)$, por definição $f(P) = 0$ para qualquer P em X, pois $f \in \mathcal{L}(X)$ ou Y, pois $f \in \mathcal{L}(Y)$. Logo, $f \in \mathcal{L}(X \cup Y)$.

5. Tome $f \in \mathcal{L}(Y) \cdot \mathcal{L}(W)$, ou seja $f = h \cdot g$, com $h \in \mathcal{L}(Y)$ e $g \in \mathcal{L}(W)$. Note que se

   $$P \in Y \Rightarrow f(P) = h(P) \cdot g(P) = 0 \cdot g(P) = 0$$

   ou se

   $$P \in W \Rightarrow f(P) = h(P) \cdot g(P) = h(P) \cdot 0 = 0$$

   concluímos que $f \in \mathcal{L}(Y \cup W)$, pois $f(P) = 0$ para todo $P \in Y$ ou W.

6. Tome $P \in \mathcal{V}(\mathcal{L}(X))$, então $f(P) = 0$ para todo $f \in \mathcal{L}(X)$, logo $P \in X$. Reciprocamente, tomando $P \in X$ onde $f(P) = 0$,implica que $f \in \mathcal{L}(X)$, como P é zero de f temos que $P \in \mathcal{V}(\mathcal{L}(X))$. Concluímos que $\mathcal{V}(\mathcal{L}(X)) = X$. Assim, pela igualdade obtida, também temos que $\mathcal{L}(\mathcal{V}(\mathcal{L}(X))) = \mathcal{L}(X)$.

□

Proposição 9. *Seja A um domínio principal, então $A[x_1, ..., x_n]$ é Noetheriano.*

Demonstração. Sendo A um domínio principal, então todo ideal de A é da forma $I = \langle c \rangle$, ou seja I é finitamente gerado. Assim, A é Noetheriano e pelo teorema da base de Hilbert, $A[x_1, ..., x_n]$ é Noetheriano.

□

Exemplo 6. *Sabemos que o anel $\mathbb{Z}$ é domínio de integridade, em particular todo ideal de $\mathbb{Z}$ é principal e portanto, $\mathbb{Z}[x_1, ..., x_n]$ é Noetheriano.*

Em particular, se K é corpo, então $K[x_1, ..., x_n]$ é Noetheriano, ou seja todo ideal de $K[x_1, ..., x_n]$ é finitamente gerado, inclusive $\mathcal{L}(X)$

Proposição 10. *Toda variedade algébrica $X \subseteq A_K^n$ se expressa como interseção finita de curvas algébricas.*

Demonstração. Seja $X = \mathcal{V}(I)$ para algum $I \subseteq k[x_1, ..., x_n]$. Sabemos que todo corpo K é um domínio principal temos que $K[x_1, ..., x_n]$ é Noetheriano. Pelo teorema da base de Hilbert:

$$\begin{aligned} I &= \langle f_1, ..., f_r \rangle \\ &= f_1 h_1 + \cdots + f_r h_r \\ &= \langle f_1 \rangle + \cdots + \langle f_r \rangle \end{aligned}$$

Para $h_1, ..., h_r$ em $K[x_1, ..., x_n]$. Logo,

$$X = \mathcal{V}(I) = \mathcal{V}\left(\sum_{i=1}^{r} \langle f_i \rangle\right) = \mathcal{V}\left(\sum_{i=1}^{r} f_i\right)$$

Vimos anteriormente que

$$X = \mathcal{V}\left(\sum_{i=1}^{r} f_i\right) = \bigcap_{i=1}^{r} \mathcal{V}(f_i)$$

Ou seja, uma variedade algébrica qualquer X se expressa como interseção de curvas algébricas.

□

2.5 Componentes Irredutíveis de uma Variedade Algébrica

Observe o seguinte exemplo

Exemplo 7. *Seja* $C = \mathcal{V}(x^3 - x^2 \cdot y + y^2 - x \cdot y) \subseteq A_K^n$, *note que*

$$f(x, y) = x^3 - x^2y + y^2 - xy = (y - x^2)(y - x)$$

isso nos diz que $\mathcal{V}(x - y^2)$ *é um conjunto de zeros para o polinômio* f. *Por outro lado, é notório que* $V(y - x)$ *também seja um conjunto de zeros do polinômio* f, *temos então*

$$C = \mathcal{V}(x - y^2) \cup \mathcal{V}(y - x).$$

Vimos acima que podemos escrever uma variedade algébrica como a união de outras variedades algébricas. O que nos interessa é saber quando esse fato pode ocorrer.

Definição 12. *Seja* K *um corpo e* $X \subseteq A_K^n$ *uma variedade algébrica. Se* Y *é subconjunto de* X *e também é uma variedade algébrica, então dizemos que* Y *é subvariedade de* X.

Definição 13. *Uma variedade algébrica* $X \subseteq A_K^n$ *é redutível quando existem subvariedades próprias* $Y, W \subsetneq X$, *com* $Y \neq W$, *tais que* $X = Y \cup W$.

Definição 14. *Quando uma variedade algébrica qualquer não é redutível dizemos que a mesma é irredutível.*

Proposição 11. *Seja* $X \subseteq A_K^n$ *uma variedade algébrica* X *é irredutível se, e somente se,* $\mathcal{L}(X)$ *é ideal primo em* $K[x_1, ..., x_n]$.

Demonstração. De forma equivalente, vamos mostrar que X é irredutível, se e somente se, $\mathcal{L}(X)$ não é ideal primo de $K[x_1, ..., x_n]$.

Para mostrar que $\mathcal{L}(X)$ não é ideal primo, vamos tomar $a, b \notin \mathcal{L}(X)$ e mostrar que $a \cdot b \in \mathcal{L}(X)$

Se X é redutível, então existem subvariedades algébricas próprias $Y, W \subsetneq X$, com $Y \neq W$, tais que $X = Y \cup W$. Sabemos que $Y \subsetneq X$, isso nos diz que $\mathcal{L}(X) \subsetneq \mathcal{L}(Y)$, assim como $\mathcal{L}(X) \subsetneq \mathcal{L}(W)$.

Tome $g \in \mathcal{L}(Y) - \mathcal{L}(X)$ e $h \in \mathcal{L}(W) - \mathcal{L}(X)$. Ou seja, $g, h \notin \mathcal{L}(X)$. Considero o produto. $g \cdot h \in \mathcal{L}(Y) \cdot \mathcal{L}(W)$. Pela propriedade vista anteriormente, temos

$$\mathcal{L}(Y) \cdot \mathcal{L}(W) \subseteq \mathcal{Y} \cup \mathcal{W} = \mathcal{L}(X)$$

conseguimos mostrar que $g \cdot h \in \mathcal{L}(X)$ mas como $g, h \notin \mathcal{L}(X)$, segue que $\mathcal{L}(X)$ não é primo.

Reciprocamente, dado $\mathcal{L}(X)$ um ideal que não é primo, vamos mostrar que X é redutível.

Considere $g, h \in K[x_1, ..., x_n] - \mathcal{L}(X)$, tal que $g \cdot h \in \mathcal{L}(X)$. Logo, $\langle g \cdot h \rangle \subseteq \mathcal{L}(X)$, aplicando a variedade nos conjuntos temos

$$\mathcal{V}(\langle g \cdot h \rangle) \supseteq \mathcal{V}(\mathcal{L}(X)) = X$$

isso nos diz que $X \subseteq \mathcal{V}(g \cdot h) = \mathcal{V}(g) \cup \mathcal{V}(h)$

Usando uma propriedade básica de conjuntos temos

$$X = [\mathcal{V}(g) \cup \mathcal{V}(h)] \cap X$$
$$X = [\mathcal{V}(g) \cap X] \cup [\mathcal{V}(h) \cap X]$$

Vamos chamar $Y = \mathcal{V}(g) \cap X$ e $W = \mathcal{V}(h) \cap X$. Assim, já conseguimos mostrar que X pode ser escrito como união de duas variedades algébricas e que $Y \neq W$, agora vamos mostrar que $Y, W \subsetneq X$

Suponha por absurdo que

$$X = Y \Rightarrow X = \mathcal{V}(g) \cap X \Rightarrow X \subseteq \mathcal{V}(g) \Rightarrow \mathcal{L}(X) \supseteq \mathcal{L}(\mathcal{V}(g)).$$

Note que $\mathcal{L}(\mathcal{V}(g)) \supseteq \langle g \rangle$, pois tomando $h \in \langle g \rangle$, temos que $h = f \cdot g,\ f \in K[x_1, ..., x_n]$ tome

$$P \in \mathcal{V}(g) \Rightarrow h(p) = f(p) \cdot g(p) = h(p) \cdot 0 = 0 \Rightarrow h \in \mathcal{L}(\mathcal{V}(g))$$

logo, $g \in \langle g \rangle \subseteq \mathcal{L}(\mathcal{V}(g)) \subseteq \mathcal{L}(X) \Rightarrow g \in \mathcal{L}(X)$, o que é um absurdo, pois tomamos $g \in K[x_1, ..., x_n] - \mathcal{L}(X)$. Podemos repetir o processo de demonstração para verificar que $W \subsetneq X$. Provamos então que X é redutível. □

Exemplo 8. *Considere a parábola* $C = \mathcal{V}(y - x^2) \subseteq A^2_{\mathbb{R}}$. *Temos que* $\mathcal{L}(C) = \langle y - x^2 \rangle$. *Podemos definir o homomorfismo sobrejetor*

$$\psi : K[x, y] \longrightarrow k[x, x^2] = k[x]$$
$$x \longmapsto x$$
$$y \longmapsto x^2$$

Afirmação: $ker(\psi) = \mathcal{L}(C) = \langle y - x^2 \rangle$.

Considere $f \in \mathcal{L}(C) \Rightarrow f = h(x,y)(y-x^2)$, aplicando a ψ em ambos os lados, temos

$$\psi(f) = \psi(h(x,y)(y-x^2)) = \psi(h(x,y))\psi(y-x^2)$$

$$= h(x,x^2)(x^2-x^2) = h(x,x)\cdot 0 = 0$$

logo, $f \in ker(\psi)$. Reciprocamente, tome $f(x,y) \in ker(\psi)$ Usando a ordem reversa e o algoritmo da divisão temos

$$f(x,y) = (y-x^2)q + r(x,y)$$

onde $r(x,y) = 0$ ou $ml(y-x^2) = y \nmid \mathbb{M}_r$ logo temos que $r(x,y)$ depende apenas de x ou seja

$$f(x,y) = (y-x^2)q + r(x)$$

aplicando ψ e sabendo que f pertence ao núcleo

$$0 = f(x,x^2) = (x-x^2)q + r(x) \Rightarrow r(x) = 0$$

podemos concluir que

$$f(x,y) = (y-x^2)q \in \mathcal{L}(C)$$

Usando o teorema do isomorfismo, temos

$$A(C) = \frac{K[x,y]}{\mathcal{L}(C)} = \frac{K[x,y]}{\langle y-x^2\rangle} \cong K[x]$$

como $k[x]$ é um domínio de integridade, conclui-se $A(C)$ é domínio de integridade, e isso ocorre se, e somente se, $\mathcal{L}(C)$ é primo. Logo, $A(C)$ é irredutível.

Exemplo 9. *Considere $C = \mathcal{V}(x\cdot y) \subseteq A^2_{\mathbb{R}}$. Vimos que $\mathcal{V}(x\cdot y) = \mathcal{V}(x) \cup \mathcal{V}(y)$. Ou seja, C é redutível.*

Lema 2. *Toda família de variedades algébrica possui um elemento minimal, ou seja, se $(X_\lambda)_{\lambda\in L}$ é uma família de variedades algébricas, onde $X_\lambda \subseteq A^n_K$, para todo $\lambda \in L$, então existe $\lambda_0 \in L$, tal que $X_\lambda \subseteq X_{\lambda_0} \Rightarrow X_\lambda = X_{\lambda_0}$*

Demonstração. Seja $(X_\lambda)_{\lambda \in L}$ uma família de ideais, tal que para cada $\lambda \in L$ vale $X_\lambda = \mathcal{V}(I_\lambda)$, ou seja, X_λ são os zeros dos polinômios I_λ. Aplicando o lema de Zorn, temos que $(X_\lambda)_{\lambda \in L}$ possui um elemento maximal, digamos que tal elemento seja I_{λ_0} ou seja

$$\cdots \subseteq I_1 \subseteq \cdots \subseteq I_{\lambda_0}$$

aplicando a variedade algébrica em cada ideal e aplicando a propriedade de variedade algébrica, temos

$$\cdots \mathcal{V}(I_1) \supseteq \cdots \supseteq \mathcal{V}(I_{\lambda_0})$$

ou seja, temos que $X_{\lambda_0} = \mathcal{V}(I_{\lambda_0})$ é o elemento mínimo da família $(X_\lambda)_{\lambda \in L}$.

□

Teorema 4. *Toda variedade algébrica $X \subseteq A_K^n$ se expressa como união finita de subvariedades irredutíveis, isto é, $X = \bigcup_{i=1}^r X_i$ tal que cada $X_i \subseteq X$ é subvariedade, e $\mathcal{L}(X_i)$ é primo em $K[x_1, ..., x_n]$.*

Demonstração. Seja $\mathcal{F}$ uma família de variedades algébricas, tal que todo elemento de $\mathcal{F}$ não se expresse como união finita de subvariedades irredutíveis. Suponha por absurdo que $\mathcal{F} \neq \varnothing$. Ou seja, existem elementos em $\mathcal{F}$ que são redutíveis.

Pelo lema anterior, existem em $mathcalF$ um elemento minimal, digamos $Y \in \mathcal{F}$, em particular Y é redutível. Assim, existem $Z, W \subsetneq Y$ subvariedades próprias tal que $Y = Z \cup W$. Podemos perceber que $Z, W \notin \mathcal{F}$. Logo, Z e W podem ser escritos como união finita de subvariedades irredutíveis.

$$Z = \bigcup_{i=1}^{r} Z_i \quad e \quad W = \bigcup_{i=1}^{s} W_i$$

portanto,

$$Y = Z \cup W = Z_1 \cup \cdots \cup Z_r \cup W_1 \cup \cdots \cup W_s$$

Encontramos então um elemento de $\mathcal{F}$ que é escrito como união finita de subvariedades irredutíveis, o que é um absurdo, logo $Y \notin \mathcal{F}$.

A expressão $X = \bigcup_{i=1}^r X_i$ fornecida pelo teorema é chamado de composição de X em componentes irredutíveis. Como cada subvariedade X_i é irredutível, então o seu ideal de definição $\mathcal{L}(X_i)$ primo em $K[x_1, ..., x_n]$.

□

Exemplo 10. *Seja $X = \mathcal{V}(I) \subseteq A_{\mathbb{R}}^3$ uma variedade algébrica no espaço tridimensional definido por $\mathbb{R}$ e $I = \langle x \cdot y, x \cdot z \rangle \subseteq K[x, y, z]$.*

3 O TEOREMA DOS ZEROS DE HILBERT

A partir do conhecimento construído acerca de álgebra comutativa, variedades algébricas e ideal de definição, vamos dar início ao nosso maior objetivo neste trabalho. Neste capítulo, veremos o Teorema dos Zeros de Hilbert, também conhecido por seu nome alemão *nullstellensats*, assim como sua demonstração e consequências. Nosso objetivo é estabelecer uma relação entre álgebra comutativa e geometria algébrica.

3.1 Versão Fraca do Teorema dos Zeros de Hilbert

Antes de estudar o Teorema dos Zeros de Hilbert, serão apresentados alguns conceitos que irão nos auxiliar na demonstração do mesmo.

O procedimento através do qual obtemos o corpo $\mathbb{Q}$ a partir do anel $\mathbb{Z}$ no curso de introdução à álgebra, pode ser estendido a um domínio de integridade R, produzindo o corpo de frações de R. A construção consiste em tomar todos os pares (a, s) com $a \in R$ e $s \neq 0$, definir uma relação de equivalência entre tais pares:

$$(a, s) \equiv (b, s) \Leftrightarrow at - bs = 0$$

Notemos que este processo só é válido em domínios de integridade, pois a verificação do que esta relação é transitiva envolve o cancelamento de termos, isto é, o fato de R não possuir divisores de zero não nulos. Entretanto, pode ser generalizado.

Seja R um anel. Um sistema multiplicativo fechado de R é um subconjunto de R que não possui divisores de zero tal que $1 \in S$ e S é fechado em relação a multiplicação. Definimos uma relação de equivalência em $R \times S$, como

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0 \quad \textit{para algum } u \in S$$

Claramente, esta relação é reflexiva e simétrica. Basta verificar que a relação é transitiva, para isso supomos $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$. Queremos mostrar que $(a, s) \equiv (c, u)$. Para isso, dada estas relações, então existem $v, w \in S$ tal que $(at - bs)v = 0$ e $(bu - ct)v = 0$ assim $atv = bsv$ e $buw = ctw$ e

$$b = \frac{atv}{sv} = \frac{ctw}{uw} \Rightarrow \frac{atv}{sv} = \frac{ctw}{uv} \Rightarrow (au - cs)tvw = 0.$$

Como S é um sistema multiplicativo fechado, temos que $tvw \in S$, e portanto, $(a, s) \equiv (c, u)$. Desta forma, a relação $\equiv$ é transitiva.

