unesp

UNIVERSIDADE ESTADUAL PAULISTA

Sobre Curvas Planas Algébricas

GABRIELA SARANSZKY PRAMPOLIM

INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

RIO CLARO

2024

UNIVERSIDADE ESTADUAL PAULISTA
“Júlio de Mesquita Filho”
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

GABRIELA SARANSZKY PRAMPOLIM

SOBRE CURVAS PLANAS ALGÉBRICAS

Dissertação de Mestrado apresentada ao Instituto de Geociências e Ciências Exatas do Câmpus de Rio Claro, da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientadora: Elíris Cristina Rizziolli

Rio Claro - SP
2024

P898c

Prampolim, Gabriela Saranszky
Sobre Curvas Planas Algébricas / Gabriela Saranszky Prampolim. -- Rio Claro, 2024
106 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Instituto de Geociências e Ciências Exatas, Rio Claro
Orientadora: Elíris Cristina Rizziolli

1. Geometria Algébrica. 2. Conjuntos Algébricos. 3. Curvas Planas Algébricas. 4. Multiplicidade de Curvas Planas. 5. Interseção de Curvas Planas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Universidade Estadual Paulista (UNESP), Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Impacto potencial desta pesquisa

Este trabalho contém a reunião dos elementos necessários ao estudo de Curvas Planas Algébricas. Tendo em vista que, na atual literatura, há uma escassez de um texto em língua portuguesa sobre o assunto, a pertinência desse trabalho se dá por essa divulgação científica de forma acessível, contendo exemplos relevantes sobre esse tema tão complexo.

Potential impact of this research

This work contains the necessary elements for the study of Algebraic Plane Curves. Considering that, in the current literature, there is a scarcity of texts in Portuguese on the subject, the relevance of this work is due to its scientific dissemination in an accessible way, containing relevant examples on this complex topic.

UNIVERSIDADE ESTADUAL PAULISTA
"Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

GABRIELA SARANSZKY PRAMPOLIM

SOBRE CURVAS PLANAS ALGÉBRICAS

Dissertação de Mestrado apresentada ao Instituto de Geociências e Ciências Exatas do Câmpus de Rio Claro, da Universidade Estadual Paulista "Júlio de Mesquita Filho", como parte dos requisitos para obtenção do título de Mestre em Matemática.

Comissão Examinadora

Profa. Dra. ELÍRIS CRISTINA RIZZIOLLI
IGCE/ UNESP/ Rio Claro (SP)

Profa. Dra. DAIANE ALICE HENRIQUE AMENT
ICET/ UFLA/ Lavras (MG)

Profa. Dra. RENATA ZOTIN GOMES DE OLIVEIRA
IGCE / UNESP/ Rio Claro (SP)

Conceito: Aprovado.

Rio Claro (SP), 25 de abril de 2024.

Dedico essa dissertação a todos os alunos de graduação e pós-graduação que acham a Álgebra Abstrata difícil e impossível, porque eu também achava e só consegui chegar até aqui porque tive ajuda. Que este trabalho seja a ajuda que vocês precisam.

Dedico também esse trabalho a minha eu de 2018, que não fazia ideia do quanto ia se apaixonar pela Álgebra Abstrata, e a minha eu de 2020, por ir atrás dos próprios sonhos.

Agradecimentos

Agradeço aos meus pais pela paciência, mas especialmente porque eles não fazem ideia do que estudo e, mesmo assim, nunca deixaram de me apoiar.

Agradeço à minha orientadora e amiga, Profa. Dra. Elíris Cristina Rizziolli, que me acompanha desde a graduação, pelos seus ensinamentos, conselhos e apoio ao longo de todos esses anos, e por fazer eu me apaixonar pela Álgebra Abstrata

Agradeço também meus amigos, pela ajuda e apoio. Mas, em especial, agradeço à Hayen Alonso, que me ouviu animadamente falar sobre algo que ela não entende, me incentivando e me ajudando quando e como possível, por estar comigo nos meus altos e baixos, por todos os conselhos, lágrimas, risadas e companhia, por todas às vezes que me tirou de crises e por estar ao meu lado sempre. E também a Brena C. Sturion, Marina Fuzaro Magossi e Heloisa Alves Souza, por me ajudarem com apresentações, com minha ansiedade e com meus surtos, por nunca me deixarem desistir, pelas risadas e companhia ao longo de toda a graduação e pós-graduação.

Agradeço à minha gata, Catie, e ao meu cachorro, Nick, porque, sem eles, eu com certeza teria ficado louca.

Agradeço aos meus colegas de mestrado, pelas risadas, apoio e choros em conjunto. Sem vocês essa pós-graduação não teria sido tão animada e divertida.

Por fim, agradeço ao Kim Seokjin, ao Min Yoongi, ao Jung Hoseok, ao Kim Namjoon, ao Park Jimin, ao Kim Taehyung, ao Jeon Jungkook, a Taylor Swift e ao Harry Styles, por fazerem dos meus dias mais felizes durante todo esse processo e por me trazerem conforto com suas músicas e vídeos.

Now just walk lightly, whenever you want
Go on hopefully, wherever you walk
j-hope

Resumo

Neste trabalho estudamos algumas noções de anéis e corpos, conjuntos algébricos, Teorema de Hilbert e Curvas Planas Algébricas, os quais são elementos importantes para o principal objetivo desse projeto que é o estudo de Curvas Planas. A relevância deste tema segue da inter e multidisciplinaridade que este promove entre as áreas: Álgebra e Geometria.

Palavras-chave: Geometria Algébrica. Conjuntos Algébricos. Curvas Planas Algébricas. Multiplicidade de Curvas Planas. Interseção de Curvas Planas.

Abstract

In this paper, we studied some notions of rings and fields, algebraic sets, Hilbert's Nullstellensatz, and Algebraic Plane Curves, which are relevant elements to the main topic: Plane Curves. The relevance of this paper follows from the inter and multidisciplinarity between the areas: Algebra and Geometry.

Keywords: Algebraic Geometry. Algebraic Set. Algebraic Plane Curves. Multiplicity of Plane Curves. Intersection Curve.

Lista de Figuras

Sumário

1 Introdução

A Geometria Algébrica é o estudo das propriedades geométricas das soluções de equações polinomiais, sendo considerada um dos ramos de estudos da Matemática mais antigos, visto que os gregos consideravam a separação entre Geometria e Álgebra impossível, se utilizando de elementos geométricos para solucionar problemas algébricos. É após os postulados de Euclides, especialmente o quinto postulado[1], que o estudo da Geometria torna-se axiomático. Porém, com o surgimento das coordenadas cartesianas, ressurge o estudo da Geometria pelo ponto de vista algébrico, bem como o estudo de outras geometrias baseadas na negação do quinto postulado de Euclides.

Durante os séculos XVI e XVII, os matemáticos acreditavam que a verdadeira ciência era a Matemática e, por essa crença, fizeram diversas tentativas de unificar áreas da Matemática ou de desenvolver métodos que classificavam todos os elementos de uma determinada área da Matemática por uma única ótica. Uma dessas tentativas foi com relação à Geometria, onde Descartes procurou um método único para investigar e classificar todas as Curvas Algébricas. Esse aspecto, somado à invenção do Cálculo, em especial pelo desenvolvimento realizado por Leibniz, o ramo analítico da Geometria é favorecido.

É nesse aspecto que, em 1950, a Geometria Algébrica, com essa nova titulação, então torna-se derivada da Geometria Analítica, sendo, resumidamente, sua generalização, já que as propriedades geométricas das soluções de equações polinomiais, com coeficientes reais, em duas e três dimensões são abordadas em Geometria Analítica Plana e Espacial, respectivamente. A Geometria Algébrica, portanto, utiliza-se de elementos da Topologia, da Análise Complexa e da Álgebra para o estudo de Curvas Algébricas, cujo conceito abordaremos de forma mais aprofundada ao longo dessa dissertação.

As Curvas Algébricas são um dos objetos mais clássicos da Matemática. Tendo sido estudadas desde os primórdios da matemática, esse fato pode ser comprovado pelo estudo das cônicas por Manaechmus em torno de 150 d.C., da cissoide de Diocles e da conchoide de Nicomedes em torno de 200 d.C., das curvas de rolete durante a época da Renascença, das curvas Cassini e da lemniscata de Bernoulli no século XVII, e tantas outras curvas ao longo da história. Seu estudo levou ao desenvolvimento de diversos ramos da Matemática, entre eles a teoria invariante, superfícies de Riemann e Geometria Algébrica, como já previamente citada, contando com alguns dos maiores nomes da Matemática, como Descartes, Bernoulli, Abel, Jacobi, Riemann, Weierstrass e Noether. Nas últimas décadas, com o desenvolvimento tecnológico, as Curvas Algébricas possuem diversas aplicações, principalmente na Teoria de Codificação Algébrica, Criptografia e Sistemas Dinâmicos.

[1] O postulado afirma que por um ponto fora de uma reta pode-se traçar uma única reta paralela à reta dada.

Este trabalho contém a reunião dos elementos necessários ao estudo de Curvas Planas Algébricas, a saber: no capítulo 2 abordamos os elementos prévios, entre eles o estudo de anel de polinômios, no capítulo 3 apresentamos os conjuntos algébricos afins, em particular o Hilbert's Nullstellensatz, e no capítulo 4 é apresentado o tema central do trabalho: as Curvas Planas Algébricas. Na construção desses capítulos, utilizamos as referências de [1] ao [5], enquanto as referências [6] e [7] foram norteados da introdução, e a referência [8] trata-se do GeoGebra, software utilizado na construção dos exemplos.

Tendo em vista que, na atual literatura, há uma escassez de um texto em língua portuguesa sobre o assunto, a pertinência desse trabalho se dá por essa divulgação científica de forma acessível, contendo exemplos relevantes sobre esse tema tão complexo, os quais foram explorados usando como ferramenta o GeoGebra.

2 Conceitos Prévios

Antes de iniciarmos nosso estudo nos elementos da Geometria Algébrica, precisaremos relembrar alguns resultados e conceitos de anéis e corpos, já que esses serão utilizados posteriormente. Para esse capítulo, utilizamos as referências [1] e [2], além de complementarmos a maioria das demonstrações e elaborarmos exemplos para melhor compreensão dos conceitos apresentados.

2.1 Noções de Anéis e Corpos

Definição 2.1. Seja R um conjunto não vazio e um par de operações binárias sobre R: $+$ e $\cdot$, onde uma é adição $(x, y) \mapsto x + y$ e a outra multiplicação $(x, y) \mapsto x \cdot y$. Dizemos que $(R, +, \cdot)$ é um anel quando:

(I) $(R, +)$ é grupo abeliano, isto é:

  (i) para todo $a, b, c \in R : a+(b+c) = (a+b)+c$, ou seja, é válida a associatividade;

  (ii) para todo $a, b \in R : a + b = b + a$, ou seja, é válida a comutatividade;

  (iii) para todo $a \in R$, existe $0_R \in R$ tal que: $a + 0_R = a = 0_R + a$, isto é, existe elemento neutro;

  (iv) para todo $a \in R$, existe $-a \in R$ tal que: $a + (-a) = 0_R = (-a) + a$, isto é, existe oposto para todo elemento de R.

(II) A multiplicação é associativa, isto é: $\forall a, b, c \in R,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(III) A multiplicação é distributiva em relação à adição, o que vale dizer que, para todo $a, b, c \in R$: $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Observação 2.2. É comum denotarmos ab ao invés de $a \cdot b$, quando nos referimos à multiplicação em um anel.

Observação 2.3. Vale lembrar que as propriedades válidas para grupo também são válidas para o anel, com relação à adição.

Exemplo 2.4. Seja F o conjunto das funções $f : \mathbb{R} \to \mathbb{R}$. Observe que a terna $(F, +, \cdot)$ é um anel, onde

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

e

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

De fato:

(I) $(F, +)$ é grupo abeliano, pois:

(i) $\forall f, g, h \in F$,

$$f(x)+[(g+h)(x)] = f(x)+[g(x)+h(x)] = [f(x)+g(x)]+h(x) = [(f+g)(x)]+h(x).$$

(ii) $\forall f, g \in F$,

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

(iii) A função nula é elemento neutro do grupo $(F, +)$, já que

$$(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x).$$

(iv) $\forall f \in F$, a função $-f$ será o elemento oposto de f, já que:

$$(f + (-f))(x) = f(x) + (-f(x)) = f(x) - f(x) = 0.$$

(II) A multiplicação é associativa, pois, $\forall f, g, h \in F$,

$$f(x) \cdot [(g \cdot h)(x)] = f(x) \cdot [g(x) \cdot h(x)] = [f(x) \cdot g(x)] \cdot h(x) = [(f \cdot g)(x)] \cdot h(x).$$

(III) A multiplicação é distributiva em relação à adição, isto é, $\forall f, g, h \in F$,

$$f(x) \cdot [(g + h)(x)] = f(x) \cdot [g(x) + h(x)] = f(x) \cdot g(x) + f(x) \cdot h(x)$$

e

$$[(f + g)(x)] \cdot h(x) = [f(x) + g(x)] \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x).$$

Exemplo 2.5. Outros anéis importantes são:

- os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com a soma e multiplicação usuais;
- o conjunto das matrizes $n \times n$ com elementos em $\mathbb{R}$, com a soma e multiplicação usuais para matriz;
- o conjunto $(\mathbb{Z}_n, +_n, \cdot_n)$, onde $(\mathbb{Z}_n, +_n)$ é grupo cíclico e $\cdot_n$ é a multiplicação módulo n.

Teorema 2.6. *Seja R um anel com a unidade aditiva 0, então para todo $a, b \in R$, temos:*

(i) $0a = 0 = a0$*;*

(ii) $a(-b) = -(ab) = (-a)b$*;*

(iii) $(-a)(-b) = ab$*.*

Demonstração. Provemos cada uma das propriedades:

(i) Note que, pela Definição 2.1, temos que:

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Pela lei do cancelamento para o grupo aditivo $(R, +)$, temos que $a0 = 0$. De forma análoga, $0a = 0$, já que:

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a.$$

Desta forma, $a0 = 0 = 0a$.

(ii) Para provar esta propriedade, precisamos lembrar que, por definição, $-(ab)$ é o elemento que, ao adicionarmos ab, obtemos 0, isto é: $-(ab) + ab = 0$. Mostremos primeiramente que $a(-b) = -(ab)$, para tal, mostraremos que $a(-b) + ab = 0$. Pela definição 2.1:

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

já que, pela propriedade (I), $a0 = 0$. De forma análoga, provemos que $(-a)b+ab = 0$:

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

Assim, $a(-b) = -(ab) = (-a)b$.

(iii) Note que $(-a)(-b) = -(a(-b))$.

Pela propriedade (II), temos que: $-(a(-b)) = -(-(ab))$.

É preciso lembrar que, por definição, $-(-(ab))$ é o elemento que, operado com $-(ab)$, resulta em 0, isto é: $-(-(ab))+(-(ab)) = 0$. Mas, por definição, $(ab)+(-(ab)) = 0$.

Como o inverso de um grupo é único, temos que $-(-(ab)) = ab$, porém, vimos que $(-a)(-b) = -(-(ab))$, logo $(-a)(-b) = ab$.

□

Definição 2.7. Sejam R um anel e L um subconjunto não vazio de R. Dizemos que L é subanel de R se:

(i) L é fechado para as operações $+$ e $\cdot$ de R;

(ii) $(L, +, \cdot)$ também é um anel, onde $+$ e $\cdot$ são as operações de R.

Teorema 2.8. *Sejam R um anel e L um subconjunto não vazio de R. L é subanel de R se, e somente se, $a - b \in L$ e $ab \in L$, para todo $a, b \in L$.*

Demonstração. ($\Rightarrow$) Se L é subanel de R então, da definição, temos que L é um subgrupo do grupo abeliano R. Desta forma, $a - b \in L, \forall a, b \in L$. Além disso, pela definição de subanel, $ab \in L, \forall a, b \in L$.

($\Leftarrow$) Se $a, b \in L$, então $a - b \in L$, por hipótese. Logo, temos que L é subgrupo do grupo $(R, +)$. Por outro lado, considerando L fechado sob $\cdot$, por hipótese, temos que:

- Se $a, b, c \in L$, então $a, b, c \in R$, logo: $a(bc) = (ab)c$, portanto, vale a associatividade da multiplicação em L;

– Se $a, b, c \in L$, então $a, b, c \in R$, logo: $a(b+c) = ab + ac$ e $(a+b)c = ac + bc$, portanto, vale a distributividade de $\cdot$ sobre $+$ em L.

□

Observação 2.9. É importante salientar, pela própria definição de subanel, que todo subanel é, em particular, um anel. Com isso, por vezes, mostramos que um conjunto é subanel ao invés de mostrar que é um anel, como é o caso do próximo exemplo.

Observação 2.10. Utilizaremos $n\mathbb{Z}$ para denotar o conjunto $\{n \cdot k;\ k \in \mathbb{Z}\}$. Deste modo,

$$n\mathbb{Z} = \{n \cdot k;\ k \in \mathbb{Z}\} = \langle n \rangle.$$

Com isso, podemos variar a notação desse conjunto entre $n\mathbb{Z}$ e $\langle n \rangle$, conforme for mais conveniente.

Exemplo 2.11. Mostremos que a terna $(2\mathbb{Z}, +, \cdot)$ é subanel de $\mathbb{Z}$. Sejam $a, b \in \mathbb{Z}$, quaisquer. Note que se $a \in 2\mathbb{Z}$, então $a = 2k_1,\ k_1 \in \mathbb{Z}$. De forma análoga, $b = 2k_2,\ k_2 \in \mathbb{Z}$. Assim,

$$a - b = 2k_1 - 2k_2 = 2(k_1 - k_2) = 2k_3 \in 2\mathbb{Z},\ \text{onde } k_3 = k_1 - k_2 \text{ e } k_3 \in \mathbb{Z}.$$

Além disso,

$$ab = 2k_1 \cdot 2k_2 = 2(2k_1k_2) = 2k_4 \in 2\mathbb{Z},\ \text{onde } k_4 = 2k_1k_2 \text{ e } k_4 \in \mathbb{Z}.$$

Deste modo, pelo Teorema 2.8, $2\mathbb{Z}$ é subanel de $\mathbb{Z}$.

Definição 2.12. Seja R um anel. Dizemos que R é um *anel comutativo* se, para todo $a, b \in R$, temos que:

$$ab = ba.$$

Exemplo 2.13. O anel $2\mathbb{Z}$ é comutativo. Já vimos, pelo Exemplo 2.11 que $2\mathbb{Z}$ é um anel, portanto, basta mostrarmos a comutatividade. Sejam $a, b \in 2\mathbb{Z}$, quaisquer, então $a = 2k_1$ e $b = 2k_2$, onde $k_1, k_2 \in \mathbb{Z}$. Assim,

$$a \cdot b = 2k_1 \cdot 2k_2 = 2k_2 \cdot 2k_1 = b \cdot a.$$

Exemplo 2.14. O anel das matrizes 2×2, com entradas em $\mathbb{R}$, não é comutativo. Considere $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ e $B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$.

$$A \cdot B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

mas

$$B \cdot A = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 + 6 \cdot 3 & 5 \cdot 2 + 6 \cdot 4 \\ 7 \cdot 1 + 8 \cdot 3 & 7 \cdot 2 + 8 \cdot 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix}$$

Deste modo, $A \cdot B \neq B \cdot A$.

De modo geral, o anel das matrizes $n \times n$, com entradas em $\mathbb{R}$, não é comutativo para $n \geq 2$.

Definição 2.15. Seja R um anel. Se R possui um elemento neutro para a multiplicação, isto é, existe $1_R \in R$, onde $1_R \neq 0_R$, tal que

$$a \cdot 1_R = a = 1_R \cdot a,$$

para qualquer $a \in R$, então dizemos que 1_R é *unidade* de R e que R é um *anel com unidade*.

Definição 2.16. Dizemos que um anel é comutativo com unidade quando a multiplicação é comutativa e possui unidade.

Exemplo 2.17. Seja F o conjunto das funções reais. Já vimos que a terna $(F, +, \cdot)$ é um anel. Observe que, mais ainda, é um anel comutativo com unidade. De fato, $\forall f, g \in F$,

$$(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x).$$

Além disso, a função constante $1(x) = 1$ é a unidade desse anel, pois, $\forall f \in F$,

$$(f \cdot 1)(x) = f(x) \cdot 1(x) = f(x) \cdot 1 = f(x).$$

Exemplo 2.18. O anel $2\mathbb{Z}$ é comutativo, porém não possui unidade. Observe que como $2\mathbb{Z}$ é subanel de $\mathbb{Z}$, poderíamos supor que o elemento unidade poderia ser o próprio 1, porém $1 \notin 2\mathbb{Z}$. Além deste, nenhum outro elemento de $2\mathbb{Z}$ satisfaz a condição $a \cdot 1_R = a$, para todo $a \in 2\mathbb{Z}$.

Definição 2.19. Um elemento u de um anel comutativo com unidade R é dito *invertível* em R se u divide 1_R, isto é, se u possui inverso multiplicativo em R.

Quando dizemos que u divide 1_R, queremos dizer que é possível obter $b \in R$ tal que $u \cdot b = 1_R$.

Exemplo 2.20. Os únicos elementos invertíveis do anel $\mathbb{Z}$ são os elementos 1 e -1, já que $1 \cdot 1 = 1$ e $(-1) \cdot (-1) = 1$. Observe que não é possível multiplicar quaisquer outros dois elementos e obter o elemento neutro da multiplicação, isto é, o elemento 1, como resultado e, portanto, 1 e -1 são os únicos elementos invertíveis de $\mathbb{Z}$.

Definição 2.21. Um elemento a de um anel R é dito irredutível se para alguma fatorização $a = bc$, $b, c \in R$, tem-se que b ou c são invertíveis.

Definição 2.22. Dois elementos $a, b \in R$ são *associados* em R se $a = bu$, onde u é invertível em R.

Definição 2.23. Seja R um anel comutativo. Um subconjunto $I \subset R$ não vazio será chamado de *ideal* de R se:

(i) para todo $x, y \in I : x - y \in I$;

(ii) para todo $a \in R$ e $x \in I : ax \in I$.

Observação 2.24. Pela Definição 2.23 e pelo Teorema 2.8, todo ideal de um anel R é subanel de R. Entretanto, a afirmação recíproca não é verídica (vide Exemplos 2.26 e 2.27).

Exemplo 2.25. Seja F o anel das funções reais. Observe que o subanel N formado pelas funções tais que $f(2) = 0$ é um ideal de F, pois:

(i) $\forall f, g \in N$, $(f-g)(2) = f(2) - g(2) = 0 - 0 = 0 \in N$;

(ii) $\forall f \in F$, $\forall g \in N$, $(fg)(2) = f(2)g(2) = f(2) \cdot 0 = 0 \in N$.

Exemplo 2.26. Seja F o anel das funções reais. Observe que o subconjunto C de F, formado pelas funções tais que $f(x)$ é uma constante não nula, é um subanel, porém não é um ideal de F. Note que é um subanel fechado para o produto, pois:

$$\forall f, g \in C,\ (f-g)(x) = f(x) - g(x) = k - l = m \in C,\ \text{onde } k, l, m \in \mathbb{Z} \text{ são constantes.}$$

No entanto, não é um ideal, já que, se supormos $f(x) = 2 \in C$ e $g(x) = \operatorname{sen} x \in F$, teremos:

$$(f \cdot g)(x) = f(x)g(x) = 2\operatorname{sen} x \notin C,\ \text{já que } 2\operatorname{sen} x \text{ não é uma função constante.}$$

Exemplo 2.27. Considere $\mathbb{Q}$ o anel dos números racionais e $\mathbb{Z}$ seu sub-anel dos números inteiros. Note que $\mathbb{Z}$ não é ideal de $\mathbb{Q}$, pois considerando $\frac{1}{2} \in \mathbb{Q}$ e $1 \in \mathbb{Z}$ temos que

$$1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}.$$

Isso nos mostra que nem todo subanel será ideal.

Proposição 2.28. *Seja I um ideal de um anel comutativo R, então:*

1. *$0_R \in I$;*
2. *Se $a \in I$, então $-a \in I$;*
3. *Se $a, b \in I$, então $a + b \in I$;*
4. *Se o anel possui unidade e se algum elemento invertível do anel pertence a I, então $I = R$.*

Demonstração. Demonstremos cada um dos itens da proposição:

1. Seja $a \in I$. Como $I \neq \emptyset$ e I é ideal, então $a - a \in I$, pela Definição 2.23. Logo, $0_R \in I$.
2. Como $0_R \in I$, pelo item 1, e $a \in I$, então $0_R - a \in I$, pela Definição 2.23, deste modo $-a \in I$.
3. Sejam $a, b \in I$. Pelo item 2, temos que $-b \in I$. Assim, pela Definição 2.23, $a - (-b) \in I$, por propriedade de grupo aditivo, temos que $a + b \in I$.
4. Já temos, por definição, que $I \subset R$ e assim mostremos que $R \subset I$. Para isso, tomemos $a \in R$ qualquer. Como R possui unidade, temos que $a = a \cdot 1$. Agora, veja que algum elemento dentro de I, digamos u, é invertível. Por hipótese, então existe $v \in R$ tal que $uv = 1$. Pela Definição 2.23, temos que, como $u \in I$ e $v \in R$, então $uv \in I$. Como $uv = 1$, logo $1 \in I$ e, assim, $a = a \cdot 1 \in I$. Portanto, $R \subset I$.

□

Definição 2.29. Dizemos que um ideal I do anel R é próprio se $I \neq R$.

Definição 2.30. Seja P um ideal em um anel comutativo R. Dizemos que P é *ideal primo* se:

(i) $P \neq R$;

(ii) Para todo $a, b \in R$ tal que $ab \in P$, então $a \in P$ ou $b \in P$.

Definição 2.31. Seja M um ideal em um anel comutativo R. Dizemos que M é *ideal maximal* se:

(i) $M \neq R$;

(ii) Os únicos ideais de R que contém M são o próprio M e R, isto é, se P é um ideal de R diferente de M tal que:

$$M \subsetneq P \subseteq R \Rightarrow P = R.$$

Proposição 2.32. *Todo ideal maximal de um anel comutativo com unidade é um ideal primo.*

Demonstração. Seja M um ideal maximal de um anel comutativo R com unidade. Mostremos que M é um ideal primo, ou seja, $\forall a, b \in R$ tais que $ab \in M$, teremos $a \in M$ ou $b \in M$.

Para tanto, sejam $a, b \in R$ tais que $a \notin M$ e $ab \in M$.

Defina o ideal $J = \langle a \rangle + M$ em R. Veja que, $M \subset J$, por definição de J. Mais ainda, $M \neq J$, já que $a \in J$ e $a \notin M$. Desta forma, temos a seguinte relação:

$$M \subsetneq J \subset R.$$

Mas M é ideal maximal de R, por hipótese, logo $J = R$. Consequentemente,

$$1 \in R = J = \langle a \rangle + M,$$

ou seja, $1 \in \langle a \rangle + M$. Assim, existem $r \in R$ e $m \in M$ tal que:

$$1 = ra + m.$$

Multiplicando essa igualdade por b temos que:

$$1b = (ra)b + mb \Rightarrow b = r(ab) + mb.$$

Como $ab \in M$ e $m \in M$ então temos que $r(ab) \in M$ e $mb \in M$, já que M é ideal. Deste modo, $r(ab) + mb \in M$ e, portanto, $b \in M$. Com isso, temos que M é um ideal primo. □

Definição 2.33. Se R é um anel comutativo e S é um subconjunto de R, podemos definir o ideal gerado por S como o conjunto: $I = \{\sum a_i s_i;\ s_i \in S, a_i \in R\}$ um ideal gerado por S.

Definição 2.34. Sejam $(R, +_R, \cdot_R)$ e $(S, +_S, \cdot_S)$ anéis e $\phi : R \longrightarrow S$ uma aplicação. Dizemos que ϕ é um *homomorfismo de anéis* se, para todo $a, b \in R$:

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{e} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b).$$

Exemplo 2.35. Tomemos $\mathbb{Z}$ e $\mathbb{Z}_m$. Note que $\phi : \mathbb{Z} \to \mathbb{Z}_m$, definida por $\phi(a) = \overline{a}$ é um homomorfismo de anéis. De fato, $\forall a, b \in \mathbb{Z}$,

- $\phi(a+b) = \overline{a+b} = \overline{a} +_m \overline{b} = \phi(a) +_m \phi(b)$;
- $\phi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot_m \overline{b} = \phi(a) \cdot_m \phi(b)$.

Definição 2.36. Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Damos o nome *núcleo de* ϕ, denotado por $\ker(\phi)$, ao subconjunto de R:

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

Observação 2.37. Note que $\phi(0_R) = 0_S$, já que ϕ é homomorfismo do grupo aditivo R no grupo aditivo S, logo $0_R \in \ker(\phi)$. Portanto, $\ker(\phi) \neq \emptyset$, pois ao menos $0_R \in \ker(\phi)$.

Exemplo 2.38. Seja $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por $\phi(a, b) = a$. Veja que ϕ é um homomorfismo de anéis, pois: $\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$,

- $\phi((a, b) + (c, d)) = \phi(a + c, b + d) = a + c = \phi(a, b) + \phi(c, d)$.
- $\phi((a, b) \cdot (c, d)) = \phi(a \cdot c, b \cdot d) = a \cdot c = \phi(a, b) \cdot \phi(c, d)$.

Agora, analisemos o $ker(\phi)$:

$$\begin{aligned} ker(\phi) &= \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ \phi(a, b) = 0\} \\ &= \{(a, b) \in \mathbb{Z} \times \mathbb{Z};\ a = 0\} \\ &= \{(0, b);\ b \in \mathbb{Z}\}. \end{aligned}$$

Proposição 2.39. *Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Então é válido:*

(i) $\ker(\phi)$ *é subanel de* R*;*

(ii) ϕ *é injetor se, e somente se,* $\ker(\phi) = \{0_R\}$.

Demonstração. Mostremos ambas as propriedades:

(i) Sejam $a, b \in \ker(\phi)$, logo $\phi(a) = \phi(b) = 0_S$. Com isso, temos que:

$$\phi(a - b) = \phi(a) - \phi(b) = 0_S$$

e

$$\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b) = 0_S \cdot_S 0_S = 0_S.$$

Portanto, $a - b \in \ker(\phi)$ e $ab \in \ker(\phi)$, logo, pelo Teorema 2.8, $\ker(\phi)$ é subanel de R.

(ii) ($\Rightarrow$) Por hipótese, temos que ϕ é injetora. Queremos mostrar que $\ker(\phi) = 0_R$, e, para isso, tomemos $a \in \ker(\phi)$ para mostrar que $a = 0_R$.
Se $a \in \ker(\phi)$, então $\phi(a) = 0_S$. Mas, como já mencionado, $\phi(0_R) = 0_S$. Como ϕ é injetora, temos que $a = 0_R$.

($\Leftarrow$) Sejam $a, b \in R$ tais que $\phi(a) = \phi(b)$. Multiplicando cada membro da igualdade pelo inverso multiplicativo de $\phi(b)$, $[\phi(b)]^{-1}$ temos que:

$$\phi(a) \cdot_S [\phi(b)]^{-1} = 1_S.$$

Mas ϕ é homomorfismo de anel, logo:

$$\phi(a) \cdot_S [\phi(b)]^{-1} = \phi(a \cdot_R b^{-1}).$$

Portanto, $\phi(a \cdot_R b^{-1}) = 1_S$, logo $ab^{-1} \in \ker(\phi)$. Como, por hipótese, $\ker(\phi) = 0_R$, temos que $a \cdot_R b^{-1} = 0_R$. Operando b nos dois lados da equação temos que:

$$a = b.$$

Logo, ϕ é injetora.

□

Exemplo 2.40. Seja $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definida por $\phi(n) = (n, 0)$. Veja que ϕ é um homomorfismo: $\forall m, n \in \mathbb{Z}$,

- $\phi(m + n) = (m + n, 0) = (m + n, 0 + 0) = (m, 0) + (n, 0) = \phi(m) + \phi(n)$.
- $\phi(m \cdot n) = (m \cdot n, 0) = (m \cdot n, 0 \cdot 0) = (m, 0) \cdot (n, 0) = \phi(m) \cdot \phi(n)$.

Analisemos agora o $ker(\phi)$:

$$\begin{aligned} ker(\phi) &= \{x \in \mathbb{Z};\ \phi(x) = (0, 0)\} \\ &= \{x \in \mathbb{Z};\ (x, 0) = (0, 0)\} \\ &= \{x \in \mathbb{Z};\ x = 0\} \\ &= \{0\}. \end{aligned}$$

Pela proposição anterior, item (ii), temos que ϕ é um homomorfismo de anéis injetor.

Proposição 2.41. *Se R um anel, com $\phi : R \longrightarrow S$ um homomorfismo de anel, então* $\ker(\phi)$ *é ideal de R.*

Demonstração. Por propriedade de homomorfismo, temos que $\ker(\phi) \neq \emptyset$. Basta mostrar que, para quaisquer $r \in R$ e $a \in \ker(\phi)$, temos $r \cdot_R a \in \ker(\phi)$.

Seja $r \in R$ e $a \in \ker(\phi)$. Note que $\phi(a) = 0_S$. Além disso, veja que:

$$\phi(r \cdot_R a) = \phi(r) \cdot_S \phi(a) = \phi(r) \cdot_S 0_S = 0_S.$$

Logo, $r_R \cdot a \in \ker(\phi)$. Portanto, $\ker(\phi)$ é ideal de R. □

Proposição 2.42. *Se R e S são anéis, com $\phi : R \longrightarrow S$ um homomorfismo de anéis, então $\phi(R)$ é subanel de S.*

Demonstração. Já temos, por definição, que $\phi(R) \subset S$. Para mostrar que $\phi(R)$ é subanel de S, pelo Teorema 2.8, basta mostrar que $s_1 - s_2 \in \phi(R)$ e $s_1 s_2 \in \phi(R)$, para todo $s_1, s_2 \in \phi(R)$.

Para tal, tomemos $s_1, s_2 \in \phi(R)$ quaisquer. Então, existem $r_1, r_2 \in R$ tais que $\phi(r_1) = s_1$ e $\phi(r_2) = s_2$. Deste modo:

$$s_1 - s_2 = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2) \in \phi(R).$$

Além disso,

$$s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(R).$$

□

Definição 2.43. Seja $\phi : R \longrightarrow S$ um homomorfismo de anéis. Se ϕ for uma bijeção, então será chamado de *isomorfismo* de R em S. Neste caso, chamamos ϕ de *isomorfismo de anéis*.

Definição 2.44. Seja $\phi : R \longrightarrow S$. Um isomorfismo é *canônico* quando ϕ é uma função inversível, então dizemos que R é canonicamente isomorfo a S.

Definição 2.45. Sejam $a, b \in R$, R anel, onde $a \neq 0_R$ e $b \neq 0_R$, dizemos que a e b são divisores de zero quando $ab = 0_R$.

Definição 2.46. Seja R um anel comutativo com unidade $1_R \neq 0_R$. Dizemos que R é um *anel de integridade*, ou *domínio de integridade*, quando R não possui divisores de zero, isto é:

$$ab = 0_R \Leftrightarrow a = 0_R \text{ ou } b = 0_R,$$

para quaisquer $a, b \in R$.

Definição 2.47. Sejam R um domínio e $a, b \in R$. Dizemos que a *divide* b, ou que a é um divisor de b, e escrevemos $a \mid b$ se existe $x \in R$ tal que $b = ax$. Caso contrário, escrevemos $a \nmid b$ e dizemos que a não é divisor de b, ou que a não divide b. Dizemos que a e b são *associados* ou que a é associado de b se existe u invertível em R, tal que $a = bu$ e neste caso, escrevemos $a \sim b$.

Definição 2.48. Sejam R um domínio e $a, b \in R$. Dizemos que a divide b, ou que a é um *divisor próprio* de b se $a \mid b$, com a não invertível e $a \nsim b$, ou seja, $b = a \cdot b$, com a e x não invertíveis.

Um elemento $q \in R$ é um *elemento irredutível* de R se $q \neq 0$, q não invertível e q não tem divisores próprios de R, isto é, se $a \mid q$, então a é invertível ou $a \sim q$.

Um elemento $p \in R$ é um *elemento primo* de R se $p \neq 0$, p não invertível e, se $a, b \in R$ tais que $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.

Definição 2.49. Sejam R um anel comutativo, I um ideal e S um subconjunto de R. I é finitamente gerado se ele é gerado por um conjunto finito $S = \{a_1, a_2, \cdots, a_n\} \subset R$, ou seja, $I = \langle a_1, \cdots, a_n \rangle$.

O ideal gerado por um conjunto unitário $\{a\}$ é chamado de *ideal principal* gerado por a e denotador por $\langle a \rangle$.

Lema 2.50. *Sejam R um domínio e $a, b \in R$. Então:*

(i) $a \mid b \iff \langle b \rangle \subseteq \langle a \rangle$;

(ii) $a \sim b \iff \langle b \rangle = \langle a \rangle$;

(iii) *a é um divisor próprio de b se, e só se,* $\langle a \rangle \neq R$ *e* $b \subsetneqq \langle a \rangle$;

(iv) *a é invertível se, e só se,* $\langle a \rangle = R$.

Demonstração. (i) $a \mid b$ se, e somente se, existe $c \in R$ tal que $b = c \cdot a \iff b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle$;

(ii) $a \sim b \iff a \mid b$ e $b \mid a \iff \langle b \rangle \subseteq \langle a \rangle$ e $\langle a \rangle \subseteq \langle b \rangle \iff \langle a \rangle = \langle b \rangle$;

(iii) a é um divisor próprio de $b \iff a \mid b$, a não invertível e $a \nsim b \iff a \neq R$ e $\langle a \rangle \neq \langle b \rangle$ e $\langle b \rangle \nsubseteq \langle a \rangle$;

(iv) a é invertível $\iff a \sim 1 \iff \langle a\rangle = \langle 1\rangle = R$, onde 1 é a unidade de R.

□

Teorema 2.51. *Seja R um anel comutativo com unidade. Então $p \in R$ é um elemento primo de R se, e somente se, $\langle p\rangle$ é um ideal primo não nulo de R.*

Demonstração. Se p é um elemento primo de R, então $p \neq 0$ e p não é invertível, o que implica que $\langle p\rangle \neq \langle 0\rangle$ e $\langle p\rangle \neq R$.

