



Universidade Federal de Uberlândia
Faculdade de Matemática

Bacharelado em Matemática

**PRIMEIROS PASSOS EM TEORIA DE
MÓDULOS E VARIEDADES
ALGÉBRICAS AFINS**

Gabriel Eurípedes de Jesus Farias

Uberlândia-MG

2018

Gabriel Eurípedes de Jesus Farias

**PRIMEIROS PASSOS EM TEORIA DE
MÓDULOS E VARIEDADES
ALGÉBRICAS AFINS**

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

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann

**Uberlândia-MG
2018**



**Universidade Federal de Uberlândia
Faculdade de Matemática**

Coordenação do Curso de Bacharelado em Matemática

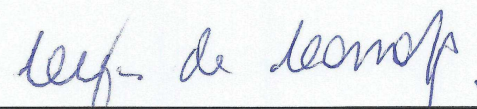
A banca examinadora, conforme abaixo assinado, certifica a adequação deste trabalho de conclusão de curso para obtenção do grau de Bacharel em Matemática.

Uberlândia, 13 de dezembro de 2018.

BANCA EXAMINADORA



Prof. Dr. Victor Gonzalo Lopez Neumann



Prof. Dr. Cícero Fernandes de Carvalho



Prof. Dr. Neiton Pereira da Silva

Uberlândia-MG

2018

AGRADECIMENTOS

Primeiramente, agradeço a Deus por me fornecer força, saúde e boas oportunidades durante esta jornada. Agradeço aos meus pais por me concederem cuidado, carinho e apoio nos estudos. Agradeço a todos os meus amigos pela companhia ao longo desta jornada, na qual compartilhamos experiências e diversos momentos.

Agradeço a todos os meus professores pelos ensinamentos e conselhos. Em particular, agradeço ao meu orientador, Victor Gonzalo Lopez Neumann, por guiar-me nos estudos com sua experiência, paciência e dedicação ao longo desses três anos e meio de orientação. Agradeço também aos professores Cícero Fernandes de Carvalho e Neiton Pereira da Silva por participarem da banca examinadora do presente trabalho e por suas sugestões para o aperfeiçoamento do mesmo.

Por fim, agradeço ao PICME-CNPq por me conceder a oportunidade de realizar iniciação científica e o apoio financeiro durante a graduação.

RESUMO

Neste trabalho, construiremos o produto tensorial de módulos e demonstraremos que qualquer variedade algébrica afim pode ser decomposta como a união finita de suas componentes irredutíveis. Para fundamentar essas construções, apresentaremos conceitos e resultados básicos de Álgebra Comutativa.

Palavras-chave: Álgebras, módulos, produto tensorial, Teorema da Base de Hilbert, variedades algébricas afins.

ABSTRACT

In this work, we will construct the tensor product of modules and demonstrate that any affine algebraic variety can be decomposed as the finite union of its irreducible components. To substantiate these constructions, we will present basic concepts and results of Commutative Algebra.

Keywords: Algebras, modules, tensor product, Hilbert's Basis Theorem, affine algebraic varieties.

SUMÁRIO

1	Introdução	1
2	Fundamentação Teórica	3
2.1	Noções de Teoria de Conjuntos	3
2.2	Noções de Topologia Geral	4
2.3	Noções de Teoria de Anéis	6
2.3.1	Domínios e Corpos	6
2.3.2	Ideais	7
2.3.3	Anel Quociente	8
2.3.4	Domínios Principais e Domínios Fatoriais	9
3	Módulos	11
3.1	Módulos e Homomorfismos de Módulos	11
3.2	Submódulos e Módulos Quocientes	13
3.3	Operações sobre Submódulos	16
3.4	Produto Direto e Soma Direta	18
3.5	Produto Tensorial de Módulos	21
3.6	Álgebras	33
3.7	Produto Tensorial de Álgebras	36
4	Variedades Algébricas Afins	43
4.1	Variedades Algébricas Afins e seus Respetivos Ideais	43
4.2	O Teorema da Base de Hilbert	51
4.3	Decomposição de Variedades em Componentes Irredutíveis	55
5	Conclusões	63
	Referências Bibliográficas	65