Denotaremos por $\frac{a}{s}$ a classe de equivalência de (a, s) e por $S^{-1}R$ o conjunto desta classe de equivalência. Ao definir duas operações em $S^{-1}R$, denominada *soma*:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

e produto

$$\frac{a}{c} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Este conjunto passa a ter estrutura de anel. Vamos mostrar qu as operações estão bem definidas, isto é, pegar dois representantes da mesmas classe, fazer as duas operações com eles e verificar que o resultado é o mesmo. Tomemos então, $\frac{a}{s} \equiv \frac{a'}{s'}$ e $\frac{b}{t} \equiv \frac{b'}{t'}$. Assim,

$$\frac{a}{b} + \frac{s}{t} \equiv \frac{a'}{s'} + \frac{c'}{t'} \Rightarrow \frac{at + bs}{st} \equiv \frac{a't' + c's'}{s't'}$$

$$\Rightarrow (s't'(at + bs) - (a't' + c's')st)u = 0 \ (para \ algum \ u \in S)$$

$$\Rightarrow \frac{at + bs}{st} = \frac{a't' + b's'}{s't'}$$

e também

$$\frac{a}{s} \cdot \frac{b}{t} \equiv \frac{a'}{s'} \cdot \frac{b'}{t'} \Rightarrow \frac{ab}{st} \equiv \frac{a'b'}{s't'}$$

$$\Rightarrow (s't'(ab) - (a'b')(st))v = 0 \ (para \ algum \ v \in S)$$

$$\Rightarrow \frac{ab}{st} = \frac{a'b'}{s't'}$$

o anel $S^{-1}R$ é chamado anel de frações de R em relação a S. Em particular, se R é um domínio de integridade, temos que $S^{-1}R$, é corpo de frações de R, onde $S = R - \{0\}$

Construindo o corpo de frações, vamos para a seguinte definição:

Definição 15. *(Corpo de frações) Seja K um corpo. Chamamos corpo de frações do anel de polinômios $K[x_1, ..., x_n]$, o conjunto*

$$K(x_1, ..., x_n) = \left\{ \frac{f}{p}; f, p \in K[x_1, ..., x_n], p \neq 0 \right\}$$

Definição 16. *Sejam K um corpo e A um anel. Dizemos que A é uma K-álgebra ou um álgebra sobre o corpo K se A tem as três operações a seguir:*

$$+ : A \times A \longrightarrow A$$
$$(a, b) \longmapsto a + b$$

$$\cdot : A \times A \longrightarrow A$$
$$(a, b) \longmapsto a \cdot b$$

$$\cdot : A \times K \longrightarrow A$$
$$(a, \lambda) \longmapsto a \cdot \lambda$$

de modo que para $\lambda \in K$ e $a, b, c \in A$, tenhamos:

1. *A é um espaço vetorial sobre o corpo K;*
2. *$\lambda(ab) = a(\lambda b) = (\lambda a)b$;*
3. *$(a + \lambda b)c = ac + \lambda bc$ e também $a(b + \lambda c) = ab + a\lambda c$.*

Ou seja, uma K-álgebra (sendo K um corpo) é um conjunto híbrido, que tem estrutura de espaço vetorial, mas também tem estrutura de anel, ainda vale notar que o mesmo contém o copo K.

Exemplo 11. *Dada uma extensão de corpos $K \subset L$, vimos anteriormente que L pode ser visto como um K- espaço vetorial vetorial. Além disso, L satisfaz as outras dus condições, pois todo corpo é um anel. O que faz de L uma K-álgebra.*

Definição 17. *Seja A uma K-álgebra. Dizemos que A é finitamente gerado como K-álgebra se existem um número finito de elementos $a_1, ..., a_n \in A$, tal que*

$$A = K[x_1, ..., x_n] = \{f(a_1, ..., a_n); f \in K[x_1, ..., x_n]\}$$

onde $K[x_1, ..., x_n]$ é o anel de polinômios sobre K com n variáveis.

Lema 3. *(Lema de Zariski) Seja $K \subseteq L$ uma extensão de corpos. Se L é finitamente gerado como $K-$álgebra, então L é algébrico sobre K.*

A demonstração do lema de Zariski pode ser encontrada em (GONÇALVES,2010). O uso de tal lema será de grande importância para a demonstração do nullstellensatz.

Exemplo 12. *Temos que $R \subseteq \mathbb{C}$ é uma extensão de corpos. Por outro lado sabemos que $i = \sqrt{-1} \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$ pois é raiz do polinômio $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Note que $C = \mathbb{R}[i]$, logo pelo lema de Zariski, $\mathbb{C}$ é algébrico sobre $\mathbb{R}$. Esse fato pode ser verificado explicitamente. De fato, dado $z = a + b \cdot i \in \mathbb{C}$ arbitrariamente, considere $f_z(x) =\in \mathbb{R}[x]$, dado por $f_z(x) = (x - a)^2 + b^2$, daí temos que*

$$f_z(z) = ((a + b \cdot i) - a)^2 + b^2$$

$$= (b \cdot i)^2 + b^2 = 0$$

Portanto, $\mathbb{C}$ é algébrico sobre $\mathbb{R}$.

Lema 4. *Seja A um anel e $a_1, ..., a_n \in A$. Considere o ideal*

$$I = \langle x_1 - a_1, ..., x_n - a_n \rangle$$

de $A[x_1, ..., x_n]$. Para todo $f \in A[x_1, ..., x_n]$ existe $b \in A$ tal que $f - b \in I$.

Demonstração. Considere o isomorfismo de anéis

$$\varphi : A[x_1, ..., x_n] \to A[x_1, ..., x_n]$$

$$g \longmapsto g(x_1 - a_1, ..., x_n - a_n)$$

temos então que a inversa do homomorfismo é

$$\varphi^{-1} : A[x_1, ..., x_n] \longrightarrow A[x_1, ..., x_n]$$

$$g \longmapsto g(x_1 + a_1, ..., x_n + a_n)$$

como $f \in A[x_1, ..., x_n]$ então existe $g \in A[x_1, ..., x_n]$ tal que

$$f(x_1, ..., x_n) = g(x_1 - a_1, ..., x_n{-}_n)$$

seja $b \in A$ o termo independente do polinômio g. A igualdade acima implica que $f - b \in I$, pois ao fazer $g(x_1 - a_1, ..., x_n{-}_n) - b$ os termos independentes serão cancelados.

□

Proposição 12. *Sejam k um corpo e considere o ideal*

$$I = \langle x_1 - a_1, ..., x_n - a_n \rangle$$

de $K[x_1, ..., x_n]$onde $a_1, ..., a_n \in K$. Então

$$\psi : K \longrightarrow \frac{K[x_1, ..., x_n]}{I}$$

$$a \longmapsto \bar{a}$$

é um isomorfismo de anéis. Em particular $I = \langle x_1 - a_1, ..., x_n - a_n \rangle$ é ideal maximal de $K[x_1, ..., x_n]$

Demonstração. Claramente I é um ideal próprio de $K[x_1, ..., x_n]$. Por exemplo, $x_1 - a_1 + 1 \notin I$ mas $x_1 - a_1 + 1 \in K[x_1, ..., x_n]$.

Note que se $\in ker(\psi)$ então $\psi(a) = \bar{a} = \bar{0}$, ou seja $a - 0 \in I$, por outro lado, se $a \neq 0$, e $a \in K$, temos que $a \cdot a^{-1} = 1 \in I$, mas como I não é ideal próprio, concluímos que $a = 0$ ou seja $ker(\psi) = \{0\}$, eψ é injetiva.

Para mostrar que é sobrejetiva, vamos tomar $z \in \frac{K[x_1,...,x_n]}{I}$ e mostrar que $z \in Im(\psi)$. Para isso, considere z arbitrariamente, então existe $f \in K[x_1, ..., x_n]$ tal que $z = \bar{f}$, pelo lema anterior, vimos que $f - b \in I$ ou seja $\bar{f} = \bar{b} = \psi(b)$ ou seja, ψ é sobrejetiva.

Como $\frac{K[x_1,...,x_n]}{I}$ é isomorfo a um corpo, podemos afirmar que I é ideal maximal.

□

Corolário 4. *Seja $P = (a_1, ..., a_n) \in A^n_K$. Então,*

$$\mathcal{L}(P) = \langle x_1 - a_1, ..., x_n - a_n \rangle$$

Demonstração. Claramente $I = \langle x_1 - a_1, ..., x_n - a_n \rangle \subseteq \mathcal{L}(P)$, pois tomando $f \in \langle x_1 - a_1, ..., x_n - a_n \rangle$ temos que

$$f(x_1, ..., x_n) = (x_1 - a_1)h_1 + \cdots + (x_n - a_n)h_n$$

com $h_i \in K[x_1, ..., x_n]$, onde $i \in \{1, ..., n\}$ perceba que

$$f(a_1, ..., a_n) = (a_1 - a_1)h_1 + \cdots + (a_n - a_n)h_n$$

$$= 0h_1 + \cdots + 0h_n = 0$$

logo $f \in \mathcal{L}(P)$.

Por outro lado, como sabemos que I é um ideal maximal e conseguimos mostrar que

$$I \subseteq \mathcal{L}(P) \subseteq K[x_1, ..., x_n]$$

e $\mathcal{L}(P) \neq K[x_1, ..., x_n]$ a igualdade está devidamente mostrada.

□

O teorema dos zeros de Hilbert possui várias versões, o teorema que será enunciado a seguir é uma destas, e é conhecido como o teorema fraco da base de Hilbert.

Teorema 5. *(Versão fraca do teorema dos zeros de Hilbert) Seja K um corpo algebricamente fechado. Todo ideal $M \subseteq K[x_1, ..., x_n]$ é da forma*

$$M = \langle x_1 - a_1, ..., x_n - a_n \rangle$$

para cada $a_1, ..., a_n \in K$

Demonstração. Considere o anel $L = \frac{K[x_1,...,x_n]}{M}$. Como M é maximal, temos que L é corpo.Considere também o homomorfismo de anéis

$$\phi : K \longrightarrow L$$

$$a \longmapsto \bar{a}$$

Note que $\overline{K} = \{\bar{a}; a \in K\} \subset L$, pois podemos ver os elementos do corpo L como polinômios constantes. Note que $ker(\phi) = \{0\}$, pois dado $a \in Ker(\phi)$, então $a \in K$, já que $Ker(\phi)$ é subanel de K, mas pela mesma razão, temos que $\bar{a} = \bar{0}$, ou seja $a - 0 \in M \Rightarrow a \in M$. Portanto, $a \in K \cap M$.

Mas se isto acontece, temos então duas possibilidades para a. São elas: $a = 0$ ou $a \neq 0$. Suponha que $a \neq 0$, como $a \in K \cap M$, a seria invertível, isso significa que $a \cdot a^{-1} = 1 \in M$, mas se $1 \in M$ teríamos que $M = K[x_1, ..., x_n]$, o que contraria o fato de M ser um ideal maximal de $K[x_1, ..., x_n]$. Logo $Ker(\phi) = \{0\}$, temos então que ϕ é injetiva.

Chamando $\overline{K} := \phi(K)$ que é um subcorpo de L, note que a aplicação π é ϕ restrito a imagem

$$\pi : K \longrightarrow \overline{K}$$

$$a \mapsto \phi(a) = \bar{a}$$

é isomorfismo de anéis. E pelo teorema do isomorfismo, temos que $K \cong \bar{K}$, donde $K \subset L$ é uma extensão de corpos. Por outro lado $K[x_1, ..., x_n]$ é

finitamente gerada como $K-$álgebra , o que implica que L seja finitamente gerado como $K-$álgebra, pois L é quociente de $K[x_1, ..., x_n]$ por M.

Aplicando o lema de Zariski podemos afirmar que $K \subset L$ é algébrico. Dessa forma, temos que dado $a \in L \Rightarrow f(a) = 0$ para todo $f \in K[x_1, ..., x_n]$, mas sabemos que K é algebricamente fechado, logo $a \in K \Rightarrow L \subseteq K$, como já era conhecida a inclusão contrária. Segue que $L = K$

Logo, cada $x_i \in L$ com $i \in \{1, ..., n\}$ existe $a_i \in K$, tal que $\bar{x_i} = \bar{a_i} \Rightarrow \bar{x_i} - \bar{a_i} \in M$. Assim, $\langle x_1 - a_1, ..., x_n - a_n \rangle \subset M$. Porém, vimos que todo ideal do tipo $\langle x_1 - a_1, ..., x_n - a_n \rangle$ é maximal, e portanto

$$M = \langle x_1 - a_1, ..., x_n - a_n \rangle.$$

□

Corolário 5. *Seja K um corpo algebricamente fechado. Se $I \subsetneq K[x_1, ..., x_n]$ é um ideal próprio, então $\mathcal{V}(I) \neq \varnothing$*

Demonstração. Como I é ideal próprio de $K[x_1, ..., x_n]$, então usando o lema de Zorn, existe um ideal maximal $M \subseteq K[x_1, ..., x_n]$ tal que $I \subseteq M$. Assim, $\mathcal{V}(I) \supseteq \mathcal{V}(M)$. Mostrando que $\mathcal{V}(M) \neq \varnothing$, em particula estaremos mostrando que $\mathcal{V}(I) \neq \varnothing$. Claramente isso ocorre, pois

$$\mathcal{V}(M) = \mathcal{V}(\langle x_1 - a_1, ..., x_n - a_n \rangle) = \{a_1, ..., a_n\} \neq \varnothing.$$

□

Proposição 13. *Seja I um ideal radical de $K[x_1, ..., x_n]$, então $I \subseteq \mathcal{L}(\mathcal{V}(I))$*

Demonstração. Demonstração. Tome $h \in \sqrt{I}$, então existe $l \in \mathbb{N} - \{0\}$ tal que $h^l \in I$. Seja $p \in \mathcal{V}(I)$, segue que $h^l(p) = 0$, o que implica $(h(p))^l = 0$, mas como $K[x_1, ..., x_n]$ é domínio, temos que $h(p) = 0$. Logo $h \in \mathcal{L}(I)$ Como, $\sqrt{I} = I$, segue que $I \subseteq \mathcal{L}(\mathcal{V}(I))$.

□

Anteriormente, vimos que $\mathcal{V}(\mathcal{L}(X)) = X$. De certa forma $\mathcal{V}$ é uma inversa à esquerda de $\mathcal{L}$, que por sua ver é uma inversa à direita de $\mathcal{V}$. Naturalmente, suje a pergunta: O que é $\mathcal{L}(\mathcal{V}(I))$, com I um ideal do anel de polinômios $K[x_1, ..., x_n]$. Fato é que já respondemos parcialmente esta pergunta, pois para I um ideal radical qualquer em $K[x_1, ..., x_n]$ sabemos que $\sqrt{I} \subseteq \mathcal{L}(\mathcal{V}(I))$. A versão forte do teorema dos zeros de Hilbert é justamente provar a inclusão contrária, ou seja $\sqrt{I} \supseteq \mathcal{L}(\mathcal{V}(I))$.

Para provar a inclusão contrária, vamos precisar que K seja um corpo algebricamente fechado. Quando isso ocorre, teremos que $\mathcal{L}(\mathcal{V}(I)) = \sqrt{I}$, e evidentemente no caso em que I seja um ideal radical, teremos que $\mathcal{L}(\mathcal{V}(I)) = I$. Ou seja, nessas condições $\mathcal{L}$ será uma inversa à esquerda de V, que por sua vez será uma inversa à direita de $\mathcal{L}$.

A hipótese de que K seja algebricamente fechado não pode ser descartada. De fato, sabemos que $\mathbb{R}$ não é algebricamente fechado, devido ao fato de que alguns polinômios em $R[x]$ não possuem raízes em $\mathbb{R}$, o ideal $I = \langle x^2+1 \rangle \subset \mathbb{R}$ é próprio, mas $\mathcal{V}(I) = \varnothing$.

3.2 Teorema dos Zeros de Hilbert

Teorema 6. *(Teorema dos zeros de Hilbert) Sejam, K corpo algebricamente fechado. Se J é um ideal de $K[x_1, ..., x_n]$. Então, $\mathcal{L}(\mathcal{V}(J)) = \sqrt{J}$.*

Demonstração. Já sabemos que $\mathcal{L}(\mathcal{V}(I)) \supseteq \sqrt{I}$. Vamos mostrar a inclusão contrária, ou seja, $\mathcal{L}(\mathcal{V}(I)) \subseteq \sqrt{I}$. Como $K[x_1, ..., x_n]$ é um anel Noetheriano, então para todo ideal J no anel de polinômios, podemos escrever

$$J = \langle f_1, ..., f_r \rangle$$

onde $f_1, ..., f_r \in K[x_1, ..., x_n]$. Para mostrar tal inclusão, vamos usar uma ferramente chamada "truque de Rabinovich", que consiste em acrescentar uma variável no anel de polinômios.

Tome então g um elemento qualquer em $\mathcal{L}(\mathcal{V}(J))$, nosso objetivo é mostrar que $g \in \sqrt{J}$, ou seja $g^d \in J$, para algum $d \in \mathbb{N} - \{0\}$. Considere o corpo de frações do anrel $K[x_1, ..., x_n]$ o conjunto $L := K(x_1, ..., x_n)$.