Se $a, b \in R$ são tais que $a \cdot b \in \langle p\rangle$, então $p \mid a \cdot b$ e, como p é primo, temos que $p \mid a$ ou $p \mid b$. Do Lema 2.50 obtemos $\langle a\rangle \subseteq \langle p\rangle$ ou $\langle b\rangle \subseteq \langle p\rangle$, ou seja, $a \in \langle p\rangle$ ou $b \in \langle p\rangle$, o que mostra que $\langle p\rangle$ é um ideal primo não nulo de R.

Reciprocamente, se $\langle p\rangle$ é um ideal primo não nulo de R, então $\langle p\rangle \neq \langle 0\rangle$ e $\langle p\rangle \neq R$. Logo, $p \neq 0$ e p não é invertível. Se $p \mid a \cdot b$, então $a \cdot b \in \langle p\rangle$. Como $\langle p\rangle$ é um ideal primo, temos que $a \in \langle p\rangle$ ou $b \in \langle p\rangle$, o que implica que $p \mid a$ ou $p \mid b$. Portanto p é um elemento primo de R. □

Definição 2.52. Se todos os ideais de um anel comutativo são principais, então esse anel recebe o nome de *anel principal*.

Definição 2.53. Um domínio de integridade em que todo ideal é principal é chamado de *domínio de ideais principais* ou PID.

Exemplo 2.54. $\mathbb{Z}$ é PID. De fato, seja I um ideal em $\mathbb{Z}$. Se $I = \{0\}$, então segue que I é ideal principal de $\mathbb{Z}$, pois $\langle 0\rangle = \{x \cdot 0;\ x \in \mathbb{Z}\} = \{0\}$. Se $I \neq \{0\}$, então I possui um elemento a não nulo e, portanto, $-a \in I$. Como a ou $-a$ é estritamente positivo, então I possui elementos estritamente positivos, o menor dos quais chamaremos de b.

Queremos, então, provar que $I = \langle b\rangle$. Como $b \in I$, então $\langle b\rangle \subset I$.

Mostremos agora que $I \subset \langle b\rangle$. Para tal, tome $m \in I$ qualquer. Aplicando o algoritmo da divisão euclidiana, utilizando m como dividendo, b como divisor, q sendo o quociente e r o resto ($0 \leq r < b$), temos que:

$$m = bq + r.$$

Disto, temos que

$$r = m - bq$$

e, portanto, $r \in I$, já que $m, b \in I$ e I é ideal. Mas como b é o menor inteiro estritamente positivo em I e $r < b$, então, necessariamente, $r = 0$. Assim, $m = bq$, isto é, $m \in \langle b\rangle$. Deste modo, $I \subset \langle b\rangle$. Com isso, temos que $I = \langle b\rangle$.

Relembrando da Observação 2.10, quando falamos do subanel $n\mathbb{Z}$, que indicamos por $\langle n\rangle$, vemos então que o mesmo é, também, um ideal. E, por isso, continuamos, por vezes, denotando o ideal gerado por n por $\langle n\rangle$ ou $n\mathbb{Z}$.

Definição 2.55. Seja R um domínio de integridade. A característica de R, $char(R)$, é o menor inteiro positivo p tal que $\underbrace{1 + \cdots + 1}_{p \text{ vezes}} = 0$. Se tal p não existe, $char(R) = 0$.

Teorema 2.56. *Se R é um PID, então todo elemento de R não nulo diferente da unidade é um produto de fatores irredutíveis.*

Demonstração. Seja $a \in R$, onde $a \neq 0_R$ e $a \neq 1_R$. Se a for irredutível, não há o que mostrar. Se a não for irredutível, mostremos que ele tem ao menos um fator irredutível.

Como a é não irredutível, então podemos escrever $a = a_1 b_1$, onde tanto a_1 quanto b_1 são diferentes da unidade. Note que $\langle a \rangle$ está contido propriamente em $\langle a_1 \rangle$, pois se $\langle a \rangle = \langle a_1 \rangle$, então b seria uma unidade, o que não ocorre, por hipótese. Continuando esse processo a partir de a_1, construímos uma cadeira ascendente de ideais contidos propriamente.

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$$

Pelo Lema 45.10[1] ([1], p.392), essa cadeia estaciona em algum $\langle a_r \rangle$ e, então, a_r necessariamente é irredutível, pois, caso contrário, a_r se escreveria da forma $a_r = b \cdot c$, em que b e c diferem da unidade, então $\langle a_r \rangle \subsetneqq \langle b \rangle$, contradizendo o fato da cadeira supracitada ser estacionária. Portanto, a tem um fator irredutível a_r.

Pelo que acabamos de mostrar, para um elemento a, que é diferente de zero e não é uma unidade em R, temos que: ou a é irredutível, ou $a = p_1 c_1$, em que p_1 é um elemento irredutível de R, c_1 não é a unidade e, por consequência, $\langle a \rangle \subset \langle c_1 \rangle$.

Se c_1 não é irredutível, então $c_1 = p_2 c_2$, onde p_2 é irredutível e c_2 não é uma unidade. Continuando esse processo, temos a seguinte cadeira ascendente de ideais propriamente contidos:

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots$$

a qual é estacionária, pelo Lema 45.10 ([1], p.392), logo necessariamente algum $c_r = q_r$ é irredutível, e então:

$$c = p_1 p_2 \cdots p_r q_r.$$

□

Proposição 2.57. *Um ideal $\langle a \rangle$ em um PID é maximal se, e somente se, a é irredutível.*

Demonstração. ($\Rightarrow$) Seja $\langle a \rangle$ um ideal maximal de S, sendo S um PID. Suponha $a = xy \in S$, então $\langle a \rangle \subseteq \langle x \rangle$.

Se $\langle x \rangle = \langle a \rangle$, então, x e a estão associados, logo y é invertível em S.

Se $\langle x \rangle \neq \langle a \rangle$, então teremos $\langle x \rangle = \langle 1 \rangle = S$, já que $\langle a \rangle$ é maximal. Mas x e 1 estão associados, logo x é invertível em S.

Portanto, se $a = xy$, então x ou y são invertíveis, assim a é irredutível.

($\Leftarrow$) Seja a irredutível em S. Suponha $\langle x \rangle$ ideal de S tal que

$$\langle a \rangle \subsetneqq \langle x \rangle \subseteq S.$$

Veja que $\langle x \rangle = S$. De fato, como $\langle a \rangle \subset \langle x \rangle$, então podemos dizer que $a = xy$, para algum $y \in S$. Mas a é irredutível, por hipótese, assim x ou y são unidades de S.

Se x for uma unidade de S, então $\langle x \rangle = \langle 1 \rangle = S$.

Se x não for uma unidade de S, então y o é. Logo existe $u \in S$ tal que $yu = 1$. Com isso, podemos afirmar que $au = xyu = x$, portanto $\langle x \rangle \subseteq \langle a \rangle$. Consequentemente, $\langle x \rangle = \langle a \rangle$, o que é absurdo por hipótese.

[1] **Lema 45.10 [Condição para Cadeia Ascendente para um PID]:** Seja R um PID. Se $N_1 \subseteq N_2 \subseteq \cdots$ é uma cadeira ascendente de ideias N_i, então existem inteiros positivos r tais que $N_r = N_s$ para todo $s \geq r$. Equivalentemente, toda cadeia de ideias estritamente ascendente (todas propriamente contidas) em um PID é finita. A demonstração desse Proposição encontra-se na página 392 de [1].

Portanto, necessariamente x é uma unidade de S e $\langle x\rangle = S$, onde concluímos que $\langle a\rangle$ é maximal.

□

Proposição 2.58. *Em um PID, se um irredutível p divide ab, então p divide a ou p divide b.*

Demonstração. Seja S um PID e suponha p seja um elemento irredutível em S tal que $p \mid ab$, logo $ab \in \langle p\rangle$. Como $\langle p\rangle$ é ideal maximal em S, pela Proposição anterior, e todo ideal maximal é ideal primo, pela Proposição 2.32, então $ab \in \langle p\rangle$ implica que $a \in \langle p\rangle$ ou $b \in \langle p\rangle$, ou seja, $a = r_1 p$ ou $b = r_2 p$, com $r_1, r_2 \in S$, o que nos dá que $p \mid a$ ou $p \mid b$. □

Observação 2.59. Podemos utilizar o Princípio da Indução Finita na proposição anterior e concluir que se p é um irredutível em um PID S e $p \mid a_1 a_2 \cdots a_n$, para $a_i \in S$, então $p \mid a_i$, para algum i.

Definição 2.60. Um domínio de integridade R é domínio de fatoração única, ou UFD, se todo elemento não nulo em R pode ser unicamente fatorado, a menos de elementos invertíveis e da ordem de fatores, em elementos irredutíveis.

Proposição 2.61. *Em um UFD, todo elemento irredutível é primo.*

Demonstração. Sejam R UFD e $q \in R$ um elemento irredutível. Então $q \neq 0$ e q não invertível. Se $a, b \in R$ são tais que $q \mid a \cdot b$, escrevendo $a = p_1 \cdots p_r$ e $b = q_1 \cdots q_s$, com p_i e q_j elementos irredutíveis em R, temos que uma fatoração para $a \cdot b$ é

$$a \cdot b = p_1 \cdots p_r \cdot q_1 \cdots q_s.$$

Como $q \mid a \cdot b$, temos que $a \cdot b = q \cdot c$, para algum $c \in R$.

Pela unicidade da fatoração de $a \cdot b$, temos que $q \sim p_i$ ou $q \sim q_j$, para algum índice i, j. Agora, $q \mid p_i$ e $p_i \mid a$, implica que $q \mid a$ ou $q \mid q_j$ e $q_j \mid b$, implica que $q \mid b$, o que mostra que q é primo. □

Teorema 2.62. *Todo PID é UFD.*

Demonstração. Veja que, pelo Teorema 2.56, já temos que se S é um PID, então todo $a \in S$ pode ser fatorado em fatores irredutíveis $a = p_1 p_2 \cdots p_r$. Basta mostrar que essa fatoração é única, a menos da ordem dos fatores. Seja

$$a = q_1 q_2 \cdots q_s$$

outra fatorização de a em fatores irredutíveis. Com isso, temos que $p_1 \mid (q_1 q_2 \cdots q_s)$. Desta forma, podemos afirmar que $p_1 \mid q_j$, para algum j. Como podemos alterar a ordem dos fatores se necessário, podemos assumir que $p_1 \mid q_1$, então $q_1 = p_1 u_1$. Como p_1 é irredutível, u_1 é uma unidade, e, assim, p_1 e q_1 estão associados. Desta forma:

$$p_1 p_2 \cdots p_r = p_1 u_1 q_2 \cdots q_s.$$

Pela lei do cancelamento em S, podemos afirmar que

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

De forma contínua e análoga, chegaremos que

$$1 = u_1 u_2 \cdots u_r q_{r+1} \cdots q_s.$$

Como q_j são irredutíveis temos que $r = s$. Logo, a fatorização é única, a menos da ordem dos elementos. □

Exemplo 2.63. Observe que, como $\mathbb{Z}$ é PID, então $\mathbb{Z}$ é um domínio de fatoração única (UFD). Se tomarmos $-6 \in \mathbb{Z}$ podemos fatorá-lo em:

$$-6 = 2 \cdot -3 \text{ ou } -6 = -2 \cdot 3$$

Veja ainda que $-3 = -1 \cdot 3$ e $-2 = -1 \cdot 2$, deste modo podemos reescrever -6 como:

$$-6 = -1 \cdot 3 \cdot 2.$$

Com isso, temos que -6 pode ser reescrito por elementos irredutíveis de forma única, a menos da ordem de fatores e de elementos invertíveis.

Mais ainda, é fácil observar que podemos fazer isso para qualquer elemento de $\mathbb{Z}$.

Corolário 2.64. *Um ideal principal $I = \langle a \rangle$ em um UFD é primo se, e somente se, a é irredutível.*

Demonstração. ($\Rightarrow$) Mostremos a contrapositiva, isto é, se a é irredutível, então $\langle a \rangle$ não é primo.

Como a é irredutível, então $a = bc$, onde b e c não são elementos invertíveis. Logo, necessariamente, $b \notin \langle a \rangle$ e $c \notin \langle a \rangle$. Portanto, $\langle a \rangle$ não é primo.

($\Leftarrow$) Como, por hipótese, a é um elemento irredutível em um UFD segue pela Proposição 2.61 que a é um elemento primo deste UFD.

Consequentemente, pelo Teorema 2.51, o ideal principal $\langle a \rangle$ é um ideal primo.

□

Definição 2.65. Seja R um anel com unidade. Dizemos que R é um *anel com divisão*, ou um *quase corpo*, se $(R - \{0\}, \cdot)$ é um grupo, ou seja, $1 \in R$ e, para todo $a \in R$, $a \neq 0$, existe $b \in R$, tal que:

$$a \cdot b = b \cdot a = 1,$$

onde b é chamado de inverso de a e denotado por a^{-1}.

Definição 2.66. Dizemos que R é corpo quando R é um anel com divisão comutativo e denotaremos por k.

Proposição 2.67. *Seja k um anel comutativo com unidade. Dizemos que k é corpo se, e somente se, os únicos ideais de k são os triviais: $\{0\}$ e k.*

Demonstração. ($\Rightarrow$) Suponha que k é um corpo, logo todo ideal I, diferente do ideal $\{0\}$, contém 1_k, já que para todo $x \neq 0_k \in I$, existe $x^{-1} \in k$ tal que $x^{-1} \cdot x \in I$, mas $x^{-1} \cdot x = 1_k$, logo $1_k \in I$.

Agora, tome $r \in k$ qualquer e $1_k \in I$. Veja que $r = r \cdot 1 \in I$ e desse modo $r \in I$. Assim, $I = k$.

Portanto, temos que, se k é corpo, então os únicos ideais possíveis são $\{0\}$ e o próprio k.

($\Leftarrow$) Para isso, supomos que k não seja corpo e, assim, existe algum $x \neq 0_k \in k$ que não possui inverso. Com isso, temos que $\langle x \rangle = \{rx;\ r \in k\} \neq \{0\}$ e $1_k \notin \langle x \rangle$. Logo $\langle x \rangle \neq k$, mas isso contraria a hipótese de que os únicos ideais são $\{0\}$ e o próprio k. Portanto, k é corpo.

□

Teorema 2.68. *Todo corpo é domínio de integridade.*

Demonstração. Seja k um corpo. Então k é um anel comutativo com unidade 1, onde todo elemento não nulo tem inverso com relação à multiplicação, isto é, $(k - \{0\}, \cdot)$ é grupo abeliano. Queremos mostrar que k não possui divisores de zero, isto é:

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Para isso, tomemos $a, b \in k$ tais que $a \cdot b = 0$, com $a \neq 0$. Note que $a^{-1} \in k$. Daí:

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

Desta forma, temos que k é um domínio de integridade. □

Teorema 2.69. *Todo domínio de integridade finito com mais de um elemento é um corpo.*

Demonstração. Seja k um domínio de integridade com $1 \neq 0$. Então k será corpo se todo elemento não nulo tiver inverso multiplicativo.

Seja $a \in k$, $a \neq 0$. Temos que $\{a, a^2, a^3, \cdots, a^m, \cdots\} \subset k$. Como k é finito, então $\{a, a^2, a^3, \cdots, a^m, \cdots\} \subset k$ é finito.

Seja s o menor inteiro positivo tal que $a^s = a^r$, para algum $r \neq s$, com $r > s$. Como $r > s$, então, existe $t \in \mathbb{Z}^+$, tal que $r = s + t$, com $t > 0$. Note que

$$0 = a^s - a^r = a^s - a^{s+t} = a^s(1 - a^t).$$

Como k é domínio de integridade e $a \neq 0$, então $a^s \neq 0$, logo $a^t = 1$, para algum $t > 0$.
Se $t = 1$, temos que $a = 1$, logo $a^{-1} = a = 1 \in k$.
Se $t > 1$, temos que

$$1 = a \cdot a^{t-1} \Rightarrow a^{-1} \cdot 1 = (a^{-1} \cdot a) \cdot a^{t-1} \Rightarrow a^{-1} = a^{t-1} \in k.$$

Logo, para todo $a \in k$, $a \neq 0$, temos que $a^{-1} \in k$, portanto, k é corpo. □

Definição 2.70. Seja R um domínio de integridade. No conjunto $R \times R^*$ consideremos a relação de equivalência $\sim$ definida como: $\forall (a, b), (c, d) \in R \times R^*$,

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Usaremos $\dfrac{a}{b}$ para denotar a classe de equivalência determinada por (a, b). Os elementos do conjunto quociente $K = \dfrac{R \times R^*}{\sim}$ são as frações $\dfrac{a}{b}$, $a \in R, b \in R^*$, tais que:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Assim, $K = \left\{ \dfrac{a}{b};\ a \in R, b \in R^* \right\}$.

Proposição 2.71. *No contexto da Definição 2.70, K com as operações*

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

e

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

onde $\frac{a}{b}, \frac{c}{d} \in K$ *é um corpo e chamado de corpo de frações de* R.

Demonstração. Para mostrar que K é corpo, precisamos mostrar que K é um anel com divisão comutativo.

- $+$ está bem definida. De fato:

  Sejam $+ : K \times K \to K$ e $\left(\frac{a_1}{b_1}, \frac{c_1}{d_1}\right), \left(\frac{a_2}{b_2}, \frac{c_2}{d_2}\right) \in K \times K$. Note que:

  $$\left(\frac{a_1}{b_1}, \frac{c_1}{d_1}\right) = \left(\frac{a_2}{b_2}, \frac{c_2}{d_2}\right) \Leftrightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2} \text{ e } \frac{c_1}{d_1} = \frac{c_2}{d_2}.$$

  Pela Definição 2.70, temos que:

  $$\begin{cases} a_1 b_2 = a_2 b_1 \\ c_1 d_2 = c_2 d_1 \end{cases}.$$

  Multiplicando a primeira linha por $d_1 d_2$ e a segunda linha por $b_1 b_2$ teremos:

  $$\begin{cases} a_1 b_2 d_1 d_2 = a_2 b_1 d_1 d_2 \\ c_1 d_2 b_1 b_2 = c_2 d_1 b_1 b_2 \end{cases}.$$

  Somando as duas linhas, já que estamos em um sistema linear, temos

  $a_1 b_2 d_1 d_2 + c_1 d_2 b_1 b_2 = a_2 b_1 d_1 d_2 + c_2 d_1 b_1 b_2 \Rightarrow (a_1 d_1 + c_1 b_1)(b_2 d_2) = (a_2 d_2 + c_2 b_2)(b_1 d_1)$.

  Mas, pela Definição 2.70, segue que:

  $$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} = \frac{a_2 d_2 + c_2 b_2}{b_2 d_2} \Rightarrow \frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_2}{b_2} + \frac{c_2}{d_2}.$$

  Portanto, $+$ está bem definida.

- $\cdot$ está bem definida. De fato: Sejam $+ : K \times K \to K$ e $\left(\frac{a_1}{b_1}, \frac{c_1}{d_1}\right), \left(\frac{a_2}{b_2}, \frac{c_2}{d_2}\right) \in K \times K$. Note que:

  $$\left(\frac{a_1}{b_1}, \frac{c_1}{d_1}\right) = \left(\frac{a_2}{b_2}, \frac{c_2}{d_2}\right) \Leftrightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2} \text{ e } \frac{c_1}{d_1} = \frac{c_2}{d_2}.$$

  Pela Definição 2.70, temos que:

  $$\begin{cases} a_1 b_2 = a_2 b_1 \\ c_1 d_2 = c_2 d_1 \end{cases}.$$

  Multiplicando as igualdades, temos:

  $$a_1 b_2 c_1 d_2 = a_2 b_1 c_2 d_1 \Rightarrow (a_1 c_1)(b_2 d_2) = (a_2 c_2)(b_1 d_1).$$

  Pela Definição 2.70, segue que:

  $$\frac{a_1 c_1}{b_1 d_1} = \frac{a_2 c_2}{b_2 d_2} \Rightarrow \frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}.$$

  Portanto, $\cdot$ está bem definida.

- K é anel. De fato:

  (i) $(K, +)$ é grupo abeliano, pois:

  1. A operação $+$ é associativa para todo $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in K$:

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{a(df)+b(cf+de)}{b(df)}=\frac{(ad+bc)f+(bd)e}{(bd)f}$$
$$=\frac{ad+bc}{bd}+\frac{e}{f}=\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}.$$

  2. A operação $+$ possui elemento neutro para todo $\frac{a}{b} \in K$:

     Seja $\frac{0}{1} \in K$, note que:

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b}.$$

     Por outro lado,

$$\frac{0}{1}+\frac{a}{b}=\frac{0\cdot b+1\cdot a}{1\cdot b}=\frac{a}{b}.$$

  3. Para todo $\frac{a}{b} \in K$, existe seu inverso aditivo em K. Tome $\frac{-a}{b} \in K$ e note que $\frac{-a}{b}=-\left(\frac{a}{b}\right)$. De fato:

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab+(-a)b}{b^2}=\frac{b(a+(-a))}{b^2}=\frac{b\cdot 0}{b^2}=0.$$

     Por outro lado,

$$\frac{-a}{b}+\frac{a}{b}=\frac{(-a)b+ab}{b^2}=\frac{(-a+a)b}{b^2}=\frac{0\cdot b}{b^2}=0.$$

  4. A operação $+$ é comutativa para todo $\frac{a}{b}, \frac{c}{d} \in K$:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}.$$

  (ii) A operação $\cdot$ é associativa para todo $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in K$:

$$\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{ce}{df}=\frac{a(ce)}{b(df)}=\frac{(ac)e}{(bd)f}=\frac{ac}{bd}\cdot\frac{e}{f}=\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}.$$

  (iii) É válida a distributividade da multiplicação em relação à adição para todo $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in K$:

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+ed}{df}\right)=\frac{a(cf+ed)}{b(df)}=\frac{acf+aed}{bdf}=\frac{acf}{bdf}+\frac{aed}{bdf}$$
$$=\frac{ac}{bd}\cdot\frac{f}{f}+\frac{ae}{bf}\cdot\frac{d}{d}=\frac{ac}{bd}\cdot 1+\frac{ae}{bf}\cdot 1=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}.$$

Além disso,

$$\left(\frac{a}{b}+\frac{c}{d}\right)\frac{e}{f}=\frac{ad+bc}{bd}\cdot\frac{e}{f}=\frac{(ad+bc)e}{(bd)f}=\frac{ade+bce}{bdf}=\frac{ade}{bdf}+\frac{bce}{bdf}$$
$$=\frac{ae}{bf}\cdot\frac{d}{d}+\frac{ce}{df}\cdot\frac{b}{b}=\frac{ae}{bf}\cdot 1+\frac{ce}{df}\cdot 1=\frac{ae}{bf}+\frac{ce}{df}=\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}.$$

- K possui unidade. De fato, tome $\frac{1}{1}$ como a unidade em K e $\frac{a}{b}\in K$ qualquer.

  $$\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{a}{b}.$$

  Por outro lado,

  $$\frac{1}{1}\cdot\frac{a}{b}=\frac{1\cdot a}{1\cdot b}=\frac{a}{b}.$$

- Todo elemento $\frac{a}{b}\neq\frac{0}{1}\in K$ possui inverso. Tome $\frac{b}{a}\in K$ e veja que $\frac{b}{a}=\left(\frac{a}{b}\right)^{-1}$. De fato:

  $$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=\frac{1}{1},\text{ já que }(ab)\cdot 1=1\cdot(ab).$$

  Por outro lado,

  $$\frac{b}{a}\cdot\frac{a}{b}=\frac{ba}{ab}=\frac{ab}{ab}=\frac{1}{1}.$$

Com isso, temos que K é corpo. □

Exemplo 2.72. Sabemos que $\mathbb{Z}$ é um domínio de integridade. Pela Definição 2.70, o corpo de frações de $\mathbb{Z}$ é definido por:

$$K=\left\{\frac{a}{b};\ a\in\mathbb{Z},b\in\mathbb{Z}^*\right\}.$$

Por outro lado, por definição, temos que:

$$\mathbb{Q}=\left\{\frac{a}{b};\ a\in\mathbb{Z},b\in\mathbb{Z}^*\right\}.$$

Deste modo, $\mathbb{Q}$ é o corpo das frações de $\mathbb{Z}$.

Definição 2.73. Seja I um ideal de um anel R comutativo com unidade. A classe de resíduos do anel R módulo I é denotada $\frac{R}{I}$ e é o conjunto quociente das classes de equivalências dos elementos de R sob a relação de equivalência $a\sim b$ se, e somente se, $a-b\in I$. A classe de equivalência de a é denotada $\overline{a}$.

Proposição 2.74. *$\frac{R}{I}$ com as operações $+$ e $\cdot$ definidas por:*

Sejam $a+I,b+I\in\frac{R}{I}$, com $a,b\in R$,

$$(a+I)+(b+I):=(a+b)+I$$

$$(a+I)\cdot(b+I):=ab+I$$

é um anel comutativo com unidade.

Demonstração. Mostremos que $\dfrac{R}{I}$ é anel comutativo com unidade.

- $+$ está bem definida:
  Sejam $+ : \dfrac{R}{I} \times \dfrac{R}{I} \to \dfrac{R}{I}$ e $(a+I, b+I), (c+I, d+I) \in \dfrac{R}{I} \times \dfrac{R}{I}$. Note que:
  $$(a+I, b+I) = (c+I, d+I) \Leftrightarrow a+I = c+I \text{ e } b+I = d+I.$$
  Pela Definição 2.73, temos então que:
  $$a \sim c \text{ e } b \sim d \Rightarrow a - c \in I \text{ e } b - d \in I.$$
  Com isso, podemos então somar ambos os elementos de I:
  $$(a-c) + (b-d) \in I \Rightarrow (a+b) - (c+d) \in I.$$
  Mas se isso ocorre, então, pela Definição 2.73, temos que:
  $$(a+b) \sim (c+d) \Rightarrow (a+b) + I = (c+d) + I.$$
- $\cdot$ está bem definida:
  Sejam $\cdot : \dfrac{R}{I} \times \dfrac{R}{I} \to \dfrac{R}{I}$ e $(a+I, b+I), (c+I, d+I) \in \dfrac{R}{I} \times \dfrac{R}{I}$. Note que:
  $$(a+I, b+I) = (c+I, d+I) \Leftrightarrow a+I = c+I \text{ e } b+I = d+I.$$
  Pela Definição 2.73, temos então que:
  $$a \sim c \text{ e } b \sim d \Rightarrow a - c \in I \text{ e } b - d \in I.$$
  Se isso ocorre, então podemos afirmar que $a = c+x$ e $b = d+y$, para algum $x, y \in I$, portanto:
  $$ab = (c+x)(d+y) = cd + cy + xd + xy.$$
  Como I é ideal, então $cy, xd, xy \in I$. Assim, podemos dizer que $w = cy+xd+xy \in I$, logo:
  $$ab = cd + w \Rightarrow ab - cd \in I.$$
  Pela Definição 2.73, temos que:
  $$ab \sim cd \Rightarrow ab + I = cd + I.$$
- $\dfrac{R}{I}$ é anel:

  (i) $\left(\dfrac{R}{I}, +\right)$ é grupo abeliano, pois:

  1. A operação $+$ é associativa para todo $a+I, b+I, c+I \in \dfrac{R}{I}$:

  $$(a+I) + [(b+I) + (c+I)] = (a+I) + ((b+c)+I) = (a+(b+c)) + I$$
  $$= ((a+b)+c) + I = ((a+b)+I) + (c+I) = [(a+I)+(b+I)] + (c+I).$$

2. A operação + possui elemento neutro para todo $a+I \in \dfrac{R}{I}$:

   Seja $0+I \in \dfrac{R}{I}$, note que:

   $$(a+I)+(0+I) = (a+0)+I = a+I.$$

   Por outro lado,

   $$(0+I)+(a+I) = (0+a)+I = a+I.$$

3. Para todo $a+I \in \dfrac{R}{I}$, existe seu inverso aditivo em $\dfrac{R}{I}$. Tome $(-a)+I \in \dfrac{R}{I}$ e note que $(-a)+I = -(a+I)$. De fato:

   $$(a+I)+((-a)+I) = (a+(-a))+I = 0+I.$$

   Por outro lado,

   $$((-a)+I)+(a+I) = (-a+a)+I = 0+I.$$

(ii) A operação $\cdot$ é associativa para todo $a+I, b+I, c+I \in \dfrac{R}{I}$:

$$\begin{aligned}(a+I)[(b+I)(c+I)] &= (a+I)(bc+I) = a(bc)+I \\ &= (ab)c+I = (ab+I)(c+I) = [(a+I)(b+I)](c+I).\end{aligned}$$

(iii) É válida a distributividade da multiplicação em relação à adição para todo $a+I, b+I, c+I \in \dfrac{R}{I}$:

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)((b+c)+I) = (a(b+c))+I = (ab+ac)+I \\ &= ((ab)+I)+((ac)+I) = [(a+I)(b+I)]+[(a+I)(c+I)].\end{aligned}$$

e

$$\begin{aligned}[(a+I)+(b+I)](c+I) &= ((a+b)+I)(c+I) = ((a+b)c)+I = (ac+bc)+I \\ &= ((ac)+I)+((bc)+I) = [(a+I)(c+I)]+[(b+I)(c+I)].\end{aligned}$$

- $\dfrac{R}{I}$ é comutativo:

  Seja $a+I, b+I \in \dfrac{R}{I}$,

  $$(a+I)(b+I) = (ab)+I = (ba)+I = (b+I)(a+I).$$

- $\dfrac{R}{I}$ tem unidade. De fato, tome $1+I = I$ como a unidade em $\dfrac{R}{I}$ e $a+I \in \dfrac{R}{I}$ qualquer. Note que:

  $$(a+I)(1+I) = (a\cdot 1)+I = a+I.$$

  Por outro lado,

  $$(1+I)(a+I) = (1\cdot a)+I = a+I.$$

□

Observação 2.75. A função $\pi : R \longrightarrow \dfrac{R}{I}$ levando cada elemento em sua classe de equivalência é um homomorfismo de anel.

Definição 2.76. $\dfrac{R}{I}$ é caracterizado pela seguinte propriedade:

Se $\phi : R \longrightarrow S$ é um homomorfismo de anel de R em S e $\phi(1_R) = 1_S$, então existe um único homomorfismo de anel $\varphi : \dfrac{R}{I} \longrightarrow S$ tal que $\phi = \varphi \circ \pi$.

Proposição 2.77. *Um ideal próprio I em R é primo se, e somente se, $\dfrac{R}{I}$ é um domínio de integridade.*

Demonstração. ($\Rightarrow$) Veja que, pela própria caracterização de $\dfrac{R}{I}$, $\dfrac{R}{I}$ é anel comutativo com unidade. Para que ele seja um domínio de integridade basta provar que $\dfrac{R}{I}$ não possui divisores de zero.

Para tal, tome $a+I, b+I \in I$ quaisquer, não nulos, isto é, $a, b \notin I$. Como I é primo, por hipótese, então $ab \notin I$, pois para ab pertencer à I, precisaríamos ter $a \in I$ ou $b \in I$. Como $ab \notin I$, então, $ab + I$ é não nulo. Portanto, $\dfrac{R}{I}$ não possui divisores de zero e, consequentemente, é domínio de integridade.

($\Leftarrow$) Queremos mostrar que I é ideal primo, ou seja, queremos que se $ab \in I$, então $a \in I$ ou $b \in I$.

Para isso, suponha $ab \in I$. Se isso ocorre, então $ab + I = I$. Mas sabemos que $ab + I = (a + I)(b + I)$. Disto temos que $(a + I)(b + I) = I$. Como $\dfrac{R}{I}$ é domínio de integridade, isto é, não possui divisores de zero, então $a + I = I$ ou $b + I = I$, isto é, $a \in I$ ou $b \in I$. Portanto, I é ideal primo.

□

Proposição 2.78. *Um ideal próprio I em R é maximal se, e somente se, $\dfrac{R}{I}$ é um corpo.*

Demonstração. ($\Rightarrow$) Já temos que $\dfrac{R}{I}$ é um anel comutativo com unidade, para que $\dfrac{R}{I}$ seja um corpo precisamos que todo elemento, não nulo, $a + I \in \dfrac{R}{I}$ possua inverso multiplicativo.

Para tal, suponha $a + I \in \dfrac{R}{I}$ qualquer, não nulo, isto é, $a \notin I$.

Considere $A = \{ac + b;\ c \in R, b \in I\}$. Note que $I \subset A$. Como I é maximal, temos que $A = R$ ou $A = I$. Como $a \notin I$, então $A \neq I$, portanto $A = R$. Com isso, como $1 \in R$, então $1 \in A$. Portanto, podemos afirmar que existem $c \in R$ e $b' \in I$ tais que $1 = ac + b'$, e assim,

$$1 + I = (ac + b') + I = (ac + I) + (b' + I) \overset{b' \in I}{=} (ac + I) = (a + I)(c + I).$$

Logo, temos que $(a + I)(c + I) = 1 + I$, isto é, $c + I$ é inverso de $a + I$.

($\Leftarrow$) Queremos mostrar que I é maximal, ou seja, se existe J ideal de R tal que $I \subsetneq J \subset R$, então $J = R$.

Para isso, suponha I e J ideais de R tal que $I \subset J$ e $J \neq I$. Seja $a \in J$ tal que $a \notin I$, desta forma $a + I$ é não nulo e, portanto, existe $b + I \in \dfrac{R}{I}$ tal que $(a + I)(b + I) = 1 + I$. Além disso, como $a \in J$, temos que $ab \in J$. Assim:

$$1 + I = (a + I)(b + I) = ab + I.$$

Com isso, pela Definição 2.73:

$$1 - ab \in I.$$

Isto é, existe $c \in I$ tal que

$$1 - ab = c \Rightarrow 1 = ab + c.$$

Note que, se $c \in I$ e $I \subset J$, então $c \in J$, além disso $ab \in J$, logo $ab + c = 1 \in J$. Assim, pela Proposição 2.28, item 4, temos que $J = R$. Desta forma, I é maximal. □

Teorema 2.79 (Primeiro Teorema do Isomorfismo)**.** *Seja $\phi : R \to S$ um homomorfismo sobrejetor de anéis. Se $I = \ker(\phi)$, então o anel quociente $\dfrac{R}{I}$ é isomorfo a S.*

Demonstração. Precisamos definir um isomorfismo de $\dfrac{R}{I}$ em S. Como os elementos de $\dfrac{R}{I}$ são da forma $a + I$, $a \in R$ e os elementos de S são da forma $\phi(a)$, $a \in R$, pois ϕ é sobrejetor, podemos, de forma natural, definir a seguinte correspondência

$$a + I \to \phi(a),\ a \in R.$$

Chamaremos tal aplicação de σ, isto é, $\sigma(a + I) = \phi(a)$. Observe que tal correspondência é, de fato, uma função, mais ainda, uma função bijetora, pois:

- σ está bem-definida. De fato, sejam $a + I, b + I \in \dfrac{R}{I}$:

$$a + I = b + I \Rightarrow a - b \in \ker(\phi) = I \Rightarrow \phi(a - b) = 0 \Rightarrow \phi(a) - \phi(b) = 0$$
$$\Rightarrow \phi(a) = \phi(b) \Rightarrow \sigma(a + I) = \sigma(b + I)$$

- σ é sobrejetora. De fato, dado $y \in S$ temos que $y = \phi(x)$, para algum $x \in R$. Tome $x + I \in \dfrac{R}{I}$, logo:

$$\sigma(x + I) = \phi(x) = y.$$

- σ é injetora. De fato, sejam $a + I, b + I \in \dfrac{R}{I}$:

$$\sigma(a + I) = \sigma(b + I) \Rightarrow \phi(a) = \phi(b) \Rightarrow \phi(a) - \phi(b) = 0 \Rightarrow \phi(a - b) = 0$$
$$\Rightarrow a - b \in \ker(\phi) = I \Rightarrow a + I = b + I.$$

Agora, mostremos que σ é homomorfismo de anéis:

- $\sigma((a+I)+(b+I)) = \sigma((a+b)+I) = \phi(a+b) = \phi(a)+\phi(b) = \sigma(a+I)+\sigma(b+I)$.
- $\sigma((a+I)(b+I)) = \sigma((ab)+I) = \phi(ab) = \phi(a)\phi(b) = \sigma(a+I)\sigma(b+I)$.

Deste modo, σ é um homomorfismo bijetor, isto é, um isomorfismo de $\dfrac{R}{I}$ em S. □

Exemplo 2.80. Seja $\phi : \mathbb{Z} \to \mathbb{Z}_5$ dado por $\phi(a) = \overline{a}$. Observe que:

$$\begin{aligned}\ker(\phi) &= \{a \in \mathbb{Z}; \phi(a) = \overline{0}\} \\ &= \{a \in \mathbb{Z}; \overline{a} = \overline{0}\} \\ &= \{a \in \mathbb{Z}; a = 5k,\ k \in \mathbb{Z}\} \\ &= \langle 5 \rangle.\end{aligned}$$

Assim, temos, pelo Primeiro Teorema do Isomorfismo, que $\dfrac{\mathbb{Z}}{\langle 5 \rangle}$ é isomorfo a $\mathbb{Z}_5$.

2.2 Anel de Polinômios

Definição 2.81. Seja R um anel comutativo com unidade. Um polinômio $F(X)$ com coeficientes em R é descrito na forma de uma soma infinita

$$F(X) = \sum_{i=0}^{\infty} a_0 + a_1 X + \cdots + a_i X^i + \cdots,$$

onde $a_i \in R,\ i \in \mathbb{Z}$ e $a_i = 0$ para todo i exceto uma quantidade finita de índices i. Os a_i's são chamados de coeficientes de $F(X)$.