Vamos considerar também um ideal no anel de polinômios com uma variável a mais que é similar ao ideal J. Considere J_0 o ideal de $K[x_1, ..., x_n, x_{n+1}]$ gerado por

$$J_0 = \langle f_1, ..., f_r, g \cdot x_{n+1} - 1 \rangle$$

note que J_0 tem os mesmos geradores de J, mas além disso também tem $(g \cdot x_{n+1} - 1)$ como seu gerador. Vamos denotar $g_1 := g \cdot x_{n+1} - 1$

Afirmação: $\mathcal{V}(J_0) = \varnothing$. Iremos demonstrar tal afirmação, pois pelo corolário do teorema fraco dos zeros de Hilbert, teremos que J_0 não é ideal próprio, ou seja ele será igual ao anel. Isso ocorre porque se J_0 fosse próprio teríamos $\mathcal{V}(J_0) \neq \varnothing$. Segue a demonstração da afirmação acima.

Suponha por absurdo que $\mathcal{V}(J_0) \neq \varnothing$. Tome $b \in \mathcal{V}(J_0)$, ou seja $b \in A_K^{n+1}$. Escreva $b = (b', b_{n+1})$, onde $b' \in A_K^n$ e $b_{n+1} \in K$. Observe que $f_i(b) = 0$, pois $b \in \mathcal{V}(J_0)$ e f_i é um dos elementos que geram J_0.

Mas por outro lado, como $f_i(b)$ é um polinômio em n variáveis ele não depende de b_{n+1}, ou seja $f_i(b) = f_i(b')$, pois b' tem n coordenadas, temos então que $f_i(b') = 0$, para todo $i \in \{1, .., r\}$. Ou seja $b' \in \mathcal{V}(J)$. Como $g \in \mathcal{L}(\mathcal{V}(J))$, tão g anula todos os pontos de $\mathcal{V}(J)$, em particular o ponto b'. Logo $g(b') = 0$. Note também que como $g_1 \in J_0$ e $b \in \mathcal{V}(J_0)$, então $g_1(b) = 0$. Portanto

$$g_1(b) = g_1(b', b_{n+1})$$

com $g \in K[x_1, ..., x_n]$, temos que o que responde pelos n primeiras variáveis é o polinômio g

$$g_1(b', b_{n+1}) = g(b') \cdot b_{n+1} - 1 = 0 \cdot b_{n+1} - 1 = 0 \Rightarrow -1 = 0$$

o que é uma contradição. Logo, $\mathcal{V}(J_0) = \varnothing$

Pela versão fraca do teorema dos zeros de Hilbert, segue que J_0 não é um ideal próprio do anel de polinômio, o que implica $j_0 = K[x_1, ..., x_n, x_{n+1}]$. Em particular, o polinômio 1 pode ser escrito como combinação dos geradores de J_0. Ou seja, existem $\alpha_1, ..., \alpha_n, \beta \in K[x_1, ..., x_n, x_{n+1}]$ tais que

$$1 = \langle f_1, ..., f_r, g \cdot x_{n+1} - 1 \rangle = \alpha_1 f_1 + \cdots + \alpha_r f_r + \beta(g \cdot x_{n+1} - 1)$$

chame $F_i := \alpha_i f_i \in (K[x_1, ..., x_n])[x_{n+1}] \subseteq L[x_{n+1}]$, para todo $i \in \{1, ..., r\}$

É importante observar que como $\alpha_i \in K[x_1, ..., x_n, x_{n+1}]$, então cada α_i é um polinômio em x_{n+1} com coeficientes em $(K[x_1, ..., x_n])$. Assim, $i \in \{1, ..., r\}$ podemos escrever

$$\alpha_i = \alpha_{i0} + \alpha_{i1} x_{n+1} + \cdots + \alpha_{id} x_{n+1}^d$$

onde $\alpha_{i0}, ..., \alpha_{id} \in K(x_1, ..., x_n)$. Note que α_i tem coeficientes em $K(x_1, ..., x_n)$ e é um polinômio em x_{n+1}.

Sabemos que tomamos um elemento $g \in \mathcal{L}(\mathcal{V}(J))$ e queremos mostrar que $g \in \sqrt{J}$, mas antes de tudo $g \in K[x_1, ..., x_n]$. Em particular, ele está no corpo L, pois L é o corpo de frações do anel. Temos então que considerar dois casos.

1. Se $g = 0$, temos imediatamente que $g \in \sqrt{J}$

2. Suponha que $g \neq 0$. Podemos então considerar $\frac{1}{g} \in L$

Para cada $i \in \{1, ..., r\}$, note que já vimos que F_1 está no anel de polinômios na variável x_{n+1} com coeficientes em L, podemos aplicar F_i em $\frac{1}{g}$.

$$F_i\left(\frac{1}{g}\right) = (\alpha_i f_i)\left(\frac{1}{g}\right) = (f_i\alpha_{i0} + f_i\alpha_{i1}x_{n+1} + \cdots + f_i\alpha_{id}x_{n+1}^d)\left(\frac{1}{g}\right)$$

é importante lembrar que nossa variável é x_{n+1}.Logo

$$F_i\left(\frac{1}{g}\right) = f_i\alpha_{i0} + f_i\alpha_{i1}\frac{1}{g} + \cdots + f_i\alpha_{id}\left(\frac{1}{g}\right)^d$$

vamos deixar a soma acima com o denominador g^d. Para isso, tome

$$u_i := \alpha_{i0}g^d + \alpha_{i1}g^{d-1} + \cdots + \alpha_{i(d-1)}g + \alpha_{id}$$

É importante perceber que $u_i \in K[x_1, ..., x_n]$, pois cada α_{ij} com $i \in \{1, .., n\}$ e $j \in \{1, ..., d\}$ foram obtidos em $K[x_1, ..., x_n]$ e $g \in K[x_1, ..., x_n]$. Assim,

$$F_i\left(\frac{1}{g}\right) = \frac{f_i u_i}{g^d}$$

por outro lado, vimos que

$$1 = \alpha_1 f_1 + \cdots + \alpha_r f_r + \beta(g \cdot x_{n+1} - 1)$$

o que implica que a igualdade acima está em $L[x_{n+1}]$.Temos uma igualdade de polinômios em $L[x_{n+1}]$, pois $1 \in L[x_{n+1}]$. Já que estes dois polinômios são iguais, se aplicarmos em ambos os lados $\frac{1}{g} \in L$. teremos:

$$1 = F_1\left(\frac{1}{g}\right) + \cdots + F_r\left(\frac{1}{g}\right) + \beta\left(\frac{1}{g}\right)(g \cdot \frac{1}{g} - 1)$$

$$= 1 = F_1\left(\frac{1}{g}\right) + \cdots + F_r\left(\frac{1}{g}\right)$$

$$= 1 = \frac{f_1u_1}{g^d} + \cdots + \frac{f_ru_r}{g^d} = \frac{f_1u_1 + \cdots + f_rur}{g^d}$$

ou seja

$$1 = \frac{f_1u_1 + \cdots + f_rur}{g^d} \Rightarrow g^d = f_1u_1 + \cdots + f_ru_r$$

note que $f_1u_1 + \cdots + f_ru_r \in \langle f_1, ..., f_r\rangle = J$. Provamos que uma potência de g está em J. Portanto $g \in \sqrt{J}$ como queríamos.

□

A demonstração acima foi feita pela primeira vez por Rabinovich. Este teorema de um certo modo pode ser visto como uma generalização do teorema fundamental da álgebra, que estabeleceu uma relação entre álgebra e geometria ao indicar que um polinômio de uma variável nos números complexos possui seu conjunto de raízes em $\mathbb{C}$, que é um objeto geométrico. Com base neste resultado, o nullstellensatz de Hilbert estabelece uma correspondência fundamental entre ideais do anel de polinômios e os subconjuntos do espaço afim. A seguir, veremos nos corolários deste teorema que é possível capturar a noção geométrica de uma variedade em termos algébricos.

Convenção:A partir de algora sempre que falarmos do corpo K, ele será algebricamente fechado, e vamos tomar $A = K[x_1, ..., x_n]$

Corolário 6. *Se I é um ideal radical do anel A, vale que $\mathcal{L}(\mathcal{V}(I)) = I$. Então existe uma correspondência bijetiva entre ideais radicais e variedades algébricas.*

Corolário 7. *Existe uma correspondência bijetiva entre ideias primos e variedades algébricas irredutíveis.*

Corolário 8. *Os ideias maximais correspondem a pontos.*

Corolário 9. *Seja $f \in A$, e $f = f_1^{n1} \cdots f_r^{nr}$ a composição de f em fatores irredutíveis. Então $\mathcal{V}(f) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_r)$ é a decomposição de $\mathcal{V}(f)$ em componentes irredutíveis, e $\mathcal{L}(\mathcal{V}(f)) = \langle f_1, ..., f_r \rangle$. Então existe uma bijeção entre polinômios irredutíveis $f \in A$ e hipersuperficies irredutíveis em A_K^n.*

Essas correspondências vistas nas consequências do teorema dos zeros de Hilbert nos diz que informações algébricas geram informações geométricas e informações geométricas geram informações algébricas, ou seja, foi estabelecida uma ponte que liga a álgebra e a geometria.

4 CONCLUSÃO

Diante dos argumentos mostrados e resultados vistos, conseguimos chegar ao nosso propósito neste texto, como principal alvo, determinamos a existência de uma correspondência bijetiva entre ideais radicais e variedades algébricas definidas em um corpo algebricamente fechado, ou seja determinamos uma ligação entre a álgebra e a geometria. Em particular, conseguimos

mostrar que em cada ponto no espaço afim existe um ideal maximal que o define e não menos importante, conseguimos mostrar que para cada variedade algébrica irredutível existe um único ideal primo que a define, e por fim para cada hipersuperfície irredutível existe um único polinômio irredutível que a define. Além disso, em nosso trabalho podemos citar alguns objetivos que também eram almejados, tais como: Ter uma ideal inicial sobre álgebra comutativa com o estudo de anéis e ideais, e apresentar o conceito inicial acerca da geometria algébrica com o estudo de variedades algébricas, hipersuperfície, ideal de definição e etc.

Fica claro que no texto tentamos fazer uma ligação entre os elementos básico de álgebra comutativa que são vistos na grade curricular dos cursos de matemática com os elementos da geometria algébrica vista nos cursos de mestrado e doutorado. É importante salientar que os conteúdos explícito acerca de geometria algébrica é apenas uma pequena introdução do tema, tal conteúdo pode ser entendido para tópicos como: Álgebra reduzida, estudo local de uma variedade, regularidade e singularidade, normalização conjuntos algébricos projetivos e etc. espera-se que o leitor sinta-se motivado para desbravar as fontes da geometria algébrica.

Para finalizar, esperamos que a linguagem, observações e demonstrações presentes no texto tenham ajudado o leitor a compreender os resultados.

5 APÊNDICE

5.1 Anel

Definição 18. *(Anel) Um conjunto $A \neq \emptyset$, munido de duas operações binárias soma $(+)$ e produto $(\cdot)$, é dito um anel se para todo $a, b, c \in A$ são satisfeitas as seguintes condições:*

1. $a + b \in A$ (Fechamento da soma)
2. $a \cdot b \in A$ (Fechamento do produto)
3. $a + b = b + a$ (Comutatividade da soma)
4. $(a + b) + c = a + (b + c)$ (Associatividade da soma)
5. Existe $0_A \in A$ tal que $a + 0_A = 0_A + a = a$ (Existência de elemento neutro)
6. Para cada $a \in A$ existe $(-a) \in A$, tal que $a + (-a) = (-a) + a = 0_A$ (Simétrico da soma)
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associatividade do produto)
8. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (Distributividade à esquerda)
9. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (Distributividade à direita)

A será um anel e vamos denotar $(A, +, \cdot)$.

Exemplo 13. *O conjunto dos números inteiros é anel.*

Exemplo 14. *O conjunto abaixo é um anel com as operações diferentes das usuais.*

Seja $(A, +, \cdot)$ um anel, para todo $a, b \in A$ defina duas operações binárias com

$$+ : A \times A \longrightarrow A$$
$$a \oplus b = a + b + 1$$

e

$$\cdot : A \times A \longrightarrow A$$
$$a \odot b = a \cdot b + a + b$$

Proposição 14. *Seja A um anel, são válidas as seguintes propriedades.*

1. O elemento neutro 0_A é único;
2. O simétrico do elemento a é o elemento $(-a)$ que por sua vez é único;
3. Se $a + x = a + y$. Então, $x = y$.

Demonstração. Queremos mostrar que as propriedades acima são válidas.

1. Suponha que $0_A \in A$ não seja o único elemento neutro do anel A, ou seja, existe $0'_A \in A$ tal que $0'_A + a = a$, para todo $a \in A$, isso significa que $0_A + a = 0'_A + a = a$ e como A é um anel, existe $-a \in A$ tal que $a + (-a) = 0_A$. usando o fato de A ser anel, vamos somar $(-a)$ e associá-lo ao a em todas as igualdades, temos

$$0_A + [a + (-a)] = 0'_A + [a + (-a)] = a + (-a)$$

   assim

$$0_A + 0_A = 0'_A + 0'_A \Leftrightarrow 0_A = 0'_A$$

   logo $0_A = 0'_A$, isso nos dá que o 0_A é único.

2. Suponha que $(-a) \in A$ não seja único, ou seja, existe $(-a') \in A$ tal que $a + (-a') = 0_A$, assim como $a + (-a) = 0_A$, segue das igualdades e do fato de A ser um anel

$$(-a') + a = 0_A = (-a) + a$$

   somando $(-a')$ em ambos os lados

$$(-a') + [a + (-a')] = (-a) + [a + (-a')]$$

$$\Leftrightarrow -a' + 0_A = -a + 0_A \Leftrightarrow a' = a$$

   logo o simétrico da soma é único.

3. Dados $a, x, y \in A$ com a igualdade $a + x = a + y$, como A é anel, basta operar com o simétrico da soma de a

$$a + x = a + y$$

$$= [(-a) + a] + x = [(-a) + a] + y$$

$$= 0_A + x = 0_A + y \Rightarrow x = y.$$

□

Além de satisfeitas as nove condições acima, existem alguns tipos de anéis especiais onde são satisfeitas outras três condições para todo $a, b, c \in A$.

1. Existe $1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a$ (Anel com unidade)
2. $a \cdot b = b \cdot a$ (Anel comutativo)
3. Dado $a \cdot b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$ (Anel sem divisores de zero)

convenção: Iremos denotar $a \cdot b$ por ab sempre que não houver possibilidade de confusão.

Definição 19. *Seja $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um domínio de integridade (DI).*

Exemplo 15. $A = \mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1}, a, b \in \mathbb{Z}\}$

Se $a = (a_1 + a_2\sqrt{(-1)}), b = (b_1 + b_2\sqrt{(-1)}) \in \mathbb{Z}[\sqrt{-1}]$ definimos a soma por

$$a + b = (a_1 + b_1) + (a_2 + b_2)\sqrt{-1}$$

e o produto por

$$a \cdot b = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{-1}$$

é um anel comutativo e com unidade, chamado de Anel de Gauss.

Observação 4. *Em geral, se $d \in \mathbb{Z}$ não é um quadrado, então*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}, a, b \in \mathbb{Z}\}$$

é um anel comutativo com unidade.

Exemplo 16. *O conjunto $2\mathbb{Z} = \{2x, x \in \mathbb{Z}\}$ é um exemplo de anel comutativo, mas que não tem unidade.*

Definição 20. *(Corpo) Um anel K é um corpo quando o mesmo é comutativo, com unidade e todos os seus elementos diferentes de zero possuem inverso multiplicativo em K, isto é, dado $a \in k - \{0_K\}$ existe $a^{-1} \in k - \{0_k\}$, tal que*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1_K.$$

Exemplo 17. *Os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.*

Proposição 15. *Todo corpo K é domínio de integridade.*

Demonstração. Como K é corpo, temos de imediato que o anel A satisfaz as condições de anel comutativo com unidade. Agora, basta mostra que ele também é sem divisores de zero. suponha $a, b \in k - \{0_K\}$, e tome o seguinte produto em K, $a \cdot b = 0_k$, estamos supondo que a e b são divisores de zero. Como K é um corpo, sabemos que todos os elementos de $k - \{0_K\}$ possui inverso multiplicativo, logo

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K \Leftrightarrow 1_k \cdot b = 0_K \Leftrightarrow b = 0_k$$

observe que $b = 0_K$ é um absurdo, pois supomos $a, b \in k - \{0_K\}$. Chegamos a conclusão que K é sem divisor de zero. Portanto, K é domínio de integridade. □

Observação 5. *A reciproca da proposição anterior (Todo domínio de integridade é um corpo) não é verdadeira. Basta tomar o conjunto dos números inteiros, o mesmo é um domínio de integridade, mas não é um corpo.*

Convenção: Para a continuidade do nosso estudo, até o final deste trabalho, iremos supor que que todos os anéis arbitrários em questão serão comutativos e com unidade. Além disso, sempre que não houver confusão, iremos denotar o elemento neutro do anel A em relação a soma (0_A) como 0, tal qual o elemento neutro do produto (1_A) como 1.