Denotamos por $\mathcal{P}(R)$ o conjunto dos polinômios sobre R. Neste conjunto $\mathcal{P}(R)$, definimos as operações $+$ e $\cdot$ como: sejam $F(X) = a_0 + a_1 X + \cdots + a_n X^n + \cdots$ e $G(X) = b_0 + b_1 X + \cdots + b_n X^n + \cdots$ polinômios em $\mathcal{P}(R)$, quaisquer,

$$F(X) + G(X) = c_0 + c_1 X + \cdots + c_n X^n + \cdots, \text{ onde } c_i = a_i + b_i;$$

$$F(X)G(X) = d_0 + d_1 X + \cdots + d_n X^n + \cdots, \text{ onde } d_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

Teorema 2.82. *O conjunto $\mathcal{P}(R)$ munido das operações $+$ e $\cdot$ é um anel comutativo com unidade, denotado por $R[X]$.*

Demonstração. Para mostrar que $R[X]$ é anel comutativo com unidade, precisamos mostrar que:

- $R[X]$ é anel. De fato:

  (i) $(R[X], +)$ é grupo abeliano, pois:

1. A operação + é associativa para todo $F(X) = a_0 + a_1X + \cdots + a_nX^n + \cdots, G(X) = b_0 + b_1X + \cdots + b_nX^n + \cdots, H(X) = c_0 + c_1X + \cdots + c_nX^n + \cdots \in R[X]$:

$$\begin{aligned}
&F(X) + [G(X) + H(X)] \\
&= (a_0 + \cdots + a_nX^n + \cdots) + [(b_0 + \cdots + b_nX^n + \cdots) + (c_0 + \cdots + c_nX^n \\
&+ \cdots) \\
&= (a_0 + \cdots + a_nX^n + \cdots) + ((b_0 + c_0) + \cdots + (b_n + c_n)X^n + \cdots) \\
&= (a_0 + (b_0 + c_0) + \cdots + (a_n + (b_n + c_n))X^n + \cdots \\
&= ((a_0 + b_0) + c_0) + \cdots + ((a_n + b_n) + c_n)X^n + \cdots \\
&= ((a_0 + b_0) + \cdots (a_n + b_n)X^n + \cdots) + (c_0 + \cdots + c_nX^n + \cdots) \\
&= [(a_0 + \cdots + a_nX^n + \cdots) + (b_0 + \cdots + b_nX^n) + \cdots] + (c_0 + \cdots + c_nX^n \\
&+ \cdots) \\
&= [F(X) + G(X)] + H(X).
\end{aligned}$$

2. A operação + possui elemento neutro para todo $F(X) \in R[X]$:
Tome $0 \in R[X]$ o polinômio constante nulo. Note que:

$$\begin{aligned}
F(X) + 0(X) &= (a_0 + a_1 + \cdots + a_nX^n + \cdots) + (0 + 0X + \cdots + 0X^n \\
&\quad + \cdots)] \\
&= (a_0 + 0) + (a_1 + 0)X + \cdots + (a_n + 0)X^n + \cdots \\
&= a_0 + a_1X + \cdots + a_nX^n + \cdots \\
&= F(X).
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
0(X) + F(X) &= (0 + 0X + \cdots + 0X^n + \cdots) + (a_0 + a_1 + \cdots + a_nX^n \\
&\quad + \cdots) \\
&= (0 + a_0) + (0 + a_1)X + \cdots + (0 + a_n)X^n + \cdots \\
&= a_0 + a_1 + \cdots + a_nX^n + \cdots \\
&= F(X).
\end{aligned}$$

3. Para todo $F(X) = a_0 + a_1X + \cdots + a_bX^n + \cdots \in R[X]$, existe seu inverso aditivo em $R[X]$. Tome $(-F)(X) = (-a_0) + (-a_1)X + \cdots + (-a_n)X^n + \cdots$ e note que:

$$\begin{aligned}
F(X) + (-F)(X) &= (a_0 + \cdots + a_bX^n + \cdots) + ((-a_0) + \cdots + (-a_n)X^n \\
&\quad + \cdots) \\
&= (a_0 - a_0) + (a_1 - a_1)X + \cdots + (a_n - a_n)X^n + \cdots \\
&= 0 + 0X + \cdots + 0X^n + \cdots \\
&= 0(X).
\end{aligned}$$

Por outro lado,

$$\begin{aligned}(-F)(X) + F(X) &= ((-a_0) + \cdots + (-a_n)X^n + \cdots) + (a_0 + \cdots + a_bX^n \\ &\quad + \cdots) \\ &= (-a_0 + a_0) + (-a_1 + a_1)X + \cdots + (-a_n + a_n)X^n \\ &\quad + \cdots \\ &= 0 + 0X + \cdots + 0X^n + \cdots \\ &= 0(X).\end{aligned}$$

4. A operação + é comutativa para todo $F(X), G(X) \in R[X]$:

$$\begin{aligned}F(X) + G(X) &= (a_0 + a_1X + \cdots + a_nX^n + \cdots) + (b_0 + b_1X + \cdots + b_nX^n \\ &\quad + \cdots) \\ &= (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n + \cdots \\ &= (b_0 + a_0) + (b_1 + a_1)X + \cdots + (b_n + a_n)X^n + \cdots \\ &= (b_0 + b_1X + \cdots + b_nX^n + \cdots) + (a_0 + a_1X + \cdots + a_nX^n \\ &\quad + \cdots) \\ &= G(X) + F(X).\end{aligned}$$

(ii) Ainda é possível mostrar que a operação $\cdot$ é associativa e que, além disso, é válida a distributividade da multiplicação em relação à adição, já que ambos são consequência do fato de R ser um anel comutativo com unidade.

- A operação $\cdot$ é comutativa para todo $F(X), G(X) \in R[X]$:

  Sejam $F(X) = a_0 + a_1X + \cdots + a_nX^n + \cdots$ e $G(X) = b_0 + b_1X + \cdots + b_nX^n + \cdots$.

$$\begin{aligned}F(X) \cdot G(X) &= (a_0 + a_1X + \cdots + a_nX^n + \cdots) \cdot (b_0 + b_1X + \cdots + b_nX^n + \cdots) \\ &= (a_0b_0) + (a_0b_1)X + \cdots + (a_0b_n)X^n + \cdots + (a_nb_0)X^n + \cdots + \\ &\quad (a_nb_n)X^{n+n} + \cdots \\ &= (b_0a_0) + (b_1a_0)X + \cdots + (b_na_0)X^n + \cdots + (b_0a_n)X^n + \cdots + \\ &\quad (b_na_n)X^{n+n} + \cdots \\ &= (b_0a_0) + (b_0a_1)X + \cdots + (b_0a_n)X^n + \cdots + (b_na_0)X^n + \cdots + \\ &\quad (b_na_n)X^{n+n} + \cdots \\ &= (b_0 + b_1X + \cdots + b_nX^n + \cdots) \cdot (a_0 + a_1X + \cdots + a_nX^n + \cdots) \\ &= G(X) \cdot F(X).\end{aligned}$$

- $R[X]$ possui unidade. De fato, tome $1(X) = 1 + 0X + \cdots + 0X^n + \cdots$ como a unidade em $R[X]$ e $F(X) \in R[X]$ qualquer. Note que:

$$\begin{aligned}F(X)1(X) &= (a_0 + a_1X + \cdots + a_nX^n + \cdots) \cdot (1 + 0X + \cdots + 0X^n + \cdots) \\ &= (a_0 \cdot 1) + (a_0 \cdot 0)X + \cdots + (a_0 \cdot 0)X^n + \cdots + (a_n \cdot 1)X^n + \\ &\qquad (a_n \cdot 0)X^{n+1} + \cdots + (a_n \cdot 0)X^{n+n} + \cdots \\ &= a_0 + a_1X + \cdots + a_nX^n + \cdots \\ &= F(X).\end{aligned}$$

Com isso, temos que $R[X]$ é anel comutativo com unidade. □

Exemplo 2.83. Tomemos o anel de polinômios $\mathbb{Q}[X]$, isto é, um polinômio com variável X e coeficientes em $\mathbb{Q}$. Exemplos de polinômios em $\mathbb{Q}[X]$ são:

- $F(X) = 5X + 2$
- $G(X) = \dfrac{9}{2}X^2 + 4$
- $H(X) = X^3 + \dfrac{1}{5}$

Façamos $F + G$ e $F \cdot H$:

$$F + G = (5X + 2) + \left(\frac{9}{2}X^2 + 4\right) = \frac{9}{2}X^2 + 5X + 6.$$

$$F \cdot H = (5X + 2)\left(X^3 + \frac{1}{5}\right) = 5X^4 + 2X^3 + X + \frac{2}{5}.$$

Exemplo 2.84. Tomemos o anel de polinômios $\mathbb{Z}_5[X]$, isto é, um polinômio com variável X e coeficientes em $\mathbb{Z}_5$. Exemplos de polinômios em $\mathbb{Q}[X]$ são:

- $F(X) = \overline{4}X + \overline{2}$
- $G(X) = \overline{3}X^2 + \overline{4}$
- $H(X) = \overline{1}X^3 + \overline{3}$

Façamos $F + G$ e $F \cdot H$:

$$F + G = (\overline{4}X + \overline{2}) + (\overline{3}X^2 + \overline{4}) = \overline{3}X^2 + \overline{4}X + \overline{1}$$

$$F \cdot H = (\overline{4}X + \overline{2})(\overline{1}X^3 + \overline{3}) = \overline{4}X^4 + \overline{2}X^3 + \overline{2}X + \overline{1}.$$

Definição 2.85. O maior valor inteiro de índices i, digamos d, para o qual $a_d \neq 0$ é chamado de grau de $F(X)$. Se para todo índice i tem-se $a_i = 0$, então o grau de $F(X)$ é indefinido. Se $a_d = 1$, o polinômio é mônico. Se $F(X) = a_0 \neq 0$, então o polinômio tem grau 0 e chamado de polinômio constante não nulo.

Para facilitar, se podemos dizer que $F(X) = a_0 + a_1X + \cdots + a_iX^i + \cdots$ tal que $a_i = 0$ para $i > n$, então podemos denotar $F(X) = a_0 + a_1X + \cdots + a_nX^n$.

Observação 2.86. Veja que temos, pelo Teorema 2.82 que se R é um anel comutativo com unidade, então $R[X]$ também o é. Se tomarmos o anel comutativo com unidade $R[X_1]$, então podemos afirmar que $(R[X_1])[X_2]$ é anel comutativo com unidade, que denotaremos por $R[X_1, X_2]$. Se fizermos esse processo sucessivamente, podemos denotar $R[X_1, \cdots, X_n]$, que também será um anel comutativo com unidade.

Definição 2.87. Os monômios em $R[X_1, \cdots, X_n]$ são polinômios escritos na forma

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}, \text{ com } i_j \in \mathbb{Z}_+.$$

O grau do monômio é $i_1 + \cdots + i_n$.

Observação 2.88. Todo $F \in R[X_1, \cdots, X_n]$ tem uma expressão única $F = \sum a_{(i)}X^{(i)}$, onde $X^{(i)}$ são os monômios, $a_{(i)} \in R$.

Definição 2.89. Dizemos que o polinômio $F \in R[X_1, \cdots, X_n]$ de grau k é homogêneo quando

$$F(\lambda X_1, \cdots, \lambda X_n) = \lambda^k F(X_1, \cdots, X_n).$$

Denotaremos o polinômio homogêneo F de grau k por F_k.

Proposição 2.90. *O produto de polinômios homogêneos é homogêneo.*

Demonstração. Tome $F_d, G_l \in R[X_1, \cdots, X_n]$ homogêneos. Note que:

$$\begin{aligned}(F_dG_l)(\lambda X_1, \cdots, \lambda X_n) &= (F_d(\lambda X_1, \cdots, \lambda X_n)) \cdot (G_l(\lambda X_1, \cdots, \lambda X_n)) \\ &= \lambda^d F_d(X_1, \cdots, X_n) \cdot \lambda^l G_l(X_1, \cdots, X_n) \\ &= \lambda^{d+l} F_d(X_1, \cdots, X_n) \cdot G_l(X_1, \cdots, X_n) \\ &= \lambda^{d+l}(F_dG_l)(X_1, \cdots, X_n).\end{aligned}$$

□

Definição 2.91. Seja F um polinômio sobre R. Um elemento $u \in A$ é chamado de *raiz de* F se $F(u) = 0_R$.

Definição 2.92. Um corpo k é dito *algebricamente fechado* se todo polinômio não constante em uma variável, com coeficientes em k, admite uma raiz em k.

Definição 2.93. F é polinômio homogêneo de grau d se todos os coeficientes $a_{(i)}$ são zero, exceto aqueles que tem grau d.

Definição 2.94. Todo polinômio F tem expressão única $F = F_0 + F_1 + F_2 + \cdots + F_d$, onde F_i é um polinômio homogêneo de grau i. Se $F_d \neq 0$, d é o grau de F, denotado $\partial(F)$.

Se F é constante, $F = F_0$.

Observação 2.95. Note que, eventualmente, $F_0, F_1, \cdots$ podem ser nulos até algum F_{m-1}, portanto, poderíamos reescrever tal expressão como

$$F = F_m + \cdots + F_d$$

Proposição 2.96. *Se R um domínio de integridade e $F, G \in R[X_1, \cdots, X_n]$, então*

$$\partial(FG) = \partial(F) + \partial(G).$$

Demonstração. Sejam $F = F_0 + F_1 + \cdots + F_d$ e $G = G_0 + G_1 + \cdots + G_l$. Note que $\partial(F) = d$ e $\partial(G) = l$. Agora, veja que:

$$\begin{aligned}&F \cdot G = (F_0 + F_1 + \cdots + F_d) \cdot (G_0 + G_1 + \cdots + G_l) \\ &= F_0G_0 + F_0G_1 + \cdots + F_0G_l + F_1G_0 + F_1G_1 + \cdots + F_1G_l + \cdots + F_dG_0 + F_dG_1 + \cdots + F_dG_l.\end{aligned}$$

Perceba que F_0G_0 é o monômio constante. Além disso, se somarmos os monômios de mesmo grau teremos:

$$H_0 = F_0G_0$$

$$H_1 = F_0G_1 + G_0F_1$$

$$H_2 = F_0G_2 + F_1G_1 + F_2G_0$$

$$\vdots$$
$$H_{d+l-1} = F_{d-1}G_l + F_dG_{l-1}$$
$$H_{d+l} = F_dG_l$$

Perceba que o monômio de maior grau será $H_{d+l} = F_dG_l$, em que $H_{d+l} \neq 0$, pois R é domínio de integridade, cujo grau é $d+l$. Portanto, $\partial(F \cdot G) = d + l = \partial(F) + \partial(G)$. □

Proposição 2.97. *R é subanel de $R[X_1, \cdots, X_n]$.*

Demonstração. Seja $\phi : R \to R[X]$ uma aplicação dada por $\phi(a) = F_a(X)$, onde F_a é o polinômio constante dado por $F_a(X) = a$. Note que ϕ é um homomorfismo injetor de anéis. De fato:

$$\phi(a+b) = F_{a+b}(X) = a + b = F_a(X) + F_b(X) = \phi(a) + \phi(b).$$

Além disso,

$$\phi(ab) = F_{ab}(X) = ab = F_a(X)F_b(X) = \phi(a)\phi(b).$$

Ainda, ϕ é injetora, pois se $a \neq b$, então $F_a(X) \neq F_b(X)$, já que $F_a(1_R) = a$ e $F_b(1_R) = b$. Mas $F_a(X) = \phi(a)$ e $F_b(X) = \phi(b)$, logo $\phi(a) \neq \phi(b)$.

Com isso, temos que R é isomorfo a $\phi(R)$ e $\phi(R) \subseteq R[X]$, logo podemos considerar R como subanel de $R[X]$. □

Observação 2.98. $R[X_1, \cdots, X_n]$ é caracterizado por seguir a propriedade:

Se φ é um homomorfismo de anel de R em S, e $s_1, \cdots, s_n \in S$, então existe uma única extensão de φ para um homomorfismo de anel $\overline{\varphi}$ de $R[X_1, \cdots, X_n]$ em S tal que $\overline{\varphi}(X_i) = s_i$, em que $i \in \{1, \cdots, n\}$.

A imagem de um polinômio F sob $\overline{\varphi}$ é escrita $F(s_1, \cdots, s_n)$.

Proposição 2.99. *Seja u uma raiz de um polinômio não constante $F \in R[X]$. Se $F(X) = a_o + a_1X + \cdots + a_nX^n$, com $a_n \neq 0$, para todo $X \in R$, então $F(X) = (X-u)Q(X)$, para algum polinômio Q de uma forma padrão do tipo $Q(X) = b_0 + \cdots + b_nX^{n-1}$.*

Demonstração. Sejam F um polinômio não constante onde $F(X) = a_o + a_1X + \cdots + a_nX^n$, com $a_n \neq 0$, para todo $X \in R$ e $u \in R$ qualquer, assim:

$$F(X) - F(u) = a_1(X-u) + a_2(X^2 - u^2) + \cdots + a_n(X^n - u^n).$$

Mas

$$X^n - u^n = (X-u)(X^{n-1} + uX^{n-2} + \cdots + u^{n-2}X + u^{n-1}).$$

Logo, temos que:

$$\begin{aligned} &F(X) - F(u) \\ &= (X-u)[a_1 + a_2(X+u) + a_3(X^2 + uX + u^2) + \cdots + a_n(X^{n-1} + uX^{n-2} + \cdots + u^{n-1})] \\ &= (X-u)[(a_1 + a_2u + \cdots + a_nu^{n-1}) + (a_2 + a_3u + \cdots + a_nu^{n-2})X + \cdots + a_nX^{n-1}] \\ &= (X-u)Q(X), \end{aligned}$$

onde $Q(X) = (a_1 + a_2u + \cdots + a_nu^{n-1}) + (a_2 + a_3u + \cdots + a_nu^{n-2})X + \cdots + a_nX^{n-1}$.

Logo:

$$F(X) - F(u) = (X-u)Q(X) \Rightarrow F(X) = (X-u)Q(X) - F(u).$$

Mas, por hipótese, temos que $F(u) = 0_R$, pois u é raiz de F, logo:

$$F(X) = (X-u)Q(X).$$

□

Teorema 2.100 (Algoritmo da Divisão)**.** *Sejam* $F(X) = a_0+a_1X+\cdots+a_{n-1}X^{n-1}+a_nX^n$ *e* $G(X) = b_0 + b_1X + \cdots + b_{m-1}X^{m-1} + b_mX^m$ *elementos de* $k[X]$*, com* a_n *e* b_m*, não nulos, em* k *e* $m > 0$*, então existem únicos polinômios* $Q(X)$ *e* $R(X) \in k[X]$ *tais que* $F(X) = G(X)Q(X) + R(X)$*, onde* $R(X) = 0$ *ou* $\partial(R(X)) < \partial(G(X))$*. Denominamos* $Q(X)$ *de quociente e* $R(X)$ *de resto da divisão de* $F(X)$ *por* $G(X)$*.*

Demonstração. Considere $\mathcal{S} = \{F(X) - G(X)S(X);\ S(X) \in k[X]\}$.

Se $0 \in \mathcal{S}$, então existe $S(X) \in k[X]$ tal que $F(X) - G(X)S(X) = 0$. Logo,

$$F(X) = G(X)S(X).$$

Tomando $S(X) = Q(X)$ e $R(X) = 0$, provamos o teorema.

Agora, suponha que $0 \notin \mathcal{S}$. Observe que $\mathcal{S}$ é não vazio, pois $F(X) = F(X) - G(X)0$, onde 0 é o elemento neutro de $k[X]$, e como $F(X) \neq 0$, por hipótese, segue que o subconjunto de $\mathbb{N}$ formado pelos graus dos elementos de $\mathcal{S}$ também é não vazio. Consequentemente, pelo Princípio do Menor Inteiro[2] tal subconjunto tem um menor elemento. Seja $R(X)$ o elemento de grau mínimo em $\mathcal{S}$. Como $R(X) \in \mathcal{S}$, existe $Q(X) \in k[X]$ tal que

$$R(X) = F(X) - G(X)Q(X),$$

ou seja,

$$F(X) = G(X)Q(X) + R(X).$$

Observe que $R(X) \neq 0$, pois $0 \notin \mathcal{S}$, por hipótese.

Nos resta mostrar que $\partial(R(X)) < \partial(G(X))$. Para tal, tomemos

$$R(X) = c_0 + c_1X + \cdots + c_{t-1}X^{t-1} + c_tX^t, \text{ com } c_t \in k \text{ e } c_t \neq 0.$$

Se $t \geq m$, então

$$F(X) - G(X)Q(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}G(X) = R(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}G(X). \tag{2.1}$$

Note

$$\begin{aligned} R(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}G(X) &= R(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}(b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0) \\ &= R(X) - \left(\frac{c_t}{b_m}\right)b_mX^{t-m}X^m - \cdots - \left(\frac{c_t}{b_m}\right)b_0X^{t-m} \\ &= R(X) - (c_tX^t + \text{termos de grau menor}) \end{aligned} \tag{2.2}$$

que é um polinômio de grau menor que $\partial(R(X))$.

Além disso,

$$F(X) - G(X)Q(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}G(X) = F(X) - G(X)\left[Q(X) + \left(\frac{c_t}{b_m}\right)X^{t-m}\right] \tag{2.3}$$

Veja que $F(X) - G(X)\left[Q(X) + \left(\frac{c_t}{b_m}\right)X^{t-m}\right] \in \mathcal{S}$, por definição.

[2] O Princípio do Menor inteiro afirma que todo subconjunto não vazio $L \subset \mathbb{N}$ possui um menor elemento. Neste caso, utilizamos tal Princípio no conjunto dos graus dos polinômios de $\mathcal{S}$.

Assim, por (2.2) e (2.3), temos que (2.1) pode ser reescrita da forma:

$$F(X) - G(X)\left[Q(X) + \left(\frac{c_t}{b_m}\right)X^{t-m}\right] = R(X) - (c_tX^t + \text{termos de grau menor}). \quad (2.4)$$

Logo, (2.4) é um elemento de $\mathcal{S}$, mas $R(X) - (c_tX^t + \text{termos de grau menor})$ é um elemento de grau menor do que $R(X)$, contradizendo a hipótese de $R(X)$ ser o elemento de grau mínimo de $\mathcal{S}$. Assim, é absurdo supor que $\partial(R(X)) = t \geq m = \partial(G(X))$.

Com isso, o grau de $R(X)$ é necessariamente menor que o grau de $G(X)$.

Provemos agora a unicidade do quociente e do resto desta divisão. Para tal suponha

$$F(X) = G(X)Q_1(X) + R_1(X)$$

e

$$F(X) = G(X)Q_2(X) + R_2(X).$$

Subtraindo a segunda igualdade da primeira, obtemos:

$$\begin{gathered} G(X)Q_1(X) + R_1(X) - G(X)Q_2(X) - R_2(X) = 0 \Rightarrow \\ G(X)Q_1(X) - G(X)Q_2(X) = R_2(X) - R_1(X) \Rightarrow \\ G(X)[Q_1(X) - Q_2(X)] = R_2(X) - R_1(X). \end{gathered} \quad (2.5)$$

Assim, temos $R_2(X) - R_1(X) = 0$ ou $\partial(R_2(X) - R_1(X)) < \partial(G(X))$.

Suponha, primeiramente, que $\partial(R_2(X) - R_1(X)) < \partial(G(X))$. Mas isso é equivalente a dizer que $\partial(G(X)[Q_1(X) - Q_2(X)]) < \partial(G(X))$, isto é, estamos tomando $G(X)$ e multiplicando ele por outro elemento, resultando em um terceiro elemento, cujo grau é menor do que o próprio $G(X)$. Porém, pela própria definição de produto de polinômios, isso é impossível.

Sendo assim, a única opção restante é que $R_2(X) - R_1(X) = 0$, e assim

$$G(X)[Q_1(X) - Q_2(X)] = 0.$$

Como $G(X) \neq 0$ por hipótese, nos resta que $Q_1(X) - Q_2(X) = 0$, ou seja, $Q_1(X) = Q_2(X)$ e $R_1(X) = R_2(X)$. □

Teorema 2.101. *Se k é corpo, então $k[X]$ é PID.*

Demonstração. Precisamos mostrar que todo ideal I de $k[X]$ é ideal principal, ou seja, existe $G(X) \in k[X]$ tal que $I = \langle G(X)\rangle$.

Seja I um ideal qualquer de $k[X]$. Se $I = \{0\}$ então $I = \langle 0\rangle$. Suponha $I \neq \{0\}$ e $G(X) \neq 0$, onde $G(X) \in I$ é de grau mínimo, cuja existência se dá pelo Princípio do Menor Inteiro.

Se o grau de $G(X)$ é 0, então $G(X) \in k[X]$ e $G(X)$ é invertível em $k[X]$. Logo, pela Proposição 2.28 - item 4, $I = \langle 1\rangle = k[X]$, então I é ideal principal.

Se $\partial(G) \geq 1$ e $F(X) \in I$ qualquer, então, pelo Algoritmo da Divisão (Teorema 2.100), podemos afirmar que existem $Q(X), R(X) \in k[X]$ tais que:

$$F(X) = G(X)Q(X) + R(X), \text{ onde } R(X) = 0 \text{ ou } \partial(R) \leq \partial(G).$$

Note que $F(X) \in I$ e $G(X) \in I$ e assim $F(X) - G(X)Q(X) = R(X) \in I$, por definição de ideal. Como $G(X)$ é elemento não nulo de grau mínimo em I, temos que $R(X) = 0$, e

$$F(X) - G(X)Q(X) = 0 \Rightarrow F(X) = G(X)Q(X).$$

Note que $G(X)Q(X) \in \langle G(X)\rangle$, logo $F(X) \in \langle G(X)\rangle$, portanto $I \subset \langle G(X)\rangle$. Como $G(X) \in I$, temos que $\langle G(X)\rangle \subset I$. Logo, $I = \langle G(X)\rangle$. □

Corolário 2.102. *Se k é corpo, então $k[X]$ é UFD.*

Demonstração. Sabemos do Teorema 2.101 que se k é corpo, então $k[X]$ é PID. Além disso, pelo Teorema 2.62, temos que todo PID é UFD, portanto $k[X]$ é UFD. □

Definição 2.103. O *máximo divisor comum* (mdc) de uma coleção de polinômios $\{F_t\}_{t\in T}$, em $k[X]$, é o polinômio mônico p caracterizado pelas seguintes propriedades:

- p divide cada F_t na coleção;
- se $q \in k[X]$ divide cada F_t na coleção, então q divide p.

Corolário 2.104. *Seja $\{F_s\}_{s\in S}$ uma coleção de polinômios em $k[X]$. Então existem índices $s_1, \cdots, s_n \in S$ e polinômios $q_1, \cdots, q_n \in k[X]$ tais que:*

$$F = q_1F_{s_1} + \cdots + q_nF_{s_n}$$

é o mdc dessa coleção.

Demonstração. Seja I o ideal gerado por $\{F_s\}_{s\in S}$, logo:

$$I = \left\{ \sum_{1\leq i\leq m} g_iF_{s_i};\ s_1, \cdots, s_m \in S,\ g_1, \cdots, g_m \in k[X],\ m = 1, 2, \cdots \right\}.$$

Seja F o gerador mônico de I. Sendo F um elemento de I, necessariamente existem $q_1, \cdots, q_n \in k[X]$ tais que F se escreve da forma:

$$F = q_1F_{s_1} + \cdots + q_nF_{s_n}.$$

Assim, se q divide cada F_s na coleção, então q divide F. Por fim, sendo $I = \langle F\rangle$, então cada F_s é divisível por F. □

Teorema 2.105. *Seja k um corpo. Um ideal $\langle P(X)\rangle \neq 0$ de $k[X]$ é ideal maximal se, e somente se, $P(X)$ é irredutível sobre k.*

Demonstração. ($\Rightarrow$) Suponha que $\langle P(X)\rangle \neq 0$ seja um ideal maximal em $k[X]$. Então $\langle P(X)\rangle \neq k[X]$, logo $P(X) \notin k$.

Agora, seja $P(X) = F(X)G(X)$ uma fatoração de $P(X)$ em $k[X]$. Como $\langle P(X)\rangle$ é um ideal maximal, então, pela Proposição 2.32, também é um ideal primo e assim $(F(X)G(X)) \in \langle P(X)\rangle$ implica que $F(X) \in \langle P(X)\rangle$ ou $G(X) \in \langle P(X)\rangle$, isto é $F(X)$ ou $G(X)$ tem $P(X)$ como um fator. Mas não podemos ter os graus de $F(X)$ e $G(X)$ estritamente menores que o grau de $P(X)$. Isso nos mostra que $P(X)$ é irredutível sobre k, por definição.

($\Leftarrow$) Sabemos que $P(X)$ é irredutível sobre $k[X]$. Suponha que N seja um ideal tal que $\langle P(X)\rangle \subsetneq N \subseteq k[X]$. Como N é um ideal principal, pelo Teorema 2.101, segue que $N = \langle G(X)\rangle$, para algum $G(X) \in k[X]$. Assim, como $P(X) \in \langle P(X)\rangle$ e $\langle P(X)\rangle \subset N = \langle G(X)\rangle$, então $P(X) \in \langle G(X)\rangle$, logo $P(X) = G(X)Q(X)$, para algum $Q(X) \in k[X]$.

Mas $P(X)$ é irredutível, implicando, pela Definição 2.21, que ou $G(X)$ ou $Q(X)$ é invertível em $k[X]$. Entretanto, os elementos invertíveis de $k[X]$ são os elementos

não nulos em k e consequentemente, ou $G(X)$ ou $Q(X)$ é uma constante diferente de zero em k, necessariamente. Assim, temos:

Se $G(X)$ é uma constante diferente de zero em k, então $G(X)$ é invertível em $k[X]$, consequentemente $N = \langle G(X)\rangle = k[X]$, pela Proposição 2.28, item (4).

Se $Q(X)$ é uma constante diferente de zero em k, ou seja, $Q(X) = c$, onde $c \in k^*$, podemos escrever $G(X)$ como $G(X) = \frac{1}{c}P(X)$, mas $\frac{1}{c}P(X) \in \langle P(X)\rangle$, portanto $G(X) \in \langle P(X)\rangle$, isto é, $\langle G(X)\rangle \subset \langle P(X)\rangle$, com isso $N = \langle G(X)\rangle = \langle P(X)\rangle$. Mas isso contradiz a hipótese de que $\langle P(X)\rangle \neq N$, portanto, a única possibilidade é que $N = k[X]$. Logo, $\langle P(X)\rangle$ é ideal maximal.

□

Teorema 2.106. *Sejam $P(X)$ um polinômio irredutível em $k[X]$ e $R(X), S(X) \in k[X]$ polinômios quaisquer. Se $P(X)$ divide $R(X)S(X)$, então $P(X) \mid R(X)$ ou $P(X) \mid S(X)$.*

Demonstração. Note que, como $P(X)$ é irredutível, temos, pelo Teorema 2.105, que $\langle P(X)\rangle$ é ideal maximal e, pela Proposição 2.32, ideal primo. Assim, se $P(X) \mid R(X)S(X)$, então $R(X)S(X) \in \langle P(X)\rangle$, mas $\langle P(X)\rangle$ é ideal primo, logo $R(X) \in \langle P(X)\rangle$ ou $S(X) \in \langle P(X)\rangle$, ou seja, $P(X) \mid R(X)$ ou $P(X) \mid S(X)$. □

Corolário 2.107. *Se $P(X)$ é irredutível em $k[X]$ e $P(X)$ divide o produto $R_1(X) \cdot \cdots \cdot R_n(X)$, com $R_i(X) \in k[X]$, $\forall i \in \{1, \cdots, n\}$, então $P(X) \mid R_i(X)$, para algum $i \in \{1, \cdots, n\}$.*

Demonstração. Este corolário segue do Teorema 2.105 e do Princípio de Indução Finita. □

Teorema 2.108. *Se k é um corpo, então todo polinômio não constante $F(X) \in k[X]$ pode ser fatorado em $k[X]$ em um produto de polinômios irredutíveis de maneira única a menos da ordem no referido produto e por constantes não nulas em k.*

Demonstração. Seja $F(X)$ um polinômio não constante. Se $F(X)$ não é irredutível, então $F(X) = G(X)H(X)$, onde os graus de $G(X)$ e $H(X)$ são ambos menores que o grau de $F(X)$. Se $G(X)$ e $H(X)$ são ambos irredutíveis, o resultado está provado.

Caso contrário, pelo menos um desses se fatora em polinômios de grau menor. Continuando este processo, obtemos a fatoração:

$$F(X) = P_1(X)P_2(X)\cdots P_r(X),$$

em que cada $P_i(X)$ é irredutível, $i \in \{1, \cdots, r\}$.

Nos resta mostrar a unicidade, a menos de ordem de produto e constantes não nulas em k. Suponha que

$$F(X) = P_1(X)P_2(X)\cdots P_r(X)$$

e

$$F(X) = Q_1(X)Q_2(X)\cdots Q_s(X)$$

sejam duas fatorações de $F(X)$ em polinômios irredutíveis.

Pelo Corolário 2.107, $P_1(X)$ divide algum $Q_j(X)$. Sem perda de generalidade, podemos supor que $P_1(X) \mid Q_1(X)$.

Se $Q_1(X)$ é irredutível, então $Q_1(X) = u_1P_1(X)$, com $u_1 \in K - \{0\}$, e, portanto u é invertível em $k[X]$. Assim, substituindo $Q_1(X)$ por $u_1P_1(X)$, temos que

$$P_1(X)P_2(X)\cdots P_r(X) = u_1P_1(X)Q_2(X)\cdots Q_s(X)$$
$$\Rightarrow P_2(X)\cdots P_r(X) = u_1Q_2(X)\cdots Q_s(X).$$

De forma análoga, digamos $Q_2(X) = u_2P_2(X)$ e então

$$P_3(X)\cdots P_r(X) = u_1Q_3(X)\cdots Q_s(X).$$

Continuando esse processo, obtemos:

$$1 = u_1u_2\cdots u_rQ_{r+1}(X)\cdots Q_s(X).$$

Mas isso só faz sentido se $1 = u_1u_2\cdots u_r$. Assim, os fatores irredutíveis de $P_i(X)$ e $Q_j(X)$ são os mesmos, exceto possivelmente por ordem de fatores e elementos invertíveis de $k[X]$. □

Definição 2.109. Seja R um UFD. Um polinômio $F(X) = a_0+a_1X+\cdots+a_nX^n \in R[X]$, não constante, é primitivo se $mdc(a_0, \cdots, a_n) = 1$.

Proposição 2.110. *Se R é UFD, então para cada polinômio não constante $F(X) \in R[X]$ temos $F(X) = rG(X)$, onde $r \in R$ e $G(X) \in R[X]$ é primitivo. O elemento r é único, a menos de um fator invertível em R, e chamado* ***conteúdo de*** $\mathbf{F(X)}$*. Além disso, $G(X)$ é único a menos de um fator invertível em R.*

Demonstração. Seja $F(X) \in R[X]$ qualquer, onde $F(X) = a_0 + a_1X + \cdots + a_nX^n$ é não-constante. Seja $r = mdc(a_0, \cdots, a_n)$. Então temos $a_i = rg_i$ para algum $g_i \in R$, $i \in \{1, \cdots, n\}$.

Pela distributividade, temos:

$$\begin{aligned} F(X) &= a_0 + a_1X + \cdots + a_nX^n \\ &= rg_0 + rg_1X + \cdots + rg_nX^n \\ &= r(g_0 + g_1X + \cdots + g_nX^n) \\ &= rG(X), \end{aligned}$$

onde $mdc(g_0, \cdots, g_n) = 1$. Assim, $G(X)$ é primitivo.

Note que r é único. De fato, se $F(X) = kH(X)$, para $k \in R$ e $H(X) \in R[X]$ primitivo, então cada fator irredutível de r deverá dividir k, e vice-versa.

Considerando $rG(X) = kH(X)$ e cancelando os fatores irredutíveis de r em k, obteremos $uG(X) = vH(X)$, onde u é invertível em R. Mas v também deve ser invertível em R ou poderíamos cancelar fatores irredutíveis de v em u. Portanto, tanto u quanto v são invertíveis em R, logo r é único, a menos de um fator invertível. Além disso, como $F(X) = rG(X)$, temos que o polinômio primitivo $G(X)$ também é único a menos de um fator irredutível. □

Lema 2.111 (Lema de Gauss)**.** *Se R é UFD, então um produto de dois polinômios primitivos em $R[X]$ ainda é primitivo.*

Demonstração. Considere $F(X) = a_0 + a_1X + \cdots + a_nX^n$ e $G(X) = b_0 + b_1X + \cdots + b_mX^m$ primitivos em $R[X]$, e seja $H(X) = F(X)G(X)$.

Seja p irredutível em R. Então p não divide todos os a_i,$i \in \{1, \cdots, n\}$ e não divide todos os b_j, $j \in \{1, \cdots, m\}$, pois $F(X)$ e $G(X)$ são primitivos. Logo, $mdc(a_0, \cdots, a_n) = 1 = mdc(b_0, \cdots, b_m)$.

Seja a_r o primeiro coeficiente de $F(X)$ não divisível por p, ou seja, $p \mid a_i,\ \forall i < r$, mas $p \nmid a_r$. De forma análoga, $p \mid b_j,\ \forall j < s$, mas $p \nmid b_s$.

O coeficiente de X^{r+s} em $H(X) = F(X)G(X)$ é

$$c_{r+s} = (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0).$$

Como $p \mid a_i,\ \forall i < r$, segue que $p \mid (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1})$ e como $p \mid b_j,\ \forall j < s$, então $p \mid (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0)$. Mas $p \nmid a_r$ e $p \nmid b_s$, logo $p \nmid a_rb_s$, portanto $p \nmid c_{r+s}$.

Com isso temos que dado um irredutível $p \in R$, existe algum coeficiente de $H(X) = F(X)G(X)$ não divisível por p. Portanto, $H(X)$ é primitivo. □

Corolário 2.112. *Se R é um UFD, então o produto finito de polinômios primitivos em $R[X]$ é também primitivo.*

Demonstração. Este corolário segue do lema anterior, utilizando o Princípio da Indução Finita. De fato, vimos, na demonstração do lema anterior, que o produto de dois polinômios primitivos, em $R[X]$, é primitivo. Isto é:

$$H(X) = F(X)G(X) \text{ é primitivo, com } F(X) \text{ e } G(X) \text{ primitivos.}$$

Agora, suponha que o produto de k polinômios primitivos em $R[X]$ é primitivo, isto é:

$$H(X) = F_1(X)F_2(X)\cdots F_k(X) \text{ é primitivo, com } F_i(X) \text{ primitivo, } \forall i \in \{1, \cdots, k\}.$$

Agora, mostremos que é válido para $k+1$ polinômios primitivos em $R[X]$, isto é, se:

$$L(X) = F_1(X)F_2(X)\cdots F_k(X)F_{k+1}(X).$$

com $F_i(X)$ primitivo, $\forall i \in \{1, \cdots, k+1\}$, mostremos que $L(X)$ também é primitivo.