Definição 21. *(Subanel) Dizemos que um subconjunto B de A é um subanel. Se B, restritos as operações de A também é uma anel.*

Proposição 16. *Seja A um anel e seja B um subconjunto de A. Então, B é um subanel de A se, e somente se as seguintes condições são verificadas*

(i) $0_A \in B$

(ii) Dado $x, y \in B \Rightarrow x - y \in B$

(iii) Dado $x, y \in B \Rightarrow x \cdot y \in B$.

Exemplo 18. *$\mathbb{Z}$ é subanel de $\mathbb{Q}$ que por sua vez é subanel de $\mathbb{R}$.*

Observação 6. *O conjunto $B = \{2k + 1; k \in \mathbb{Z}\}$ não é um subanel de $\mathbb{Z}$.*

Iremos trabalhar com polinômios com n variáveis e coeficientes de um anel A qualquer.

Definição 22. *Uma sequência de elementos de um conjunto A é uma função $a : \mathbb{N} \longrightarrow A$, que associa cada número natural n a um elemento $a_n \in A$.*

Observação 7. *Um polinômio numa variável sobre A é uma sequência*

$$(a_0, a_1, ..., a_n, ...)$$

ou simplesmente $(a_n)_{n\in\mathbb{N}}$.

Definição 23. *Seja $(A, +, \cdot)$ um anel. Um polinômio numa variável sobre A é uma sequência $(a_0, a_1, ..., a_k, 0, ..., 0)$, onde $a_i \in A$ para todo índice e $a_i = 0$ para um certo $k \in \mathbb{N}$, onde $a_k, ..., a_1, a_0$ são chamados de coeficientes do polinômio.*

Exemplo 19. *A sequência $(3, 3, ..., 3, ..., 3)$ não é o mesmo que o conjunto $\{3\}$, trata-se de um polinômio onde todos os seus coeficientes são iguais a 3.*

Observação 8. *Caso $m = 0$ dizemos que p é um polinômio constante, nesse caso temos que $p = (a, 0, ..., 0)$ e podemos escrever $p = a$. A partir disso, podemos concluir que o anel A está contido no conjunto dos polinômio com uma variável sobre A, pois os elementos de A são polinômios constantes.*

Seja $p = (a_n)_n$ um polinômio em uma variável sobre o anel A, caso $a_n = 0$ para qualquer $n \in \mathbb{N}$, então dizemos que p é o polinômio nulo, $p = 0$.

Seja A' o conjunto de todos os polinômios em uma variável sobre A, dados dois elementos $f = (a_0, a_1, ...)$ e $g = (b_0, b_1...)$. Podemos definir as operações de soma e produto respectivamente em A'

$$+ : A' \times A' \longrightarrow A'$$

$$(f, g) \longmapsto \sum_{i=0}^{r} (a_i + b_i)$$

e o produto

$$\cdot : A' \times A' \longrightarrow A'$$

$$(f, g) \longmapsto f \cdot g = \sum_{i=0}^{m+n} c_i, \quad onde \quad c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

e fácil verificar que o polinômio numa variável sobre A é um anel onde

1. O elemento neutro da soma é o elemento $(0, 0, ...)$.

2. O elemento neutro do produto é o elemento $(1, 0, ...)$.

3. o inverso de $(a_0, a_1, ..., a_n, ...)$ com respeito a operação da soma é o elemento $(-a_0, -a_1, ..., -a_n, ...)$.

Observe que a multiplicação de A' é comutativa, pois a multiplicação em A é comutativa.

Se $(a_0, a_1, ...)$ é um elemento de A', então $(a_0, a_1, ...)^n$ designará o elemento

$$\underbrace{(a_0, a_1, ...) \cdot (a_0, a_1, ...) \cdot \cdots \cdot (a_0, a_1, ...)}_{n-vezes}.$$

Observação 9. *Por razões de ordem prática, vamos utilizar o símbolo x para de signar o elemento $(0, 1, 0, ...)$. Também, no lugar de escrever $(a_i, 0, ...)$, vamos escrever a_i; assim, o símbolo a_i vai ser usado para representar duas coisas distintas:o elemento a_i de A e o elemento $(a_i, 0, ...)$ de A'; no entanto, isto não vai criar confusão. Com essa convenção, o elemento $(a_0, a_1, ..., a_n, ...)$ é igual a soma $a_0 + a_1x + \cdots + a_nx^n$, onde a_ix^i designa $a_i \cdot x^i$, então*

$$A' = \left\{ \sum_{i=1}^{n} a_i x^i ; n \in \mathbb{N}, a_i \in A \right\}.$$

As operações com esse anel são as usuais. Vamos denotar o anel $(A', +, \cdot)$ por $A[x]$, e chamá-lo de anel de polinômios em uma variável sobre A.

Exemplo 20. *Dados $f, p \in \mathbb{Z}[x]$ com $f(x) = 2+2x+3x^2+x^3$ e $g(x) = x+x^3$ Para $f = (2, 2, 3, 1)$ e $g = (0, 1, 0, 1)$, temos que $(f + g) = (2, 3, 3, 2)$ e no produto $(f \cdot g) = (2, 2, 5, 3, 3, 1)$.*

Definição 24. *Seja A um anel e seja $p(x) := a_nx^n + \cdots + a_1x + a_0 \in A[x]$ com $a_n \neq 0$. O número natural n se chama grau de $p(x)$ e denotaremos como $\partial(p) = n$. O coeficiente a_n chama-se coeficiente líder de $p(x)$. Quando o coeficiente líder for igual a 1, o polinômio é dito mônico.*

Observação 10. *De acordo com a definição acima, podemos concluir que o polinômio nulo não tem grau. Normalmente, escrevemos $\partial(p = 0) < -\infty$.*

Observação 11. *Seja A um domínio de integridade. Dados dois polinômios $f, p \in A[x]$ temos que $\partial(p \cdot f) = \partial(p) + \partial(f)$.*

Proposição 17. *Se A é um domínio de integridade, então $A[x]$ também é.*

Demonstração. Sejam $f, p \in A[x] - \{0\}$, como A é domínio de integridade, então $\partial(p \cdot f) = \partial(p) + \partial(f)$. Seja então $\partial(p) = n$ e $\partial(f) = m$ temos que $\partial(p \cdot f) = m + n$, daí o grau de $f \cdot p$ existe, e nesse caso será $n + m$ e portanto, $f \cdot p \neq 0$. Como $f \cdot p \neq 0$, temos que $A[x]$ é domínio de integridade.

□

Corolário 10. *Se A é domínio de integridade, então $A[x_1, ..., x_n]$ também é.*

Demonstração. Por indução sobre n. Para $n = 1$, temos a proposição acima. Se $n = 2$, temos $(A[x_1])[x_2]$. Como $(A[x_1])$ domínio de integridade, então $(A[x_1])[x_2]$ também é. Suponha que $A[x_1, ..., x_{n-1}]$ seja domínio de integridade, como

$$A[x_1, ..., x_n] = (A[x_1, ..., x_{n-1}])[x_n]$$

concluímos que $A[x_1, ..., x_n]$ é domínio de integridade.

□

Observação 12. *Por outro lado, mesmo que A seja um corpo, $A[x_1, ..., x_n]$ não será, pois neste caso os únicos elementos invertíveis em $A[x_1, ..., x_n]$ são os polinômios constantes.*

Definição 25. *Seja $A[x]$ um anel. $f(x) \in A[x] - \{0\}$, diz-se que $\alpha \in A$ é rais de $f(x)$ se $f(\alpha) = 0$.*

Exemplo 21. *Seja $f(x) \in \mathbb{Q}[x]$ tal que $f(x) = 7x^2 - 4x + \frac{1}{4}$ tem como raiz os números racionais $\frac{1}{2}$ e $\frac{1}{4}$.*

Observação 13. *Seja A um anel. Em alguns casos podemos encontrar um polinômio em $A[x]$ que não possui raízes em A e sim em um anel que contem A.*

Note que o polinômio $p(x) = x^2 + 1 \in \mathbb{R}[x]$, tem como raízes os números imaginários i e $-i$. Futuramente, iremos tratar de casos como este.

Teorema 7. *(Algoritmo da divisão em $K[x]$) Sejam $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que*

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = o$ ou $\partial(r) < \partial(g)$.

Demonstração. Primeiro, vamos mostrar a existência do algoritmo da divisão. Para isso, sejam $f(x) = a_0+a_1x+\cdots+a_nx^n$ e $g(x) = b_0+b_1x+\cdots+b_nx^n$. Se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponha $f(x) \neq 0$. Assim, $\partial(f) = n$. Caso $n < m$ basta tomar $q(x) = 0$ e $r(x) = f(x)$. Assim, podemos assumir $n \geqslant m$.

Seja $f_1(x)$ o polinômio definido por:

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x)$$

note que $\partial(f_1) < \partial(f)$. Vamos aplicar indução sobre o $\partial(f) = n$ para demonstrar o teorema.

Se $n = 0$, $n \geq m \Rightarrow m = 0$, logo $f(x) = a_0 \neq 0, g(x) = b_0 \neq 0$ e temos que $f(x) = a_0 b_0^{-1} \cdot g(x)$, basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$, teremos $f(x) = a_0 b_0^{-1} b_0 = a_0$. Terminamos o primeiro paço de indução.Pela igualdade acima

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x)$$
$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$$

onde $\partial(f_1) < \partial(f) = n$, podemos então aplicar a hipótese de indução (segunda forma). Ou seja, existem $q_1(x), r_1(x)$, tais que:

$$f_1(x) = q_1(x)g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\partial(r_1) < \partial(g)$. Substituindo $f_1(x)$ na equação acima

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x)$$

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + [q_1(x)g(x) + r_1(x)]$$

$$f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m})g(x) + r_1(x)$$

quando tomamos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$, temos que

$$f(x) = q(x)g(x) + r(x)$$

onde $r(x) = 0$ ou $\partial(r) < \partial(g)$. Assim, está provada a existência do algoritmo da divisão para polinômios. A seguir, vamos mostrar que esta divisão é única.

Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ tais que:

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

onde $r_i(x) = 0$ ou $\partial(r_i) < \partial(g), i \in \{1, 2\}$. Note que

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

$$[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$$

mas se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da equação é maior que o grau de g, pois vamos somar os graus e ele será maior que m. Como $\partial(r_1), \partial(r_2) < \partial(g)$, claramente $\partial(r_1 - r_2) < \partial(g)$. O que é uma contradição, pois temos a igualdade entre polinômios e o polinômio do lado esquerdo da equação tem grau diferente do polinômio do lado direito da equação. Logo $q_1(x) = q_2(x)$.

Vamos usar o fato que $q_1(x) = q_2(x)$ na seguinte igualdade

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x)$$

concluímos por transitividade que $r_1(x) = r_2(x)$. Assim, está provado o teorema do algoritmo da divisão para polinômios em $k[x]$.

□

Exemplo 22. *Considere o polinômio $f = x^3 + 3x^2 + x$ e $g = x^2 + 2$. Vamos fazer a divisão de f por g*

$$f = x^3 + 3x^2 + x = \underbrace{(x^2 + 2)}_{g} \cdot \underbrace{(x + 3)}_{q} + \underbrace{(-x - 6)}_{r}$$

5.2 Anel de Polinômios em Várias Variáveis

Nosso objetivo é estudar o anel de polinômios em várias variáveis, compreender como são seus elementos e estender a noção aprendida em polinômios em uma variável, entender as ordens monomiais com o objetivo de compreender o algoritmo da divisão em várias variáveis.

Definição 26. *Seja $K[x_1, ..., x_n]$, um elemento f do anel de polinômios em várias variáveis é definido como*

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha i}$$

com $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, $a_\alpha \in K$ e $J \subseteq \mathbb{N}^n$ finito.

Definição 27. *Um termo* $K[x_1, ..., x_n]$ *é um elemento da forma* $a_\alpha \prod_1^n x_i^{\alpha i}$ *com* $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$. *O elemento* $a_\alpha \in K$ *do termo é chamado de coeficiente do termo e* $\prod_1^n x_i^{\alpha i}$ *é denominado monômio. chamamos de grau(total) do monômio* $\prod_1^n x_i^{\alpha i}$ *o numero natural dado por* $\partial(\prod_1^n x_i^{\alpha i}) = \sum_{i=1}^n \alpha_i$.

Definição 28. *Se* $f \in K[x_1, ..., x_n]$ *é não nulo, vamos denotar*

$$\mathbb{M}(f) = \left\{ \prod_{i=1}^n x_i^{\alpha i} : a_\alpha \neq 0 \right\}$$

o conjunto de todos os monômios de f.

Para isso, vamos precisar definir uma relação de ordem.

5.3 Ordem Monomial

Sabemos que nosso objetivo é apresentar o algoritmo da divisão em $K[x_1, ..., x_n]$, devemos analisar cada passo do algoritmo para que possamos resolver todos os obstáculos que podem ser encontrados.

Para dar inicio ao nosso foco, precisamos determinar o termo líder de um polinômio $f \in K[x_1, ..., x_n]$. Isso se faz necessário pois precisamos determinar a ordem de um polinômio em relação a outro. Além disso, precisamos generalizar o coeficiente líder.

Definição 29. *O conjunto de todos os monômios de* $K[x_1, ..., x_n]$ *será denotado por*

$$\mathbb{M}_n = \left\{ \prod_{i=1}^n x_i^{\alpha i}; \alpha_1, ..., \alpha_n \in K \right\}$$

$x_1^0 \cdots x_n^0$ *será denotado por* 1.

É natural que quando estamos trabalhando com o anel $K[x_1, ..., x_n]$ tentamos utilizar o conceito de grau que temos no anel $K[x]$. Vejamos o seguinte exemplo.

Exemplo 23.

$$x^2yz^2 + x^2y^2z + 3x^4y + 3x^3y^2 - y^4z + 2x^4z$$

Usando o conceito de grau que definimos em $K[x]$ *percebemos que os monômios têm o mesmo grau. Por conta de problemas como este, é necessário estudarmos ordens monomiais para determinar o maior elemento em* $K[x_1, ..., x_n]$.

Definição 30. *(Relação Parcial de Ordem) Um conjunto $A \neq \varnothing$ é dito parcialmente ordenado se tiver munido de uma relação binária $\preceq$, satisfazendo as seguintes condições para quaisquer $x, y, z \in A$:*

(i) $a_1 \preceq a_1$. *(reflexiva);*

(ii) $a_1 \preceq a_2$ *e* $a_2 \preceq a_3$, *então* $a_1 \preceq a_3$. *(transitividade);*

(iii) $a_1 \preceq a_2$ *e* $a_2 \preceq a_1$, *então* $a_1 = a_2$. *(anti-simétrico).*

Se $a_1 \preceq a_2$, mas $a_1 \neq a_2$, então indicaremos $a_1 \prec a_2$

Exemplo 24. *O conjunto $\mathbb{Z}$ é um conjunto que parcialmente ordenado.*

Observação 14. *Uma relação de ordem sobre o conjunto A é total quando para todo $a_1, a_2 \in A$ tivermos*

(iv) $a_1 \prec a_2, a_2 \prec a_1$ *ou* $a_1 = a_2$. *(tricotomia).*

Queremos definir uma relação sobre $\mathbb{M}_n$ que seja total, pois com ela teremos bem definido o conceito de termo líder de um elemento

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha i} \neq 0$$

de fato, podemos definir o monômio líder $ml(f)$ da seguinte forma

$$ml(f) = max \left\{ \prod_{i=1}^{n} x_{i=1}^{\alpha i} \right\} \in \mathbb{M}_n(f)$$

onde o máximo é tomado com respeito à ordem $\preceq$ fixada e considerando o termo líder de f como $a_\alpha \cdot mf(f)$, isto é $tl(f) = a_\alpha \cdot ml(f)$. Precisamos nos atentar a outros pontos que existem em $K[x]$ quando trata-se da divisão de dois polinômios f e g.

Considere

$$tl(f) = a_\alpha \prod_{i=1}^{n} x_i^{\alpha i} \text{ e } tl(g) = a_\beta \prod_{i=1}^{n} x_i^{\beta i}$$

devemos verificar se $tl(g) | tl(f)$, isto é, se existe

$$m_1 = \prod_{i=1}^{n} x_i^{\gamma i} \in \mathbb{M}_n$$

e $a_\gamma \in K$ tais que

$$tl(f) = a_\gamma \cdot m_1 \cdot tl(g)$$

ou equivalentemente

$$a_\alpha \prod_{i=1}^{n} x_i^{\alpha i} = \left(a_\gamma \prod_{i=1}^{n} x_i^{\gamma i} \right) \left(a_\beta \prod_{i=1}^{n} x_i^{\beta i} \right).$$

Isso ocorre se, e somente se, $\beta_i \leq \alpha_i$, para todo $i = 1, ..., n$. Nos casos em que isso ocorre, devemos calcular $f - a_\gamma \cdot m_1 \cdot g$ e repetir o argumento para os resultados obtidos. Devemos nos lembrar que no caso de polinômios em $K[x]$, encontramos

$$\partial(f - a_\gamma \cdot m_1 \cdot g) < \partial(f)$$

que podemos reescrever utilizando a noção monomial, como

$$ml(f - a_\gamma \cdot m_1 \cdot g) \prec ml(f)$$

devemos nos atentar a uma propriedade que aparentemente é simples, mas muito importante, que se esconde nessas condições, ou seja, nas expressões

$$tl(f) = a_\gamma \cdot m_1 \cdot g \; e \; ml(a_\gamma \cdot m_1 \cdot g) \prec ml(f).$$

De fato, a última condição nos mostra que se $m_2 \in \mathbb{M}(g) \; e \; m_2 ml(g)$, então $m_1 \cdot m_2 \prec m_1 \cdot ml(g) = ml(f)$ou seja, uma ordem total sobre $\mathbb{M}_n$ deve ser compatível com o produto. Em outras palavras, se $m_1, m2 \in \mathbb{M}_n$ são tais que $m_1 \preceq m_2$ então

$$m_1 \cdot m_3 \preceq m_2 \cdot m_3 \; \forall m_3 \in \mathbb{M}_n.$$

Um dos últimos, mas não menos importante aspectos do algoritmo da divisão, é garantir que o processo de divisão seja finito, devemos ter esta garantia para conseguimos finalizar esta etapa, sabemos que

$$ml(f - a_\gamma \cdot m_1 \cdot g) \prec ml(f)$$

em cada etapa do algoritmo, que pode ser representado de modo , se requisitarmos que a ordem total $\preceq$ sobre $\mathbb{M}_n$ seja uma boa ordem, isto é, que todo subconjunto de $\mathbb{M}_n$ possua um menor elemento com respeito à $\preceq$. Portanto o algoritmo tem que parar em algum momento.

Vamos considerar sobre $\mathbb{M}_n$ ordens que possuem as propriedades que destacamos acima.

Definição 31. *(Ordem monomial) Uma ordem monomial $\preceq$ sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:*

(i) Se $m_1, m_2 \in \mathbb{M}_n$ são tais que $m_1 \prec m_2$, então $m_1 \cdot m_3 \preceq m_2 \cdot m_3$ para todo $m_3 \in \mathbb{M}_n$;

(ii) Todo subconjunto não vazio de $\mathbb{M}_n$ admite um menor elemento com respeito à $\preceq$.

Lema 5. *Seja $\preceq$ uma ordem monomial em $K[x_1, ..., x_n]$, então qualquer sequência decrescente (com respeito à $\preceq$) de monômios é finita.*

Demonstração. Seja $m_1 \succeq m_2 \succeq m_3 \succeq ...$ uma sequência decrescente de elementos de $\mathbb{M}_n$, então $S = \{m_1, m_2, m_3, ...\} \neq \varnothing$ admite uma menor elemento com respeito à $\preceq$, ou seja, a sequência é finita.

□

Agora que sabemos como ordenar monômios em uma variável, vamos ordenar monômios em $K[x_1, ..., x_n]$ usando a mesma ideia. Considere $f \neq 0$, tal que $f \in K[x_1, ..., x_n]$, podemos considerar $f \in (k[x_2, ..., x_n])[x_1]$ou seja, como um polinômio em x_1 com coeficientes em $K[x_2, ..., x_n]$. Vamos usar o argumento indutivo sobre o número de variáveis e tentar ordenar os monômios em $K[x_1, ..., x_n]$ do mesmo modo.

Exemplo 25. *considere*

$$f = x^2y^3z^2 + x^2y^2z^4 + 3x^4yz^5 - y^4z + 2x^4z + x^2 2y^2z$$

considere que $f \in k[x, y, z]$, vamos ordena-lo de modo que consideremos os coeficientes em $k[y, z]$, ordenando pelo grau de x

$$f = (3yz^5 + 2z)x^4 + (3y^2 + 2y^2z)x^3 + (y^3z^2 + y^2z^4)x^2 - y^4z$$

Agora considerando que são elementos em $K[y, z]$, com polinômios em y com coeficientes em $k[z]$. Vamos ordená-lo considerando os coeficientes em $K[z]$ e com grau em y

$$f = (3yz^5 + 2z)x^4 + ((2z + 3)y^2)x^3 + (z^2y^3 + z^4y^2)x^2 - zy^4$$

vamos fazer a multiplicação indicada acima, e usando a indicação de ordenar monômios listando suas potências em x, seguido por y e por fim z vamos obter

$$f = 3x^4yz^5 + 2x^4z + 2x^3y^2z + 3x^3y^2 + x^2y^3z^2 - y^4z$$

Perceba que aos determinar os passos acima, o que fizemos foi ordenar os monômios de tal modo que

$$x^{\alpha 1}y^{\alpha 2}z^{\alpha 3}$$

preceda

$$x^{\beta 1}y^{\beta 2}z^{\beta 3}$$

assim,

$$x^{\alpha 1}y^{\alpha 2}z^{\alpha 3} \preceq x^{\beta 1}y^{\beta 2}z^{\beta 3}$$

e isso acontece se, e somente se,

(i) $\alpha_1 < \beta_1$ ou;

(ii) $\alpha 1 = \beta_1$ e $\alpha_2 < \beta_2$ ou;

(iii) $\alpha_1 = \beta_1, \alpha_2 = \beta_2$ e $\alpha_3 < \beta_3$.

Para que possamos utilizar a ordenação acima como uma ordem monomial devemos estender o algoritmo para monômios $\mathbb{M}_n$ onde tenhamos uma relação de ordem total.

Definição 32. *(Ordem lexicográfica $\preceq_L$) Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que*

$$\prod_{i=1}^{n} x_i^{\alpha i} \preceq_L \prod_{i=1}^{n} x_i^{\beta i}$$

se $\alpha_k = \beta_k$ para todo $k \in \{1, ..., n\}$, isto é $\prod_{i=1}^{n} x_i^{\alpha i} = \prod_{i=1}^{n} x_i^{\beta i}$, ou existe $i \in \{1, ..., n\}$ tal que $\alpha_j < \beta_j$ para todo $j < i$.

Exemplo 26. *Considere os monômios $x^4, x^3y^{1000}z$, note que*

$$x^3y^{1000}z \preceq_L x^4$$

Veja que o termo x^4 pode ser descrito como $xxxx$, e o termo $x^3y1000z$ é descrito como $xxx\underbrace{yyy\cdots y}_{1000-vezes}z$. Note que pro maior que seja o expoente da variável y, ela não tem importância desde que o valor da variável x do outro polinômio seja maior.

Definição 33. *(Ordem Reversa $\preceq_R$) Dados dois monômios $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que*

$$\prod_{i=1}^{n} x_i^{\beta i} \preceq_R \prod_{i=1}^{n} x_i^{\alpha i}$$

se $\alpha_k = \beta_k$ para todo $k \in \{1, ..., n\}$, isto é $\prod_{i=1}^{n} x_i^{\alpha i} = \prod_{i=1}^{n} x_i^{\beta i}$, ou existe $i \in \{1, ..., n\}$ tal que $\beta_j < \alpha_j$ para todo $j < i$.

Exemplo 27. *Considere os monômios x^4y^2, x^3y^3, note que*

$$y^2x^4 \preceq_R y^3x^3$$

Note que pro maior que seja o expoente da variável x, ela não tem importância desde que o valor da variável y do outro polinômio seja maior.

Definição 34. *(Ordem lexicográfica graduada $\preceq_{LG}$) Dados dois $\prod_{i=1}^{n} x_i^{\alpha i}$ e $\prod_{i=1}^{n} x_i^{\beta i} \in \mathbb{M}_n$, dizemos que*

$$\prod_{i=1}^{n} x_i^{\alpha i} \preceq_{LG} \prod_{i=1}^{n} x_i^{\beta i}$$

se

i. $\partial(\prod_{i=1}^{n} x_i^{\alpha i}) < \partial(\prod_{i=1}^{n} x_i^{\beta i})$ *ou;*

ii. $\partial(\prod_{i=1}^{n} x_i^{\alpha i}) = \partial(\prod_{i=1}^{n} x_i^{\beta i})$ *e existe $k \in \{1, ..., n\}$ tal que $\alpha_k < \beta_k$ e $\alpha_j = \beta_j$ para todo $j < k$.*

Exemplo 28. *Considere os monômios $x^4, x^3y^{1000}z$, note que*

$$x^4 \preceq_{LG} x^3y^{1000}z$$

veja agora que o valor da variável x não é relevante, tendo em vesta que o grau total do monômio $x^3y^{1000}z$ é 1004, enquanto o grau do polinômio x^4 tem seu grua igual a 4. Desta forma, podemos verificar que $1004 > 4$. Logo, $x^4 \preceq_{LG} x^3y^{1000}z$.

Como podemos perceber a ordem dos monômios são distintas de acordo com a ordenação que definimos para fazer a comparação. Observe o seguinte exemplo onde são feitas as ordenação considerando a ordem lexicográfica e lexicográfica graduada.

Exemplo 29. *Sejam os monômios*

$$x^3yz, x^4y^4, y^4z^2, x^8, x^5y^2z^4, x^2y^3z^2 \in K[x,y,z]$$

vamos fazer a ordenação dos monômios considerando as definições acima.

1. $y^4z^2 \preceq_L x^2y^3z^2 \preceq_L x^3yz \preceq_L x^4y^4 \preceq_L x^5y^2z^4 \preceq_L x^8$;
2. $z^4y^2x^5 \preceq_R z^2y^4 \preceq_R z^2y^3x^2 \preceq_R zyx^3 \preceq_R y^4x^4 \preceq_R x^8$;
3. $x^3yz \preceq_{LG} y^4z^2 \preceq_{LG} x^2y^3z^2 \preceq_{LG} x^4y^4 \preceq_{LG} x^8 \preceq_{LG} x^5y^2z^4$.

Corolário 11. *(Algoritmo da divisão em $K[x_1,...,x_n]$) Fixada uma ordem monomial $\preceq$ e dado $g \in K[x_1,...,x_n] - \{0\}$, para qualquer polinômio $f \in K[x_1,...,x_n]$ existem $q, r \in K[x_1,...,x_n]$ unicamente determinados pelas condições*

$$f = q \cdot g + r, \text{ com } r = 0 \text{ ou } ml(g) \nmid m \text{ para todo } m \in \mathbb{M}(r).$$

Demonstração. (existência)
Se $f = 0$, então

$$f = 0 = 0 \cdot g + 0 = q \cdot g + r$$

ou seja $q = r = 0$, satisfazendo as condições do teorema. Suponha então $f_0 = f \neq 0$ e considere o conjunto

$$S(f_0) = \{m \in \mathbb{M}(f); ml(g)|m\}$$

se $S(f_0) = \varnothing$, então definimos $q = 0$ e $r = f$ ou seja $f = 0 \cdot g + r$ e obtemos o resultado. Considere então $S(f_0) \neq \varnothing$, tomemos

$$m_0 = max \preceq S(f_0)$$

e $a_0 \in K$ o coeficiente de m_0 que ocorre em f e definimos

$$f_1 = f - \frac{a_0 m_0}{tl(g)} g$$

agora considere o conjunto

$$S(f_1) = \{m \in \mathbb{M}(f_1); ml(g)|m\}$$

se $S(f_1) = \varnothing$, então definimos

$$q = \frac{a_0 m_0}{tl(g)}, r = f_1$$

considere então $S(f_1) \neq \varnothing$, então tomemos

$$m_1 = max \preceq S(f_1)$$

$a_1 \in K$ o coeficiente de m_1 que ocorre em f_1 e defina

$$f_2 = f_1 - \frac{a_1 m_1}{tl(g)} g$$

note que $m_0 \succeq m_1$, uma vez que

$$\mathbb{M}(f_1) \subseteq \mathbb{M}(f) \cup \left(\frac{m_0}{tl(g)} g \right)$$

de fato, pois

$$f_1 = f - \frac{a_0 m_0}{tl(g)} g$$

repetindo o processo, definimos

$$S(f_i) = \{m \in \mathbb{M}(f_i);\ ml(g)|m\}\ e\ m_i \preceq maxS(f_i)$$

onde $a_i \in K$ o coeficiente de m_i que ocorre em f_i. Assim, obtemos uma sequência

$$m_0 \succeq m_1 \succeq m_2 \succeq m_3 \succeq ...$$

mas pelo lema anterior, vimos que toda ordem monomial decrescente de monômios é finita, ou equivalentemente, existe $k \in \mathbb{N}$ tal que

$$S(f_k) = \{m \in \mathbb{M}(f_k);\ ml(g)|m\} = \varnothing$$

pelo modo que definimos f_k, existe $q \in K[x_1, ..., x_n]$ tal que

$$f_k = f - q \cdot g \Rightarrow f = q \cdot g + f_k$$

denotando $f_k = r$ a existência do teorema está provada. Vamos então provar a unicidade.

Suponha que existem $q_1, q_2, r_1, r_2 \in K[x_1, ..., x_n]$ tal que

$$q_1 g + r_1 = f = q_2 g + r_2$$

com $r_i = 0$ ou $ml(g) \nmid m$ para todo $m \in \mathbb{M}(r_i)$ e $i \in \{1, 2\}$ isto é $ml(g) \nmid m$ para todo

$$m \in \mathbb{M}(r_1) \cup \mathbb{M}(r_2) \supseteq \mathbb{M}(r_2 - r_1)$$

note que

$$0 = f - f = (q_1 - q_2)g + (r_1 - r_2)$$

ou seja

$$r_2 - r_1 = (q_1 - q_2)g$$

caso $r_1 = r_2$, a unicidade está provada, pois

$$0 = (q_1 - q_2)g \Rightarrow q_1 = q_2$$

pois $K[x_1, ..., x_n]$ é domínio de integridade e por hipótese $g \neq 0$. Suponha então que $r_1 \neq r_2$, então

$$ml(g)|ml(r_1 - r_2) \in \mathbb{M}(r_2 - r_1).$$

O que gera um absurdo, já que $\mathbb{M}(r_2 - r_1) \subseteq \mathbb{M}(r_1) \cup \mathbb{M}(r_2)$. Assim, $r_1 = r_2$ e o corolário está provado.

□

Exemplo 30. *Considere os polinômios* $f = xy^4 + x^4 + x^3y + y^3$ *e* $g = y^3 + x^2 \in \mathbb{R}[x, y]$.

Vamos ordenar seguindo a ordens monomiais vistas anteriormente e efetuar o algoritmo da divisão para polinômios em $K[x_1, ..., x_n]$

Primeiramente, ordenando os polinômios na ordem lexicográfica teremos

$$f = xy^4 + x^4 + x^3y + y^3 \ e \ g = x^2 + y^3$$

temos então, pelo algoritmo da divisão que

$$f = xy^4 + x^4 + x^3y + y^3 = \underbrace{(x^2 + y^3)}_{g}\underbrace{(x^2 + xy - y^3)}_{q} + \underbrace{(y^6 + y^3)}_{r}$$

ordenando os polinômios na ordem lexicográfica graduada temos

$$f = xy^4 + x^4 + x^3y + y^3 \ e \ g = y^3 + x^2.$$

Pelo algoritmo da divisão em $K[x_1, ..., x_n]$, *temos*

$$f = xy^4 + x^4 + x^3y + y^3 = \underbrace{(xy - 1)}_{q}\underbrace{(y^3 + x^2)}_{g} + \underbrace{(x^4 - x^2)}_{r}.$$

5.4 Ideais

Iremos dar inicio ao estudo de um conjunto que será de suma importância para continuidade do trabalho, pois será feito uma ligação entre os ideais e os conjuntos algébricos.

Definição 35. *(Ideal) Seja A um anel e I um subanel de A. I é dito um ideal de A quando para todo $a, b \in I$ e $x \in A$ são satisfeitas as seguintes condições*

i. $0 \in I$ (Elemento neutro está no ideal);

ii. Dado $a, b \in I$, temos que $a + b \in I$ (Fechamento da soma no ideal);

iii. Se $x \in A$ e $a \in I$. Então, $a \cdot x = x \cdot a \in I$ (Lei da absorção).

Observação 15. *Por definição, sabemos que todo ideal de um anel A é um subanel, mas a recíproca não é verdadeira. Observe o caso que o conjunto $\mathbb{Z}$ é subanel de $\mathbb{Q}$ tome $\frac{1}{2} \in \mathbb{Q}$ e $1 \in \mathbb{Z}$ observe que $1 \cdot \frac{1}{2} = \frac{1}{2} \cdot 1 \notin \mathbb{Z}$.*

Observação 16. *Todo anel A admite no mínimo dois ideais, o próprio A e $\{0\}$. É fácil mostrar que ambos são ideias e são chamados de ideias triviais do anel A.*

Proposição 18. *Seja A um anel e I um ideal de A. $I = A$ se, e somente se, $1 \in I$.*

Demonstração. Seja $I = A$, qu eremos mostrar que $1 \in I$. De fato, pois estamos trabalhando com anéis comutativos e com unidade, e como $I = A$ consequentemente $1 \in I$. Reciprocamente, basta mostrar $A \subset I$, pois $I \subset A$ por definição. Portanto, tome $x \in A$, como I é um ideal onde $1 \in I$, pelo terceiro item $x \cdot 1 = 1 \cdot x = x \in I$, como $x \in I$ e $x \in A$, chega-se a conclusão que $A \subset I$. Logo, $I = A$.