Por hipótese, $H(X) = F_1(X)F_2(X)\cdots F_K(X)$ é primitivo e, ainda,

$$L(X) = H(X)F_{k+1}(X).$$

Pelo Lema de Gauss, temos que $L(X)$ é primitivo, já que $H(X)$ e $F_{k+1}(X)$ são primitivos por hipótese. □

Proposição 2.113. *Sejam R um UFD, K um corpo de frações de R e $F(X) \in R[X]$ um polinômio onde $\partial(F(X)) > 0$. Se $F(X)$ é irredutível em $R[X]$, então $F(X)$ também é irredutível em $K[X]$. Além disso, de $F(X)$ é primitivo em $R[X]$ e irredutível em $K[X]$, então $F(X)$ é irredutível em $R[X]$.*

Demonstração. Suponha um polinômio não constante $F(X) \in R[X]$ que se fatora em polinômios de menor grau em $K[X]$, isto é, $F(X) = T(X)S(X)$, para algum $T(X), S(X) \in R[X]$, com $\partial(T(X)) < \partial(F(X))$ e $\partial(S(X)) < \partial(F(X))$. Assim como K é o corpo das frações de R, cada coeficiente em $T(X)$ e $S(X)$ é da forma $\dfrac{a}{b}$ para determinados $a \in R$ e $b \in R^*$. Tomemos

$$T(X) = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \cdots + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \frac{a_n}{b_n}X^n$$

e

$$S(X) = \frac{p_0}{q_0} + \frac{p_1}{q_1}X + \cdots + \frac{p_{l-1}}{q_{l-1}}X^{l-1} + \frac{p_l}{q_l}X^l.$$

Com isso, temos que

$$T(X) = \frac{1}{b_0 \cdots b_n}(a_0(b_1 \cdots b_n) + a_1(b_0 b_2 \cdots b_n)X + \cdots + a_{n-1}(b_0 \cdots b_{n-2}b_n)X^{n-1} + a_n(b_0 \cdots b_{n-1})X^n)$$
$$\Rightarrow b_0 \cdots b_n T(X) = a_0(b_1 \cdots b_n) + a_1(b_0 b_2 \cdots b_n)X + \cdots + a_{n-1}(b_0 \cdots b_{n-2}b_n)X^{n-1} + a_n(b_0 \cdots b_{n-1})X^n$$
$$\Rightarrow b_0 \cdots b_n T(X) := T_1(X).$$

De forma análoga,

$$q_0 \cdots q_l S(X) = p_0(q_1 \cdots q_l) + p_1(q_0 q_2 \cdots q_l)X + \cdots + p_{l-1}(q_0 \cdots q_{l-2}q_l)X^{l-1} + p_l(q_0 \cdots q_{l-1})X^l$$
$$\Rightarrow q_0 \cdots q_l S(X) := S_1(X).$$

Assim:

$$F(X) = T(X)S(X) \Rightarrow (b_0 \cdots b_n)(q_0 \cdots q_l)T(X)S(X) = T_1(X)S_1(X)$$
$$\Rightarrow dF(X) = T_1(X)S_1(X),$$

em que $T_1(X), S_1(X) \in R[X]$, $d = b_0 \cdots b_n q_0 \cdots q_l \in R$, $\partial(T_1(X)) = \partial(T(X))$ e, ainda, $\partial(S_1(X)) = \partial(S(X))$, respectivamente.

pela Proposição 2.110, $F(X) = rG(X)$, $T_1(X) = r_1T_2(X)$ e $S_1(X) = r_2S_2(X)$ para polinômios primitivos $G(X), T_2(X), S_2(X) \in R[X]$ e $r, r_1, r_2 \in R$. Logo,

$$drG(X) = r_1r_2T_2(X)S_2(X).$$

Pelo Lema 2.111, $T_2(X)S_2(X)$ é primitivo. Pela parte da unicidade da Proposição 2.110, segue que $r_1r_2 = dru$, para algum u invertível em R, ou seja, com isso temos que

$$drG(X) = druT_2(X)S_2(X).$$

Assim, $F(X) = rG(X) = ruT_2(X)S_2(X)$, ou seja, mostramos que se $F(X)$ fatora de forma não-trivial em $K[X]$, então $F[X]$ fatora de forma não-trivial em polinômios de mesmo grau em $R[X]$. Logo, pela contrapositiva, se $F(X)$ for irredutível em $R[X]$, então $F(X)$ também é irredutível em $K[X]$.

Mais ainda, um polinômio não constante $F(X) \in R[X]$ primitivo em $R[X]$ e irredutível em $K[X]$ é também irredutível em $R[X]$, já que $R[X] \subseteq K[X]$. □

Corolário 2.114. *Sejam R um UFD, K um corpo de frações de R e $F(X) \in R[X]$ um polinômio onde $\partial(F(X)) > 0$. Se $F(X)$ é redutível em $K[X]$, então $F(X)$ também é redutível em $R[X]$. Mais ainda, se $G \in R[X]$ e $F|G \in K[X]$, então $F|G \in A[X]$.*

Demonstração. A demonstração segue da afirmação contrapositiva da primeira parte da Proposição 2.113. □

Corolário 2.115. *Se R é UFD e K é o corpo de frações de R. Então, $F(X) \in R[X]$, um polinômio não constante, se fatora em um produto de dois polinômios de graus menores r e s em $K[X]$ se, e somente se, $F(X)$ se fatora em polinômios de mesmos graus r e s em $R[X]$.*

Demonstração. Temos, pela demonstração da Proposição 2.113, que se podemos fatorar $F(X)$ em um produto de dois polinômios de graus menores em $K[X]$, então $F(X)$ pode ser fatorado em polinômios de mesmo grau em $R[X]$. □

Observação 2.116. A Proposição 2.113 nos mostra que se R é UFD, então os irredutíveis de $R[X]$ são exatamente as constantes irredutíveis de R com os polinômios primitivos não constantes em $R[X]$ irredutíveis em $K[X]$, onde K é o corpo de fração de $R[X]$.

Teorema 2.117. *Se R é UFD, então $R[X]$ também o é.*

Demonstração. Seja $F(X) \in R[X]$ não nulo e não invertível. Se $F(X)$ é de grau 0, então já obtemos a decomposição em elementos irredutíveis, por R é UFD. Além disso, como R é UFD, temos que tal fatoração de $F(X)$ é única.

Suponha $\partial(F(X)) > 0$. Se $F(X)$ for irredutível, então F já está decomposto em elementos irredutíveis de forma única.

Suponha $F(X)$ redutível. Desta forma, podemos reescrever $F(X)$ como $F(X) = H_1(X)H_2(X)$, tal que $\partial(H_1) < \partial(F)$ e $\partial(H_2) < \partial(F)$. Se ambos forem irredutíveis, então temos $F(X)$ fatorado em elementos irredutíveis. Sem perda de generalidade, suponha que $H_1(X)$ não seja irredutível e H_2 irredutível, então, mais uma vez, podemos fatorar $H_1(X)$ como $H_1(X) = K_1(X)K_2(X)$, tal que $\partial(K_1) < \partial(H_1)$ e $\partial(H_2) < \partial(K_1)$. Se ambos forem irredutíveis, então H_1 pode ser fatorado em elementos irredutíveis e, consequentemente, $F(X)$ também. Caso K_1 ou K_2 não sejam irredutíveis, repetimos esse processo. Sucessivamente, teremos

$$F(X) = L_1(X)L_2(X)\cdots L_n(X),$$

onde $L_i(X)$ é irredutível, $\forall i \in \{1, \cdots, n\}$, com n sendo o maior número possível de fatores irredutíveis de $F(X)$.

Ainda, note que, pela Proposição 2.110, cada $L_i(X)$ pode ser reescrito como $L_i(X) = r_iG_i(X)$, $i \in \{1, \cdots, n\}$, onde cada $r_i \in R$ é conteúdo de $L_i(X)$ e $G_i(X) \in R[X]$ é primitivo. Como L_i é irredutível em $R[X]$, então G_i também o é. Assim, podemos reescrever $F(X)$ da seguinte forma:

$$F(X) = r_1G_1(X)r_2G_2(X)\cdots r_nG_n(X) = r_1r_2\cdots r_n[G_1(X)G_2\cdots G_n(X)].$$

Como R é UFD, podemos fatorar cada r_i, $i \in \{1, \cdots, n\}$, em irredutíveis de R, obteremos, portanto, uma fatorização de $F(X)$ em um produto de irredutíveis em $R[X]$.

Sobre a unicidade, veja que a fatoração de $F(X) \in R[X]$, onde $F(X)$ tem grau 0 é única, uma vez que R é UFD.

Se $F(X)$ tem grau maior que 0, podemos ver qualquer fatoração de $F(X)$ em polinômios irredutíveis de $R[X]$ como uma fatoração em $K[X]$ em fatores de K e polinômios irredutíveis em $K[X]$, pela Proposição 2.113. Além disso, pelo Teorema 2.108, esses polinômios são únicos, exceto por possíveis fatores constantes em K e da ordem no produto, já que K é o corpo de fração.

Note que, como $F(X)$ é irredutível em $R[X]$, temos, pela Observação 2.116, que cada polinômio de grau maior que zero que aparece na fatoração de $F(X)$ é primitivo em $R[X]$. Pela unicidade da Proposição 2.110, isso mostra que esses polinômios primitivos são únicos em $R[X]$ a menos de fatores invertíveis.

O produto dos fatores constantes irredutíveis em R na fatoração de $F(X)$ é o conteúdo de $F(X)$, o qual é novamente único, a menos de fatores invertíveis, pela Proposição 2.110. Portanto, todos os irredutíveis em $R[X]$ que aparecem na fatoração são únicos a menos de ordem e elementos associados. □

Definição 2.118. $F(X) = \mu \prod (X - \lambda_i)^{e_i}$, $\mu, \lambda_i \in k$, onde λ_i são as raízes distintas de F e e_i é a multiplicidade de λ_i.

Definição 2.119. Um polinômio em $k[X_1, \cdots, X_n]$ de grau d tem d raízes em k, contando as multiplicidades.

Proposição 2.120. *Se k é um corpo e $X_1, \cdots, X_n$ são variáveis indeterminadas, então $k[X_1, \cdots, X_n]$ é um UFD.*

Demonstração. Pelo Corolário 2.102, temos que $k[X_1]$ é UFD e que, pelo Teorema 2.117, $(k[X_1])[X_2]]$ também o é, mas pela Observação 2.86 $(k[X_1])[X_2]] = k[X_1, X_2]$. Utilizando o Princípio de Indução Finita, temos que $k[X_1, \cdots, X_n]$ é UFD. □

Definição 2.121. O corpo de frações de $k[X_1, \cdots, X_n]$ é escrito $k(X_1, \cdots, X_n)$ e chamado de corpo de frações racional com n variáveis sobre k.

Proposição 2.122. *Se k é um corpo, $F \in k[X_1, \cdots, X_n]$ e $a_1, \cdots, a_n \in k$, então*

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

Demonstração. Queremos mostrar que qualquer polinômio $F \in k[X_1, \cdots, X_n]$ pode ser escrito como uma combinação linear de monômios da forma $(X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$, onde $\lambda_{(i)} \in k$ e $i_1, \cdots, i_n$ são inteiros positivos. Para tal, note que cada monômio em F pode ser escrito como $X_1^{j_1} \cdots X_n^{j_n}$, para algum inteiro positivo $j_1, \cdots, j_n$. Podemos, portanto, reescrever tais monômios como

$$X_1^{j_1} \cdots X_n^{j_n} = (X_1 - a_1 + a_1)^{j_1} \cdots (X_n - a_n + a_n)^{j_n}.$$

Mas, pelo Teorema Binomial, temos que, para cada X_i

$$(X_i - a_i + a_i)^{j_i} = \sum_{i_i=0}^{j_i} \binom{j_i}{i_i} (X_i - a_i)^{i_i} a_i^{j_i - i_i}.$$

Deste modo, o monômio $X_1^{j_1} \cdots X_n^{j_n}$ pode ser escrito como uma combinação linear de monômios da forma $(X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$, onde os coeficientes são produtos de coeficientes binomiais e potências de $a_1, \cdots, a_n$. Como F é uma combinação linear de monômios, então F também pode ser escrito como uma combinação linear de monômios do tipo $X_1^{j_1} \cdots X_n^{j_n}$, como queríamos. □

Proposição 2.123. *Sejam k um corpo, $F \in k[X_1, \cdots, X_n]$ e $a_1, \cdots, a_n \in k$.*

Se $F(a_1, \cdots, a_n) = 0$, então $F = \sum_{i=1}^{n} (X_i - a_i) G_i$, em que $G_i \in k[X_1, \cdots, X_n]$.

Demonstração. Suponha $F(a_1, \cdots, a_n) = 0$. Queremos mostrar que F pode ser escrito como a soma de polinômios da forma $(X_i - a_i)G_i$, onde $G_i \in k[X_1, \cdots, X_n]$. Pela Proposição 2.122, sabemos que

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

Como $F(a_1, \cdots, a_n) = 0$, temos que

$$0 = \sum \lambda_{(i)} (0)^{i_1} \cdots (0)^{i_n},\ \lambda_{(i)} \in k.$$

Isso implica que todos os termos da soma com pelo menos um dos i_j é igual a 0 deve ter coeficiente 0, isto é, cada termo da soma deve ter pelo menos um fator $(X_i - a_i)$ para algum i. Deste modo, podemos escrever F como a soma de termos na forma $(X_i - a_i)G_i$, onde G_i é um polinômio em $k[X_1, \cdots, X_n]$. □

Agora que relembramos os resultados importantes sobre anéis e corpos, podemos finalmente abordar os conceitos de Geometria Algébrica necessários.

3 Conjuntos Algébricos Afins

Nesse capítulo abordaremos alguns conceitos e resultados importantes para a Geometria Algébrica, para tal, utilizamos as referências [3] e [4]. Vale ressaltar que todos os exemplos, com exceção do Exemplo 3.5, foram elaboradas pela autora. Além disso, esmiuçamos as demonstrações, incluindo mais detalhes e conceitos prévios.

3.1 Espaço Afim e Conjunto Algébrico

Definição 3.1. Seja k um corpo. Definimos $A^n(k)$ (ou A^n, quando k é subentendido) como o produto cartesiano de k com ele mesmo n vezes. Assim, $A^n(k)$ é o conjunto das n-uplas dos elementos de k.

Chamamos $A^n(k)$ de **n-espaço afim sobre** k e seus elementos são chamados de *pontos*. Quando temos $A^1(k)$ chamamos de reta afim e $A^2(k)$ de plano afim.

Definição 3.2. Sejam $F \in k[X_1, \cdots, X_n]$ um polinômio e $P = (a_1, \cdots, a_n) \in A^n(k)$ um ponto. Dizemos que P é **zero de F** se $F(P) = F(a_1, \cdots, a_n) = 0$.

Definição 3.3. Se F não é um polinômio constante, o conjunto de zeros de F é chamado de **hipersuperfície** definido por F e denotado por $V(F)$.

Uma hipersuperfície de $A^2(k)$ é chamada *curva do plano afim*.

Se F é um polinômio de grau 1, $V(F)$ é chamado de *hiperplano* de $A^n(k)$. Se $n = 2$, $V(F)$ será chamado de reta.

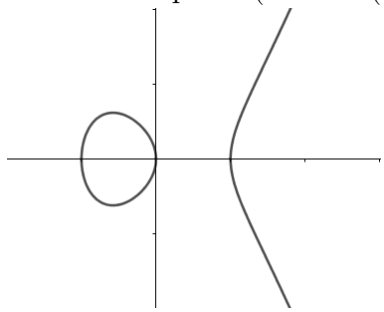
Genericamente, se tivermos S um conjunto qualquer de polinômios em $k[X_1, \cdots, X_n]$, então podemos definir $V(S) = \{P \in A^n(k);\ F(P) = 0,\ \forall F \in S\}$.

Observação 3.4. Segue diretamente da definição anterior que

$$V(S) = \bigcap_{F \in S} V(F).$$

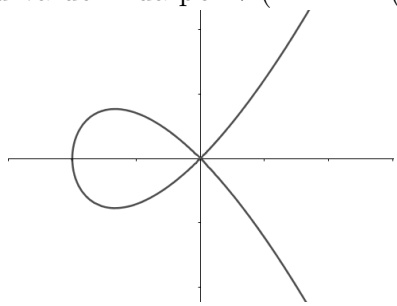
Exemplo 3.5. Seja $k = \mathbb{R}$.

Figura 3.1: Curva definida por $V(Y^2 - X(X^2 - 1)) \subset A^2$.



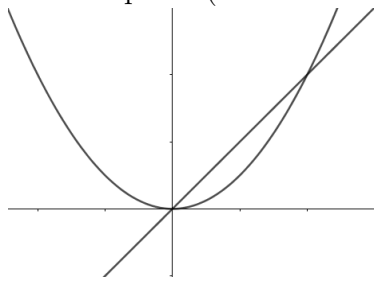
Fonte: elaborado pela autora (2022)

Figura 3.2: Curva definida por $V(Y^2 - X^2(X + 1)) \subset A^2$.



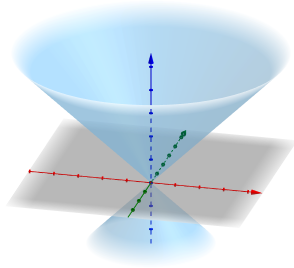
Fonte: elaborado pela autora (2022)

Figura 3.3: Curva definida por $V(Y^2 - XY - X^2Y + X^3) \subset A^2$.



Fonte: elaborado pela autora (2022)

Figura 3.4: Curva definida por $V(Z^2 - (X^2 + Y^2)) \subset A^3$.



Fonte: elaborado pela autora (2022)

Observação 3.6. Vale ressaltar que, geralmente, utilizamos $V(F_1, \cdots, F_r)$ ao invés da notação completa $V(\{F_1, \cdots, F_r\})$, como um abuso de notação. Consequentemente, teremos $V(F_1, \cdots, F_r) = \bigcap_{i=1}^{r} V(F_i)$.

Definição 3.7. Um subconjunto $X \subset A^n(k)$ é um **conjunto algébrico** (ou, de maneira mais completa, conjunto algébrico afim) se $X = V(S)$, para algum $S \subset k[X_1, \cdots, X_n]$.

Proposição 3.8. *Se I é um ideal em $k[X_1, \cdots, X_n]$ gerado por S, então $V(S) = V(I)$, ou seja, todo conjunto algébrico é igual a $V(I)$, para algum ideal I.*

Demonstração. Queremos mostrar que $V(S) = V(I)$ e para tal precisamos mostrar que: (i) $V(I) \subset V(S)$ e (ii) $V(S) \subset V(I)$.

Sejam $S = \{F_1, \cdots, F_r\}$, $F_i \in k[X_1, \cdots, X_n]$ e $I = \langle S \rangle = \langle F_1, \cdots, F_r \rangle$. Lembremos que se $F \in I$, então $F = \sum_{i=1}^{r} c_i F_i$.

(i) Seja $P \in V(I)$ qualquer, então $F(P) = 0, \forall F \in I = \langle F_1, \cdots, F_r \rangle$. Em particular, $F_1, \cdots, F_r \in I$.

Desta forma, $F_i(P) = 0, \forall i \in \{1, \cdots, r\} \Rightarrow P \in \bigcap_{i=1}^{r} V(F_1) = V(S)$, tal igualdade se dá pela definição de $V(S)$.

(ii) Seja $P \in V(S)$ qualquer. Isso significa que $F_i(P) = 0, \forall i \in \{1, \cdots, r\}$.

Para mostrar que $P \in V(I)$ tomemos $F \in I$ qualquer. Assim, como $F \in I$, temos que $F = \sum_{i=1}^{r} c_i F_i$, logo: $F(P) = \sum_{i=1}^{r} c_i F_i(P)$. Observe que $F_i(P) = 0, \forall i \in \{1, \cdots, r\}$, já que $P \in V(S)$. Logo $\sum_{i=1}^{r} c_i F_i(P) = 0$, ou seja, $F(P) = 0$ e desta forma $P \in V(I)$.

□

Proposição 3.9. *Se $\{I_\alpha\}_\alpha$ é uma coleção de ideais, então $V\left(\bigcup_\alpha I_\alpha\right) = \bigcap_\alpha V(I_\alpha)$, ou seja, a intersecção de qualquer coleção de conjuntos algébricos é um conjunto algébrico.*

Demonstração. Mostremos que: (i) $V\left(\bigcup_\alpha I_\alpha\right) \subset \bigcap_\alpha V(I_\alpha)$ e (ii) $\bigcap_\alpha V(I_\alpha) \subset V\left(\bigcup_\alpha I_\alpha\right)$. De fato:

(i) Seja $P \in V\left(\bigcup_\alpha I_\alpha\right)$ qualquer. Como $P \in V\left(\bigcup_\alpha I_\alpha\right)$, segue, por definição, que $F(P) = 0, \forall F \in \bigcup_\alpha I_\alpha$.

Em particular, $I_\alpha \subset \bigcup_\alpha I_\alpha$, $\forall \alpha$. Daí, se $F \in I_\alpha$, $\forall \alpha$, temos que $F(P) = 0$, logo $P \in V(I_\alpha), \forall \alpha$, ou seja, $P \in \bigcap_\alpha V(I_\alpha)$.

(ii) Seja $P \in \bigcap_{\alpha} V(I_\alpha)$ qualquer. Assim, se $P \in \bigcap_{\alpha} V(I_\alpha)$, então $P \in V(I_\alpha),\ \forall\alpha$. Logo

$$F(P) = 0, \forall F \in I_\alpha, \forall\alpha. \tag{3.1}$$

Agora, seja $F \in \bigcup_{\alpha} I_\alpha$ qualquer. Logo, $F \in I_\alpha$, para algum α. Por (3.1) temos que $F(P) = 0$ e, assim, $P \in V\left(\bigcup_{\alpha} I_\alpha\right)$.

□

Proposição 3.10. *Se $I \subset J$, onde I e J são ideais, então $V(I) \supset V(J)$.*

Demonstração. Seja $P \in V(J)$ qualquer, logo $F(P) = 0, \forall F \in J$. Como $I \subset J$, segue que $F(P) = 0, \forall F \in I$. Logo, $P \in V(I)$. □

Proposição 3.11. *As seguintes propriedades são válidas:*

(a) $V(F \cdot G) = V(F) \cup V(G)$, para quaisquer polinômios $F, G \in k[X_1, \cdots, X_n]$;

(b) $V(I) \cup V(J) = V(\{F \cdot G;\ F \in I, G \in J\})$, para quaisquer ideais $I, J \in k[X_1, \cdots, X_n]$,

ou seja, a união finita de conjuntos algébricos é um conjunto algébrico.

Demonstração. Mostremos os itens (a) e (b):

(a) Queremos mostrar que $V(F \cdot G) = V(F) \cup V(G)$, para isso, precisamos que:
(i) $V(F \cdot G) \subset V(F) \cup V(G)$ e (ii) $V(F) \cup V(G) \subset V(F \cdot G)$.

(i) Seja $P \in V(F \cdot G)$, qualquer. Desta forma, temos que:

$$(F \cdot G)(P) = 0 \Rightarrow F(P) \cdot G(P) = 0 \Rightarrow F(P) = 0 \text{ ou } G(P) = 0,$$

pois k é corpo e, portanto, domínio de integridade. Como $F(P) = 0$ ou $G(P) = 0 \Rightarrow P \in V(F)$ ou $P \in V(G)$. Portanto, $P \in V(F) \cup V(G)$.

(ii) Seja $P \in V(F) \cup V(G)$, qualquer. Assim, temos que:
$P \in V(F)$ ou $P \in V(G) \Rightarrow F(P) = 0$ ou $G(P) = 0 \Rightarrow F(P) \cdot G(P) = 0 \Rightarrow (F \cdot G)(P) = 0$. Logo, $P \in V(F \cdot G)$.

(b) Mostremos que $V(I) \cup V(J) = V(\{F \cdot G;\ F \in I, G \in J\}$. Para isso, precisamos mostrar que:
(i) $V(I) \cup V(J) \subset V(\{F \cdot G;\ F \in I, G \in J\}$ e (ii) $V(\{F \cdot G;\ F \in I, G \in J\}) \subset V(I) \cup V(J)$.

(i) Seja $P \in V(I) \cup V(J)$, qualquer. Disto, temos que:

$$\begin{aligned} &P \in V(I) \text{ ou } P \in V(J) \Rightarrow F(P) = 0,\ \forall F \in I,\ \text{ou } G(P) = 0,\ \forall G \in J \\ &\Rightarrow F(P) \cdot G(P) = 0,\ \forall F \in I,\ \forall G \in J \Rightarrow (F \cdot G)(P) = 0,\ \forall F \in I,\ \forall G \in J. \end{aligned}$$

Desta forma, $P \in V(\{F \cdot G;\ F \in I, G \in J\})$.

(ii) Seja $P \in V(\{F \cdot G;\ F \in I, G \in J\})$, qualquer. Assim, temos que:

$$(F \cdot G)(P) = 0,\ \forall F \in I,\ \forall G \in J \Rightarrow F(P) \cdot G(P) = 0,\ \forall F \in I,\ \forall G \in J$$
$$\Rightarrow F(P) = 0,\ \forall F \in I,\ \text{ou } G(P) = 0,\ \forall G \in J,$$

pois k é corpo e, portanto, domínio de integridade. Como $F(P) = 0,\ \forall F \in I,$ ou $G(P) = 0,\ \forall G \in J$, então $P \in V(I)$ ou $P \in V(J)$. Com isso, $P \in V(I) \cup V(J)$.

□

Proposição 3.12. *São válidas as seguintes propriedades:*

(a) $V(0) = A^n(k)$*, onde* 0 *é o polinômio nulo.*

(b) $V(1) = \emptyset$*, em que* 1 *é o polinômio constante* 1*.*

(c) $V(X_1 - a_1, \cdots, X_n - a_n) = \{(a_1, \cdots, a_n)\}$*, para qualquer* $a_i \in k$*. Consequentemente, um subconjunto finito de* $A^n(k)$ *é um conjunto algébrico.*

Demonstração. Demonstremos as propriedades (a), (b) e (c):

(a) Queremos mostrar que $V(0) = A^n(k)$, onde 0 é o polinômio nulo. De fato, $\forall P \in A^n(k)$,

$$0(P) = 0_k \Rightarrow P \in V(0).$$

Assim, $A^n(k) \subset V(0)$. Além disso, $V(0) \subset A^n(K)$ por definição.

(b) Mostremos que $V(1) = \emptyset$. De fato: $\forall P \in A^n(k)$,

$$1(P) = 1_k \neq 0 \Rightarrow V(1) = \emptyset.$$

(c) Agora, mostremos que $V(X_1 - a_1, \cdots, X_n - a_n) = \{(a_1, \cdots, a_n)\}, \forall a_i \in k$. Para tal, precisamos mostrar que:
(i) $V(X_1 - a_1, \cdots, X_n - a_n) \subset \{(a_1, \cdots, a_n)\}$;
(ii) $\{(a_1, \cdots, a_n)\} \subset V(X_1 - a_1, \cdots, X_n - a_n)$.

Com efeito:

(i) Seja $P = (b_1, \cdots, b_n) \in V(X_1 - a_1, \cdots, X_n - a_n)$. Sabemos que $F(P) = 0$, em que $F_i = X_i - a_i$, $\forall i \in \{1, \cdots, n\}$. Porém, isso apenas ocorre se $b_i - a_i = 0, \forall i \in \{1, \cdots, n\} \Rightarrow b_i = a_i, \forall i \in \{1, \cdots, n\}$. Assim, $P = (a_1, \cdots, a_n) \in \{(a_1, \cdots, a_n)\}$.

(ii) Se $P = (a_1, \cdots, a_n) \in \{(a_1, \cdots, a_n)\}$, então $F(P) = 0$, em que $F_i = X_i - a_i,\ \forall i \in \{1, \cdots, n\}$. Logo, $P \in V(X_1 - a_1, \cdots, X_n - a_n)$.

Veja que esta última parte pode ser generalizada para um conjunto $X = \{P_1, \cdots, P_s\}$, qualquer, com $X \subset A^n(k)$, onde cada $P_i = (a_{i_1}, \cdots, a_{i_n}), 1 \leq i \leq s$. Já que:

$$X = \{P_1, \cdots, P_s\} = \bigcup_{i=1}^{s} \{P_i\} = \bigcup_{i=1}^{s} V(\{X_1 - a_{i_1}, \cdots, X_n - a_{i_n}\}) = \bigcup_{i=1}^{s} V(I_i)$$
$$= V(\{F_1 \cdot \cdots \cdot F_s;\ F_i \in I_i\}),\ \text{em que } I_i = \langle X_1 - a_{i_1}, \cdots, X_n - a_{i_n} \rangle,\ \text{com } 1 \leq i \leq s.$$

□

Exemplo 3.13. Mostremos que $W = \{P = (t, t^2) \in A^2(\mathbb{R});\ t \in \mathbb{R}\}$ é um conjunto algébrico. Para tal, precisamos achar algum conjunto de polinômios tais que os elementos de W sejam zeros desses polinômios.

Considere $F = Y - X^2$. Veja que qualquer elemento de W zera o polinômio F, de fato:

$$F(P) = (t^2) - (t)^2 = t^2 - t^2 = 0 \Rightarrow F(P) = 0, \forall P \in W.$$

Assim, $W \subset V(F)$.

Por outro lado, seja $P = (a, b) \in V(F)$. Deste modo, por definição,

$$F(P) = F(a, b) = 0 \Rightarrow b - a^2 = 0 \Rightarrow b = a^2.$$

Deste modo, podemos reescrever P como $P = (a, a^2) \in W$. Logo, $V(F) \subset W$. Portanto, $W = V(F)$.

Exemplo 3.14. Mostremos que $W = \{P = (\cos(t), \text{sen}(t)) \in A^2(\mathbb{R});\ t \in \mathbb{R}\}$ é um conjunto algébrico. Para tal, precisamos achar algum conjunto de polinômios tais que os elementos de W sejam zeros desses polinômios.

Considere $G = X^2 + Y^2 - 1$. Veja que qualquer elemento de W zera o polinômio G. De fato:

$$G(P) = (\cos t)^2 + (\text{sen}\, t)^2 - 1 = 0 \Rightarrow G(P) = 0, \forall P \in W.$$

Logo, $W \subset V(G)$.

Por outro lado, $P = (a, b) \in V(G)$. Com isso,

$$G(P) = a^2 + b^2 - 1 = 0 \Rightarrow a^2 + b^2 = 1.$$

Note que o conjunto de pontos tais que $a^2 + b^2 = 1$ é uma circunferência de raio 1 e centro na origem. Sendo assim, podemos parametrizar essa curva tomando $a = \cos(u)$ e $b = \text{sen}(u)$. Com isso, podemos rescrever P com $P = (\cos(u), \text{sen}(u)) \in W$. Logo, $V(G) \subset W$. Portanto, $W = V(G)$.

3.2 O Ideal de Um Conjunto de Pontos

Definição 3.15. Sejam $X \subset A^n(k)$ um subconjunto qualquer, $P = (a_1, \cdots, a_n) \in X$ e $F \in k[X_1, \cdots, X_n]$.

Os polinômios que anulam sobre X formam um ideal em $k[X_1, \cdots, X_n]$ que chamamos de **ideal de X** e escrevemos $I(X)$. Tal ideal é definido por:

$$I(X) = \{F \in k[X_1, \cdots, X_n];\ F(P) = 0, \forall P \in X\}.$$

Exemplo 3.16. Seja $X \subset A^2(\mathbb{R}) = \mathbb{R}^2$, onde $X = \{(0, t);\ t \in \mathbb{R}\}$. Assim,

$$I(X) = \{F \in R[X_1, X_2];\ F(P) = 0, \forall P \in X\}.$$

Veja que os polinômios pertencentes a $I(X)$ serão aqueles que não possuem monômios puros da forma $X_2^k,\ k \in \mathbb{N}$ em sua composição.

Assim, um exemplo de polinômio pertencente a $I(X)$ seria $F = X_1X_2^3 + X_1^5$. De fato, tomando qualquer ponto da forma $(0, t)$ teremos

$$0 \cdot t^3 + 0^5 = 0.$$

Assim, $F \in I(X)$.

Por outro lado, $G = X_1X_2^3 + X_1^5 + X_2^4$ não pertence a $I(X)$ pois, tomando o ponto $(0, t)$, qualquer:

$$0 \cdot t^3 + 0^5 + t^4 = t^4$$

e isso só será igual a zero caso $t = 0$. Portanto, $G \notin I(X)$.

Proposição 3.17. *$I(X)$ é ideal de $k[X_1, \cdots, X_n]$.*

Demonstração. Para mostrar que $I(X)$ é ideal de $k[X_1, \cdots, X_n]$ temos que mostrar que:
(i) $I(X)$ é subgrupo de $k[X_1, \cdots, X_n]$ e (ii) $\forall G \in k[X_1, \cdots, X_n], \forall F \in I(X) : FG \in I(X)$. De fato:

(i) Sejam $F, G \in I(X)$, quaisquer.

Se $G \in I(X)$, então $G(P) = 0, \forall P \in X$, logo $(-G)(P) = -(G(P)) = 0, \forall P \in X$. Desta forma, $-G \in I(X)$. Veja que $F + (-G) \in I(X)$. De fato:

$$(F + (-G))(P) = F(P) + (-G)(P) = 0 + 0 = 0.$$

(ii) Tomemos $G \in k[X_1, \cdots, X_n]$ e $F \in I(X)$, quaisquer. Mostremos que $GF \in I(X)$, de fato:

$$(GF)(P) = (G(P))(F(P)) = G(P) \cdot 0 = 0.$$

□

Proposição 3.18. *Se $X \subset Y$, então $I(X) \supset I(Y)$.*

Demonstração. Seja $F \in I(Y)$ qualquer. Como $F \in I(Y)$, segue que:

$$F(P) = 0, \forall P \in Y.$$

Mas $X \subset Y$, logo $F(P) = 0, \forall P \in X$. Assim, $F \in I(X)$. □

Observação 3.19. Convencionamos que $I(\emptyset) = k[X_1, \cdots, X_n]$.

Proposição 3.20. *São válidas as seguintes propriedades:*

(a) $I(A^n(k)) = \langle 0 \rangle$, se k é um corpo infinito, onde 0 é o polinômio nulo.

(b) $I(\{(a_1, \cdots, a_n)\}) = \langle X_1 - a_1, \cdots, X_n - a_n \rangle$, para $a_i \in k$.

Demonstração. Mostremos os itens (a) e (b):

(a) Observe que $I(A^n(k)) = \{F \in k[X_1, \cdots, X_n];\ F(P) = 0, \forall P \in A^n(k)\}$. Considerando que precisamos abranger todos os elementos de $A^n(k)$, o único F possível para que isso ocorra é o polinômio nulo.

(b) Precisamos mostrar que $I(\{(a_1, \cdots, a_n)\}) = \langle X_1 - a_1, \cdots, X_n - a_n \rangle$. Para tal, mostremos que:
(i) $I(\{(a_1, \cdots, a_n)\}) \subset \langle X_1 - a_1, \cdots, X_n - a_n \rangle$;
(ii) $I(\{(a_1, \cdots, a_n)\}) \supset \langle X_1 - a_1, \cdots, X_n - a_n \rangle$.

De fato:

(i) Seja $F \in I(\{(a_1, \cdots, a_n)\})$, qualquer. Desta forma,

$$F(a_1, \cdots, a_n) = 0, \forall i \in \{1, \cdots, n\}.$$

Com isso, segue, da Proposição 2.123, que $F = \sum_{i=1}^{n}(X_i - a_i)G_i$, para algum $G_i \in k[X_1, \cdots, X_n]$, que pertence ao $\langle X_1 - a_1, \cdots, X_n - a_n\rangle$.

(ii) Seja $F \in \langle X_1 - a_1, \cdots, X_n - a_n\rangle$, qualquer. Se isso ocorre, então

$$F = \sum_{i=1}^{n} G_i(X_i - a_i) \text{ , para algum } G_i \in k[X_1, \cdots, X_n]$$

$$\Rightarrow F(a_1, \cdots, a_n) = \sum_{i=1}^{n} G_i(a_i - a_i) = 0.$$

Logo, $F \in I(\{(a_1, \cdots, a_n)\})$.

□

Proposição 3.21. *São válidas as propriedades:*

(a) $I(V(S)) \supset S$, $\forall S \subset k[X_1, \cdots, X_n]$.

(b) $V(I(X)) \supset X$, $\forall X \subset A^n(k)$.

Demonstração. Mostremos que (a) e (b) são válidas:

(a) Seja S um conjunto de polinômios qualquer, então sabemos que

$$V(S) = \{P \in A^n(k);\ F(P) = 0, \forall F \in S\}.$$

Com isso, temos que

$$I(V(S)) = \{F \in k[X_1, \cdots, X_n];\ F(P) = 0, \forall P \in V(S)\}.$$

Veja que, para qualquer $F \in S$, temos que $F(P) = 0, \forall P \in V(S)$. Logo, $F \in I(V(S))$, consequentemente, $S \subset I(V(S))$.

(b) Seja X um conjunto de pontos qualquer, então sabemos que

$$I(X) = \{F \in k[X_1, \cdots, X_n];\ F(P) = 0, \forall P \in X\}.$$

Com isso, temos que

$$V(I(X)) = \{P \in A^n(k);\ F(P) = 0, \forall F \in I(X)\}.$$

Observe que para qualquer $P \in X$, temos que $F(P) = 0, \forall F \in I(X)$. Logo, $X \in V(I(X))$ e, por consequência, $X \subset V(I(X))$.

□

Proposição 3.22. *As seguintes propriedades são válidas:*

(a) $V(I(V(S))) = V(S)$*, para qualquer conjunto* S *de polinômios.*

(b) $I(V(I(X))) = I(X)$*, para qualquer conjunto* X *de pontos.*

Assim, se V *é um conjunto algébrico, então* $V = V(I(V))$*. Além disso, se* I *é um ideal de um conjunto algébrico, então* $I = I(V(I))$*.*

Demonstração. Mostremos os itens (a) e (b):

(a) Precisamos mostrar que (i) $V(S) \subset V(I(V(S)))$ e (ii) $V(I(V(S))) \subset V(S)$. De fato:

(i) Seja $P_0 \in V(S)$, qualquer. Se $P_0 \in V(S)$, então $F(P_0) = 0, \forall F \in S$. Mostremos, portanto, que $P_0 \in V(I(V(S)))$, para isso, precisamos mostrar que $G(P_0) = 0, \forall G \in I(V(S))$. Para isso, seja $F \in I(V(S))$, qualquer.
Como $F \in I(V(S))$, segue que $F(P) = 0, \forall P \in V(S)$. Em particular, $P_0 \in V(S)$, por hipótese, assim, temos que:

$$F(P_0) = 0 \Rightarrow P_0 \in V(I(V(S))).$$

(ii) Seja $P \in V(I(V(S)))$, qualquer. Assim, segue que: $F(P) = 0, \forall F \in I(V(S))$. Sabemos, pela Proposição 3.21, item (a), que $S \subset I(V(S))$. Desta forma, temos que $F(P) = 0, \forall F \in S$ e, portanto, $P \in V(S)$.