□

Corolário 12. *Todo corpo K só admite os ideias triviais.*

Demonstração. Suponha que $I \neq \{0\}$, queremos mostrar que $I = K$. Seja $a \in I - \{0\}$ como K é um corpo, temos a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$, logo $1 \in I$, e pela proposição anterior temos que $I = K$.

□

Proposição 19. *Seja A um anel de e $X = \{x_1, x_2, ..., x_n\} \subset A$, então o conjunto*

$$\langle X \rangle = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n; a_j \in A, j \in \{1, ..., n\}\}$$

é um ideal de A chamado ideal de A gerado por $x_1, ..., x_n$.

Demonstração. Para mostrar que o conjunto X é um ideal de A, vamos mostrar que $\langle X \rangle$ satisfaz as três condições definidas acima.

i. Queremos mostrar que $0 \in \langle X \rangle$. De fato, basta termos $a_j = 0$, sendo assim $0x_1 + 0x_2 + \cdots + 0x_n = 0 \in \langle X \rangle$

ii. Queremos mostrar que dado dois elementos em $\langle X \rangle$ a soma deles está no conjunto. Tome $a_1x_1 + \cdots + a_nx_n$ e $b_1x_1 + \cdots + b_nx_n$, ambos em $\langle X \rangle$, a soma deles é: $(a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \cdots + (a_n + b_n)x_n$. Claramente está soma está em $\langle X \rangle$,

iii. Queremos mostrar a lei da absorção de um ideal. Dado $y \in A$ queremos mostrar que $y \cdot \langle X \rangle \in A$. Segue com facilidade, pois

$$y \cdot \langle X \rangle = y(a_1x_1 + \cdots + a_nx_n) = (a_1y)x_1 + \cdots + (a_ny)x_n \in \langle X \rangle$$

temos então que$\langle X \rangle$ é um ideal de A. .

□

Definição 36. *Seja $X = \{c\} \subset A$ o ideal*

$$\langle X \rangle = \langle c \rangle = \{a \cdot c; a \in A\}.$$

Chamamos $\langle c \rangle$ de Ideal principal de A gerado por c.

Exemplo 31. *Sabe-se que $\mathbb{R}[x, y]$ é o anel de polinômios nas variáveis x, y sobre $\mathbb{R}$, dado o conjunto $\{x^2, xy\} \subseteq \mathbb{R}[x, y]$, então o conjunto*

$$\langle x^2, xy \rangle = \{f(x, y)x^2 + g(x, y)xy : f(x, y), g(x, y) \in R[x, y]\}$$

é um ideal de $\mathbb{R}[x, y]$ gerado pelos polinômios x^2 e xy.

Exemplo 32. *Tomando $A = \mathbb{Z}$, podemos definir o conjunto*

$$\langle 2 \rangle = 2\mathbb{Z} = \{2a; a \in \mathbb{Z}\}$$

onde $2\mathbb{Z}$ é um ideal principal de $\mathbb{Z}$, gerado por 2.

Proposição 20. *Se I e J são ideais de um anel A. Então, $I \cap J$ é um ideal de A.*

Demonstração. Queremos mostrar que $I \cap J$ é um ideal, basta mostrar que são satisfeitas as três condições.Segue:

i. Queremos mostrar que $0 \in I \cap J$. Como I e J são ideais do anel A, temos que $0 \in I$ e $0 \in J$, logo $0 \in I \cap J$.

ii. Dados $a, b \in I \cap J$, queremos mostrar que sabemos que $a + b \in I \cap J$. Tome $a, b \in I \cap J$ por definição, $a, b \in I$ assim como $a, b \in J$ Segue então que $a + b \in I$, tal como $a + b \in J$ concluímos que $a + b \in I \cap J$.

iii. Seja $x \in A$ e $a \in I \cap J$, queremos mostrar que $ax \in J \cap I$. De fato, pois sendo $a \in I \cap J$ temos que $x \cdot a \in I$ pelo fato de $a \in I$ assim como $x \cdot a \in J$ já que $a \in J$. Logo, $ax \in I \cap J$.

□

Observação 17. *Acabamos de mostrar que a interseção entre dois ideais de um mesmo anel é um ideal. Contudo, o mesmo não é válido para a união entre dois ideias de um anel A. Para essa verificação, tome os ideias $2\mathbb{Z}$ e $3\mathbb{Z}$, $2 \in 2\mathbb{Z}$ e $3 \in 3\mathbb{Z}$, note que $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.*

Proposição 21. *Sejam A um anel, I e J ideais de A. Então o conjunto*

$$I + J = \{a + b; a \in I, b \in J\}$$

é um ideal chamado soma de ideias.

Demonstração. Queremos mostrar que o conjunto acima é um ideal. Para isso, vamos verificar três condições.

i. Queremos mostrar que $0 \in I + J$. Como $0 \in I$ e $0 \in J$, temos que $0 + 0 = 0 \in I + J$.

ii. Dados $c, d \in I + J$, queremos mostrar que $c + d \in I + J$. Observe que $c + d = (a + b) + (a' + d')$, podemos associar e comutar a soma, $(a+a')+(b+b')$, como $a, a' \in I$ e $b, b' \in J$. Concluímos que $c+d \in I+J$.

iii. Queremos mostrar a lei da absorção de ideais. Dado $x \in A$ $x(I + J) = x(a + b) = xa + xb \in I + J$. logo, $I + J$ é um ideal do anel A.

□

Proposição 22. *Seja A um anel e I, J ideais do anel A. Então o conjunto*

$$I \cdot J = \left\{ \sum_{i=1}^{n} x_i y_i \ / \ n \in \mathbb{N}, x_i \in I, y_i \in J \right\}$$

é um ideal do anel A chamado de produtos dos ideais I, J.

Demonstração. Queremos mostrar que o conjunto acima é um ideal. Para isso, vamos verificar três condições.

i. Queremos mostrar que $0 \in I \cdot J$. Seja $x_i = 0$ e $y_i = 0$, temos

$$\sum_{i=0}^{n} 00 = 0 \cdot 0 + \cdots + 0 \cdot 0 = 0 \in IJ$$

ii. Dado $a = \sum_{i=0}^{n} x_i y_i$ e $b = \sum_{i=0}^{n} x'_i y' i$, ambos em $I \cdot J$, queremos mostrar que $a + b \in I \cdot J$. De fato,

$$a + b = \sum_{i=0}^{n} x_i y_i + \sum_{i=0}^{n} x'_i y'_i$$

$$= (x_1 y_1 + \cdots + x_n y_n) + (x'_1 y'_1 + \cdots + x'_n y'_n)$$

associando e comutando os elementos desta soma:

$$(x_1 y_1 + x'_1 y'_1) + \cdots + (x_n y_n x'_n y'_n)$$

e essa soma é uma soma de $I \cdot J$. Portanto, $a + b \in I \cdot J$.

iii. Queremos mostrar que vale a lei da absorção de ideais. Dado $z \in A$ e $a \in I \cdot J$, onde $a \sum_{i=1}^{n} x_i y_i$ tal que $x_i \in I, y_i \in J, i \in \{1, ..., n\}$ temos

$$z \cdot a = z \cdot \sum_{i=1}^{n} x_i y_i = z(x_1 y_1 + \cdots + x_n y_n)$$

$$= (z x_1) y_1 + \cdots + (z x_n) y_n$$

observe que cada $z x_j \in I$ com $j = \{1, ..., n\}$. Logo $z \cdot a \in I \cdot J$. Então $I \cdot J$ é um ideal do anel A.

□

Quando trabalhamos com números inteiros, estudamos alguns números especiais que são chamado de números primos. Vamos buscar nos ideias essas mesmas características. Para isso, vamos estudar a seguir dois tipos de ideais particulares, os ideais primos e maximais.

Definição 37. *Seja A um anel e P um ideal de A. Dizemos que P é um ideal primo de A quando $P \neq A$ e dados $a, b \in A$ tal que $a \cdot b \in P$, então $a \in P$ ou $b \in P$.*

Proposição 23. *O ideal $2\mathbb{Z}$ é um ideal primo.*

Demonstração. Dado $a, b \in 2\mathbb{Z}$, então $2|ab \Leftrightarrow (a \cdot b) = 2 \cdot r$ para algum r inteiro e portanto, como 2 é primo $2|a$ ou $2|b$, logo $a \in 2\mathbb{Z}$ ou $b \in 2\mathbb{Z}$.

□

Definição 38. *Seja A um anel e M um ideal de A. Dizemos que M é um ideal maximal de A quando $M \neq A$ e dado I ideal de A, tal que $M \subseteq I \subseteq A$. Então $I = A$ ou $I = M$.*

Proposição 24. *O ideal $2\mathbb{Z}$ é maximal em $\mathbb{Z}$.*

Demonstração. Queremos mostrar que $I = 2\mathbb{Z}$ ou $I = \mathbb{Z}$. Suponha que $I \neq 2\mathbb{Z}$, com efeito, se I é um ideal que contem $2\mathbb{Z}$ como subconjunto próprio, então certamente existe um elemento em I da forma $2k + 1$ com $k \in \mathbb{Z}$. Por outro lado, é fácil verificar que $-2k \in \mathbb{Z}$, basta fazer $0 - 2k = -2k$. Logo, $(2k + 1) + (-2k) = 1 \in I$. Pela proposição já mencionada acima, temos que $I = \mathbb{Z}$.

□

Exemplo 33. *Também podemos encontrar ideais que não são maximais e nem primos. Considere o conjunto $6\mathbb{Z} = \{6 \cdot a; a \in \mathbb{Z}\}$ é um ideal do anel $\mathbb{Z}$, mas não é ideal primo, pois o produto $ab \in 6\mathbb{Z}$ podemos tomar $2 \in 2\mathbb{Z}$ e $3 \in 3\mathbb{Z}, 3 \cdot 2 = 6 \in 6\mathbb{Z}$. E não é maximal, pois $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ e $2\mathbb{Z} \neq 6\mathbb{Z}$ e $2\mathbb{Z} \neq \mathbb{Z}$.*

Proposição 25. *Um anel A é domínio de integridade se, e somente se, o conjunto $\{0\}$ é um ideal primo.*

Demonstração. Seja A um domínio de integridade, queremos mostrar que $\{0\}$ é ideal primo. Dados $a, b \in A$ se $a \cdot b = 0$, como A é domínio de integridade, temos que $a = 0$ ou $b = 0$ o que nos leva $\{0\}$ a ser um ideal primo. Reciprocamente, seja $\{0\}$ um ideal primo, temos que dado $a, b \in A, a \cdot b \in \{0\} \Rightarrow a = 0$ ou $b = 0$.

□

Proposição 26. *Todo ideal maximal de um anel A é primo.*

Demonstração. Seja M um ideal maximal de A, queremos mostrar que o ideal M é primo. Ou seja, Dados $a, b \in A$ e o produto $a * b \in M$, vamos mostrar que $a \in M$ ou $b \in M$. Suponha que $a \notin M$, observe que o ideal $(a) + M$ contém estritamente M. Como M é um ideal maximal, então $(a) + M = A$. Em particular, $1 \in A = (a) + M$, logo existe $m \in M$ e $x \in A$ tal que $1 = (ax) + m$, multiplicando b à esquerda em ambos os lados da igualdade, temos $b = (ba)x + bm$, como (a) É ideal, podemos verificar que $(ba)x \in M$, logo a soma desses elementos pertence a M, isto significa que $b \in M$.

□

Observação 18. *Em uma conta simples, podemos constatar que a recíproca da proposição anterior não é válida.Ou seja, existem ideais que são primos mas não são maximais. Considere o ideal trivial $\{0\}$ de $\mathbb{Z}$, note que $\{0\}$ é primo, pois dado $a * b \in \{0\}$ temos que $a \in \{0\}$ ou $b\{0\}$.Entretanto não é maximal, pois $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.*

Definição 39. *Seja A um anel. Para cada ideal I de A definimos o radical de I como:*

$$\sqrt{I} = Rad(I) = \{x \in A; x^n \in I, n \in \mathbb{N}\} \subseteq A.$$

Proposição 27. *$Rad(I)$ é um ideal do anel A que contém I.*

Demonstração. Queremos mostrar que $Rad(I)$ é um ideal e também a inclusão $I \subseteq Rad(I)$. Para mostrar a inclusão, tome $x \in I$, podemos escrever $x^1 \in I$, logo $Rad(I)$ contém I. Para mostrar que $Rad(I)$ é um ideal, basta mostrar três condições

i. Queremos mostra que $0 \in Rad(I)$. De fato, pois $0 \in I$, pelo fato de I ser um ideal.

ii. Queremos mostrar que dado dado $x, y \in Rad(I)$, teremos que $x + y \in Rad(I)$. Sejam então $x, y \in Rad(I)$, então existem $m, n\ in\mathbb{N}$ tal que $x^m \in I$ e $x_n \in I$, logo $x^r \in I$ para todo $r \geq m$, assim como $y^s \in I$ para todo $s \geq n$. isso ocorre, pois com $r \geq m$ podemos escrever $x^r = x^{r-m}x^m \in I$ e pelo binômio de Newton

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{n+m-i}$$

$$= \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^n y^{m-i}$$

em cada parcela desse somatório, teremos $y^n \in I$ ou $x^m \in I$. Por isso, $(x+y)^{m+n} \in I \Rightarrow x + y \in Rad(I)$.

iii. Queremos mostrar que dado $\alpha \in A$ e $x \in Rad(I)$ o produto $\alpha x \in Rad(I)$. tal afirmação é equivalente a mostrar que $(\alpha x)^n \in I$. Observe que $(\alpha x)^n = \alpha^n x^n$ e como $x^n \in I$, concluímos que $(\alpha x)^n \in I$. Portanto, $\alpha x \in Rad(I)$

□

Definição 40. *(Ideal radical) Seja A um anel e I um ideal de A. I é dito ideal radical do anel A se $Rad(I) = I$*

Proposição 28. *Se I é um ideal do anel A. Então, $Rad(I)$ é um ideal radical.*

Demonstração. Como $Rad(I)$ é um ideal do anel A, então $Rad(I) \subseteq Rad(Rad(I))$. Reciprocamente, seja $x \in Rad(Rad(I))$, logo existe $n \in \mathbb{N}$ tal que $x^n \in Rad(I)$, e como $x^n \in Rad(I)$, esxiste $m \in \mathbb{N}$ tal que $(x^n)^m = x^{nm} \in I$, isso implica que $x \in Rad(I)$. Portanto, o radical de um ideal $Rad(I)$ sempre é ideal radical.

□

Observação 19. *Um caso particular de ideal radical são os nilradicais. Com efeito*

$$\eta_A = Rad(0) = \{x \in A, x^n = o, para\ algum\ n \in \mathbb{N}\}$$

Proposição 29. *$Raf(I)$ satisfaz as seguintes propriedades*

1. $Rad(IJ) = Rad(I) \cap Rad(J)$

2. $Rad(I) = (1) \Leftrightarrow I = (1)$

3. $Rad(I + J) = Rad(Rad(I) + Rad(J))$

4. *Se P é um ideal primo de A, $Rad(P^n) = P$, para todo $n > 0$.*

Demonstração. Queremos mostrar que as quatro condições acima são verdadeiras.

1. Como $IJ \subseteq I$ *capJ* , tão $Rad(IJ)$ *subseteqRad*$(I \cap J)$. Por outro lado, tomando $x \in Rad(I \cap J)$, então existe $x^n \in I$ e $x^n \in J$ tal que $x^n x^n = x^{2n} \in IJ$ e então $x \in Rad(IJ)$ como queríamos.

2. Vamos usar a contrapositiva, como $I \subseteq Rad(I)$, se $I = (1)$ obviamente $Rad(I) = (1)$. Por outro lado, se $I \neq (1)$, então existe $x \in (1)$ tal que $x \notin I$. Assim, $x^n \notin I$ para qualquer n e $I \neq (1)$ como queríamos.

3. Como $I \subseteq Rad(I)$ e $J \subseteq Rad(J)$ implica que

$$I + J \subseteq Rad(I) + Rad(J)$$

   e consequentemente,

$$Rad(I + J) \subseteq Rad(Rad(I) + Rad(J))$$

   por outro lado, pela proposição mostrada acima

$$(Rad(I) + Rad(J)) \subseteq Rad(Rad(I) + Rad(J))$$

   pela proposição acima,

   $Rad(Rad(I)+Rad(J)) = Rad(Rad(Rad(I))+Rad(Rad(J)) = Rad(I+J)$

   mostrando a inclusão contrária.

4. Seja então $x \in P$, logo $x^n \in P^n$, assim $x \in Rad(P^n)$. Para inclusão contrária, se $x \in Rad(P^n)$, temos que $x^m \in P^n$ para algum m. Como P é um ideal primo do anel A, o produto: $x^m = \underbrace{x \cdots x}_{m-vezes} \in P$.

□

5.5 Anéis Quociente

Definição 41. *Seja I um ideal de um anel A. Dados $a \in A$ chamamos de classe de equivalência de módulo I ao conjunto de todos os elementos de A que são congruentes ao elemento a módulo I.*

Para indicarmos esses elementos, temos: $\bar{a} = \{x \in A; x \equiv a(modI)\}$

Observação 20. *Por definição, $x \equiv a(modI)$ se, e somente se, $x - a \in I$.*

Definição 42. *Sejam I, J ideais de um anel A, o ideal quociente é o conjunto dado por:*

$$(I : J) = \{x \in A; xy \in I, \forall\ y \in J\}$$

Proposição 30. *Definido o ideal quociente, são válidos os seguintes itens*

(i) $I \subseteq (I : J)$

(ii) $(I : J)J \subseteq I$

(iii) $(I : J) : K) = (I : JK)$

Lema 6. *Seja A um anel, I um ideal de A e $a \in A$. A classe de equivalência de a módulo I pode ser reescrita como*

$$\bar{a} = a + I = \{a + x; x \in I\}$$

Demonstração. Dado $b \in \bar{a}$, queremos mostrar que $b \in a + I$. Como $b \in \bar{a}$, então $b - a \in I$, daí $a + (b - a) \in a + I$. Reciprocamente, Tome $b \in a + I$, então $b = a + x$, para algum $x \in I$, temos que $x = b - a$ onde $b \equiv a(modI)$, logo $b \in \bar{a}$.

□

Proposição 31. *Seja A um anel. O conjunto $\{0\}$ é ideal maximal se, e somente se A é um corpo.*

Demonstração. Seja $\{0\}$ um ideal maximal. Ou seja $\{0\} \subseteq I \subseteq A$, onde $I = \{0\}$ ou $I = A$, queremos mostrar que A é um corpo. Como $\{0\}$ é ideal maximal ele também é um ideal primo, ou seja $a, b \in A$ onde $a \cdot b \in \{0\} \Rightarrow a \in \{0\}$ ou $b \in \{0\}$. Logo, A é um domínio de integridade, então basta mostrar que os elementos não-nulos de A possuem inverso multiplicativo em A. Dado $a \in A - \{0\}$, temos que (a) é ideal de A, assim, $\{0\} \subseteq (a) \subseteq A$,

como $\{0\}$ é maximal, então $(a) = A$, em particular $1 \in A = (a)$, logo, existe $a^{-1} \in A$ tal que $a \cdot a^{-1} = 1$, sendo A então um corpo. Reciprocamente, Seja A um corpo, queremos mostrar que $\{0\}$ é maximal. Para isso, dado um ideal I de A, tal que $\{0\} \subseteq I \subseteq A$, chegaremos a conclusão que $\{0\} = I$ ou $I = A$. Suponha então que $I \neq \{0\}$, vamos mostrar que $I = A$, basta mostrar que I contém a unidade, como $I \neq \{0\}$ então existe $a \in I - \{0\}$ e $a^{-1} \in A$, tal que $a \cdot a^{-1} = 1 \in I$ pela proposição mostrada anteriormente, concluímos que $I = A$.

□

Definimos as operações binárias do conjunto $\frac{A}{I} = \{\bar{a}; a \in A\}$ como sendo a soma: $\frac{A}{I} \times \frac{A}{I}$ tal que $(\bar{a}, \bar{b}) \longmapsto \overline{a+b}$ e do produto $\frac{A}{I} \times \frac{A}{I}$ sendo $(\bar{a}, \bar{b}) \longmapsto \overline{a \cdot b}$. É fácil verificar que o conjunto de $\frac{A}{I}$ é um anel.

Exemplo 34. *Tomando o anel $\mathbb{Z} = A$ e o ideal $6\mathbb{Z} = I$ de $\mathbb{Z}$, temos que $\frac{\mathbb{Z}}{6\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ é uma anel.*

De fato, basta observar que $\bar{a} = a + 6\mathbb{Z} = \{a + x; x \in 6\mathbb{Z}\}$.

Teorema 8. *Seja A um anel e I um ideal de A. $\frac{A}{I}$ é domínio de integridade se, e somente se, I é ideal primo.*

Demonstração. Seja $\frac{A}{I}$ um domínio de integridade, queremos mostrar que dado $a, b \in A$ e $a \cdot b \in I \Rightarrow a \in I$ ou $b \in I$. Seja então $a, b \in A$, tais que $ab \in I$, como $ab - 0 \in I$, pois $ab, 0\ in I$, por definição temos que $\overline{a \cdot b} = \bar{0}$ e pelo fato de A/I ser domínio de integridade (em particular, ser sem divisores de zero), temos que $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Suponha então que $\bar{a} = \bar{0}$, então $a - 0 \in I$, logo I é primo. Reciprocamente, Seja I um ideal primo, queremos mostrar que o anel $\frac{A}{I}$ é domínio de integridade. Dados $\bar{a}, \bar{b} \in \frac{A}{I}$, tais que $\bar{a}\bar{b}$, segue que $a \cdot b - 0 = a \cdot b \in I$, mas I é um ideal primo, então $a \in I$ ou $b \in I$. Suponha que seja $a \in I$, logo $a - 0 \in I$ e portanto $\bar{a} = \bar{0}$ como queríamos.

□

Teorema 9. *Seja A um anel e I um ideal de A. $\frac{A}{I}$ é corpo se, e somente se, I é ideal maximal de A.*

Demonstração. Seja $\frac{A}{I}$ um corpo e I, J ideais de A, queremos mostrar que dado a inclusão $I \subseteq J \subseteq A, \Rightarrow I = J$ ou $J = A$. Seja J um ideal de A, tal que $I \subsetneq J \subseteq A$, existe $b \in J$ tal que $b \notin I$, daí $\bar{b} \neq \bar{0}$, como por hipótese A/I é um corpo $\bar{a} \cdot \bar{b} = \bar{1}$, por definição, temos $b * a - 1 \in I$, isto

é $1 = ab + u$ para algum $u \in I \subseteq J$, note que $ab \in J$, pois $b \in J$, como $u, ab \in J$, temos que $b \cdot a + u = 1 \in J$, daí $J = A$ e I é um ideal maximal como queríamos. Reciprocamente, queremos mostrar que $\frac{A}{I}$ é um corpo. Para isso, basta mostrar que todo elemento de $\frac{A}{I}$ tem inverso multiplicativo em $\frac{A}{I}$. Tome $\bar{a} \neq \bar{0}$, então $\bar{a} \notin I$ e consequentemente, $I \subsetneq (a) + I \subseteq A$, daí $(a) + I = A$. Em particular, $1 \in A = (a) + I$, logo $1 = ab + u$ com $ab \in I$ e $u \in I$, daí $1 - ba \in I$ donde $\bar{a}\bar{b} = \bar{1}$. Concluímos que $\frac{A}{I}$ é corpo.

□

5.6 Homomorfismo de Anéis

Anteriormente estudamos separadamente o que é necessário para um conjunto A ser um anel. Agora, iremos prosseguir estudando uma relação entre dois anéis.

Definição 43. *(Homomorfismo de anéis) Sejam $(A, +, \cdot)$ e $(B, +, \cdot)$ anéis, um homomorfismo entre anéis A e B é uma função $f : A \longrightarrow B$, onde as operações de A e B são preservadas satisfazendo duas condições para todo $a, b \in A$*

1. $f(a + b) = f(a) + f(b)$;
2. $f(a \cdot b) = f(a) \cdot f(b)$.

Exemplo 35. *A função $p : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, definida por $p(x, y) = x$ é chamada de projeção, é um homomorfismo de anéis*

Demonstração. Vamos verificar que as duas condições para homomorfismo de anéis são satisfeitas respectivamente.

1. $p((x, y) + (w, z)) = p(x + w, y + z) = x + w = p(x, y) + p(w, z)$;
2. $p((x, y) \cdot (w, z)) = p(xw, yz) = x \cdot w = p(x, y) \cdot p(w, z)$.

□

Proposição 32. *Seja f um homomorfismo entre anéis, para todo $a, b \in A$ são satisfeitas as seguintes propriedades*

1. $f(a^n) = (f(a))^n$
2. $f(0_A) = 0_B$
3. $f(-a) = -f(a)$
4. $f(1_A) = 1_B$
5. $f(a-b) = f(a) - f(b)$

Demonstração. Vamos verificar que as cinco propriedades são verdadeiras.

1. $f(a^n) = f(\underbrace{a \cdot a \cdot ... \cdot a}_{n-vezes}) = \underbrace{f(a) \cdot f(a) \cdot \cdots \cdot f(a)}_{n-vezes} = (f(a))^n$
2. $0_A = 0_A \Leftrightarrow 0_A + 0_A = 0_A \Leftrightarrow f(0_A + 0_A) = f(0_A) \Leftrightarrow f(0_A) + f(0_A) = f(0_A) \Leftrightarrow f(0_A) = f(0_A) - f(0_A) = 0_B$
3. Seja $a + (-a) = 0_A \Leftrightarrow f(a + (-a)) = f(0_A) = 0_B \Leftrightarrow f(a) + f(-a) = 0_B \Leftrightarrow f(-a) = -f(a)$.
4. $1_A = 1_A \Leftrightarrow 1_A \cdot 1_A = 1_A \Leftrightarrow f(1_A)^2 = f(1_A) \Leftrightarrow f(1_A)^2 - f(1_A) = 0_B \Leftrightarrow f(1_A) \cdot f(1_A - 1_B) = 0_B \Leftrightarrow f(1A) = 1_B$
5. $f(a-b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b)$

□

Exemplo 36. *Seja I um ideal do anel A, a aplicação $\phi : A \longrightarrow \frac{A}{I}$, com $\phi(x) = \bar{x}$, é um homomorfismo.*

Definição 44. *O núcleo (ou kernel) de f é o conjunto formado pelos elementos de A que tem como imagem 0_B. Denotamos tal conjunto como*

$$ker(f) = \{a \in A; f(a) = 0_B\}.$$

Exemplo 37. *Seja $I_A : A \longrightarrow A$ como $I_A(a) = a$, temos como $ker(I_A = \{0_A\})$. Em particular, I_A é chamado homomorfismo identidade.*

Definição 45. *Seja $f : A \longrightarrow B$ um homomorfismo de aneis. A imagem de f é o conjunto*

$$Im(f) = \{f(a); a \in A\}.$$

Exemplo 38. *No homomorfismo $\mu : A \longrightarrow \frac{A}{I}$, a imagem de μ é todo anel quociente $\frac{A}{I}$, isto é $Im(\mu) = \frac{A}{I}$.*

Proposição 33. *Seja $f : A \longrightarrow B$ um homomorfismo de anéis, o $ker(f)$ é um ideal do anel A.*

Demonstração. Como queremos mostrar que $ker(f)$ é ideal do anel A, vamos mostrar que o conjunto satisfaz as três condições para ser um ideal.

i. Queremos mostrar que $f(0_A) = f(0_B)$
Segue da propriedade de homomorfismo que $f(0_A) = f(0_B)$, então $0_A \in Ker(f)$.

ii. Queremos mostrar que se $a, b \in Ker(f)$,então$a + b \in Ker(f)$
Dados $a, b \in Ker(f)$, sege que $f(a + b) = f(a) + f(b) = 0_B + 0_B = 0_B$, logo $a + b \in ker(f)$.

iii. Queremos mostrar que se $x \in A$ e $a \in ker(f)$,então $x \cdot a \in Ker(f)$. Dado $x \in A$ e $a \in ker(f)$ temos que $f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0_B = 0_B$
Logo, $x \cdot a \in ker(f)$, e $ker(f)$ é um ideal.

□

Proposição 34. *Seja $f : A \longrightarrow B$ um homomorfismo de anéis, $Im(f)$ é subanel de B.*

Demonstração. Queremos mostrar que a imagem é um subanel do anel B. Para isso, vamos mostrar que $Im(f)$ satisfaz três condições

i. Queremos mostrar que se $a, b \in Im(f)$, então $a - b \in Im(f)$. De fato, tome $a, b \in Im(f)$, então existe $x, y \in A$ tal que $f(x) = a$ 3 $f(y) = b$, sabemos que A e um anel, logo $x-y$ inA e pelo fato de ser homomorfismo, $f(a - b) = f(a) - f(b) = x - y$, onde $x - y \in Im(f)$.

ii. Queremos mostrar que se $a, b \in Im(f)$, então $a * b \in Im(f)$. Note que $f(x \cdot y) = f(x) \cdot f(y) = a \cdot b$ onde $a \cdot b \in Im(f)$.

□

Corolário 13. *Se J é ideal de A, então $f(J)$ é um ideal da $Im(f)$.*

Demonstração. Note que $f : A \longrightarrow B$ é um homomorfismo de anéis e $J \subset B$ é um ideal, então $f^{-1}(J) \subset A$ é um ideal. Com efeito, sabemos que $f(0_A) = 0_B \in J$, logo $0_A \in f^{-1}(J)$. Dados $a, b \in f^{-1}(J)$, existem $x, y \in J$ tais que $f(a) = x$ e $f(b) = y$, logo $f(a+b) = f(a) + f(b) = x + y \in J$, onde $a + b \in f^{-1}(J)$. Por fim, dados $\alpha \in A$ e $a \in f^{-1}(J)$, então $f(\alpha \cdot a) = f(\alpha) \cdot f(a) \in J$, onde $f(\alpha) \in B$ e $f(a) \in J$. Perceba que $f^{-1}(J)$ é primo, pois dado $a, b \in A$, então existe $x, y \in B$ tais que $f(a) = x$ e $f(b) = y$, daí se $a \cdot b \in f^{-1}(J)$, temos que $f(a \cdot b) = f(a) \cdot f(b) = x \cdot y \in J$ logo, $x \in J$ ou $y \in J$, onde $a \in f^{-1}(J)$ ou $b \in f^{-1}(J)$.

□

Definição 46. *Seja $f : A \longrightarrow B$ um homomorfismo de anéis. Então*

1. *Dizemos que f é sobrejetora se $Im(f) = B$;*
2. *Dizemos que f é injetora se $f(x) = f(y)$, tivermos $x = y$, para todo $x, y \in A$.*

Proposição 35. *Um homomorfismo de anéis $f : A \longrightarrow B$ é injetora se, e somente se, $Ker(f) = \{0_A\}$.*

Demonstração. Seja f um homomorfismo injetor, queremos mostrar que $Ker(f) = \{0_A\}$. Dados $x \in Ker(f)$, temos que $f(x) = 0_B$ e como f é um homomorfismo e uma função injetora, segue que $f(x) = 0_B = f(0_A) \Rightarrow x = 0_A$, logo $Ker(f) = \{0_A\}$. Reciprocamente,sabendo que $Ker(f) = \{0_A\}$, queremos mostrar que f é uma função injetora.Seguindo nessa linha, dados $a, b \in A$, tais que $f(a) = f(b)$, por f ser homomorfismo, temos

$$f(a) = f(b) \Rightarrow f(a) - f(b) = 0_B \Rightarrow f(a - b) = 0_B$$

como $Ker(f) = \{0_A\}$ e $a - b \in Ker(f)$ concluímos que $a = b$ e f é injetiva.

□

Proposição 36. *Seja $f : A \longrightarrow B$ um homomorfismo sobrejetor de anéis. Se $a \in A$ possui inverso multiplicativo em A. Então, $f(a)$ possui inverso multiplicativo em B e $f(a^{-1}) = f(a)^{-1}$.*

Demonstração. Suponha que $a \in A$ admita inverso multiplicativo no anel A. Queremos mostrar que $f(a^{-1}) = f(a)^{-1}$. Observe que $f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$, logo $f(1_A) = f(a) \cdot f(a^{-1})$, por outro lado $f(1_A) = f(1_B)$, isso implica $1_B = f(a) \cdot f(a^{-1})$, daí $f(a^{-1})$ é o inverso multiplicativo de

$f(a)$ e como $a^{-1} \in A$, então $f(a^{-1}) \in B$ e portanto, $f(a^{-1}) = f(a)^{-1}$ como queríamos.

□

Definição 47. *Dezemos que $f : A \longrightarrow B$ é um isomorfismo de anéis se f é um homomorfismo bijetor, isto é f é homomorfismo injetivo e sobrejetivo.*

Observação 21. *Quando existe pelo menos um isomorfismo entre dois anéis quaisquer A e B, dizemos que A é isomorfo a B e usamos a notação: $A \cong B$.*

Proposição 37. *Seja $f : A \longrightarrow B$ um isomorfismo de anéis. A é um domínio de integridade se, e somente se, B é um domínio de integridade.*

Demonstração. Seja A um domínio de integridade, queremos mostrar que B também é um domínio de integridade. Assim, dados $x, y \in B$ tais que $x \cdot y = 0$, existem $a, b \in A$ com $f(a) = x$ e $f(b) = y$, sabemos que $f(a \cdot b) = f(a) \cdot f(b)$ e $f(0_A) = 0_B$, logo $f(a \cdot b) = f(a) \cdot f(b) = x \cdot y = 0_B$ mas f é injetora (pelo fato de f ser isomorfismo), então $a \cdot b = 0_A$, A sendo um domínio de integridade, $a = 0$ ou $b = 0$, portanto $x = 0_B$ ou $y = 0_B$. Reciprocamente, temos que B é um domínio de integridade e vamos mostrar que A também é um domínio de integridade.Para isso, basta usar f^{-1}, já que f é bijetiva. Dados $x, y \in B$, exitem $x, y \in A$ com$f^{-1}(x) = a$ e $f^{-1}(y) = b$ como $f^{-1}(x \cdot y) = f^{-1}(x) \cdot f^{-1}(y)$ e $f^{-1}(0_B) = 0_A$, temos que

$$f^{-1}(x \cdot y) = f^{-1}(x) \cdot f^{-1}(y) = a \cdot b = 0_A$$

mas como f é injetora, $x \cdot y = 0_B$ e como B é um domínio de integridade, nota-se que $x = 0$ ou $y = 0$, portanto$a = 0_A$ ou $b = 0_A$.