(b) Precisamos mostrar que (i) $I(X) \subset I(V(I(X)))$ e (ii) $I(V(I(X))) \subset I(X)$. Assim:

(i) Seja $F_0 \in I(X)$, qualquer. Assim, $F_0(P) = 0, \forall P \in X$. Mostremos, então, que $F_0 \in I(V(I(X)))$, para isso, basta mostrar que $F_0(T) = 0, \forall T \in V(I(X))$. Desta forma, seja $T \in V(I(X))$ qualquer.
Como $T \in V(I(X))$, então $F(T) = 0, \forall F \in I(X)$. Em particular, F_0 está em $I(X)$, logo $F_0(T) = 0$. Assim, $F_0 \in I(X)$ e, portanto, $I(X) \subset I(V(I(X)))$.

(ii) Seja $F \in I(V(I(X)))$, qualquer. Se isso ocorre, então $F(P) = 0, \forall P \in V(I(X))$. Mas temos da Proposição 3.21, item (b), que $X \subset V(I(X))$, desta forma, $F(P) = 0, \forall P \in X$. Logo, $F \in I(X)$.

□

Um ideal de um conjunto algébrico possui uma propriedade particular, não compartilhada por todos os ideais, sendo essa:

Proposição 3.23. *Sejam* X *um conjunto algébrico e* I *um ideal de* X*. Se* $I := I(X)$ *e* $F^n \in I$*, para algum inteiro* $n > 0$*, então* $F \in I$*.*

Demonstração. Seja $F^n \in I(X)$, então temos que $(F^n)(P) = 0, \forall P \in X$. No entanto, observe que

$$(F^n)(P) = (F(P))^n = F(P) \cdot F(P) \cdot \ \cdots \ \cdot F(P) = 0$$

e isso só é possível se $F(P) = 0$.
Assim, como $F(P) = 0, \forall P \in X$, então $F \in I(X)$. □

Definição 3.24. Se I é um ideal no anel R, definimos o radical de I por

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

Proposição 3.25. *No contexto da definição anterior, $Rad(I)$ é um ideal de R.*

Demonstração. Para que $Rad(I)$ seja um ideal, precisamos mostrar que:

(i) Sejam $a, b \in Rad(I)$ quaisquer, então $a + b \in Rad(I)$:
Como $a, b \in Rad(I)$, então $a^n, b^m \in I$, com $m, n \in \mathbb{Z}^*$.
Assim,

$$(a+b)^{m+n} = \binom{m+n}{0}a^{m+n} + \binom{m+n}{1}a^{m+n-1}b + \cdots + \binom{m+n}{m+n-1}ab^{m+n-1} + \binom{m+n}{m+n}b^{m+n}.$$

Observe que cada $\binom{m+n}{j}a^ib^j \in I,\ i, j \in \{0, \cdots, m+n\}$. De fato:

Sabemos que $a^i = a^{n+k} = a^n a^k,\ k \in \{0, \cdots, m\}$. Como $a^n \in I$, então $a^n a^k \in I,\ k \in \{0, \cdots, m\}$. Além disso, temos $a^i b^j \in I$, com $0 \leq j < m$, já que $a^i \in I$.

De forma análoga, $b^j = b^{m+l} = b^m b^l,\ l \in \{0, \cdots, n\}$. Como $b^m \in I$, então $b^m b^l \in I,\ l \in \{0, \cdots, n\}$. Ainda, temos $a^i b^j \in I$, com $0 \leq i < n$, já que $b^j \in I$.

Desta forma, temos que cada $a^i b^j \in I,\ i, j \in \{0, \cdots, m+n\}$.

Como $\binom{m+n}{j}$ é um número inteiro não negativo, temos então que $\binom{m+n}{j}a^ib^j,\ i, j \in \{0, \cdots, m+n\}$, é um múltiplo de $a^ib^j,\ i, j \in \{0, \cdots, m+n\}$ e, logo, também está em I.

Além disso, como cada $a^ib^j \in I,\ i, j \in \{0, \cdots, m+n\}$, então temos que a soma deles também está em I. Consequentemente, $(a+b)^{m+n} \in I$. Logo, $a+b \in Rad(I)$.

(ii) Sejam $a \in Rad(I)$ e $r \in R$, então $ar \in Rad(I)$, pois, como $a \in Rad(I)$, então, temos que $a^n \in I$. Mostremos que $(ar)^n \in Rad(I)$. De fato,

$$(ar)^n = a^n r^n.$$

Observe que $a^n \in I$ e $r^n \in R$. Como I é ideal de R, temos que $(ar)^n = a^n r^n \in I$. E, por definição de $Rad(I)$, temos que $ar \in Rad(I)$.

□

Definição 3.26. Quando $I = Rad(I)$, chamamos I de **ideal radical**.

Exemplo 3.27. Tomemos $4\mathbb{Z}$ ideal em $\mathbb{Z}$. Mostremos que $2\mathbb{Z}$ é ideal radical de $4\mathbb{Z}$.
Seja $x \in Rad(4\mathbb{Z})$ qualquer, então $x^n \in 4\mathbb{Z}$, para algum $n \in \mathbb{Z}$. Deste modo,

$$x^n = 4m, m \in \mathbb{Z}.$$

Mas

$$x^m = 4m = 2 \cdot 2m, m \in \mathbb{Z}.$$

Assim, temos que 2 divide x^n, além disso, como 2 é primo, 2 divide x, ou seja, $x = 2k, k \in \mathbb{Z}$. Com isso, $x \in 2\mathbb{Z}$. Portanto, $Rad(4\mathbb{Z}) \subset 2\mathbb{Z}$.
Por outro, se $x \in 2\mathbb{Z}$ qualquer, então $x = 2k, k \in \mathbb{Z}$. Assim,

$$x^2 = (2k)^2 = 2^2k^2 = 4k^2 = 4m, m = k^2 \in \mathbb{Z}.$$

Deste modo, $x^2 \in 4\mathbb{Z}$. Logo, $x \in Rad(4\mathbb{Z})$. Portanto, $2\mathbb{Z} \subset Rad(4\mathbb{Z})$. Com isso, temos que $Rad(4\mathbb{Z}) = 2\mathbb{Z}$.

Observação 3.28. Veja que $I \subset Rad(I)$, pois se $a \in I$, então $a^1 \in I$, logo $a \in Rad(I)$.

Proposição 3.29. *$I(X)$ é um ideal radical de $k[X_1, \cdots, X_n]$, para qualquer conjunto $X \subset A^n(k)$.*

Demonstração. Mostremos que $I(X) = Rad(I(X))$. Para isso, precisamos mostrar que:

(i) $I(X) \subset Rad(I(X))$:
Isto já se dá pela Observação 3.28.

(ii) $Rad(I(X)) \subset I(X)$:
Seja $F \in Rad(I(X))$ qualquer. Como $F \in Rad(I(X))$, então $F^n \in I(X)$, para algum $n \in \mathbb{Z}_+^*$. Do fato que $F^n \in I(X)$, temos que $F^n(P) = 0, \forall P \in X$. Assim, $0 = F^n(P) = (F(P))^n \in k$, em que k é corpo, logo domínio de integridade, então $F(P) = 0, \forall P \in X$. Consequentemente, $F \in I(X)$.

□

Proposição 3.30. *Se I é ideal primo, então I é ideal radical.*

Demonstração. Temos que mostrar que $I = Rad(I)$ quando I é primo. Veja que $I \subset Rad(I)$, pela Observação 3.28.

Mostremos que $Rad(I) \subset I$. Se a é um elemento qualquer de $Rad(I)$, então temos que $a^m \in I$, para algum $m > 0$. Como I é primo, temos que se $a^m = a_1 \cdots a_m \in I$, então $a_i \in I$, para algum $i \in \{1, \cdots, m\}$. Porém, $a_i = a,\ \forall a_i,\ i \in \{1, \cdots, m\}$. Assim, $a \in I$. □

3.3 Teorema da Base de Hilbert

Mesmo que o conjunto algébrico seja definido para qualquer conjunto de polinômios, de fato um número finito sempre será suficiente.

Definição 3.31. Um anel é dito **noetheriano** se todo ideal do anel é finitamente gerado.

Exemplo 3.32. Veja que $\mathbb{Z}$ é um anel noetheriano, já que todos os seus ideais são gerados por um único inteiro, isto é, $n\mathbb{Z}$ são os ideais de $\mathbb{Z}$ e $\langle n \rangle = n\mathbb{Z}$.

Proposição 3.33. *Todo PID (Domínio de Ideais Principais) é noetheriano.*

Demonstração. Seja I um ideal de forma que I seja ideal principal. Se isso ocorre, então I é gerado por um único elemento, logo, I é finitamente gerado. □

Proposição 3.34. *Todo corpo é noetheriano.*

Demonstração. Se k é um corpo, então ele tem apenas dois ideais, os triviais, são eles: o gerado pelo elemento neutro, que é o próprio elemento, e o gerado pelo 1, que é o corpo todo. Desta forma, ambos os ideais são gerados por um único elemento e, portanto, finitamente gerados. □

Teorema 3.35. *Se R é um anel noetheriano, então $R[X_1, \cdots, X_n]$ é um anel noetheriano.*

Demonstração. Primeiramente, note que se R é um anel noetheriano, então $R[X]$ também o é. De fato:

Seja I um ideal qualquer em $R[X]$, devemos mostrar que I é finitamente gerado, ou seja, procuramos um conjunto finito de geradores para I.

Sejam $F = a_0 + a_1X + \cdots + a_dX^d \in R[X],\ a_d \neq 0$, onde a_d é o coeficiente líder de F, e J o conjunto gerado pelos coeficientes líderes de todos os polinômios em I. Observe que J é um ideal de R e como R é noetheriano, existem $b_1, \cdots, b_r \in I$, tal que $J = \langle b_1, \cdots, b_r \rangle$. Logo, existem polinômios $F_1, \cdots, F_r \in I$ cujos coeficientes líderes são, respectivamente, $b_1, \cdots, b_r$.

Tomemos um inteiro N maior do que o grau de cada F_i, $i \in \{1, \cdots, r\}$. Para cada $m \leq N$, tomemos J_m o ideal de R que consiste em todos os coeficientes líderes de todos os polinômios $F \in I$ tal que $\partial(F) \leq m$. Como J_m é um ideal em R e R é noetheriano, existem $c_{1_m}, \cdots, c_{s_m} \in I$ tal que $J_m = \langle c_{1_m}, \cdots, c_{s_m} \rangle$. Seja $\{F_{j_m}\}$, $j \in \{1, \cdots, s\}$, um conjunto finito de polinômios em I de grau menor ou igual que m, tais que o coeficiente líder de F_{j_m} é c_{j_m}, para todo $j \in \{1, \cdots s\}$. Seja I' o ideal gerado por F_i, $i \in \{1, \cdots, r\}$, e por todos os F_{j_m}, $j \in \{1, \cdots, s\}$.

Mostremos que $I = I'$. Note que $I' \subseteq I$, já que $F_i \in I,\ \forall i \in \{1, \cdots, r\}$ e $F_{j_m} \in I,\ \forall j \in \{1, \cdots, s\}$, bem como suas combinações.

Suponha que I' está contido propriamente em I, isto é, $I' \neq I$. Portanto, existe ao menos um elemento de I que não está pertence em I'. Seja G o elemento de I de menor grau de forma que $G \notin I'$.

- Se $\partial(G) > N$, então, é possível determinar polinômios Q_i tais que $\sum Q_iF_i$ e G têm o mesmo termo líder, digamos g_k. Note então que se fizermos $G - \sum Q_iF_i$, teremos eliminado o termo líder g_k. Observe que $\sum Q_iF_i \in I'$, já que I' é ideal. Assim $\partial(G - \sum Q_iF_i) < \partial(G)$, então $G - \sum Q_iF_i \in I'$, pois G é o polinômio de menor grau tal que $G \notin I'$, logo, todo polinômio com grau menor que G pertence a I'. Ainda, $G = (G - \sum Q_iF_i) + \sum Q_iF_i \in I'$, logo $G \in I'$, já que é a soma de elementos de I'. Mas isso é um absurdo, pois supomos $G \notin I'$.

- Se $\partial(G) = m \leq N$, então, é possível determinar polinômios Q_j tais que $\sum Q_jF_{j_m}$ e G têm o mesmo termo líder, digamos g_k. Note então que se fizermos $G - \sum Q_jF_{j_m}$, teremos eliminado o termo líder g_k. Observe que $\sum Q_jF_{j_m} \in I'$, já que I' é ideal. Assim $\partial(G - \sum Q_jF_{j_m}) < \partial(G)$, então $G - \sum Q_jF_{j_m} \in I'$, pois G é o polinômio de menor grau tal que $G \notin I'$. Logo, todo polinômio com grau menor que G pertence a I'. Ainda, $G = (G - \sum Q_jF_{j_m}) + \sum Q_jF_{j_m} \in I'$, logo $G \in I'$, já que é a soma de elementos de I'. Mas isso é um absurdo, pois supomos $G \notin I'$.

Desta forma, podemos concluir que G não existe e, portanto, $I = I'$.

Agora, note que, pela Observação 2.86, temos $R[X_1, X_2] = R[X_1][X_2]$, podemos mais uma vez fazer a demonstração anterior e concluiremos que $R[X_1, X_2]$ também é noetheriano, caso R o seja. Se fizermos isso sucessivamente, teremos que o teorema segue por indução da demonstração previamente realizada. □

Corolário 3.36. *$k[X_1, \cdots, X_n]$ é noetheriano para qualquer corpo k.*

Demonstração. Se k é corpo, então k é, em particular, um anel noetheriano pela Proposição 3.34. Assim, pelo Teorema 3.35, $k[X_1, \cdots, X_n]$ é noetheriano. □

Teorema 3.37. *Todo conjunto algébrico é a intersecção de um número finito de hipersuperfícies.*

Demonstração. Seja $I \subset k[X_1, \cdots, X_n]$ e $V(I)$ o conjunto algébrico determinado por I.

Pelo Corolário 3.36, I é finitamente gerado, ou seja, existem $F_1, \cdots, F_r \in I$ tais que $I = \langle F_1, \cdots, F_r \rangle$. Consequentemente, de Observação 3.4 e Proposição 3.8, segue que

$$V(I) = V(F_1) \cap \cdots \cap V(F_r).$$

□

3.4 Componentes Irredutíveis de um Conjunto Algébrico

Um conjunto algébrico pode ser a união de diversos conjuntos algébricos menores.

Definição 3.38. Dizemos que um conjunto algébrico $V \subset A^n$ é redutível se $V = V_1 \cup V_2$, em que V_1, V_2 são conjuntos algébricos em A^n e $V_i \neq V,\ i = 1, 2$.

Do contrário, V é irredutível.

Exemplo 3.39. Sejam $(a_0, b_0) \in A^2(\mathbb{R})$ e $r \in \mathbb{Z}_+^*$, quaisquer. Defina $F \in \mathbb{R}(X, Y)$ por

$$F = (X - a_0)^2 + (Y - b_0)^2 - r^2.$$

A curva plana afim $V(F)$ é uma circunferência de centro (a_0, b_0) e raio r.

Veja que, como F é um polinômio irredutível, tal curva também é irredutível.

Exemplo 3.40. Defina $F \in R(X, Y)$ por

$$F = X^2 - Y^2.$$

Note que podemos reescrever F como

$$F = (X + Y)(X - Y).$$

Portanto, F não é irredutível, já que pode ser fatorado nos polinômios irredutíveis $F_1 = X + Y$ e $F_2 = X - Y$, logo, $V(F)$ também não o é, já que pode ser reescrita como $V(F) = V(F_1) \cup V(F_2)$.

Exemplo 3.41. Defina $G \in R(X, Y)$ por

$$G = X^3 - XY.$$

Note que podemos reescrever G como

$$G = X(X^2 - Y).$$

Portanto, G não é irredutível, já que pode ser fatorado nos polinômios irredutíveis $G_1 = X$ e $G_2 = X^2 - Y$, logo, $V(G)$ também não o é, já que pode ser reescrita como $V(G) = V(G_1) \cup V(G_2)$.

Proposição 3.42. *Um conjunto algébrico V é irredutível se, e somente se, o ideal $I(V)$ é primo.*

Demonstração. Para mostrar tal proposição, usaremos a contrapositiva, ou seja, mostraremos que um conjunto algébrico V é redutível se, e somente se, o ideal $I(V)$ não é primo.

($\Rightarrow$) Suponha que V seja redutível, ou seja, existem V_1 e V_2, $V_1 \subsetneqq V$ e $V_2 \subsetneqq V$, tais que $V = V_1 \cup V_2$.

Com isso, temos:

$$I(V) = I(V_1 \cup V_2) \overset{\text{Prop. 3.18}}{\subsetneqq} I(V_1) \text{ e } I(V) = I(V_1 \cup V_2) \subsetneqq I(V_2).$$

Logo, existe $F_1 \in I(V_1)$ tal que $F_1 \notin I(V)$ e existe $F_2 \in I(V_2)$ tal que $F_2 \notin I(V)$.
Mas, $\forall p \in V = V_1 \cup V_2$,

$$(F_1F_2)(p) = F_1(p)F_2(p) = 0, \text{ pois } p \in V_1 \text{ ou } p \in V_2.$$

Logo, $F_1F_2 \in I(V)$, ou seja, $F_1F_2 \in I(V)$ com $F_1 \notin I(V)$ e $F_2 \notin I(V)$. Portanto, se V é redutível, então $I(V)$ não é ideal primo. Isto é, se $I(V)$ é ideal primo, então V é irredutível.

($\Leftarrow$) Agora, suponha que $I(V)$ não é primo, logo, existem $F_1, F_2 \in k[X_1, \cdots, X_n]$ tais que $F_1F_2 \in I(V)$, porém $F_1, F_2 \notin I(V)$. Com isso,

$$V = (V \cap V(F_1)) \cup (V \cap V(F_2)).$$

De fato:

(i) $(V \cap V(F_1)) \cup (V \cap V(F_2)) \subset V$, pois,

$V \cap V(F_1) \subset V$ e $V \cap V(F_2) \subset V$. Além disso, a união de conjuntos contidos em V também está em V.

(ii) $V \subset (V \cap V(F_1)) \cup (V \cap V(F_2))$.

Seja $p \in V$, qualquer. Como $F_1F_2 \in I(V)$ temos que $(F_1F_2)(p) = 0 \Rightarrow F_1(p) = 0$ ou $F_2(p) = 0$.

Segue, então, que $p \in V(F_1)$ ou $p \in V(F_2)$, assim: $p \in V \cap V(F_1)$ ou $p \in V \cap V(F_2)$. Logo, $p \in (V \cap V(F_1)) \cup (V \cap V(F_2))$.

Além disso, como $F_1 \notin I(V)$ segue que $V \cap V(F_1) \subsetneqq V$ e, também, como $F_2 \notin I(V)$ segue que $V \cap V(F_2) \subsetneqq V$, ou seja, V é redutível pela Definição 3.38. Portanto, se $I(V)$ não é ideal primo, então V é redutível, isto é, se V é irredutível, então $I(V)$ é ideal primo. □

Nosso próximo objetivo é mostrar que um conjunto algébrico é a união finita de conjuntos algébricos irredutíveis. De modo natural, podemos pensar que se V é redutível, então é possível reescrevê-lo como $V = V_1 \cup V_2$, o mesmo ocorre se V_2 é redutível, então $V_2 = V_3 \cup V_4$, e assim sucessivamente. Precisamos mostrar que esse processo para em algum momento e, com isso, alcançamos nosso objetivo. Neste sentido, a próxima proposição é fundamental.

Proposição 3.43. *Seja $\mathscr{S}$ uma coleção não vazia de ideais em um anel noetheriano R. Então $\mathscr{S}$ tem um membro maximal, isto é, existe um ideal I em $\mathscr{S}$ que não é contido em nenhum outro ideal de $\mathscr{S}$.*

Demonstração. Seja $\mathscr{S} = \{I : \ I \text{ é ideal de } R\}$. Queremos mostrar que existe $I_M \in \mathscr{S}$ tal que $I \subset I_M, \ \forall I \in \mathscr{S}$.

Utilizando o Axioma da Escolha[1] escolhemos um ideal para cada subconjunto de $\mathscr{S}$. Nesse sentido, seja I_0 o ideal escolhido para o próprio $\mathscr{S}$, já que, em particular, $\mathscr{S}$ é um subconjunto dele mesmo. Agora, escolha I_1 para $\mathscr{S}_1 = \{I \in \mathscr{S}; \ I \supsetneqq I_0\}$, escolha I_2 para $\mathscr{S}_2 = \{I \in \mathscr{S}; \ I \supsetneqq I_1\}$, e assim por diante.

Ou seja, temos:

$$I_0 \in \mathscr{S} \text{ e } \mathscr{S}_1 = \{I \in S; \ I \supsetneqq I_0\} \subset \mathscr{S}.$$
$$I_1 \in \mathscr{S}_1 \text{ e } \mathscr{S}_2 = \{I \in S; \ I \supsetneqq I_1\} \subset \mathscr{S}$$
$$I_2 \in \mathscr{S}_2 \text{ e } \mathscr{S}_3 = \{I \in S; \ I \supsetneqq I_2\} \subset \mathscr{S}.$$
$$\vdots$$
$$I_{n-2} \in \mathscr{S}_{n-2} \text{ e } \mathscr{S}_{n-1} = \{I \in S; \ I \supsetneqq I_{n-2}\} \subset \mathscr{S}.$$
$$I_{n-1} \in \mathscr{S}_{n-1} \text{ e } \mathscr{S}_n = \{I \in S; \ I \supsetneqq I_{n-1}\} \subset \mathscr{S}.$$

Consequentemente, pela definição de cada $\mathscr{S}_j$, tem-se a seguinte cadeia de ideais:

$$\cdots \supsetneqq I_j \supsetneqq \cdots \supsetneqq I_{n-1} \supsetneqq I_{n-2} \supsetneqq \cdots \supsetneqq I_2 \supsetneqq I_1 \supsetneqq I_0.$$

Com isso, para mostrar que $\mathscr{S}$ tem um elemento maximal é suficiente mostrar que algum $\mathscr{S}_n$ é vazio, já que se existir $n \in \mathbb{N}$ com $\mathscr{S}_n = \emptyset$, então

$$I_{n-1} \subsetneqq I, \ \forall I \in \mathscr{S}.$$

Desta forma,

$$I_m = I_{n-1} \supsetneqq I_{n-2} \supsetneqq \cdots \supsetneqq I_2 \supsetneqq I_1 \supsetneqq I_0, \ \forall m \geq n.$$

E, portanto, $\mathscr{S}$ tem um elemento maximal, a saber I_{n-1}.

Suponha, por absurdo, que $\mathscr{S}_n \neq \emptyset, \ \forall n \in \mathbb{N}$, e defina $J := \bigcup_{n\in\mathbb{N}} I_n$. Veja que J é um ideal de R, pois cada I_n é um ideal e $I_j \subset I_{j+1}, \ \forall j \in \mathbb{N}$. Como R é noetheriano e J é ideal de R, então J é finitamente gerado, ou seja, existem $F_1, \cdots, F_k \in J$ que geram J, cada $F_i \in I_i$, para algum $i \in \mathbb{N}$, mas pela definição desses ideais, via construção anterior, podemos escolher n_0 suficientemente grande tal que $I_i \subsetneqq I_{n_0}, \ \forall i \in \{1, \cdots, k\}$, ou seja, $F_i \in I_{n_0}, \ \forall i \in \{1, \cdots, k\}$.

Assim, temos que

$$J = \langle F_1, \cdots, F_k \rangle \subset I_{n_0} \subset J = \bigcup_{n\in\mathbb{N}} I_n \Rightarrow J = I_{n_0}.$$

Logo, como $\bigcup_{n\in\mathbb{N}} I_n = J = I_{n_0}$ segue que $I_m = I_{n_0}, \forall m \geq n_0$. Então,

$$I_m = I_{n_0} \supsetneqq I_{n_0-1} \supsetneqq \cdots \supsetneqq I_0.$$

Consequentemente, $I_{n_0} \in \mathscr{S}_{n_0}$, entretanto $\mathscr{S}_{n_0+1} = \{I \in \mathscr{S}; \ I \supsetneqq I_{n_0}\} = \emptyset$, o que é uma contradição, pois supomos que $\mathscr{S}_n \neq \emptyset$, para qualquer $n \in \mathbb{N}$.

Portanto, pela argumentação cima, $\mathscr{S}_n \neq \emptyset, \ \forall n \in \mathbb{N}$, não ocorre, ou seja, existe $n \in \mathbb{N}$ tal que $\mathscr{S}_n = \emptyset$ e segue o resultado. □

[1] O Axioma da Escolha nos diz que dado um conjunto S cujos elementos são conjuntos não vazios. Uma função ψ de domínio D, tal que $\psi(d) \in D, \ \forall d \in D$, é denominada função de escolha. Para todo conjunto D de conjuntos não vazios, existe uma função escolha.

Corolário 3.44. *Qualquer coleção de conjuntos algébricos em $A^n(k)$ tem um membro mínimo.*

Demonstração. Pois se $\{V_\alpha\}_\alpha$ é uma coleção de conjuntos algébricos em $A^n(k)$, segue do teorema anterior que a coleção $\{I(V_\alpha)\}$ de ideais do anel noetheriano $k[X_1, \cdots, X_n]$ tem um membro maximal, digamos $I(V_{\alpha_0})$. Desta forma, segue da Proposição 3.21 que $V(I(V_{\alpha_0})) \supset V_{\alpha_0}$, logo, V_{α_0} é o membro mínimo da coleção $\{V_\alpha\}_\alpha$. □

Teorema 3.45. *Se V um conjunto algébrico em $A^n(k)$, então existem únicos conjuntos algébricos irredutíveis $V_1, \cdots, V_m$ tais que $V = V_1 \cup \cdots \cup V_m$ e $V_i \not\subset V_j$, para todo $i \neq j$.*

Chamamos cada V_i de ***componente irredutível*** *de V e $V = V_1 \cup \cdots \cup V_m$ é a decomposição de V em componentes irredutíveis.*

Demonstração. Seja

$$\mathscr{S} = \{V \subset A^n(k);\ V \text{ não é uma união finita de conjuntos algébricos irredutíveis}\}.$$

Veja que se mostramos que $\mathscr{S}$ é vazio, segue o resultado de modo natural.

Suponha que $\mathscr{S}$ não seja vazio, desta forma, pelo corolário anterior, existe um membro mínimo de $\mathscr{S}$, digamos V.

Pela definição de $\mathscr{S}$ e do fato que $V \in \mathscr{S}$, segue que V não é irredutível, logo $V = V_1 \cup V_2$, $V_i \subsetneqq V$, $i = 1, 2$, pela minimalidade de V, temos que necessariamente $V_i \notin \mathscr{S}$, ou seja, V_i é uma reunião finita de conjuntos algébricos irredutíveis: $V_i = V_{i_1} \cup \cdots \cup V_{i_{m_i}}$, V_{i_j} irredutível. Então $V = V_1 \cup V_2 = \bigcup_{j=1}^{m_1} V_{1_j} \cup \bigcup_{j=1}^{m_2} V_{2_j}$, com cada V_{i_j} irredutível, o que implica que $V \notin \mathscr{S}$, o que é uma contradição.

Portanto, $\mathscr{S}$ é vazio e então qualquer conjunto algébrico V pode ser escrito como $V = V_1 \cup \cdots \cup V_m$, V_i irredutível, $i = 1, \cdots, m$.

Para garantir que $V_i \not\subset V_j$, para $i \neq j$, basta descartar da reunião aqueles V_l tais que $V_l \subset V_k$ para $l \neq k$, já que estes são supérfluos.

Agora, analisemos a unicidade, para tanto seja $V = W_1 \cup \cdots \cup W_m$ outra decomposição de V em conjuntos algébricos irredutíveis tais que $W_i \not\subset W_j$, para $i \neq j$. Consequentemente,

$$V_1 \cup \cdots \cup V_m = V = W_1 \cup \cdots \cup W_m. \tag{3.2}$$

Veja que cada $V_i \subset V_1 \cup \cdots \cup V_m$ e então pela Equação 3.2, $V_i \subset W_1 \cup \cdots \cup W_m$. Logo $V_i \subset W_{j(i)}$, para algum $W_{j(i)}$, $j(i) \in \{1, \cdots, m\}$.

Por outro lado, $W_{j(i)} \subset W_1 \cup \cdots \cup W_m$ e então pela Equação 3.2, $W_{j(i)} \subset V_1 \cup \cdots \cup V_m$. Desta forma, $W_{j(i)} \subset V_k$, para algum $k \in \{1, \cdots, m\}$.

Portanto,

$$V_i \subset W_{j(i)} \subset V_k.$$

Mas, pelo que já foi previamente provado, $V_i \subset V_k$ implica que $i = k$, então $V_i \subset W_{j(i)} \subset V_i$, ou seja, $V_i = W_{j(i)}$. Da mesma forma, cada W_j é igual a algum $V_{i(j)}$. □

3.5 Subconjuntos Algébricos do Plano

Antes de desenvolvermos ainda mais a teoria, exploraremos particularidades intrínsecas ao plano afim $A^2(k)$ e determinaremos, com exatidão, todos os seus subconjuntos algébricos, o que, como vimos, pelo Teorema 3.45, basta analisar quais são os conjuntos algébricos irredutíveis de $A^2(k)$.

Proposição 3.46. *Se F e G são polinômios em $k[X,Y]$ sem fatores comuns, então $V(F,G)$ é um conjunto finito de pontos.*

Relembremos que $V(F,G) = V(F) \cap V(G)$, pela Observação 3.6.

Demonstração. Se F e G são polinômios, sem fatores comuns, em $k[X,Y]$, então F e G também não tem fatores comuns em $k(X)[Y]$, em que $k(X)$ é o corpo de frações de $k[X]$. Este fato segue do Teorema 2.117 e, consequentemente, o máximo divisor comum entre F e G é 1, isto é, $(F,G) = 1$ em $k(X)[Y]$.

Como $k(X)$ é corpo, $k(X)[Y]$ é PID e com isso, segue da Identidade de Bezout[2], que existem $R, S \in k(X)[Y]$ tais que $RF + SG = 1$.

Digamos que

$$R = a_n Y^n + \cdots + a_1 Y + a_0 \in k(X)[Y],$$

onde cada $a_i = \dfrac{f_i(X)}{g_i(X)} \in k(X)$, tal que $g_i \neq 0$, onde $f_i, g_i \in k[X]$. Assim,

$$R = \frac{f_n(X)}{g_n(X)} Y^n + \cdots + \frac{f_1(X)}{g_1(X)} Y + \frac{f_0(X)}{g_0(X)}.$$

Além disso, considere

$$S = b_m Y^m + \cdots + b_1 Y + b_0 \in k(X)[Y],$$

em que cada $b_i = \dfrac{h_i(X)}{j_i(X)} \in k(X)$, tal que $j_i \neq 0$, onde $h_i, j_i \in k[X]$, ou seja,

$$S = \frac{h_m(X)}{j_m(X)} Y^m + \cdots + \frac{h_1(X)}{j_1(X)} Y + \frac{h_0(X)}{j_0(X)}.$$

Com isso, defina $D \in k[X]$ por:

$$D = g_n(X) \cdot \cdots \cdot g_0(X) \cdot j_m(X) \cdot \cdots \cdot j_0(X).$$

Observe que quando fazemos DR temos:

$$DR = D\frac{f_n(X)}{g_n(X)} Y^n + \cdots + D\frac{f_1(X)}{g_1(X)} Y + D\frac{f_0(X)}{g_0(X)} = \hat{D}_n f_n(X) Y^n + \cdots + \hat{D}_1 f_1(X) Y + \hat{D}_0 f_0(X),$$

em que $\hat{D}_i = g_n(X) \cdot \cdots \cdot g_{i-1}(X) \cdot g_{i+1}(X) \cdot \cdots \cdot g_0(X) \cdot j_m(X) \cdot \cdots \cdot j_0(X) \in k[X]$, ou seja, $\hat{D}_i$ é o produto D sem o fator $g_i(X)$.

Chamaremos $DR = A \in k[X][Y]$ em que $A = \hat{D}_n f_n(X) Y^n + \cdots + \hat{D}_1 F_1(X) Y + \hat{D}_0 f_0(X) \in k[X][Y]$, que por sua vez é isomorfo a $k[X,Y]$. Assim, $A \in k[X,Y]$.

De forma análoga, teremos $DS = B \in k[X,Y]$, em que

$$B = \tilde{D_m} h_m(X) Y^n + \cdots + \tilde{D}_1 h_1(X) Y + \tilde{D}_0 h_0(X),$$

onde $\tilde{D}_i = g_n(X) \cdot \cdots \cdot g_0(X) \cdot j_m(X) \cdot \cdots \cdot j_{i-1}(X) \cdot j_{i+1}(X) \cdot \cdots \cdot j_0(X) \in k[X]$, e $\tilde{D}_i$ é o produto D sem o fator $j_i(X)$.

[2] A Identidade de Bezout nos diz que: *"Dois elementos quaisquer, a e b, de um anel principal R são primos entre si se, e somente se, existem elementos $x_0, y_0 \in R$ tais que $ax_0 + by_0 = 1$"*. Vide [2], p. 332.

Note que

$$AF + BG = (DR)F + (DS)G = D(RF + SG) = D \cdot 1 = D.$$

Se $(a, b) \in V(F, G)$, então $F(a, b) = 0$ e $G(a, b) = 0$. Assim,

$$D(a) = (AF + BG)(a) = A(a, b) \cdot F(a, b) + B(a, b) \cdot G(a, b) = A(a, b) \cdot 0 + B(a, b) \cdot 0 = 0.$$

Com isso, teremos $D(a) = 0$. Mas D tem apenas um número finito de zeros, pela Definição 2.119. Com isso, temos que irá aparecer apenas um número finito de coordenadas X nos pontos de $V(F, G)$, isto é, a quantidade de a será limitado pela quantidade de raízes que D possuir, então se D tiver r raízes, existirá r coordenadas abscissas nos pontos de $V(F, G)$. Assim, há apenas um número finito de X-coordenadas entre os pontos de $V(F, G)$.

Fazendo o mesmo processo para obter o D e suas consequências, podemos fazer o mesmo para obter um polinômio $D' \in k[Y]$ e, portanto, haverá um número finito de coordenadas ordenadas, digamos t.

Desta forma, há apenas um número finito de pontos em $V(F, G)$, a saber $r \cdot t$. □

Observação 3.47. Se F, G são polinômios em $k[X, Y]$ tais que $V(F, G)$ é um conjunto infinito, então F divide G ou G divide F.

Corolário 3.48. *Se F é um polinômio irredutível em $k[X, Y]$ tal que $V(F)$ é infinito, então $I(V(F)) = \langle F \rangle$ e $V(F)$ é irredutível.*

Demonstração. $V(F)$ ser infinito significa que existem infinitos pontos $P \in A^2(k)$ tal que $V(F) = \{P \in A^2(k);\ F(P) = 0\}$. Por outro lado, $G \in I(V(F))$ significa que $G(P) = 0,\ \forall P \in V(F)$.

Logo, $P \in V(G) \cap V(F) = V(F, G)$. Deste modo, $V(F, G)$ é infinito, já que há um número infinito de P.

Desta forma, pela observação anterior, F divide G, isto é, $G \in \langle F \rangle$. Logo, $I(V(F)) \subset \langle F \rangle$. Reciprocamente, temos que $\langle F \rangle \subset I(V(F))$, pois se $H \in \langle F \rangle$, então $H = LF,\ L \in k[X]$. Assim, para todo $P \in V(F)$, isto é $F(P) = 0$, temos:

$$H(P) = (LF)(P) = L(P) \cdot F(P) = L(P) \cdot 0 = 0,$$

ou seja, $H \in I(V(F))$.

Além disso, como F é irredutível, segue que $\langle F \rangle$ é maximal[3]. Sabemos que todo ideal maximal é primo, logo $\langle F \rangle$ é primo. Temos ainda que $\langle F \rangle = I(V(F))$, que acabamos de provar. Disto temos que $I(V(F))$ é primo e, pela Proposição 3.42, $V(F)$ é irredutível. □

Corolário 3.49. *Se k é infinito, então os subconjuntos algébricos irredutíveis de $A^2(k)$ são: $A^2(k), \emptyset$, conjunto unitário de pontos em $A^2(k)$ e curvas planas irredutíveis $V(F)$, onde F é um polinômio irredutível e $V(F)$ é infinito.*

Demonstração. Observe que $A^2(k), \emptyset$ e o conjunto unitário de pontos em $A^2(k)$ são todos os conjuntos algébricos irredutíveis em $A^2(k)$, já que $A^2(k) = V(0),\ \emptyset = V(H)$, tal que $H \neq 0$ e H é polinômio constante, e $\{P\} = V(F)$, onde $F = X - P$. Além disso, qualquer conjunto finito em $A^2(k)$, com pelo menos dois pontos, é redutível. Consequentemente, se V é um conjunto algébrico irredutível em $A^2(k)$, tal que $V \neq A^2(k)$ e $V \neq \emptyset$ e

[3]Vide [1], p. 251, Teorema 27.25.

$V \neq \{P\}$, $P \in A^2(k)$, então V é necessariamente um conjunto infinito. Mostremos, a seguir, que neste caso V é uma curva plana irredutível.

Desta forma, $I(V)$ contém algum polinômio $F \in k[X,Y]$ não constante. Por outro lado, pela Proposição 3.42, como V é irredutível, então $I(V)$ é primo. Assim, alguns fatores irredutíveis de F necessariamente pertence a $I(V)$, consequentemente, podemos assumir, sem perda de generalidade, que F é um polinômio irredutível.

Veja que, com isso, $\langle F\rangle \subset I(V)$. Afirmamos ainda que $I(V) \subset \langle F\rangle$, pois supondo por absurdo que $I(V) \not\subset \langle F\rangle$, ou seja, que existe $G \in I(V)$ tal que $G \notin \langle F\rangle$, então $V \subset V(F,G)$ em que $V(F,G)$ é finito pela Proposição 3.46, uma vez que F, G não tem fatores em comum, já que $G \notin \langle F\rangle$. Portanto V é finito, o que é absurdo, já que V é infinito por hipótese. Logo, $I(V) = \langle F\rangle$. Temos ainda, pela Proposição 3.22, que $V = V(I(V))$, porém $I(V) = \langle F\rangle$, logo $V = V(F)$, em que F é um polinômio irredutível não nulo, logo V é uma curva plana irredutível. □

Corolário 3.50. *Suponha k algebricamente fechado, $F \in k[X,Y]$. Se $F = F_1^{n_1}\cdots F_r^{n_r}$ seja a decomposição de F em fatores irredutíveis. Então $V(F) = V(F_1)\cup\cdots\cup V(F_r)$ é a decomposição de $V(F)$ em componentes irredutíveis e $I(V(F)) = \langle F_1 \cdot \cdots \cdot F_r\rangle$.*

Demonstração. Observe que, através do item (a) da Proposição 3.11 e da Indução Finita, temos que $V(F) = V(F_1^{n_1} \cdot \cdots \cdot F_r^{n_r}) = V(F_1)\cup\cdots\cup V(F_r)$.

Como nenhum F_i divide qualquer F_j, $j \neq i$, então não há nenhuma relação de inclusão entre os $V(F_i)$, $1 \leq i \leq r$. Portanto, a decomposição acima é a desejada.

Observe que:

$$I(V(F)) = I(V(F_1)\cup\cdots\cup V(F_r)) = \bigcup_{i=1}^{r} V(F_i).$$

Veja que $I(V(F)) = \bigcap_{i=1}^{r} I(V(F_i))$, pois:

(i) $I(V(F)) \subset \bigcap_{i=1}^{r} I(V(F_i))$:

Veja que $V(F_i) \subset \bigcup_{i=1}^{r} V(F_i)$, para todo $i \in \{1,\cdots,r\}$. Pela Proposição 3.18, se isso ocorre, então $I(\bigcup_{i=1}^{r} V(F_i)) \subset I(V(F_i)), \forall i \in \{1,\cdots,r\}$.

Mas, se $I(\bigcup_{i=1}^{r} V(F_i)) \subset I(V(F_i)), \forall i \in \{1,\cdots,r\}$, então $I(\bigcup_{i=1}^{r} V(F_i)) \subset \bigcap_{i=1}^{r} I(V(F_i))$.

Isto é, $I(V(F)) \subset \bigcap_{i=1}^{r} I(V(F_i))$, como queríamos.

(ii) $\bigcap_{i=1}^{r} I(V(F_i)) \subset I(V(F))$:

Veja que se $f \in \bigcap_{i=1}^{r} I(V(F_i))$, então $f \in I(V(F_i))$, $\forall i \in \{i,\cdots,r\}$. Deste modo, $f(P) = 0, \forall P \in V(F_i), \forall i \in \{1,\cdots,r\}$. Mas $V(F_i) \subset \bigcup_{i=1}^{r} V(F_i)$, desta forma temos que $f \in I(\bigcup_{i=1}^{r} V(F_i)) = I(V(F))$.

Ainda, $\bigcap_{i=1}^{r} I(V(F_i)) = \bigcap_{i=1}^{r} \langle F_i \rangle$ pelo Corolário 3.48. Além disso, $\bigcap_{i=1}^{r} \langle F_i \rangle = \langle F_1 \cdot \cdots \cdot F_r \rangle$, pois:

(I) $\langle F_1 \cdot \cdots \cdot F_r \rangle \subset \bigcap_{i=1}^{r} \langle F_i \rangle$:

Se $H \in \langle F_1 \cdot \cdots \cdot F_r \rangle$, então $H = L(F_1 \cdot \cdots \cdot F_r)$.

Desta forma, $H = L_1F_1 = L_2F_2 = \cdots = L_rF_r$, ou seja, $H \in \bigcap_{i=1}^{r} \langle F_i \rangle$.

(II) $\bigcap_{i=1}^{r} \langle F_i \rangle \subset \langle F_1 \cdot \cdots \cdot F_r \rangle$:

Se $H \in \bigcap_{i=1}^{r} \langle F_i \rangle$, então $H \in \langle F_i \rangle,\ \forall i \in \{1, \cdots, r\}$.

Assim, podemos escrever H das seguintes formas:
$H = L_1F_1$
$H = L_2F_2$
$\vdots$
$H = L_rF_r$,

ou seja, $H = L_1F_1 = L_2F_2 = \cdots = L_rF_r$.

Lembremos agora que F_i é irredutível, $\forall i \in \{1, \cdots, r\}$, então F_i não divide F_j, $i \neq j$. Assim, se $H = L_1F_1 = L_2F_2$, então obrigatoriamente $H = (G_1F_2)F_1$. Mas temos ainda que $H = L_3F_3$, logo $H = (G_1F_2)F_1 = L_3F_3$ e isso só é possível se $H = (G_2F_3)(G_1F_2)F_1 = (G_1G_2)F_3F_2F_1$.

Se fizermos esse processo sucessivamente, então teremos $H = (G_{r-1} \cdot \cdots \cdot G_1)F_r \cdot \cdots \cdot F_1$. Assim sendo, podemos dizer que $H = G_0F_r \cdot \cdots \cdot F_1$ e, desta forma, $H \in \langle F_r \cdot \cdots \cdot F_1 \rangle$.

Assim, temos que $I(V(F)) = \langle F_r \cdot \cdots \cdot F_1 \rangle$.
Note que $V(F_i)$ é infinito[4] já que k é algebricamente fechado. □

3.6 Teorema dos Zeros de Hilbert (Hilbert's Nullstellensatz)

Se nos é dado um conjunto algébrico V, a Proposição 3.42 nos dá critérios para afirmar se V é irredutível ou não. O que nos falta é um modo de descrever V em termos de um dado conjunto de polinômios que define V. É o Teorema Hilbert's Nullstellensatz, ou Teorema de Zeros de Hilbert, que nos diz a exata relação entre ideais e conjuntos algébricos. Iniciamos esse problema com um teorema mais fraco e mostramos como reduzi-lo para um fato puramente algébrico. No restante dessa seção mostraremos como deduzir o resultado principal de tal teorema mais fraco, e dar algumas aplicações.

Durante toda essa seção, assumiremos que k é algebricamente fechado.

Teorema 3.51 (Weaker Nullstellensatz)**.** *Se I é um ideal próprio em $k[X_1, \cdots, X_n]$, então $V(I) \neq \emptyset$.*

[4]Vide [4], p. 5, resultado 1.14.

Demonstração. Veja que, como k é corpo, segue da Proposição 3.34 e do Teorema 3.35, que $k[X_1, \cdots, X_n]$ é um anel noetheriano.

Seja I um ideal próprio qualquer do anel noetheriano $k[X_1, \cdots, X_n]$. Segue da Proposição 3.43 que, nessas condições, existe J ideal maximal, de $k[X_1, \cdots, X_n]$, tal que $I \subset J$ e, pela Proposição 3.10, temos que $V(J) \subset V(I)$. Assim, para mostrar que $V(I) \neq \emptyset$, basta mostrar que $V(J) \neq \emptyset$.

Veja que, como J é maximal, temos que $L = \dfrac{k[X_1, \cdots, X_n]}{J}$ é um corpo e k pode ser visto como um subcorpo de L. Além disso, k é algebricamente fechado e a aplicação

$$\begin{array}{rccc} \phi: & k[X_1, \cdots, X_n] & \longrightarrow & \dfrac{k[X_1, \cdots, X_n]}{J} \\ & P(X) & \longmapsto & \phi(P(X)) = P(X) + J \end{array}$$

é um epimorfismo, então:

$$L = \frac{k[X_1, \cdots, X_n]}{J} = k.^{5}$$

Assim, para cada $i \in \{1, \cdots, n\}$, $X_i \in k[X_1, \cdots, X_n]$ e então $\phi(X_i) \in Im(\phi) = L = k$. Logo, existe $a_i \in k$ tal que $a_i = \phi(X_i)$, mas $\phi(X_i) = X_i + J = a_i$, consequentemente $X_i + J = a_i$. Disto segue que $X_i - a_i \in J$, $\forall i \in \{1, \cdots, n\}$. Logo:

$$\langle X_1 - a_1, \cdots, X_n - a_n \rangle \subset J.$$

Mas $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$ é um ideal maximal de $k[X_1, \cdots, X_n]$. Isso se dá, pois $\dfrac{k[X_1, \cdots, X_n]}{\langle X_1 - a_1, \cdots, X_n - a_n \rangle}$ é isomorfo a k e k é corpo, consequentemente,

$$J = \langle X_1 - a_1, \cdots, X_n - a_n \rangle.$$

Com isso

$$V(J) = V(X_1 - a_1, \cdots, X_n - a_n) = \{a_1, \cdots, a_n\} \neq \emptyset.$$

Desta forma, $V(J) \neq \emptyset$ e, por consequência, $V(I) \neq \emptyset$. □

Teorema 3.52 (Hilbert's Nullstellensatz)**.** *Se I um ideal em $k[X_1, \cdots, X_n]$, onde k é algebricamente fechado, então $I(V(I)) = Rad(I)$.*

Observação 3.53. Em outros termos, esse teorema diz:

"Se $F_1, \cdots, F_r$, $G \in k[X_1, \cdots, X_n]$ e G desaparece sempre que $F_1, \cdots, F_r$ desaparece, então existe uma equação $G^N = A_1F_1 + \cdots + A_rF_r$, para algum $N > 0$ e algum $A_i \in k[X_1, \cdots, X_n]$."

Demonstração. Veja que, como I é um ideal no anel noetheriano $k[X_1, \cdots, X_n]$, segue da Definição 3.31 que I é finitamente gerado. Assim, existem $F_1, \cdots, F_r \in k[X_1, \cdots, X_n]$ tais que $I = \langle F_1, \cdots, F_r \rangle$.

Mostremos então que a igualdade $I(V(I)) = Rad(I)$ é válida.

[5] Se um corpo k algebricamente fechado é um subcorpo de um corpo L e existe um homomorfismo de anel de $k[X_1, \cdots, X_n]$ em L (que é a unidade em k), então $k = L$. Tal resultado está demonstrado no Corolário 3.85, ao final deste capítulo.

(i) $Rad(I) \subset I(V(I))$.

Seja $G \in Rad(I)$, qualquer. Logo, dela definição de $Rad(I)$, existe $N \in \mathbb{Z}_+^*$ tal que $G^N \in I = \langle F_1, \cdots, F_r \rangle$. Assim, existem $A_1, \cdots, A_r \in k[X_1, \cdots, X_n]$, tal que

$$G^N = A_1F_1 + \cdots + A_rF_r.$$

Deste modo, tomemos $P \in V(I) = V(F_1, \cdots, F_r)$, consequentemente, $F_i(P) = 0$, para todo $i \in \{1, \cdots, r\}$. Com isso, $G^N(P) = A_1(P)F_1(P) + \cdots + A_r(P)F_r(P) = 0$, desta forma, $G(P) = 0$, já que k é corpo e todo corpo é domínio de integridade.

Portanto, $G(P) = 0, \forall P \in V(I)$, assim, $G \in I(V(I))$.

(ii) $I(V(I)) \subset Rad(I)$.

Seja $G \in I(V(I)) = I(V(F_1, \cdots, F_r))$, $F_i \in k[X_1, \cdots, X_n]$.

Assim, temos que $G(P) = 0,\ \forall P \in V(F_1, \cdots, F_r)$.

Além disso, como $P \in V(F_1, \cdots, F_r)$, então $F_i(P) = 0,\ \forall i \in \{1, \cdots, r\}$.

Seja $J = \langle F_1, \cdots, F_r, X_{n+1}G - 1 \rangle \subset k[X_1, \cdots, X_n, X_{n+1}]$. Observe que $V(J) = \emptyset$ em $A^{n+1}(k)$, pois se $Q \in V(J)$, temos que $F_i(Q) = 0,\ \forall i \in \{1, \cdots, r\}$, assim como $G \in I(V(F_1, \cdots F_r))$, segue que $G(Q) = 0$, daí:

$$(X_{n+1}G - 1)(Q) = q_{n+1}G(Q) - 1 = -1.$$

E isso é um absurdo, pois se $Q \in V(J)$, então teríamos que $F_i(Q) = 0,\ \forall i \in \{1, \cdots, r\}$ e $(X_{n+1}G - 1)(Q) = 0$. Assim, isso só é possível se $V(J) = \emptyset$.

Pela contra positiva do Teorema 3.51, temos que se $V(J) = \emptyset$, então J não é um ideal próprio, ou seja, $J = \{0\}$ ou $J = k[X_1, \cdots, X_{n+1}]$. Porém, $J \neq \{0\}$, pois $F_i \in J$ e $F_i \neq 0$, assim $J = k[X_1, \cdots, X_{n+1}]$. Veja que $1 \in k \subset k[X_1, \cdots, X_{n+1}]$ e assim, $1 \in J$, mas $J = \langle F_1, \cdots, F_r, X_{n+1}G - 1 \rangle$. Deste modo:

$$1 = \sum A_i(X_i, \cdots, X_{n+1})F_i + B(X_1, \cdots, X_{n+1}) \cdot (X_{n+1}G - 1).$$

Tomando $Y = \dfrac{1}{X_{n+1}} \in k$ e multiplicando a equação acima por uma potência de Y, de modo que essa potência seja suficientemente grande para podermos substituir X_{n+1} por Y, ou seja, N é maior do que a maior potência de X_{n+1} na equação anterior. Assim:

$$Y^N = \sum C_i(X_1, \cdots, X_n, Y)F_i + D(X_1, \cdots, X_n, Y)(G - Y) \in k[X_1, \cdots, X_n].$$

Substituindo G por Y teremos a equação desejada, isto é:

$$G^N = \sum C_i(X_1, \cdots, X_n, Y)F_i + D(X_1, \cdots, X_n, Y)(G - G).$$

Deste modo:

$$G^N = \sum C_i(X_1, \cdots, X_n, Y)F_i \in \langle F_1, \cdots, F_r \rangle = I.$$

Assim, como $G^N \in I$, temos que $G \in Rad(I)$.

□

Corolário 3.54. *Se I é um ideal radical em $k[X_1, \cdots, X_n]$, então $I(V(I)) = I$. Logo, existe uma correspondência biunívoca entre ideais radicais e conjuntos algébricos.*

Demonstração. Como I é ideal radical, temos que $Rad(I) = I$. Pelo Hilbert's Nullstellensatz (Teorema 3.52), temos que $I(V(I)) = Rad(I)$. Assim, $I(V(I)) = I$. □

Corolário 3.55. *Se I é um ideal primo, então $V(I)$ é irredutível, ou seja, existe uma correspondência biunívoca entre ideais primos e conjuntos algébricos irredutíveis. Além disso, o ideal maximal corresponde a pontos.*

Demonstração. Veja que se I é primo, então I é radical, pela Proposição 3.30, ou seja, $Rad(I) = I$. Pelo Hilbert's Nullstellensatz (Teorema 3.52), temos que $Rad(I) = I(V(I))$. Assim, $I = I(V(I))$. Logo, temos que $I(V(I))$ é ideal primo. Pela Proposição 3.42, temos que $V(I)$ é irredutível.

Veja que se I é um ideal e M é um ideal maximal, então $I \subset M$ e, pela Proposição 3.10, temos que $V(M) \subset V(I)$. Assim, $V(M)$ é o menor conjunto algébrico possível, sendo este os conjuntos de pontos unitários, isto é $V(M) = \{P\}$. □

Corolário 3.56. *Seja $F \in k[X_1, \cdots, X_n]$. Se $F = F_1^{n_1} \cdot \cdots \cdot F_r^{n_r}$ é a decomposição de F em fatores irredutíveis, então $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ é a decomposição de $V(F)$ em componentes irredutíveis e $I(V(F)) = \langle F_1 \cdot \cdots \cdot F_r \rangle$, isso é, há uma correspondência biunívoca entre polinômios irredutíveis $F \in k[X_1, \cdots, X_n]$ (a menos da multiplicação por elementos não nulos de k) e hipersuperfícies irredutíveis em $A^n(k)$.*

Demonstração. A demonstração desse corolário segue do Corolário 3.50.

Mostremos agora a correspondência biunívoca: veja que, se F é irredutível, então teremos que $V(F)$ é irredutível, isto é, uma hipersuperfície irredutível. Isso pode ser observado pela decomposição de $V(F)$ considerando F irredutível.

Por outro lado, se $V(F)$ é uma hipersuperfície irredutível, então I(V(F)) é primo, pela Proposição 3.42. E se $I(V(F))$ é primo, então ele também é radical, pela Proposição 3.30. Desta forma, pelo Hilbert's Nullstellensatz (Teorema 3.52), temos que $I(V(F)) = \langle F \rangle$, ou seja, para cada superfície irredutível teremos um polinômio irredutível associada a ela. □

Proposição 3.57. *Seja V um conjunto algébrico em $A^n(k)$.*

(i) Se $P \in A^n(k)$ é um ponto tal que $P \notin V$, então existe um polinômio F em $k[X_1, \cdots, X_n]$ tal que $F(Q) = 0$, para todo $Q \in V$, e $F(P) = 1$, para $P \notin V$.

(ii) Se $P_1, \cdots, P_r \in A^n(k)$ pontos distintos, tais que $P_i \notin V, \forall i \in \{1, \cdots, r\}$, então existem polinômios $F_1, \cdots, F_r \in I(V)$ tal que $F_i(P_j) = 0$, para $i \neq j$, e $F_i(P_i) = 1$, para $i = j$.

Demonstração. Mostremos os dois itens da Proposição.

(i) Sejam $V \in A^n(k)$ um conjunto algébrico e $P \in A^n(k)$ tal que $P \notin V$.

Como V é um conjunto algébrico, então existe $I \in k[X_1, \cdots, X_n]$ tal que $I = I(V)$. Tome $G \in I(V)$ qualquer. Note que para cada $G \in I(V)$ temos:

$$G(Q) = 0, \forall Q \in V.$$

Escolha $G \in I(V)$ tal que $G \notin I(V \cup \{P\})$, ou seja, $G(Q) = 0, \forall Q \in V$, mas $G(P) \neq 0$.

Agora, defina $F(X)$ por

$$F(X) = \frac{1}{G(P)} \cdot G(X), \text{ em que } X = (X_1, \cdots, X_n).$$

Veja que

$$F(Q) = \frac{1}{G(P)} \cdot G(Q) = \frac{1}{G(P)} \cdot 0 = 0$$

e

$$F(P) = \frac{1}{G(P)} \cdot G(P) = 1.$$

(ii) Sejam $V \in A^n(k)$ um conjunto algébrico e $P_1, \cdots, P_r \in A^n(k)$ tais que $P_i \notin V, \forall i \in \{1, \cdots, r\}$.

Escolha G_1 tal que $G_1 \in I(V \cup \{P_2, \cdots, P_r\})$, mas $G_1 \notin I(V \cup \{P_1, \cdots, P_r\})$, ou seja, $G_1(P_1) \neq 0, \forall P_i \notin V$. Agora, defina

$$F_1(X) = \frac{1}{G_1(P_1)} \cdot G_1(X), \text{onde } X = (X_1, \cdots, X_n).$$

Veja que, pelo item (i),

$$F_1(P_2) = \frac{1}{G_1(P_1)} \cdot G_1(P_2) = 0$$

$$\vdots$$

$$F_1(P_n) = \frac{1}{G_1(P_1)} \cdot G_1(P_n) = 0$$

e

$$F_1(P_1) = \frac{1}{G_1(P_1)} \cdot G_1(P_1) = 1.$$

Agora, escolha G_2 tal que $G_2 \in I(V \cup \{P_1, P_3, \cdots, P_r\})$ tal que $G_2 \notin I(V \cup \{P_1, P_2, P_3, \cdots, P_r\})$, ou seja, $G_2(P_2) \neq 0$, e defina

$$F_2(X) = \frac{1}{G_2(P_2)} \cdot G_2(X), \text{onde } X = (X_1, \cdots, X_n).$$

Note que, mais uma vez,

$$F_2(P_1) = \frac{1}{G_2(P_2)} \cdot G_2(P_1) = 0$$

$$F_2(P_3) = \frac{1}{G_2(P_2)} \cdot G_2(P_3) = 0$$

$$\vdots$$

$$F_2(P_n) = \frac{1}{G_2(P_2)} \cdot G_2(P_n) = 0$$

e

$$F_2(P_2) = \frac{1}{G_2(P_2)} \cdot G_2(P_2) = 1.$$

Fazendo isso de forma análoga, escolha G_r tal que $G_r \in I(V \cup P_1, \cdots, P_{r-1})$ tal que $G_r \notin I(V \cup P_1, \cdots, P_r)$, ou seja, $G_r(P_r) \neq 0$. Defina:

$$F_r(X) = \frac{1}{G_r(P_r)} \cdot G_r(X), \text{onde } X = (X_1, \cdots, X_n).$$

Note que, de forma análoga,

$$F_r(P_1) = \frac{1}{G_r(P_r)} \cdot G_r(P_1) = 0$$

$$\vdots$$

$$F_r(P_{r-1}) = \frac{1}{G_r(P_r)} \cdot G_r(P_{r-1}) = 0$$

e

$$F_r(P_r) = \frac{1}{G_r(P_r)} \cdot G_r(P_r) = 1.$$

□

Corolário 3.58. *Se I é um ideal em $k[X_1, \cdots, X_n]$, então $V(I)$ é um conjunto finito se, e somente se, $\dfrac{k[X_1, \cdots, X_n]}{I}$ é um espaço vetorial de dimensão finita sobre k. Se isso ocorre, o número de pontos em $V(I)$ é menor ou igual a $dim_k \left(\dfrac{k[X_1, \cdots, X_n]}{I} \right)$.*

Demonstração. ($\Rightarrow$) Sejam $V(I) = \{P_1, \cdots, P_r\}$ um conjunto finito, onde cada $P_i = (a_{i1}, \cdots, a_{in})$, e $F_j = \prod_{i=1}^{r} (X_j - a_{ij})$, $j \in \{1, \cdots, n\}$. Observe que:

$$F_1 = (X_1 - a_{11})(X_1 - a_{21}) \cdots (X_1 - a_{r1})$$

$$\vdots$$

$$F_j = (X_j - a_{1j})(X_j - a_{2j}) \cdots (X_j - a_{rj}).$$

$$\vdots$$

$$F_n = (X_n - a_{1n})(X_n - a_{2n}) \cdots (X_n - a_{rn}).$$

Deste modo, $F_j(P_i) = 0$, $\forall P_i \in V(I)$, $i \in \{1, \cdots, r\}$. De fato, calculando $F_1(P_1)$, teremos $F_1(P_1) = (a_{11} - a_{11}) \cdots (a_{1n} - a_{r1}) = 0$, já que é um produto e $a_{11} - a_{11} = 0$. Isso irá se repetir em todos os $F_j(P_i)$, para cada $j \in \{1, \cdots, n\}$ e $P_i \in V(I)$, $i \in \{1, \cdots, r\}$, ou seja, sempre haverá um fator do produto que irá se anular, logo $F_j \in I(V(I))$.

Pelo Hilbert's Nullstellensatz (Teorema 3.52), $I(V(I)) = Rad(I)$, segue que $F_j \in Rad(I)$. Logo, existe $N_j \in Z_+^*$ tal que $F_j^{N_j} \in I$. Tomemos $N = \max\{N_j, 1 \leq j \leq n\}$ e, assim, temos que $F_j^N \in I$, $\forall j \in \{1, \cdots, n\}$.

Veja que, se $F_j^N \in I$, então $\overline{F_j^N} = F_j^N + I = I = 0$, ou seja, $\overline{F_j^N} = 0$, $\forall j \in \{1, \cdots, n\}$, em $\dfrac{k[X_1, \cdots, X_n]}{I}$.

Disto, segue que $\overline{X_j^N}$ é uma combinação linear de $1, \overline{X_j}, \cdots, \overline{X_j^{N-1}}$, com escalares em k, pois:

$$0 = \overline{F_j^N} = \overline{X_j^{rN} + \alpha_{rN-1}X_j^{rN-1} + \cdots + \alpha_1 X_j + 1} = \overline{X_j^{rN}} + \overline{\alpha_{rN-1}X_j^{rN-1}} + \cdots + \overline{\alpha_1 X_j} + 1,$$

que podemos reescrever como:

$$\overline{X_j^{rN}} = -\left(\alpha_{rN-1}\overline{X_j^{rN-1}} + \cdots + \alpha_1\overline{X_j^1} + 1\right).$$

Note que estamos considerando os escalares em k como polinômios constantes em $k[X_1, \cdots, X_n]$. Logo, $\overline{X_j^{rN}}$ é combinação linear dos outros fatores, isto é, $\overline{X_j^{rN}} \in \langle 1, \overline{X_j}, \cdots, \overline{X_j^{rN-1}}\rangle$. Observe que $\langle 1, \overline{X_j}, \cdots, \overline{X_j^{rN-1}}\rangle$ é ideal, já que cada um dos fatores é irredutível.

Disso, segue por indução, que $\overline{X_j^s}$ é uma combinação linear com coeficientes em k de $1, \overline{X_j}, \cdots, \overline{X_n^{N-1}}$, para todo s, já que: $\overline{X_j^{rN+1}} = \overline{X_j^{rN}} \cdot \overline{X_j}$. Mas $\overline{X_j^{rN}} \in \langle 1, \overline{X_j}, \cdots, \overline{X_j^{rN-1}}\rangle$. Logo, $\overline{X_j^{rN}} \cdot \overline{X_j} \in \langle \overline{X_j}, \cdots, \overline{X_j^{rN}}\rangle \subset \langle 1, \overline{X_j}, \cdots, \overline{X_j^{rN-1}}\rangle$.

Mostremos agora que o conjunto $\{\overline{X_1^{m_1}}, \cdots, \overline{X_n^{m_n}};\ m_i < rN\}$ gera o espaço vetorial $\dfrac{k[X_1, \cdots, X_n]}{I}$ sobre k.

Seja $f(X_1, \cdots, X_n) \in k[X_1, \cdots, X_n]$, qualquer. Deste modo, $\overline{f(X_1, \cdots, X_n)} \in \dfrac{k[X_1, \cdots, X_n]}{I}$, logo, $\overline{f(X_1, \cdots, X_n)} \in \langle\{\overline{X^\alpha};\ \alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}\}\rangle$, em que $\overline{X}^\alpha = \overline{X^\alpha}$, no qual $X^\alpha = X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \ \cdots \ \cdot X_n^{\alpha_n}$.

Assim, como todo $\overline{X_j^s} \in \langle \overline{X_1^{m_1}}, \cdots, \overline{X_n^{m_n}};\ m_i < rN\rangle$, então

$$\overline{f(X_1, \cdots, X_n)} \in \langle \overline{X_1^{m_1}}, \cdots, \overline{X_n^{m_n}};\ m_i < rN\rangle.$$

Portanto, $\{\overline{X_1^{m_1}} \cdot \ \cdots \ \cdot \overline{X_n^{m_n}};\ m_i < rN\}$ gera o espaço vetorial $\dfrac{k[X_1, \cdots, X_n]}{I}$ sobre k. Logo, $\dfrac{k[X_1, \cdots, X_n]}{I}$ é um espaço vetorial de dimensão finita.

($\Leftarrow$) Sejam $P_1, \cdots, P_r \in V(I)$, quaisquer. Veja que, pela Proposição 3.57, item (ii), podemos garantir que existem

$$F_1, \cdots, F_r \in k[X_1, \cdots, X_n], \text{ tal que } F_i(P_j) = 0 \text{ se } i \neq j \text{ e } F_i(P_i) = 1. \tag{3.3}$$

Então, tomemos $F_1, \cdots, F_r$ desta forma.

Seja $\overline{F_i}$ a classe residual de F_i, ou seja, $\overline{F_i} = F_i + I \in \dfrac{k[X_1, \cdots, X_n]}{I}$.

Afirmação. O conjunto $\{\overline{F_1}, \cdots, \overline{F_r}\}$ é linearmente independente no k-espaço vetorial finito $\dfrac{k[X_1, \cdots, X_n]}{I}$.

De fato: Suponha que $\lambda_1\overline{F_1} + \cdots + \lambda_r\overline{F_r} = 0$, com $\lambda_i \in k,\ \forall i \in \{1, \cdots, r\}$. Como

$$0 = \lambda_1\overline{F_1} + \cdots + \lambda_r\overline{F_r} = \overline{\lambda_1 F_1 + \cdots + \lambda_r F_r},$$

segue que $\lambda_1 F_1 + \cdots + \lambda_r F_r \in I$.
Como $P_j \in V(I),\ \forall j \in \{1, \cdots, r\}$, e $\lambda_1 F_1 + \cdots + \lambda_r F_r \in I$, segue que

$$\left(\sum_{i=1}^{r} \lambda_i F_i\right)(P_j) = 0.$$

Por outro lado, por (3.3), temos que:

$$\left(\sum_{i=1}^{r} \lambda_i F_i\right)(P_j) = \lambda_1 F_1(P_j) + \lambda_2 F_2(P_j) + \cdots + \lambda_j F_j(P_j) + \cdots \lambda_r F_r(P_j) = \lambda_j.$$

Assim, $\sum_{i=1}^{r} \lambda_i F_i(P_j) = \lambda_j$. Daí, $\lambda_j = 0,\ \forall j \in \{1, \cdots r\}$. Deste modo, temos que $\{F_1, \cdots, F_r\}$ é linearmente independente.

Note que, como $\{\overline{F_1}, \cdots, \overline{F_r}\}$ é linearmente independente, então $\langle\overline{F_1}, \cdots, \overline{F_r}\rangle$ é subespaço vetorial de $\dfrac{k[X_1, \cdots, X_n]}{I}$ de dimensão r. Desta forma temos que

$$r \leq dim_k\left(\frac{k[X_1, \cdots, X_n]}{I}\right).$$

Além disso, como $dim_k\left(\dfrac{k[X_1, \cdots, X_n]}{I}\right)$ é finita, então r também é finito. Logo, $V(I)$ tem dimensão finita.

□

A partir deste momento até o final do capítulo iremos nos dedicar a provar o resultado "Se um corpo k algebricamente fechado é um subcorpo de um corpo L e existe um homomorfismo de anel de $k[X1, \cdots, Xn]$ em L, então $k = L$.", já utilizado anteriormente. Para tanto, adentraremos, de modo superficial, no território de Teoria de Corpos.

Definição 3.59. Sejam R um anel comutativo com unidade e M um grupo abeliano aditivo munido de uma multiplicação por escalar, isto é, de uma função $\cdot : R \times M \to M$, dada por $(a, m) \mapsto a \cdot m$, onde $a \in R$ e $m \in M$.

Se M satisfaz as propriedades, $\forall a, b \in R,\ \forall m, n \in M$:

(i) $(a +_R b) \cdot m = a \cdot m + b \cdot m$;

(ii) $a \cdot (m + n) = a \cdot m + a \cdot n$;

(iii) $(a \cdot_R b) \cdot m = a \cdot (b \cdot m)$;

(iv) $1_R \cdot m = m$, onde 1_R é o elemento unidade multiplicativa R.

dizemos que M é um R-módulo.

Observação 3.60. No que segue, embora usado na notação da Definição 3.59, omitiremos o subscrito R nas operações binárias do anel R.

Observamos ainda que, a partir deste momento, sempre que mencionarmos *anel* estaremos falando sobre um anel comutativo com unidade.

Proposição 3.61. *Se M é um R-módulo, então $0_R \cdot m = 0_M,\ \forall m \in M$.*

Demonstração. Veja que podemos reescrever $0_R \cdot m = (0_R + 0_R) \cdot m$. Logo,

$$0_R \cdot m = (0_R + 0_R) \cdot m \overset{\text{Def. 3.59(i)}}{=} 0_R \cdot m + 0_R \cdot m \Rightarrow 0_R \cdot m = 0_R \cdot m + 0_R \cdot m.$$

Mas M é grupo abeliano aditivo, logo existe o elemento oposto de $0_R \cdot m$.

$$\begin{aligned} 0_R \cdot m = 0_R \cdot m + 0_R \cdot m &\Rightarrow 0_R \cdot m + (-(0_R \cdot m)) = [0_R \cdot m + 0_R \cdot m] + (-(0_R \cdot m)) \\ &\Rightarrow 0_R \cdot m + (-(0_R \cdot m)) = 0_R \cdot m + [0_R \cdot m + (-(0_R \cdot m))] \Rightarrow 0_M = 0_R \cdot m + 0_M \\ &\Rightarrow 0_M = 0_R \cdot m. \end{aligned}$$

□

Exemplo 3.62. Todo grupo abeliano aditivo M é um $\mathbb{Z}$-módulo, com a multiplicação por escalar dada por:

$$\begin{aligned} \cdot : \mathbb{Z} \times M &\to M \\ (a, m) &\mapsto a \cdot m := \underbrace{m + m + m + \cdots + m}_{a \text{ parcelas}} \end{aligned}$$

De fato:

Para que o grupo M seja $\mathbb{Z}$-módulo com a multiplicação por escalar definida acima, precisamos mostrar as propriedades da Definição 3.59, isto é:

$\forall a, b \in \mathbb{Z},\ \forall m, n \in M$,

(i) $(a +_{\mathbb{Z}} b) \cdot m = a \cdot m + b \cdot m$, pois

$$(a +_{\mathbb{Z}} b) \cdot m = \underbrace{m + m + m + \cdots + m}_{a +_{\mathbb{Z}} b \text{ parcelas}} = \underbrace{m + m + m + \cdots + m}_{a \text{ parcelas}} + \underbrace{m + m + m + \cdots + m}_{b \text{ parcelas}} = a \cdot m + b \cdot m.$$

(ii) $a \cdot (m + n) = a \cdot m + a \cdot n$, já que

$$\begin{aligned} a \cdot (m + n) &= \underbrace{(m + n) + (m + n) + (m + n) + \cdots + (m + n)}_{a \text{ parcelas}} \\ &= \underbrace{m + m + m + \cdots + m}_{a \text{ parcelas}} + \underbrace{n + n + n + \cdots + n}_{a \text{ parcelas}} = a \cdot m + a \cdot n. \end{aligned}$$

(iii) $(a \cdot_{\mathbb{Z}} b) \cdot m = a \cdot (b \cdot m)$, a saber:

$$\begin{aligned} (a \cdot_{\mathbb{Z}} b) \cdot m = \underbrace{m + m + m + \cdots + m}_{a \cdot_{\mathbb{Z}} b \text{ parcelas}} &= \underbrace{\underbrace{m + m + \cdots + m}_{b \text{ parcelas}} + \cdots + \underbrace{m + m + \cdots + m}_{b \text{ parcelas}}}_{a \text{ parcelas}} \\ &= \underbrace{b \cdot m + b \cdot m + \cdots + b \cdot m}_{a \text{ parcelas}} = a \cdot (b \cdot m). \end{aligned}$$

(iv) $1 \cdot m = m$, onde 1 é o elemento unidade multiplicativa de $\mathbb{Z}$, já que

$$1 \cdot m = \underbrace{m}_{1 \text{ parcela}} = m.$$

Exemplo 3.63. Se R é um corpo, então dizemos que R-módulo é um espaço vetorial sobre R. Note que isso se dá pelas definições de espaço vetorial e R-módulo.

Exemplo 3.64. Todo ideal I de R é um R-módulo com a multiplicação por escalar dada pela própria multiplicação do R. Uma vez que essa multiplicação por escalar está bem-definida, já que $\forall a \in R, \forall x \in I$, o produto $ax \in I$. Além disso, pelas propriedades de I ser ideal e R ser anel comutativo com unidade, segue de forma natural as propriedades da Definição 3.59.

Exemplo 3.65. Sejam R, S anéis comutativos com unidade.

Se $\varphi : R \to S$ é um homomorfismo de anéis, então S é um R-módulo com a seguinte multiplicação por escalar:

$$\begin{aligned} \cdot : R \times S &\to S \\ (a, m) &\mapsto a \cdot m := \varphi(a)m. \end{aligned}$$

Note que são válidas as propriedades da Definição 3.59, tendo em vista que φ é homomorfismo de anéis:

$\forall a, b \in R,\ \forall m, n \in S$,

(i) $(a +_R b) \cdot m = a \cdot m + b \cdot m$, pois

$$(a +_R b) \cdot m = \varphi(a +_R b)m = (\varphi(a) + \varphi(b))m = \varphi(a)m + \varphi(b)m = a \cdot m + b \cdot m.$$

(ii) $a \cdot (m + n) = a \cdot m + a \cdot n$, já que

$$a \cdot (m + n) = \varphi(a)(m + n) = \varphi(a)m + \varphi(a)n = a \cdot m + a \cdot n.$$

(iii) $(a \cdot_R b) \cdot m = a \cdot (b \cdot m)$, a saber:

$$(a \cdot_R b) \cdot m = \varphi(a \cdot b)m = (\varphi(a)\varphi(b))m = \varphi(a)(\varphi(b)m) = \varphi(a)(b \cdot m) = a \cdot (b \cdot m).$$

(iv) $1_R \cdot m = m$, onde 1_R é o elemento unidade multiplicativa de R, pois

$$1_R \cdot m = \varphi(1_R)m = 1_S \cdot m = m.$$

Exemplo 3.66. Todo subanel R de um anel S é um R-módulo, sendo R um subanel com unidade, cuja unidade é a mesma do anel S. Basta considerarmos no exemplo anterior φ como a aplicação inclusão, isto é,

$$\begin{aligned} \varphi : R &\hookrightarrow S \\ a &\mapsto \varphi(a) = a. \end{aligned}$$

Além disso, se R é subanel de S e S é subanel de T, então sabemos que S é um R-módulo e T é um S-módulo. Mais ainda, podemos fazer a composição das inclusões $\varphi : R \hookrightarrow S$ e $\gamma : S \hookrightarrow T$ de modo que $\gamma \circ \varphi : R \hookrightarrow T$ seja a inclusão de R em T. Com isso, obtemos que T é um R-módulo.

Definição 3.67. Um subgrupo N do R-módulo M é um submódulo de M se $a \cdot m \in N,\ \forall a \in R, \forall m \in N$.

Observação 3.68. Se isso ocorre, então N também é um R-módulo. E, então, são válidas as propriedades da Definição 3.59, tendo em vista que a multiplicação por escalar de N é a multiplicação por escalar de M restrita ao $R \times N$, garantindo então que N herda as propriedades de M.

Proposição 3.69. *Seja S é um conjunto de elementos de um R-módulo M, o conjunto definido por*

$$\left\{\sum r_i \cdot s_i;\ r_i \in R,\ s_i \in S\right\}$$

é um submódulo de M. Denominamos este submódulo por submódulo gerado por S. Além disso, este submódulo é o menor submódulo de M que contém S.