□

Proposição 38. *Seja $f : A \longrightarrow B$ um isomorfismo de anéis. A é corpo, se e somente se, B é corpo.*

Demonstração. Suponha que A seja corpo. Vamos mostrar que B é corpo. Com $x \in B$, existe $a \in A$ tal que $f(a) = x$, como A é corpo, existe $a^{-1} \in A$ onde $a \cdot a^{-1} = 1_A$, pelo fato de f ser um isomorfismo sabemos que

$$f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

e $f(1_A) = 1_B$ perceba que

$$f(a) \cdot f(a^{-1}) = xf(a)^{-1} = 1_B.$$

Portanto, B é corpo, pois tem algum elemento que multiplicado por x dá a identidade. Analogamente, tendo que B é um corpo, basta usar f^{-1}, para mostrar que A é um corpo.

□

Teorema 10. *(Teorema do Isomorfismo) Seja $f : A \longrightarrow B$ um homomorfismo de anéis. Então, $\psi : \frac{A}{Ker(f)} \longrightarrow Im(f)$, com $\psi(\bar{a}) = f(a)$ é um isomorfismo de anéis.*

Demonstração. Sabemos que $Im(f)$ é subanel de B, em particular $Im(f)$ é um anel com as operações de B. Para demonstrar o teorema, precisamos mostrar que o ψ está bem definida. Isto é, vamos tomar dois representantes da mesma classe, e mostrar que eles tem a mesma imagem. Tome então

$$\bar{a} = \bar{b}, \Rightarrow a - b \in Ker(f) \Rightarrow 0_B = f(a-b) = f(a) - f(b)$$

$$= \psi(\bar{a}) - \psi(\bar{b}) \Rightarrow \psi(\bar{a}) = \psi(\bar{b})$$

portanto, ψ está bem definida. Podemos verificar que ψ é um homomorfismo,sabendo que f é homomorfismo, temos

$$\psi(\bar{a} + \bar{b}) = \psi(a \bar{+} b) = f(a+b)\psi(\bar{a} + \bar{b}) = f(a) + f(b) = \psi(\bar{a}) + \psi(\bar{b}).$$

de forma análoga

$$\psi(\bar{a} \cdot \bar{b}) = \psi(\overline{a \cdot b}) = f(a \cdot b) = f(a) \cdot f(b) = \psi(\bar{a}) \cdot \psi(\bar{b}).$$

Para verificar que ψ é sobrejetiva, basta tomar $y \in Im(f)$, logo $y = f(x)$, para algum $x \in A$, como $\bar{x} \in A/ker(f)$, então $\psi(\bar{x}) = f(x) = y$, onde ψ é sobrejetora.

Por último, vamos mostrar que ψ é injetiva. Para isso, vamos tomar $\psi(\bar{a}) = \psi(\bar{b})$ verificar que $\bar{a} = \bar{b}$. Tomando então $\psi(\bar{a}) = \psi(\bar{b})$, temos

$$\psi(\bar{a}) = \psi(\bar{b}) \Rightarrow f(a) = f(b) \Rightarrow f(a-b) = 0 \Rightarrow a - b \in Ker(f) \Rightarrow \bar{a} = \bar{b}.$$

□

O teorema do isomorfismo nos diz que sempre que $f : A \longrightarrow B$ for um homomorfismo de anéis, vale $A/ker(f) \cong Im(f)$. Em particular, se f é sobrejetiva, então $A/Ker(f) \cong B$.

5.7 Espaços Vetoriais

Definição 48. *(Espaço vetorial) Um conjunto V não vazio é um espaço vetorial sobre (um corpo) K se seus elementos, denominados vetores, estiverem definidos as seguintes operações:*

1. *Cada par u, v de vetores de V corresponde a um vetor $u + v \in V$, chamado soma de u e v. (Fechamento da soma);*
2. $u + v = v + u, \forall\ u, v \in V$ *(Comutatividade da soma);*
3. $(u + v) + w = u(v + w), \forall\ u, v, w \in V$ *(Associatividade da soma);*
4. *existe em V um vetor, denominado vetor nulo e denotado por 0 tal que $0 + v = v + 0 = v, \forall v \in V$ (Existência de elemento neutro da soma);*
5. *A cada vetor $v \in V$ existe um vetor $-v$ in$V$, tal que $v + (-v) = 0$ (Inverso aditivo);*
6. *A cada $\alpha \in K$ e $v \in V$, corresponde a um vetor $\alpha v \in V$ denotado produto por escalar (Fechamento do produto);*
7. $(\alpha\beta)v = \alpha(\beta v), \forall\ \alpha, \beta \in K$ *e* $\forall\ v \in V$ *(Associatividade do produto);*
8. $1v = v, \forall\ v \in V$ *(Elemento neutro do produto);*
9. $\alpha(v + u) = \alpha v + \alpha u, \forall\ \alpha \in K, \forall\ u, v \in V$. *(Distributividade do escalar);*
10. $(\alpha + \beta)v = \alpha v + \beta v, \forall\ \alpha, \beta \in K, \forall\ v \in V$ *(Distributividade do vetor).*

Em um espaço vetorial V sobre um corpo K é comum que seja escrito k-espaço vetorial.

Exemplo 39. *O conjunto de polinômios*

$$P(K) = \{p(x) = a_n x^n + \cdots + a_1 x + a_0;\ a_i \in K \text{ e } n \geq 0\}$$

é um espaço vetorial sobre o corpo K, com as operações usuais de soma de polinômios e multiplicação por escalar.

Definição 49. *Seja V um espaço vetorial sobre K*

1. *Um vetor $v \in V$ é a combinação linear dos vetores $v_1, .., v_n \in V$ se existir $\alpha_1, ..., \alpha_n \in K$ tais que $v = \sum_{i=1}^{n} \alpha_i v_i$;*

2. *Seja β um subconjunto de V.β é dito conjunto gerador de V se todo elemento de V for uma combinação linear de um número finito de elementos de β.*

Definição 50. *Dizemos que um $K-$espaço vetorial e $A = \{v_1, ..., v_n\} \subset V, A$ é linearmente independente (ou simplesmente LI) se $\sum_{i=1}^{n} \alpha_i v_i = 0$, com $\alpha_i \in K$ só admite a solução $\alpha_i = 0$ para todo $i = \{1, ..., n\}$. Caso contrário, A é dito linearmente dependente (LD).*

Considere $\beta \subseteq V$, onde V é um espaço vetorial Quando todos os vetores de V são combinações lineares dos vetores de β, e além disso, β for linearmente independente, então dizemos que β é base de V.

Exemplo 40. *O conjunto $\{(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, ..., 1)\}$ é uma base de K^n sobre K. Esta base é chamada de base canônica de K^n.*

Exemplo 41. *O conjunto $B = \{cos^2 x, sen^2 x, -1\}$ é linearmente dependente, pois*

$$\alpha \cdot (cos^2 x) + \beta \cdot (sen^2 x) + \lambda \cdot (-1) = 0 \Rightarrow \alpha = \beta = \lambda = 1.$$

Observação 22. *Seja $K \subseteq L$ uma extensão de corpos, L pode ser visto como um espaço vetorial sobre K. Com efeito, as operações*

$$+ : L \times L \longrightarrow L$$

$$(u, v) \longmapsto u + v$$

e

$$\cdot : L \times K \longrightarrow L$$

$$(u, \lambda) \longmapsto v\lambda$$

já estão naturalmente definidas em L, e pode-se verificar que as condições de espaço vetorial são satisfeitas.

Definição 51. *(Subespaço vetorial) Seja V um espaço vetorial sobre um corpo K. Um subconjunto W de V é dito subespaço vetorial de V se W restrito as operações de V torne este conjunto um $K-$espaço vetorial.*

Exemplo 42. *Seja V um K-espaço vetorial, e seja $v \in V$. O conjunto $K \cdot v = \{\alpha v; \alpha \in K\}$ é um subespaço vetorial de V.*

5.8 Extensão de Corpos

Sabemos que $\mathbb{Q}$ e $\mathbb{R}$ são corpos. Neste capítulo, vamos alguns tipos de conjunto X que satisfazem as seguintes condições $\mathbb{Q} \subseteq X \subset R$. A verdade é que existe e vamos construir esse tipo de conjunto.

Exemplo 43. *Pode-se verificar que o conjunto* $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p}; a, b \in \mathbb{Q}\}$ *munido das operações usuais de soma e produto é um corpo para qualquer* p *primo.*

Definição 52. *Seja* K *um corpo* L *é dito uma extensão de* K *se* $K \subseteq L$.

Exemplo 44. *No exemplo acima vale as inclusões* $\mathbb{Q} \subset \mathbb{Q}[\sqrt{p}] \subset \mathbb{R}$.

Exemplo 45. *Sabemos que vale as inclusões* $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \subset \mathbb{C}$, *logo* $\mathbb{Q}[\sqrt{2}]$ *é uma extensão de* $\mathbb{Q}, \mathbb{R}$ *é uma extensão em ambos e por fim,* $\mathbb{C}$ *é uma extensão de cada um dos três.*

Definição 53. *Seja* K *um corpo e* $K \subseteq L$, *dizemos que* $\alpha \in L$ *é algébrico sobre* K *se existir* $f(x) \in K[x]$, *tal que* $f(\alpha) = 0$.

Exemplo 46. *Seja* $L = \mathbb{R}$, $K = \mathbb{Q}$ *e* $\alpha = \sqrt{2} \in \mathbb{R}$ *é algébrico sobre* $\mathbb{Q}$, *pois existe* $f(x) \in \mathbb{Q}[x]$ *tal que* $f(\sqrt{2}) = 0$, *basta tomar* $f(x) = x^2 - 2$.

Observação 23. *Caso contrário,* $\alpha \in L$ *é dito transcendente sobre* K. *Um exemplo é o número real* π *que é transcendente sobre* $\mathbb{Q}$.

Definição 54. *Seja* $K \subseteq L$ *uma extensão de corpos.* L *é dito uma extensão algébrica de* K *ae todo elemento de* L *é algébrico sobre* K

Exemplo 47. $\mathbb{Q}[\sqrt{2}]$ *é uma extensão algébrica sobre* $\mathbb{Q}$, *tome*

$$p(x) = x^2 - 2bx + (b^2 - 2a^2)$$

temos que qualquer elemento do conjunto $\mathbb{Q}[\sqrt{2}]$ *é raiz do polinômio* $p \in \mathbb{Q}[x]$.

Observação 24. $K \subseteq K$ *é uma extensão algébrica sobre* K, *pois dado* $\beta \in K$, *existe um polinômio* $f \in K[x]$ *tal que* β *é raiz. Basta tomar* $f(x) = x - \beta$.

Definição 55. *Dizemos que um corpo* K *é algebricamente fechado quando todo polinômio de grau maior do que ou igual a* 1 *em* $K[x]$ *admite pelo menos uma raiz em* K

Sejam $K \subset L$ uma extensão de corpos, $\alpha \in L$. Definimos o conjunto

$$K[\alpha] = \{f(\alpha); f(x) \in K[X]\}$$

é fácil de ver que $K[\alpha]$ é um domínio de integridade que contém K.

Exemplo 48. *Temos que $\mathbb{Q} \subset \mathbb{R}$ é uma extensão de corpos. Dado $\sqrt{2} \in \mathbb{R}$, podemos mostrar que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$. Com efeito, por definição $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}; f(x) \in \mathbb{Q})\}$. Por outro lado, se $f(x) \in \mathbb{Q}[x]$ então o algoritmo da divisão nos diz que existem únicos $q(x), r(x) \in \mathbb{Q}[x]$, tais que $f(x) = q(x) \cdot (x^2 - 2) + r(x)$, onde $r(x) = a + bx$ com $a, b \in \mathbb{Q}$, logo $f(\sqrt{2}) = a + b\sqrt{2}$.*

Proposição 39. *Sejam $K \subset L$ uma extensão de corpos, $\alpha \in L$ e $\psi : K[x] \longrightarrow L$, definido por $\psi(f(x)) = f(a)$. Então, ψ é um homomorfismo tal que:*

(i) $Im(\psi) = k[\alpha], K \subset K[\alpha] \subset L$;

(ii) α *é transcendente sobre* K *se, e somente se,* $ker(\psi) = \{0\}$

(iii) Se α *é algébrico sobre* K *e* $p(x) = irr(\alpha, K)$ *então* $ker(\psi) = \langle p(x) \rangle$ *é ideal maximal de* $k[x]$;

(iv) $\frac{K[x]}{ker(\psi)} \cong K[\alpha]$.

Corolário 14. *Se $\alpha \in L$ é algébrico sobre K então $K[\alpha]$ é corpo.*

Corolário 15. *Se $\alpha \in L$ é transcendente sobre K então $K[\alpha]$ é domínio de integridade.*

Proposição 40. *Seja $K \subset L$ uma extensão de corpos, e $\alpha in L$ algébrico sobre k. Se o grau do polinômio $irr(\alpha, K)$ é n, então para todo $f \in K[x], f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1 \cdot \alpha + \cdots + a_{n-1} \cdot \alpha^{n-1}$, de $a_0, a_1, ..., a_{n-1} \in K$.*

Demonstração. Seja $p(x) = irr(\alpha, K)$, sabemos que $\partial(p) = n$. Se $f \in K[x]$, o algoritmo da divisão nos garante que existem e são únicos $q(x), r(x) \in K[x]$, tais que $f(x) = q(x) \cdot p(x) + r(x)$, onde $\partial(r) = 0$ ou $\partial(r) < \partial(p)$, assim $r(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, onde $a_0, a_1, ..., a_n \in K$. Temos então que

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha) = r(\alpha)$$

o que nos diz que $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Queremos mostrar também que $f(\alpha)$ é único. Suponha então $f(\alpha) = a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, onde $a_i, b_i \in K$ com $i \in \{1, ..., n\}$, segue que o polinômio $h \in K[x]$, onde $h(x) = (a_0-b_0)+(a_1-b_1)\cdot x+\cdots+(a_{n-1}-b_{n-1})\cdot x^{n-1}$ é que

$$h(\alpha) = (a_0 - b_0) + (a_1 - b_1) \cdot \alpha + \cdots + (a_{n-1} - b_{n-1}) \cdot \alpha^{n-1}$$

$$= (a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) - (b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1})$$

$$= f(\alpha) - f(\alpha) = 0$$

note que $\partial(h) < n$ daí podemos afirmar que $h(x) = 0$, já que o $\partial(irr(\alpha, K)) = n$, então não pode haver nenhum outro polinômio, (com exceção do polinômio nulo) que tenha grau menor que n e α seja raiz. Por isso, $h(x) = 0$. Portanto, $a_i = b_i$, para todo $i \in \{1, ..., n\}$.

□

Definição 56. *Uma extensão de corpos $K \subset L$ diz-se finita se $[L : K] = n$ para algum $n \in \mathbb{N}$. Caso contrário $K \subset L$ diz-se uma extensão finita.*

Proposição 41. *Seja $K \subset L$ uma extensão de corpos então.*

1. *Se $K \subset L$ é finita então $K \subset L$ é uma extensão algébrica.*
2. *Se $\alpha \in L$ é algébrico sobre K e $\partial(irr(\alpha, K)) = n$ o conjunto $\beta = \{1, \alpha, ..., \alpha^{n-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre o corpo K e $[k[\alpha] : K] = n$.*
3. *Se $\alpha \in L$ é algébrico sobre K então $K \subset K[\alpha]$ é uma extensão finita.*

REFERÊNCIAS

1. ATIYAH, M.F.; MACDONALD, I.G. *introduction to commutative algebra*. Massachussetts;
2. Addison-Wesley Publishing Company, 1969.
3. COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties and algorithms*. New York: Springer, 2007.
4. DOMINGUES, H.; IEZZI, G. *Álgebra moderna*. Saõ Paulo; Atual, 1982.
5. ENDLER, O. *Teoria dos corpos*. Rio de Janeiro: IMPA, 2006.
6. GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. Rio de Janeiro: IMPA, 2008.
7. GONÇALVES, A. *Introdução à álgebra*. 5. ed. Rio de Janeiro: IMPA, 2008.
8. GONÇALVES, F.S *Introdução à geometria algébrica*. 2010. Trabalho de conclusão de curso (Graduação em matemática)- Universidade Federal de São Carlos, São Carlos, 2010.
9. HALMOS, P.R. *Teoriaingênua dos conjuntos*. Rio de Janeiro: Ciência Moderna, 2001.
10. JANESCH, O.R; TANEJA, I.J *Álgebra I*. 2.ed. Florianópolis: UFSC/EAD/CED/CFM, 2011.
11. MONTEIRO, L. H. J. *Elementos de álgebra* 2.ed. Rio de Janeiro: Livro e cientifico, 1978.