Em particular, se $S = \{s_1, \cdots, s_n\}$ é finito, o submódulo gerado por S é denotado por $\sum Rs_i$.

Demonstração. Seja $a \in R$ e $\sum r_j \cdot s_j \in \left\{\sum r_i \cdot s_i;\ r_i \in R,\ s_i \in S\right\}$. Note que

$$\sum r_j \cdot s_j = r_1 \cdot s_1 + r_2 \cdot s_2 + \cdots + r_j \cdot s_j + r_{j+1} \cdot s_{j+1} + \cdots .$$

Como M é R-módulo, temos que:

$$\begin{aligned} a \cdot \sum r_j \cdot s_j &= a \cdot (r_1 \cdot s_1 + r_2 \cdot s_2 + \cdots + r_i \cdot s_i + r_{i+1} \cdot s_{i+1} + \cdots) \\ &= a \cdot (r_1 \cdot s_1) + a \cdot (r_2 \cdot s_2) + \cdots + a \cdot (r_j \cdot s_j) + a \cdot (r_{j+1} \cdot s_{j+1}) + \cdots \\ &= (ar_1) \cdot s_1 + (ar_2) \cdot s_2 + \cdots + (ar_j) \cdot s_j + (ar_{j+1}) \cdot s_{j+1} + \cdots = \sum (ar_j) \cdot s_j. \end{aligned}$$

Perceba que cada $ar_j = t_j \in R$ e $s_j \in S$, logo

$$a \cdot \sum r_j \cdot s_j = \sum (ar_j) \cdot s_j = \sum t_j \cdot s_j \in \left\{\sum r_i \cdot s_i;\ r_i \in R,\ s_i \in S\right\}.$$

Com isso, $\left\{\sum r_i \cdot s_i;\ r_i \in R,\ s_i \in S\right\}$ é submódulo de M.

Suponha P um submódulo de M que contém S, qualquer. Como P é submódulo de M temos, da Definição 3.67, que $a \cdot p \in P,\ \forall a \in R,\ \forall p \in P$.

Como $S \subset P$, então $a \cdot s_i \in P,\ \forall a \in R,\ \forall s_i \in S$. Se tomarmos $a = r_i$, teremos que $r_i \cdot s_i \in P,\ \forall r_i \in R,\ \forall s_i \in S$.

Observe que, por definição, P é grupo abeliano aditivo, logo $\sum r_i \cdot s_i \in P,\ r_i \in R,\ s_i \in S$. Deste modo, $\left\{\sum r_i \cdot s_i;\ r_i \in R,\ s_i \in S\right\} \subset P$, portanto, é o menor submódulo de M que contém S. □

Definição 3.70. Seja M um R-módulo. Dizemos que M é finitamente gerado se existem $s_1, \cdots, s_n \in M$ tais que $M = \sum Rs_i$.

Observe que este conceito está em consonância com a noção de grupos comutativos e ideais finitamente gerados, bem como com a noção de espaços vetoriais de dimensão finita, quando R é corpo.

Proposição 3.71. *Sejam R um subanel de S e S um subanel de T. Se $S = \sum Rv_i$, $T = \sum Sw_j$, então $T = \sum Rv_iw_j$.*

Demonstração. Queremos mostrar que $T = \sum Rv_iw_j$, isto é: $T \subset \sum Rv_iw_j$ e $\sum Rv_iw_j \subset T$.

Observe que, pelo Exemplo 3.66, temos que S e T são R-módulos.

- $T \subset \sum Rv_iw_j$. De fato:

  Seja $a \in T$ qualquer. Como $T = \sum Sw_j$ e $a \in T$, então

  $$a = \sum_j s_jw_j,\ s_j \in S. \tag{3.4}$$

  Mas $s_j \in S$ e $S = \sum_i Rv_i$ e então

  $$s_j = \sum_i r_{ij}v_i,\ r_{ij} \in R. \tag{3.5}$$

  Assim, por (3.4) e (3.5), temos que:

  $$a = \sum_j s_jw_j = \sum_j \left(\sum_i r_{ij}v_i\right) w_j = \sum_{i,j} r_{ij}v_iw_j \in \sum_{i,j} Rv_iw_j.$$

- $\sum Rv_iw_j \subset T$.

  Seja $b \in \sum Rv_iw_j$ qualquer, então

  $$b = \sum_{i,j} r_{ij}v_iw_j,\ r_{ij} \in R.$$

  Assim,

  $$b = \sum_{i,j} r_{ij}v_iw_j = \sum_j \left(\sum_i r_{ij}v_i\right) w_j.$$

  Mas $\sum_i r_{ij}v_i \in S = \sum Rv_i$, logo $\sum_i r_{ij}v_i = s_j$. Com isso:

  $$b = \sum_j \left(\sum_i r_{ij}v_i\right) w_j = \sum_j s_jw_j \in \sum_j Sw_j = T.$$

□

Agora, abordaremos as condições de finitude. Seja R um subanel do anel S, veremos que há diversos tipos de condições de finitude de S sobre R, dependendo se consideramos S como R-módulo, anel ou corpo.

Definição 3.72. Seja R um subanel do anel S, sendo R um subanel com unidade, cuja unidade é a mesma do anel S. S é dito módulo finito sobre R se S é finitamente gerado como um R-módulo, no sentido do Exemplo 3.66.

Se R e S são corpos, denotamos a dimensão de S sobre R como $[S : R]$.

Proposição 3.73. *Sejam S um módulo finito sobre R, $v_1, \cdots, v_n \in S$ e a aplicação $\phi : R[X_1, \cdots, X_n] \to S$ que leva X_i em v_i, $i \in \{1, \cdots, n\}$, isto é,*

$$\phi(F) = \phi\left(\sum a_{(i)} X^{(i)}\right) = \sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n},\ a_{(i)} \in R.$$

Nestas condições, ϕ é um homomorfismo de anéis e a imagem de ϕ é denotada por $R[v_1, \cdots, v_n]$, ou seja, $R[v_1, \cdots, v_n] = \{\sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n};\ a_{(i)} \in R\}$.

Ainda, $R[v_1, \cdots, v_n]$ é subanel de S contendo R e $v_1, \cdots, v_n$ e, em particular, é o menor subanel em que isso ocorre.

Demonstração. De fato, ϕ é homomorfismo de anéis:
$\forall F, G \in R[X_1, \cdots, X_n]$,

- Veja que

  $$\phi(F+G) = \phi\left(\sum a_{(i)} X^{(i)} + \sum b_{(j)} X^{(j)}\right) = \phi\left(\sum c_{(k)} X^{(k)}\right) = \sum c_{(k)} v_1^{k_1} \cdots v_n^{k_n},$$

  onde $c_{(k)} = a_{(k)} + b_{(k)}$.

  Por outro lado,

  $$\phi(F) + \phi(G) = \phi(\sum a_{(i)} X^{(i)}) + \phi(\sum b_{(j)} X^{(j)}) = \sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n} + b_{(j)} v_1^{j_1} \cdots v_n^{j_n} = \sum c_{(k)} v_1^{k_1} \cdots v_n^{k_n},$$

  onde $c_{(k)} = a_{(k)} + b_{(k)}$.

  Logo, $\phi(F+G) = \phi(F) + \phi(G)$.

- Observe que

  $$\phi(FG) = \phi\left(\left(\sum a_{(i)} X^{(i)}\right)\left(\sum b_{(j)} X^{(j)}\right)\right) = \phi\left(\sum d_{(l)} X^{(l)}\right) = \sum d_{(l)} v_1^{l_1} \cdots v_n^{l_n},$$

  onde $d_l = \sum_{i+j=l} a_{(i)} b_{(j)}$ e $l = i + j$.

  Por outro lado,

  $$\phi(F)\phi(G) = (\phi(\sum a_{(i)} X^{(i)}))(\phi(\sum b_{(j)} X^{(j)})) = (\sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n})(\sum b_{(j)} v_1^{j_1} \cdots v_n^{j_n}) = \sum d_{(l)} v_1^{l_1} \cdots v_n^{l_n},$$

  onde $d_l = \sum_{i+j=l} a_{(i)} b_{(j)}$ e $l = i + j$.

  Deste modo, $\phi(FG) = \phi(F)\phi(G)$.

Agora, note que $R[v_1, \cdots, v_n]$ é subanel de S, pela Proposição 2.42. Além disso, $v_1, \cdots, v_n \in R[v_1, \cdots, v_n]$, já que $v_i = \phi(X_i) \in R[v_1, \cdots, v_n],\ \forall X_i \in R[X_1, \cdots, X_n]$.

Mais ainda, como $R \subset R[X_1, \cdots, X_n]$, pela Proposição 2.97, e $R[v_1, \cdots, v_n] = Im(\phi)$ podemos afirmar que, seja $a \in R$ qualquer, se tomarmos $F = a \in R[X_1, \cdots, X_n]$, então $\phi(F) = \phi(a) = a$ e, portanto, $R \subset Im(\phi) = R[v_1, \cdots, v_n]$.

Basta mostrar que $R[v_1, \cdots, v_n]$ é o menor subanel de S contendo R e $v_1, \cdots, v_n$. Para tal, suponha P subanel de S contendo R e $v_1, \cdots, v_n$, qualquer. Como P é subanel de S, P é, em particular, um anel, logo qualquer combinação dos elementos de P pertence a P, portanto $\sum a_{(i)} v_i^{i_1} \cdots v_n^{i_n} \in P,\ \forall a_{(i)} \in R$. Deste modo, $R[v_1, \cdots, v_n] \subset P$. □

Observação 3.74. Quando necessário, denotaremos

$$F(v_1, \cdots, v_n) := \phi(F) = \sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n}.$$

Definição 3.75. Se $S = R[v_1, \cdots, v_n]$, para algum $v_i \in S$, então dizemos que S é anel finito sobre R.

Observação 3.76. Veja que

(i) Seja K um corpo de fração, então $K[v]$ é um domínio de integridade, pois:

Sejam $Y_1, Y_2 \in K[v]$. Como $K[v] = Im(\phi)$, então $Y_1 = \phi(G_1)$ e $Y_2 = \phi(G_2)$, em que $G_1, G_2 \in R[X]$, com isso, se $Y_1 Y_2 = 0$. Então:

$$Y_1 Y_2 = 0 \Rightarrow \phi(G_1)\phi(G_2) = 0 \Rightarrow \phi(G_1 G_2) = 0 \Rightarrow G_1 G_2 \in \ker(\phi) \Rightarrow$$
$$G_1 \in \ker(\phi) \text{ ou } G_2 \in \ker(\phi) \Rightarrow \phi(G_1) = 0 \text{ ou } \phi(G_2) = 0 \Rightarrow Y_1 = 0 \text{ ou } Y_2 = 0.$$

(ii) Sejam $R = K$ e $S = L$ corpos, $v_1, \cdots, v_n \in L$ e $K(v_1, \cdots, v_n)$ o corpo de fração de $K[v_1, \cdots, v_n]$. Observe que $K(v_1, \cdots, v_n)$ pode ser visto como um subcorpo de L, mais ainda, ele é o menor subcorpo de L que contém K e $v_1, \cdots, v_n$.

No que segue, por vezes, ao invés de citarmos K como subcorpo de L, diremos que L é extensão de corpo de K.

Definição 3.77. Nas condições da observação anterior, se existem $v_1, \cdots, v_n \in L$ tais que $L = K(v_1, \cdots, v_n)$, dizemos que L é uma extensão de corpo finitamente gerado de K.

Proposição 3.78. *Sejam R um subanel de S e S um subanel de T. Se $S = R[v_1, \cdots, v_n]$, $T = S[w_1, \cdots, w_m]$, então $T = R[v_1, \cdots, v_n, w_1, \cdots, w_m]$.*

Demonstração. Sabemos que

$$T = S[w_1, \cdots, w_m] = R[v_1, \cdots, v_n][w_1, \cdots, w_m].$$

Isso significa que cada elemento de T pode ser expresso como um polinômio em w_i com coeficientes em $R[v_1, \cdots, v_n]$. Mas como cada v_i está em R, podemos expressar cada um desses coeficientes como um polinômio em v_i, com coeficientes em R. Deste modo, cada elemento de T pode ser expresso como um polinômio de v_i e w_i, com coeficientes em R, isto é, $T = R[v_1, \cdots, v_n, w_1, \cdots, w_m]$. □

Definição 3.79. Seja R um subanel do anel S.

(i) Dizemos que um elemento $v \in S$ é inteiro sobre R se existe um polinômio mônico da forma $F = X^n + a_1 X^{n-1} + \cdots + a_n \in R[X]$ tal que $F(v) = 0$.

(ii) Se S é uma extensão de corpo do corpo R e v é inteiro sobre R, então dizemos que v é algébrico sobre R.

Proposição 3.80. *Se R um subanel de um domínio de integridade S e $v \in S$, então as seguintes propriedades são equivalentes:*

(i) v é inteiro sobre R.

(ii) $R[v]$ é módulo finito sobre R.

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

Demonstração. Para isso, mostremos que $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$ e $(iii) \Rightarrow (i)$. De fato:

$(i) \Rightarrow (ii)$: Como v é um inteiro sobre R, segue, por definição, que existe um polinômio mônico $F = X^n + a_1X^{n-1} + \cdots + a_n$ tal que $F(v) = 0$, isto é:

$$v^n + a_1v^{n-1} + \cdots + a_n = 0.$$

Então,

$$v^n = -a_1v^{n-1} - a_2v^{n-2} - \cdots - a_n \Rightarrow v^n = (-a_1)v^{n-1} + (-a_2)v^{n-2} + \cdots + (-a_n).$$

Desta forma, $v^n \in \sum_{i=0}^{n-1} Rv^i$, já que $a_i \in R,\ \forall i \in \{1, \cdots, n\}$ e, consequentemente, como R é anel, $-a_i \in R,\ \forall i \in \{1, \cdots, n\}$.

Afirmação. $R[v] = \sum_{i=0}^{n-1} Rv^i$.

De fato:

(i) $R[v] \subset \sum_{i=0}^{n-1} Rv^i$.

Seja $a \in R[v]$, qualquer. Logo, $a = \phi(G)$, para algum $G \in R[X]$, em que $G = \sum_{j=0}^{m} b_jX^j$, onde $b_j \in R, \forall j \in \{1, \cdots, m\}$, ou seja,

$$a = \phi\left(\sum_{j=0}^{m} b_jX^j\right) = b_mv^m + b_{m-1}v^{m-1} + \cdots + b_1v^1 + b_0.$$

- Se $m < n$, então $a \in \sum_{i=0}^{n-1} Rv^i$, já que podemos colocar os coeficientes b_{m+1} até b_{n-1} iguais a zero.
- Se $m \geq n$, então existe l inteiro tal que $m = l + (n-1)$:

$$\begin{aligned} a &= b_mv^m + b_{m-1}v^{m-1} + \cdots + b_nv^n + b_{n-1}v^{n-1} + \cdots + b_1v + b_0 \\ &= (b_mv^l)v^{n-1} + (b_{m-1}v^l)v^{n-2} + \cdots + (b_nv^l)v + b_{n-1}v^{n-1} + \cdots + b_1v + b_0 \\ &= (b_mv^l + b_{n-1})v^{n-1} + (b_{m-1}v^l + b_{n-2})v^{n-2} + \cdots + (b_nv^l + b_1)v + b_0. \end{aligned}$$

Logo, $a \in \sum_{i=0}^{n-1} Rv_i$, pois $b_jv^r \in R,\ \forall j, r$.

(ii) $\sum_{i=0}^{n-1} Rv^i \subset R[v]$.

Seja $a \in \sum_{i=0}^{n-1} Rv^i$, qualquer. Logo,

$$a = s_{n-1}v^{n-1} + \cdots + s_1v^1 + s_0 = \phi(H),$$

em que $H = s_{n-1}X^{n-1} + \cdots + s_1X^1 + s_0$.
Deste modo, $a \in Im(\phi) = R[v]$.

$(ii) \Rightarrow (iii)$: Para tal, basta tomarmos $R' = R[v]$, assim, como $R[v]$ é módulo finito sobre R, R' também o é.

$(iii) \Rightarrow (i)$: Como R' é um módulo finito sobre R de S contendo $R[v]$, então, pela Definição 3.70, podemos afirmar que existem $w_1, \cdots, w_n \in R'$ tais que $R' = \sum_{i=1}^{n} Rw_i$. Assim, como $v \in R[v]$ e $R[v] \subset R'$, então $v \in R'$, logo, para cada $i \in \{1, \cdots, n\}$ o produto vw_i pertencem a R', consequentemente existem $a_{ij} \in R$ tais que

$$vw_i = \sum_{j=1}^{n} a_{ij} w_j.$$

Então,

$$\sum_{j=1}^{n} (\delta_{ij} v - a_{ij}) w_j = 0, \ \forall i,$$

onde $\delta_{ij} = 0$ se $i \neq j$ e $\delta_{ii} = 1$. Já que:

$$\sum_{j=1}^{n} (\delta_{ij} v - a_{ij}) w_j = 0 \iff \sum_{j=1}^{n} \delta_{ij} v w_j - \sum_{j=1}^{n} a_{ij} w_j = 0 \iff \sum_{j=1}^{n} a_{ij} w_j = \sum_{j=1}^{n} \delta_{ij} v w_j.$$

Observe que, quando $i \neq j$, temos $\delta_{ij} = 0$. Logo,

$$\sum_{j=1}^{n} (\delta_{ij} v w_j) = v w_i,$$

ou seja,

$$vw_i = \sum_{j=1}^{n} a_{ij} w_j.$$

Se considerarmos essas equações no corpo de frações de S, veremos que $(w_1, \cdots, w_n)$ é uma solução não-trivial, então $det(\delta_{ij} v - a_{ij}) = 0$. Como v aparece apenas na diagonal da matriz, tal determinante tem a forma $v^n + a_1 v^{n-1} + \cdots + a_n, \ a_i \in R$. Logo, $v^n + a_1 v^{n-1} + \cdots + a_n = 0$ e, portanto, v é inteiro sobre R.

□

Corolário 3.81. *O conjunto dos elementos de S que são inteiros sobre R é um subanel de S que contém R.*

Demonstração. Defina $B := \{v \in S; \ v \text{ é inteiro sobre } R\}$.

Afirmação. B é subanel de S que contém R.

De fato, sejam $v, w \in B$, quaisquer. Como w é inteiro sobre R e $R \subset R[v]$, segue que w é inteiro sobre $R[v]$. Isso se dá pois se temos um polinômio em $R[X]$ que tem w como raiz também terá em $R[v][X]$, pois os coeficientes que estão em R também estão em $R[v]$.

Logo, pela implicação $(i) \Rightarrow (ii)$ da Proposição 3.80, segue que $R[v][w]$ é módulo finito sobre R, ou seja, pela Proposição 3.71, $R[v, w]$ é um módulo finito sobre R.

Sendo $v, w \in R[v, w]$ e $R[v, w]$ um módulo finito sobre R, temos que $v - w$ e $vw \in R[v, w]$. Pela implicação $(ii) \Rightarrow (i)$ da Proposição 3.80, segue que $v - w$ e vw são inteiros sobre R e, portanto, $v - w$ e vw estão em B.

Pela definição de B tem-se, de modo natural, que $R \subset B$, pois todo elemento a de R é inteiro sobre R, tome, por exemplo, o polinômio $F(X) = X - a$, temos que $F(a) = 0$. □

Suponha L uma extensão de corpo do corpo K e suponha $L = K(v)$, para algum $v \in L$, em que $\varphi : K[X] \to K[v]$ é um homomorfismo sobrejetor levando X em v, com $K[v] = Im(\varphi)$. Seja $\ker(\varphi) = \langle F \rangle$, $F \in K[X]$ (já que, pelo Teorema 2.101, $K[X]$ é um PID, pois K é corpo). Então, pelo Primeiro Teorema do Isomorfismo (Teorema 2.79), temos que $\dfrac{K[X]}{\langle F \rangle}$ é isomorfo a $K[v]$, como $K[v]$ é domínio de integridade, pela Observação 3.76, item (i), temos que $\langle F \rangle$ é primo. A partir disso, dois casos podem ocorrer:

1. $F = 0$. Neste caso, temos que $\langle F \rangle = \langle 0 \rangle$ e, então, o homomorfismo sobrejetor φ também será injetor, pela Proposição 2.39. Consequentemente, $K[v]$ é isomorfo a $K[X]$, logo $K(v) = L$ é isomorfo a $K(X)$. Neste caso, L não é módulo finito sobre K, pois v não é algébrico sobre K.

2. $F \neq 0$. Assuma que F é mônico. Como $\langle F \rangle$ é primo, então, pela Proposição 2.57 e Corolário 2.64, F é irredutível e $\langle F \rangle$ é maximal. Deste modo, pela Proposição 2.78, $\dfrac{K[X]}{\langle F \rangle}$ é corpo, assim $K[v]$ é um corpo, já que $\dfrac{K[X]}{\langle F \rangle}$ é isomorfo a $K[v]$. E $F(v) = 0$, visto que $F \in \ker(\varphi)$, então v é algébrico sobre K e $L = K[v]$ é módulo finito sobre K.

Para finalizar essa seção, completaremos a demonstração do Teorema 3.52 (Hilbert's Nullstellensatz), iniciada na Seção 3.6, pois, na ocasião, afirmamos que "Se L é extensão de corpo de um corpo k algebricamente fechado e existe um homomorfismo de anel de $K[X_1, \cdots, X_n]$ em L, então $k = L$", mas não foi demonstrado isso anteriormente, pois não tínhamos as ferramentas necessárias. Segue, agora, a demonstração deste fato.

Provaremos que L é módulo finito sobre k. Isso garante que uma extensão de corpo finito já é módulo finito. A próxima proposição mostra que isso é sempre verdade e conclui a prova de Nullstellensatz.

Proposição 3.82 (Zariski)**.** *Se um corpo L é anel finito sobre um subcorpo K, então L é módulo finito (e, portanto, algébrico) sobre K.*

Demonstração. Suponha $L = K[v_1, \cdots, v_n]$. O caso $n = 1$ já foi previamente abordado pelos casos acima, então assumiremos o resultado para todas as extensões geradas por $n-1$ elementos. Seja $K_1 = K(v_1)$. Por indução, $L = K[v_2, \cdots, v_n]$ é módulo finito sobre K_1. Podemos assumir que v_1 não é algébrico sobre K (caso contrário, a Proposição 3.78 resolveria a demonstração).

Cada v_i satisfaz a equação $v_i^{n_i} + a_{i1}v^{n_i-1} + \cdots = 0$, $a_{ij} \in K_1$. Tomamos $a \in K[v_1]$ como um múltiplo e todos os denominadores de a_{ij}, teremos a equação $(av_i)_i^n + aa_{i1}(av)^{n_i-1} + \cdots = 0$. Segue do Corolário 3.81 que, para qualquer $z \in L = K[v_1, \cdots, v_n]$, existe um N tal que $a^N z$ é inteiro sobre $K[v_1]$. Em particular, isso é válido para $z \in K(v_1)$. Mas como $K(v_1)$ é isomorfo ao anel de funções racionais de uma variável sobre K, isso é impossível. □

Proposição 3.83. *Se k é um corpo algebricamente fechado e L é uma extensão do corpo k, então qualquer elemento de L que é algébrico sobre k é um elemento de k.*

Demonstração. Seja $a \in L$ um elemento algébrico sobre k, qualquer. Então, existe um polinômio não nulo $F(X) \in k[X]$ tal que $F(a) = 0$. Como k é algebricamente fechado, $F(X)$ se fatora completamente em fatores lineares em $k[X]$. Isto é, podemos escrever

$$F(x) = c(X - r_1)(X - r_2) \cdots (X - r_n),$$

para algum $c \in k$, não nulo, e $r_1, r_2, \cdots, r_n \in k$. Além disso, $F(a) = 0$ implica que

$$c(a - r_1)(a - r_2) \cdots (a - r_n) = 0.$$

Como k é um corpo e $c \neq 0$, algum dos fatores $(a - r_i)$ é, necessariamente, zero. Deste modo, $a = r_i \in k$, para algum $i \in \{1, \cdots, n\}$. Portanto, qualquer elemento de L algébrico sobre k, pertence a k □

Proposição 3.84. *Se k é algebricamente fechado, então qualquer extensão L do corpo k, não é módulo finito sobre k. Em particular, o único módulo finito sobre k é o próprio k.*

Demonstração. Suponha L uma extensão do corpo k, $L \neq k$ e k algebricamente fechado. Suponha, por absurdo, que L seja um módulo finito sobre k, ou seja, um k-módulo finitamente gerado. Sejam $a_1, a_2, \cdots, a_n$ um conjunto finito que gera L como um k-módulo. Como cada a_i é algébrico sobre L e k é algebricamente fechado, então a_i é algébrico sobre k. Deste modo, existem polinômios não nulos $F_i(X) \in k[X]$ tais que $F_i(a_i) = 0$, para cada $i \in \{1, \cdots, n\}$.

Seja $F(X)$ o polinômio formado pela multiplicação de cada F_i, isto é,

$$F(X) = F_1(X)F_2(X) \cdots F_n(X).$$

Deste modo, $F(X)$ é um polinômio não nulo e, para cada $i \in \{1, \cdots, n\}$, temos $F(a_i) = 0$.

Agora, considere o elemento $b \in L$. Como $a_1, a_2, \cdots, a_n$ geram L como um k-módulo, podemos escrever

$$b = c_1a_1 + c_2a_2 + \cdots + c_na_n$$

para determinados $c_1, \cdots, c_n \in k$. Logo,

$$F(b) = F(c_1a_1 + c_2a_2 + \cdots + c_na_n) = 0.$$

Assim, $F(X)$ é um polinômio não nulo em $k[X]$ o qual todos os elementos de L são raízes. No entanto, isso contradiz que k é algebricamente fechado, já que, nesse contexto, um polinômio não nulo pode ter, no máximo, $deg(F)$ raízes em k. Portanto, a único módulo finito sobre k é o próprio k. □

Corolário 3.85. *Se L é extensão de corpo de um corpo k algebricamente fechado e existe um homomorfismo de anel de $K[X_1, \cdots, X_n]$ em L, então $k = L$.*

Demonstração. A demonstração segue das Proposições 3.82 e 3.84. □

Exploramos, portanto, alguns elementos de forma geral da Geometria Algébrica para o caso de n variáveis. No próximo capítulo, iremos nos concentrar no caso específico de $n = 2$, onde estudaremos algumas particularidades interessantes.

4 Curvas Planas Algébricas

Nos capítulos anteriores abordamos os conceitos básicos da Geometria Algébrica. Neste capítulo, focamos no estudo das Curvas Algébricas Planas. Para tal, utilizamos o livro [5], além de complementarmos as demonstrações e definições sempre que necessário. Vale ressaltar que os exemplos 4.11, 4.12, 4.19, 4.24 e 4.28 foram elaborados pela autora, e o exemplo 4.25 foi complementado pela mesma.

Além disso, utilizaremos o software GeoGebra para a exibição das curvas apresentadas nos exemplos ao longo do capítulo, a fim de facilitar a visualização dos mesmos. Aos interessados em reproduzir os exemplos no GeoGebra, todas as constantes fixadas podem ser substituídas por controles deslizantes e o leitor pode, então, observar a movimentação das curvas conforme as constantes escolhidas.

Definição 4.1. Uma curva algébrica plana é o lugar dos pontos cujas coordenadas cartesianas satisfazem a uma dada equação polinômial $F(X, Y) = 0$, onde F é um polinômio não constante.

Exemplo 4.2. Seguem alguns exemplos de curvas algébricas planas:

(I) Elipse, definida pela equação

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} - 1 = 0, \tag{4.1}$$

onde a e b são constantes.

(II) Parábola, definida pela equação

$$Y - aX^2 - bX - c = 0, \tag{4.2}$$

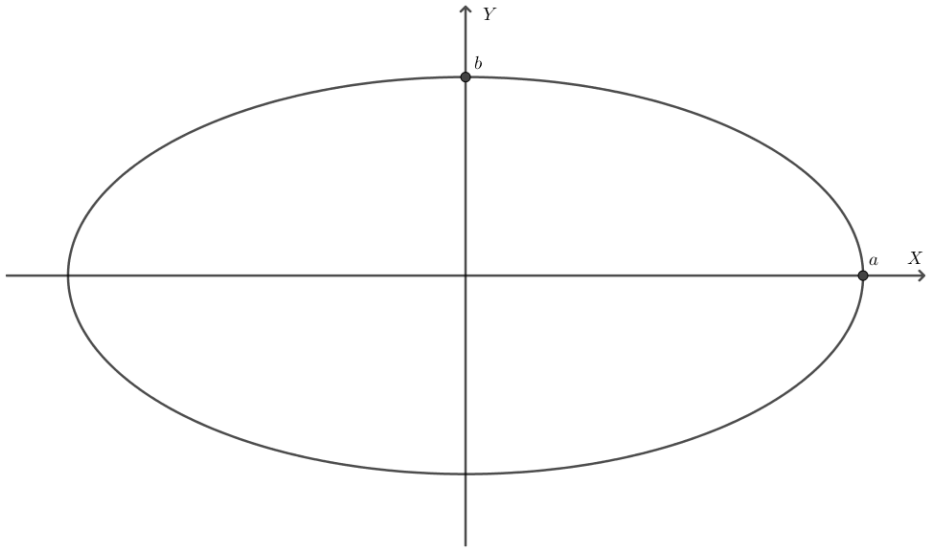
onde a, b e c são constantes.

(III) Caracol de Pascal, definido por

$$(X^2 + Y^2 - bX)^2 - a^2(X^2 + Y^2) = 0, \tag{4.3}$$

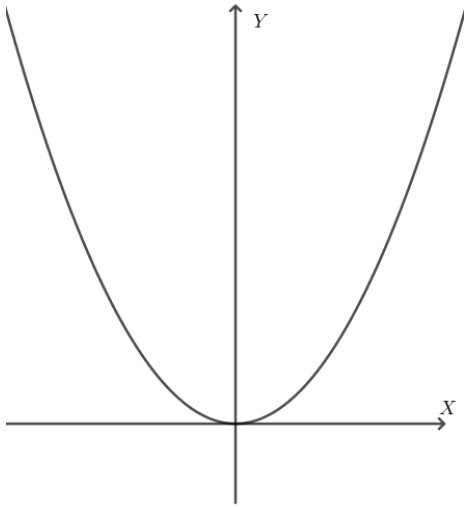
onde a e b são constantes.

Figura 4.1: Elipse dada pela equação 4.1, onde $a = 2$ e $b = 1$.



Fonte: elaborado pela autora (2023)

Figura 4.2: Parábola dada pela equação 4.2, onde $a = 2$, $b = 0$ e $c = 0$.



Fonte: elaborado pela autora (2023)

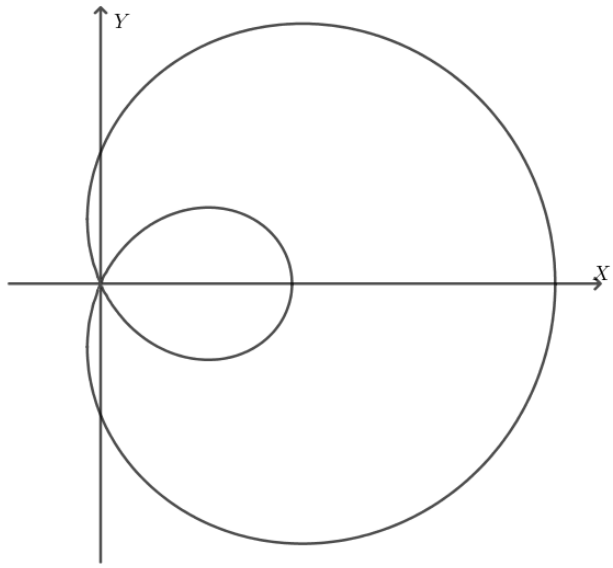
(IV) Hipérbole, definido por

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} - 1 = 0, \tag{4.4}$$

onde a e b são constantes.

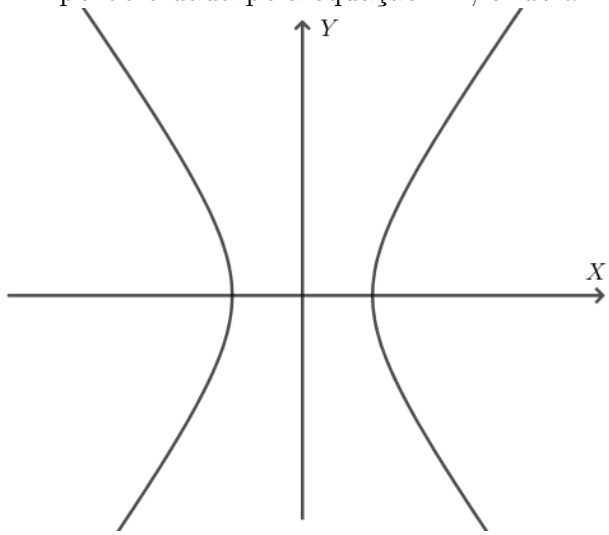
Uma pergunta que pode surgir da Definição 4.1 é se a equação polinomial $F(X, Y) = 0$ está bem determinada pela curva, isto é, pelo lugar das soluções. Observe que $F = 0$ e $F^2 = 0$ possuem as mesmas soluções e, portanto, nossa resposta para a pergunta anterior é não. Poderíamos então pensar que apenas as curvas da forma $F^m = 0$ teriam, então, as mesmas soluções, porém se pensarmos nas equações $XY = 0$ e $X^2Y = 0$ veremos que elas possuem mesma solução e não satisfazem essa proposta. Note que poderíamos pensar, intuitivamente, diversas outras generalizações de equações que cumpririam a regra de terem as mesmas soluções e, ainda assim, encontraríamos equações que fogem dessas

Figura 4.3: Caracol de Pascal dada pela equação 4.3, onde $a = 2$ e $b = 5$.



Fonte: elaborado pela autora (2023)

Figura 4.4: Hipérbole dada pela equação 4.4, onde $a = 2$ e $b = 3$.



Fonte: elaborado pela autora (2023)

propostas. Então quais as condições necessárias para que duas curvas algébricas sejam iguais?

Observação 4.3. Sejam $F(X, Y) \in k[X, Y]$ e $(x, y) \in k^2$ quaisquer. Indicamos por $F(x, y)$ o valor do polinômio F neste ponto.

Proposição 4.4. *Sejam F, G polinômios em duas variáveis com coeficientes no corpo k algebricamente fechado. $F(X, Y) = 0$ e $G(X, Y) = 0$ terão as mesmas soluções (ou seja, mesmas curvas algébricas) em k^2 se, e somente se, os fatores irredutíveis de F e G são os mesmos.*

Demonstração. ($\Rightarrow$) Seja $(x, y) \in k^2$ uma solução de F e suponha T um fator irredutível de F tal que $T(x, y) = 0$. Deste modo, se $T(x, y) = 0$, então $F(x, y) = 0$. Mais ainda, como $F(x, y) = 0$, por hipótese, $G(x, y) = 0$.

Para mostrarmos que T é fator irredutível de G, mostremos que T divide G em $k[X,Y]$.

Tomaremos agora $A = k[X]$ e $L = k(X)$, o corpo de frações de A. Podemos supor que Y ocorra efetivamente em T (caso necessário, ainda podemos trocar X por Y). Pela Proposição 2.113, se T é irredutível em $A[Y]$, então também o é em $L[Y]$. Suponha, por absurdo, que T não divide G. Deste modo, $mdc(T,G) = 1$. Assim, pelo Corolário 2.104,

$$aT + bG = 1,$$

onde $a, b \in L[Y]$. Como $L[Y]$ é o corpo de frações de $A[Y]$, podemos reescrever $a = \dfrac{a'}{c}$ e $b = \dfrac{b'}{c}$, com $a', b' \in A[Y]$ e $c \in A$ e $c \neq 0$, assim:

$$aT + bG = 1 \Rightarrow \frac{a'}{c}T + \frac{b'}{c}G = 1 \Rightarrow a'T + b'G = c.$$

Agora, como Y ocorre efetivamente em T, segue que, exceto para um número finito de $x \in k$ a equação $T(x,Y) = 0$ admite solução (k, por hipótese, é algebricamente fechado). Logo, para tais $x \in k$ a equação $G(x,Y) = 0$ também admite solução e, portanto, para tais elementos $x \in k$, $c(x) = 0$. Entretanto, Y pode ser valorado em k infinitamente, já que k é um corpo infinito, consequentemente existirão para cada valor fixo de Y em k, finitos tais elementos x em k, ou seja, teremos quantidades infinitas de $x \in k$ em que resultarão $c(x) = 0$, portanto, necessariamente, $c = 0$, o que absurdo.

Portanto, $T|G$ em $L[Y]$, ou seja, G é redutível em $L[Y]$, então pelo Corolário 2.114, G é redutível em $K[X,Y]$, em que $T|G$ em $K[X,Y]$.

($\Leftarrow$) Seja T um fator irredutível de F tal que $T(x,y) = 0$, para algum $(x,y) \in k^2$. Deste modo, se $T(x,y) = 0$, então $F(x,y) = 0$. Além disso, por hipótese, os fatores irredutíveis de F e G são os mesmos, logo T é fator irredutível de G e se $T(x,y) = 0$, para algum $(x,y) \in k^2$, então $G(x,y) = 0$. Portanto, $F(X,Y) = 0$ e $G(X,Y) = 0$ têm as mesmas soluções.

□

A partir dessa proposição, podemos reescrever a Definição 4.1, para podermos identificar a curva algébrica com sua equação.

Proposição 4.5. *A relação em $k[X,Y]$ dada por, $\forall F, G \in k[X,Y]$,*

$$F \sim G \iff \exists c \in k^*;\ F(X,Y) = cG(X,Y)$$

é uma relação de equivalência.

Demonstração. $\sim$ é uma relação de equivalência. De fato:

(i) $\sim$ é reflexiva: $\forall F \in K[X,Y]$,

$$F \sim F \Rightarrow F(X,Y) = 1 \cdot F(X,Y),$$

onde 1 é o elemento identidade de k.

(ii) $\sim$ é simétrica: $\forall F, G \in k[X,Y]$,

$$F \sim G \Rightarrow F(X,Y) = cG(X,Y) \Rightarrow c^{-1}F(X,Y) = c^{-1}cG(X,Y) \Rightarrow$$
$$c^{-1}F(X,Y) = G(X,Y) \Rightarrow G(X,Y) = dF(X,Y) \Rightarrow G \sim F.$$

(iii) $\sim$ é transitiva: $\forall F, G, H \in k[X,Y]$,

$$F \sim G \text{ e } G \sim H \Rightarrow F(X,Y) = c_1G(X,Y) \text{ e } G(X,Y) = c_2H(X,Y) \Rightarrow$$
$$F(X,Y) = c_1(c_2H(X,Y)) \Rightarrow F(X,Y) = (c_1c_2)H(X,Y) \Rightarrow$$
$$F(X,Y) = c_3H(X,Y) \Rightarrow F \sim H,$$

onde $c_3 = c_1c_2$

□

Definição 4.6. Uma curva algébrica plana afim é uma classe de equivalência de polinômios não constantes $F(X,Y) \in k[X,Y]$, módulo a relação que identifica dois tais polinômios se um é múltiplo do outro por uma constante diferente de zero.

Desta forma, a equação de uma curva algébrica é qualquer um dos polinômios nessa classe.

Definição 4.7. O traço de uma curva algébrica é o conjunto das soluções da equação.

Observação 4.8. Quando $k = \mathbb{R}$ chamamos de *traço real* a curva definida sobre $\mathbb{R}$ que é o conjunto das soluções reais da equação.

Definição 4.9. O grau de uma curva F é o grau do polinômio F que define tal curva, e será denotado por ∂F.

As curvas de grau 1 são chamadas de retas, de grau 2 de cônicas e grau 3, cúbicas.

Definição 4.10. A multiplicidade de uma componente P de F é o expoente com que o fator P ocorre na decomposição de F.

Quando $\partial P \geq 2$, dizemos que P é componente múltipla de F.

Exemplo 4.11. Seja $F(X,Y) = X^3 + 3X^2Y - 4Y^3$ uma curva algébrica com coeficientes em $\mathbb{R}$. Observe que $\partial F = 3$.

Mais ainda, podemos fatorar F em duas componentes irredutíveis:

$$X^3 + 3X^2Y - 4Y^3 = (X + 2Y)^2(X - Y).$$

Tomando $P(X,Y) = (X + 2Y)^2$ e $R(X,Y) = X - Y$, temos que a multiplicidade de P é 2 e a multiplicidade de R é 1.

Exemplo 4.12. Seja $G(X,Y) = 16X^3 - 32X^2Y + 8X^2Y^2 - 16XY^3 + XY^4 - 2Y^5$ uma curva algébrica com coeficientes em $\mathbb{R}$. Observe que $\partial G = 5$.

Mais ainda, podemos fatorar G em duas componentes irredutíveis:

$$16X^3 - 32X^2Y + 8X^2Y^2 - 16XY^3 + XY^4 - 2Y^5 = \left(4X + Y^2\right)^2 (X - 2Y).$$

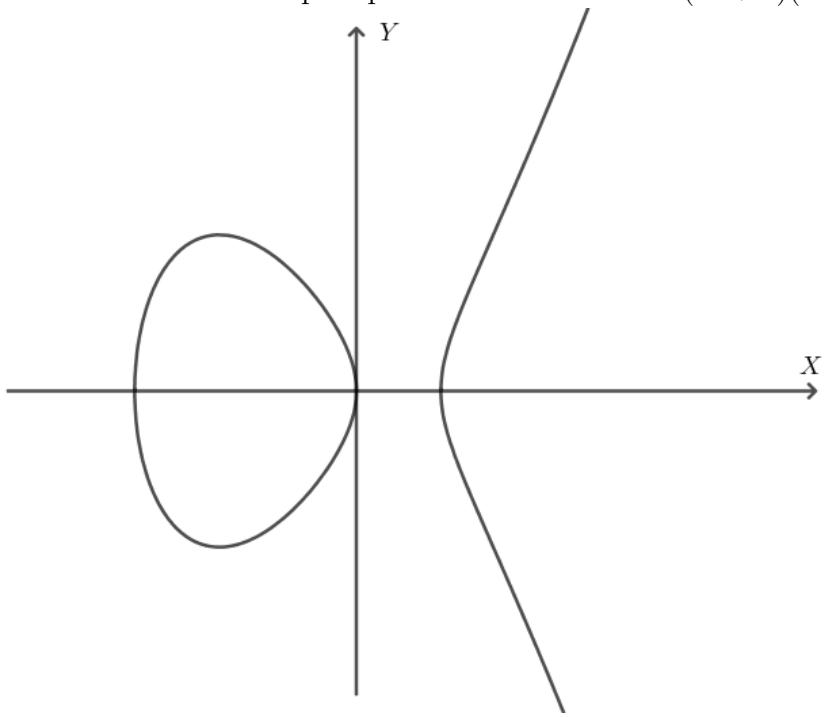
Tomando $U(X,Y) = (4X + Y^2)^2$ e $V(X,Y) = X - 2Y$, temos que a multiplicidade de U é 4 e a multiplicidade de V é 1.

Observação 4.13. Fazendo um abuso de notação, designaremos pelo mesmo símbolo tanta a curva, quanto seu traço ou sua equação. Também utilizaremos os termos "a curva F" ou "a curva dada pela equação $F = 0$" ou "a curva $F = 0$" como sinônimos. O contexto deixará claro se estamos nos referindo ao traço ou ao polinômio.

Intuitivamente, podemos pensar nas componentes irredutíveis de uma curva F como os "pedaços" que constituem F e também são curvas, ou seja, se F contém o traço de uma curva irredutível P, então P é uma componente irredutível de F. Isso nos foi mostrado na Proposição 4.4. No entanto, é preciso estar atento, pois uma curva pode ser irredutível mesmo que seu traço real seja formado por duas ou mais partes disjuntas, como é o caso da hipérbole ou do exemplo abaixo.

Exemplo 4.14. Seja $F = Y^2 - X(X - a)(X - b)$, com $a, b \in \mathbb{R}$ e $b < 0 < a$.

Figura 4.5: Curva definida pelo polinômio $F = Y^2 - X(X + 2)(X - 1)$.



Fonte: elaborado pela autora (2023)

Apesar de seu traço ser formado partes distintas, F é uma curva irredutível.

A seguir, veremos como obter uma curva a partir de um isomorfismo linear seguido de uma translação.

Definição 4.15. Um referencial, ou sistema de coordenadas afim, no plano k^2 consiste na escolha de um ponto $O \in k^2$ chamado de origem do referencial, e de uma base $\{v_1, v_2\}$ do espaço vetorial k^2.

Definição 4.16. Uma transformação afim, ou afinidade, em k^2 é uma aplicação $T : k^2 \to k^2$ composta de uma translação em um isomorfismo linear.

Definição 4.17. O k-automorfismo do anel de polinômios em 2 variáveis

$$T_\bullet : k[X_1, X_2] \to k[X_1, X_2]$$

associado à afinidade $T : k^2 \to k^2$ é dado por:

$$\forall (x_1, x_2) \in k^2,\ (T_\bullet F)(x_1, x_2) = F(T^{-1}(x_1, x_2)).$$

Mais precisamente, se

$$T^{-1}(x_1, x_2) = (b_{11}x_1 + b_{12}x_2 + b_1,\ b_{21}x_1 + b_{22}x_2 + b_2),$$

então

$$(T_\bullet F)(X_1, X_2) = (b_{11}X_1 + b_{12}X_2 + b_1,\ b_{21}X_1 + b_{22}X_2 + b_2).$$

Observação 4.18. Note que, dessa definição, podemos afirmar que se F é uma curva e T um afinidade, então o traço de $T_\bullet F$ é igual à imagem do traço de F por T.

Exemplo 4.19. Tomemos $T : \mathbb{R}^2 \to \mathbb{R}^2$ definida por $T(x_1, x_2) = (y_1, y_2)$, onde y_1 e y_2 são dados por:

$$\begin{cases} y_1 = 2x_1 - 3x_2 + 1 \\ y_2 = -2x_1 + 4x_2 + 0 \end{cases}$$

Observe que

$$\begin{vmatrix} 2 & -3 \\ -2 & 4 \end{vmatrix} = 2 \neq 0$$

e, portanto, pela Definição 4.16, T é uma afinidade.

Calculando $T^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ dada por $T^{-1}(y_1, y_2) = (z_1, z_2)$, obtemos:

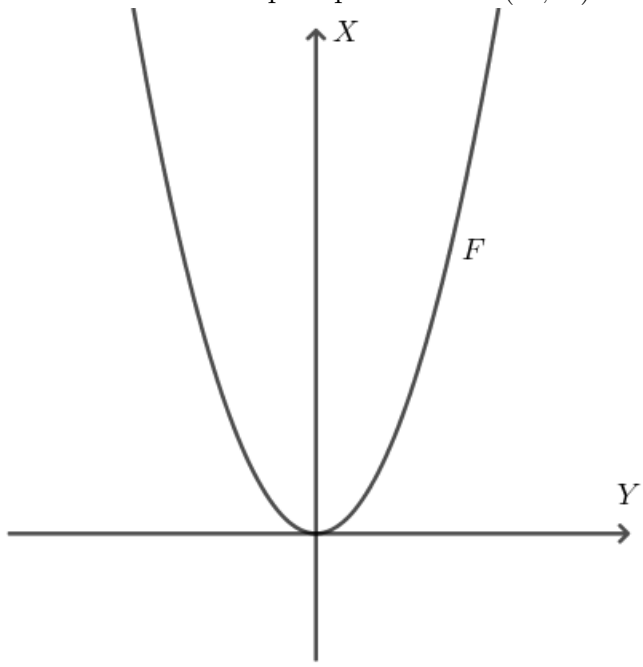
$$\begin{cases} z_1 = 2y_1 + \dfrac{3}{2}y_2 - 2 \\ z_2 = y_1 + y_2 - 1 \end{cases}$$

Tomemos agora $F(X, Y) = X^2 - Y$ e calculemos $T_\bullet F$:

$$\begin{aligned} T_\bullet F(X, Y) = F(T^{-1}(X, Y)) = F\left(2X + \frac{3}{2}Y - 2\right) &= \left(2X + \frac{3}{2}Y - 2\right)^2 - (X + Y - 1) \\ &= 4X^2 + \frac{9}{4}Y^2 + 6XY - 9X - 7Y + 5. \end{aligned}$$

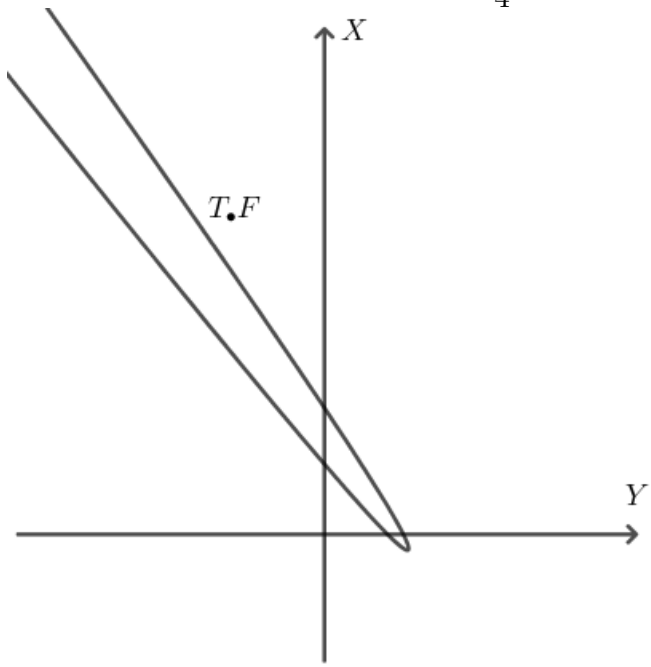
Com relação ao traço, observe os traços de F e $T_\bullet F$, em específico, note a relação entre os traços apontada pela Observação 4.18.

Figura 4.6: Curva definida pelo polinômio $F(X,Y) = X^2 - Y$.



Fonte: elaborado pela autora (2023)

Figura 4.7: Curva definida por $T_\bullet F(X,Y) = 4X^2 + \frac{9}{4}Y^2 + 6XY - 9X - 7Y + 5$.



Fonte: elaborado pela autora (2023)

Agora, estudaremos a interseção de curvas planas. O interesse principal nesse estudo é fornecer soluções geométricas a equações algébricas por meio de interseção de curvas do menor grau possível.

Proposição 4.20. *Sejam $F, G \in k[X,Y]$ polinômios sem fatores irredutíveis em comum.*

Então existe uma relação

$$aF + bG = c(X)$$

onde $a, b \in k[X, Y]$, e c é um polinômio apenas na variável X, não nulo. O resultado é análogo se trocarmos X por Y.

Demonstração. Seja $A = k[X]$ e L o corpo de frações de A. Consideremos F e G como elementos de $L[Y]$. Como F e G não possuem fatores em comum em $A[Y]$, então também não o possuem em $L[Y]$, pelo Corolário 2.115. Consequentemente, o mdc é 1, já que não há fatores em comum. Como $L[Y]$ é um domínio de ideais principais (pelo Teorema 2.101) e o mdc entre F e G é 1, segue do Corolário 2.104, que existem $r, s \in L[Y]$, tais que:

$$rF + sG = 1 \text{ em } L[Y].$$

Eliminando os denominadores de r e s, obtemos a relação desejada. □

É interessante que relembremos agora a Proposição 3.46, que dizia: "*Se F e G são polinômios em $k[X, Y]$ sem fatores comuns, então $V(F, G)$ é um conjunto finito de pontos. É válido lembrar que $V(F, G) = V(F) \cap V(G)$, pela Observação 3.6*". Em outras palavras:

Proposição 4.21. *O conjunto das soluções de um sistema de duas equações polinomiais a duas incógnitas sem fator irredutível em comum é finito, ou seja, a interseção de duas curvas algébricas planas sem componentes em comum é finita.*

Demonstração. Vide Proposição 3.46. □

Agora, abordaremos o conceito de multiplicidade. Primeiramente, temos o fato de que todo polinômio de grau n, em um corpo algebricamente fechado, em uma variável, possui n raízes. Intuitivamente, a multiplicidade indica a quantidade de vezes que as raízes coincidem com um mesmo valor. Nossa ideia agora é dar sentido à ideia de uma curva passar repetidas vezes por um mesmo ponto.

Primeiro, analisaremos a interseção de uma curva e uma reta, nesse sentido, apresentamos a seguir o processo para determinar os pontos dessa interseção:

Sejam F uma curva e ℓ uma reta de equação $Y = aX + b$, defina:

$$F_\ell(X) := F(X, aX + b) = 0.$$

Para obter os pontos da interseção $F \cap \ell$ precisamos resolver a equação acima. Assim, obteremos as seguintes possibilidades:

(i) $F_\ell = 0$, caso ℓ seja uma componente de F.

(ii) $F_\ell = t$, onde t é uma constante não nula, caso $F \cap \ell = \emptyset$.

(iii) F_ℓ é um polinômio não constante, que se decompõe na forma:

$$F_\ell(X) = c \prod_{i=1}^{r} (X - x_i)^{m_i},$$

onde c é uma constante e x_i são as abscissas (duas a duas distintas) dos pontos de interseção. Isso se dá quando $X = cY + d$.

Observação 4.22. Pode-se mostrar que os inteiros m_i independem do referencial afim.

Definição 4.23. A multiplicidade, ou índice de interseção de ℓ e F, no ponto P é dada por:

$$\begin{cases} 0, & \text{se } P \notin \ell \cap F \\ \infty, & \text{se } P \in \ell \subset F \\ m_i, & \text{se } P = (x_i, ax_i + b), \text{ (como no caso } \textit{(iii)}) \end{cases}.$$

Se $\ell \subsetneqq F$, chamamos o inteiro

$$m_\infty := \partial F - \sum_{i=1}^{r} m_i$$

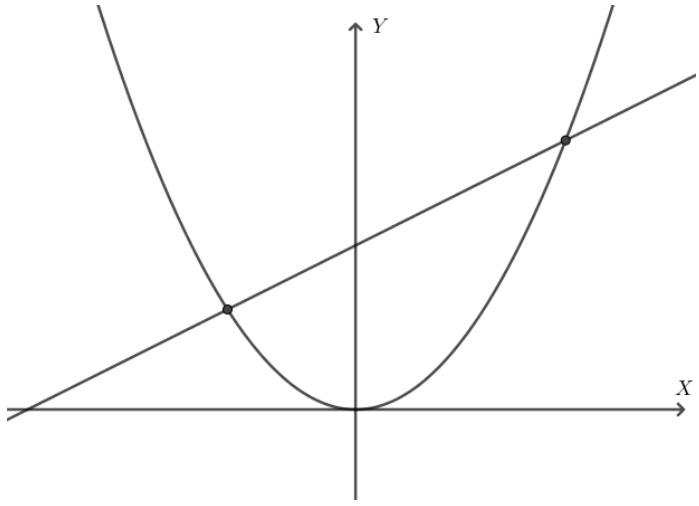
de multiplicidade de interseção de ℓ e F no ponto impróprio, ou ponto de interseção de ℓ no infinito.

Exemplo 4.24. Seja $F = Y - X^2$.

Primeiramente, tomemos a reta $\ell : Y = \dfrac{X}{2} + 1$. Note que a reta possui duas interseções com a curva e, deste modo, $F_\ell(X)$ é um polinômio constante:

$$F_\ell(X) = F\left(X, \frac{X}{2} + 1\right) = \frac{X}{2} + 1 - X^2 = 0.$$

Figura 4.8: Interseção definida pela curva $F = Y - X^2$ e reta $Y = \dfrac{X}{2} + 1$.



Fonte: elaborado pela autora (2023)

Observe que esse polinômio irá zerar nos pontos de interseção da reta com a curva, sendo eles onde $X_1 = \dfrac{1}{4} + \dfrac{\sqrt{17}}{4}$ e $X_2 = \dfrac{1}{4} - \dfrac{\sqrt{17}}{4}$, isto é, nos pontos $\left(\dfrac{1}{4} + \dfrac{\sqrt{17}}{4}, \dfrac{9}{8} + \dfrac{\sqrt{17}}{8}\right)$ e $\left(\dfrac{1}{4} - \dfrac{\sqrt{17}}{4}, -\dfrac{9}{8} - \dfrac{\sqrt{17}}{8}\right)$.

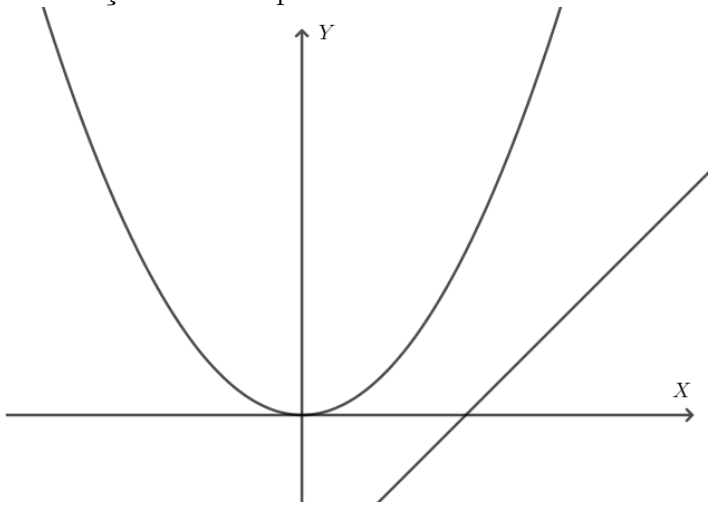
Deste modo, podemos reescrever:

$$F_\ell(X) = \left(X - \frac{1}{4} + \frac{\sqrt{17}}{4}\right)\left(X - \frac{1}{4} - \frac{\sqrt{17}}{4}\right) = 0.$$

Assim, a multiplicidade nesses pontos é um.

Agora, tomemos a reta $\ell : Y = X - 1$. Note que, dessa vez, a reta não possui interseções com a curva. Assim, $F_\ell(X) = t$.

Figura 4.9: Interseção definida pela curva $F = Y - X^2$ e reta $Y = X - 1$.



Fonte: elaborado pela autora (2023)

Veja que:

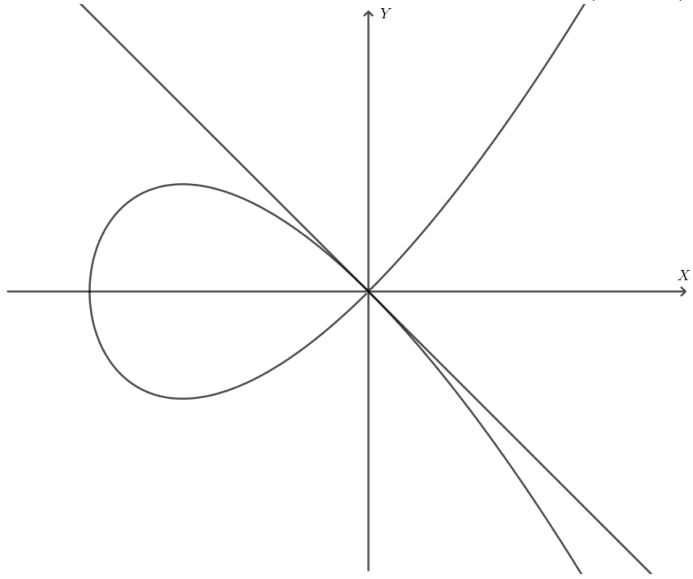
$$F_\ell(X) = f(X, X - 1) = X - 1 - X^2.$$

Observe que para cada valor de X, teremos um diferente resultado, sempre constante, e, ainda assim, $F \cap \ell = \emptyset$. Deste modo, dizemos que $F_\ell(X) = t$ e a multiplicidade é zero.

Exemplo 4.25. Sejam $F = Y^2 - X^2(X + 1)$ e $\ell = Y - aX$.

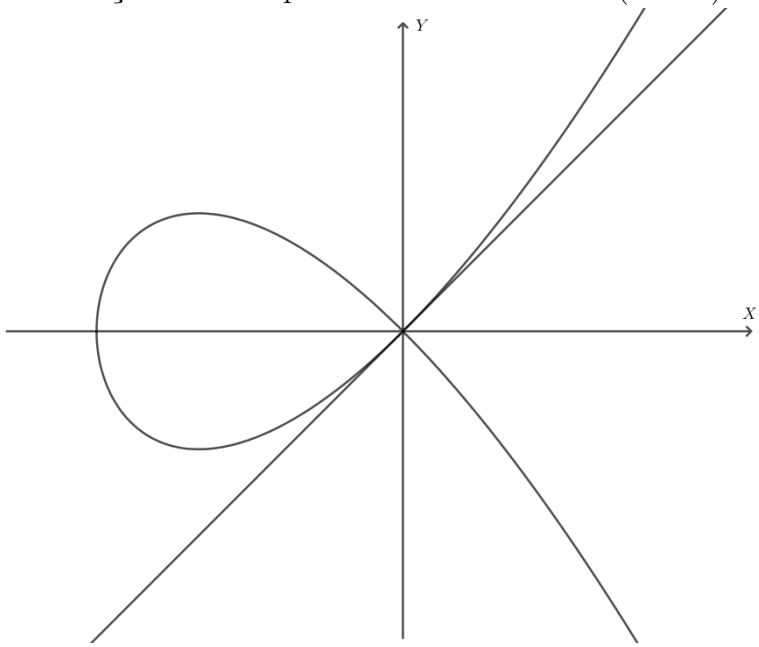
Na origem já há duas interseções. Mais ainda, se $a = \pm 1$, a multiplicidade da origem é 3. Do contrário, teremos a origem com multiplicidade 2 e outro ponto de interseção com multiplicidade 1.

Figura 4.10: Interseção definida pela curva $F = Y^2 - X^2(X + 1)$ e reta $Y + X$.



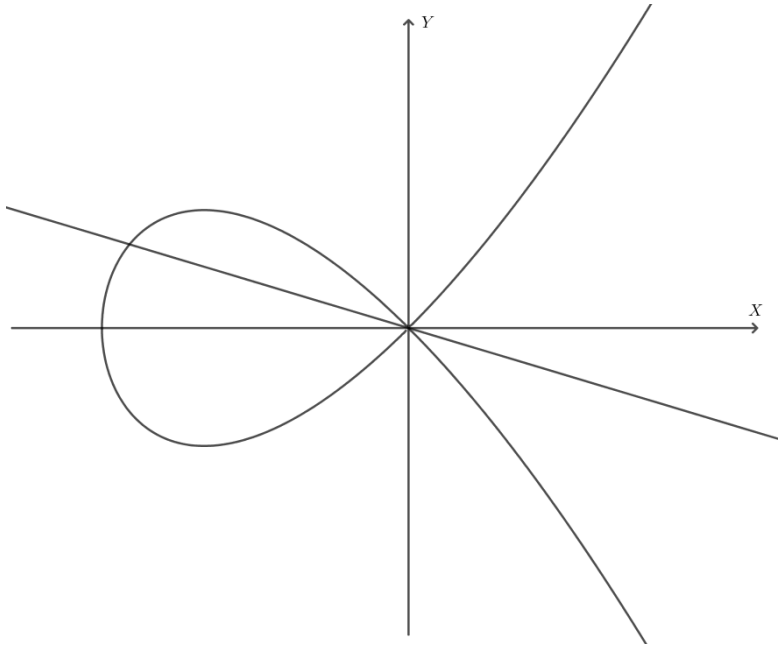
Fonte: elaborado pela autora (2023)

Figura 4.11: Interseção definida pela curva $F = Y^2 - X^2(X+1)$ e reta $Y - X$.



Fonte: elaborado pela autora (2023)

Figura 4.12: Interseção definida pela curva $F = Y^2 - X^2(X+1)$ e reta $Y + \frac{1}{3}X$.



Fonte: elaborado pela autora (2023)

Observação 4.26. Denotamos a multiplicidade de P, ou índice de interseção de ℓ e F em P, por $(\ell, F)_P$.

Proposição 4.27. *Sejam F uma curva e P um ponto de F. Existe um inteiro $m = m_P(F) \geq 1$, tal que, para toda reta ℓ passando por P, temos*

$$(\ell, F)_P \geq m,$$

ocorrendo a igualdade no caso de m retas e a desigualdade estrita para no máximo $m-1$ retas e no mínimo uma reta.

Demonstração. Considere o ponto em F como sendo O a origem, sem perda de generalidade. Podemos escrever, pela Observação 2.95,

$$F = F_m + \cdots + F_d,$$

com F_i homogêneo de grau i, para $m \leq i \leq d$ e $F_m \neq 0$.

Como $O \in F$, temos que $m \geq 1$. Podemos supor que $X \nmid F_m$. Observe que

$$F(0, Y) = Y^m(F_m(0, 1) + \cdots + F_d(0, 1)Y^{d-m})$$

e $F_m(0, 1) \neq 0$. Logo, $(X, F)_O = m$. Para as demais retas passando por O, façamos $\ell_t = Y - tX$. Temos então,

$$F(X, tX) = X^m(F_m(1, t) + F_{m+1}(1, t)X + \cdots + F_d(1, t)X^{d-m}).$$

Deduzimos que

$$(\ell_t, F)_O \geq m,$$

ocorrendo igualdade se, e somente se, $F_m(1, t) \neq 0$. Como $X \nmid F_m$, segue-se que $F_m(1, t)$ é um polinômio em t grau m (≥ 1) e que, portanto, se anula para ao menos um e no máximo m valores de t distintos. □

Para ilustrar os objetos utilizados na demonstração anterior, em cada etapa, apresentamos o exemplo a seguir:

Exemplo 4.28. Seja $F(X, Y) = X^2Y^3 + XY^4 + 3Y^4 + 2Y^3 + 8X^3Y + X^4Y^3 + XY^2$. Observe que podemos reescrevê-lo como

$$F = (2Y^3 + XY^2) + (3Y^4 + 8X^3Y) + (XY^4 + X^2Y^3) + (X^4Y^3),$$

isto é, $F_3 = 2Y^3 + XY^2$, $F_4 = 3Y^4 + 8X^3Y$, $F_5 = XY^4 + X^2Y^3$ e $F_7 = X^4Y^3$.

Note que $F(0, Y) = 2Y^3 + 3Y^4$.

Calculemos agora a seguinte expressão:

$$Y^3(F_3(0, 1) + F_4(0, 1)Y + F_5(0, 1)Y^2 + F_6(0, 1)Y^3 + F_7(0, 1)Y^4).$$

Assim,

- $F_3(0, 1) = 2$
- $F_4(0, 1) = 3$
- $F_5(0, 1) = 0$

- $F_6(0,1) = 0$
- $F_7(0,1) = 0$

Assim, a expressão de torna

$$Y^3(2 + 3Y + 0Y^2 + 0Y^3 + 0Y^4) = Y^3(2 + 3Y) = 2Y^3 + 3Y^4.$$

Portanto, temos que

$$F(0,Y) = Y^3(F_3(0,1) + F_4(0,1)Y + F_5(0,1)Y^2 + F_6(0,1)Y^3 + F_7(0,1)Y^4).$$

Observe que $F_3(0,1) = 2 \neq 0$. Logo, $(X,F)_O = 3$.

Definição 4.29. O inteiro $m = m_P(F)$, descrito na proposição anterior, é a multiplicidade do ponto P na curva F (ou multiplicidade de P em F).

Definição 4.30. Dizemos que um ponto P de uma curva F é *liso* (ou *não singular*, ou *simples*, ou *suave*) em F e que F é *lisa* (ou *não singular*, ou *simples*, ou *suave*) em P se $m_P(F) = 1$.

Se $m_P(F) \neq 1$, então dizemos que P é *singular* em F e F é *singular* em P.

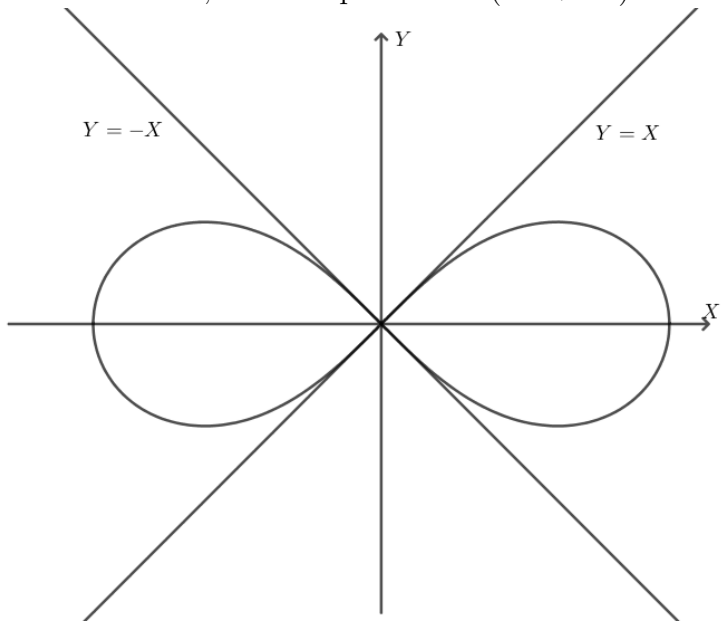
Se $m_P(F) = 2, 3, \cdots, n$, P é dito duplo, triplo, $\cdots$, n-uplo.

Definição 4.31. Um ponto n-uplo $P \in F$ é dito *ordinário* se admitir n tangentes distintas no ponto P.

Definição 4.32. Definimos por *cúspide* um ponto duplo com tangentes coincidentes, e definimos por *nó* um ponto duplo ordinário.

Exemplo 4.33. A lemniscata $(X^2 + Y^2)^2 - X^2 + Y^2 = 0$ apresenta um nó na origem, com tangentes $Y = \pm X$.

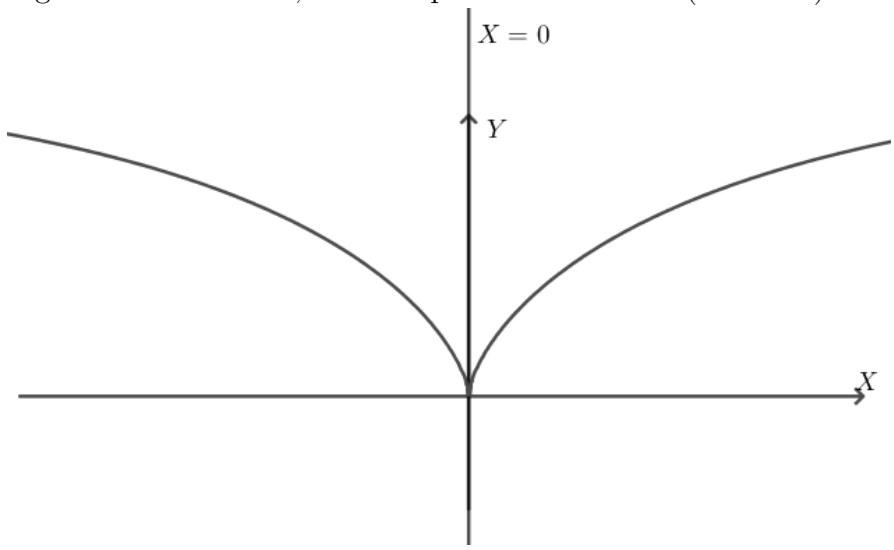
Figura 4.13: Lemniscata, definida pela curva $(X^2 + Y^2)^2 - X^2 + Y^2 = 0$.



Fonte: elaborado pela autora (2023)

Exemplo 4.34. A cissoide $X^2 - Y(Y^2 + X^2) = 0$ possui cúspide na origem com tangente vertical $X = 0$.

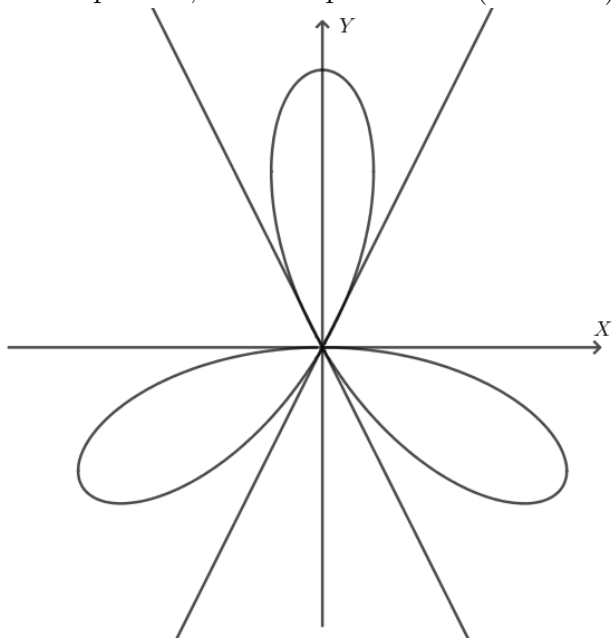
Figura 4.14: Cissoide, definida pela curva $X^2 - Y(Y^2 + X^2) = 0$.



Fonte: elaborado pela autora (2023)

Exemplo 4.35. A rosácea de 3 pétalas, $(X^2+Y^2)^2 - Y^3 + 3X^2Y = 0$ possui ponto triplo ordinário na origem.

Figura 4.15: Rosácea de 3 pétalas, definida pela curva $(X^2 + Y^2)^2 - Y^3 + 3X^2Y = 0$.



Fonte: elaborado pela autora (2023)

Com esse capítulo, finalizamos esse trabalho e observamos que foram necessários desde elementos prévios, como a estrutura algébrica de anel de polinômios, e, de modo implícito, da Teoria de Corpos e Álgebra Linear, bem como ferramentas clássicas da Geometria Algébrica, como os conjuntos algébricos e o Teorema de Hilbert's Nullstellensatz, para explorar exemplos importantes na área, que impactaram outras linhas de pesquisa, como a Teoria de Singularidades, Sistemas Dinâmicos e Criptografia.

5 Conclusão

Percebemos, ao longo do desenvolvimento deste trabalho, que os conceitos matemáticos são cumulativos e necessários para o prosseguimento do estudo. Iniciamos nosso estudo com as noções iniciais de anéis e ideais, aprofundando posteriormente nos conceitos de anéis de polinômio, domínio de ideais principais (PID), domínio de fatoração única (UFD) e corpo, ambos conceitos necessários para nosso próximo conceito. Em seguida, abordamos as definições e propriedades dos conjuntos algébricos, extremamente necessários para a Geometria Algébrica e, em particular para esse trabalho, as Curvas Planas Algébricas.

Durante nosso estudo sobre os conjuntos algébricos, abordamos conceitos relevantes como o ideal de um conjunto de pontos, o Teorema da Base de Hilbert, componentes irredutíveis de um conjunto algébrico e o Hilbert's Nullstellensatz (Teorema dos Zeros de Hilbert). Todos esses conceitos nos permitem avançar no estudo dos elementos da Geometria Algébrica, utilizando-os diretamente para prosseguir com nosso estudo, contribuindo imediatamente para a compreensão de novos conceitos, ou para a demonstração de proposições e teoremas que afetam diretamente nosso avanço pela Geometria Algébrica.

Por fim, estudamos de forma mais aprofundada as Curvas Planas Algébricas, que possibilitam uma generalização do estudo de curvas planas na Geometria, de forma geral, mas especialmente para a Geometria Algébrica. É nesse momento que desenvolvemos os conceitos necessários para o estudo das Curvas Algébricas Planas, salientando as definições e propriedades necessárias para a classificação e estudo desse conceito.

Salientamos a necessidade do estudo dos conceitos básicos da Geometria Algébrica, como os Conjuntos Algébricos, para uma melhor contextualização e compreensão dos conceitos mais avançados, como as Curvas Planas Algébricas. Vale ressaltar que as Curvas Planas Algébricas são importantes na área da Geometria Algébrica e impacta diretamente outras linhas de pesquisa, como a Teoria de Singularidades, Sistemas Dinâmicos e Criptografia.

Referências

[1] FRALEIGH, J. B. *A First Course in Abstract Algebra*. 7. ed. Massachusetts: Addison-Wesley, 2002.

[2] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 2. ed. São Paulo: Atual Editora, 1982.

[3] ATIYAH, M. F.; MACDONALD, G. I. *Introduction to Commutative Algebra*. 1. ed. Massachusetts: Addison-Wesley, 1969.

[4] FULTON, W. *Algebraic Curves: an introduction to Algebraic Geometry*. 3. ed. Nova York: W.A. Benjamin, 2008.

[5] VEINSENCHER, I. *Introdução às Curvas Algébricas Planas*. 1. ed. Rio de Janeiro: IMPA, 1979.

[6] BRIESKORN, E.; KNöRRER, H. *Plane Algebraic Curves*. [S.l.]: Springer, 1986.

[7] GARZA, Z. *A History of Algebraic Geometry*. Publicado em 2020 em: <https://bit.ly/AHistoryofAlgebraicGeometry>, último acesso em 31 jan. 2024.

[8] GEOGEBRA. *Software GeoGebra*. Publicado em 2016 em: <https://www.geogebra.org/>, último acesso em 12 mar. 2024.