1. INTRODUÇÃO

A Geometria Algébrica desempenhou um papel central na Matemática do século XIX, recebendo importantes contribuições de Abel, Klein, Poincaré, Riemann e Weierstrass. Entretanto, na virada do século XX, houve uma grande mudança de atitude em relação a tal área, a qual se distanciou do rigor que determinava o desenvolvimento da Matemática na época.

Essa área conseguiu recuperar o lugar que havia ocupado na Matemática em meados do século XX, quando sua fundamentação ocorreu de forma intensa e grande parte de suas melhores conquistas foram reformuladas de modo rigoroso. Além disso, o domínio de aplicação de suas ideias ampliou-se consideravelmente na direção tanto de variedades algébricas sobre corpos arbitrários quanto de variedades complexas mais gerais.

A Álgebra foi a base para essa reconstrução. A princípio, o emprego de ferramentas algébricas precisas conduziu frequentemente a uma perda do notável estilo geométrico que marcou o período anterior. Contudo, as décadas de 1950 e 1960 trouxeram simplificações à fundação da Geometria Algébrica, a qual alcançou, desse modo, um equilíbrio entre a transparência lógica e a intuição geométrica.

O presente trabalho foi escrito assumindo conhecimentos elementares a respeito de Teoria de Conjuntos, Topologia Geral, Teoria de Grupos e Teoria de Anéis. Alguns tópicos dessas áreas foram abordados, de forma resumida, no segundo capítulo. Assim, o leitor poderá consultar o capítulo “Fundamentação Teórica” para relembrar o enunciado de algum resultado ou conferir o significado de alguma notação.

O terceiro e o quarto capítulos deste trabalho são independentes. No terceiro capítulo, apresentaremos desde conceitos e resultados elementares da Teoria de Módulos até a construção do produto tensorial. No quarto capítulo, trataremos das variedades algébricas afins. Com o auxílio do Teorema da Base de Hilbert, concluiremos que elas são espaços topológicos noetherianos com a topologia de Zariski. Isso será fundamental para mostrarmos que qualquer variedade algébrica afim pode ser decomposta como a união finita de suas componentes irredutíveis.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo reúne alguns pré-requisitos para o presente trabalho. Aqui, poderão ser consultadas definições, notações e proposições que serão frequentemente empregadas ao longo deste trabalho. Este capítulo foi elaborado com base nas referências [1], [2], [3], [4], [5] e [7].

2.1 NOÇÕES DE TEORIA DE CONJUNTOS

Bons livros para o estudo de Teoria de Conjuntos são [3] e [5]. Um dos tópicos abordados nesses livros é a interessante construção do conjunto dos números naturais, que, neste trabalho, será denotado por $\mathbb{N}$ e incluirá o zero como um de seus elementos. E, por falar nesse conjunto, imaginemo-nos com o objetivo de definir uma função h de $\mathbb{N}$ em um conjunto não vazio Γ de modo que tenhamos

$$h(0) = a, \quad h(1) = f(h(0)), \quad h(2) = f(h(1)), \quad h(3) = f(h(2))$$

e assim por diante, onde a é um elemento de Γ e $f: \Gamma \rightarrow \Gamma$ é uma função. O teorema seguinte garante a existência de funções definidas dessa forma.

Teorema 1 (Recursão em $\mathbb{N}$). *Sejam Γ um conjunto, a um elemento de Γ e $f: \Gamma \rightarrow \Gamma$ uma função. Então, existe uma única função $h: \mathbb{N} \rightarrow \Gamma$ tal que $h(0) = a$ e, para todo $n \in \mathbb{N}$, $h(n+1) = f(h(n))$.*

Demonstração. Uma demonstração desse resultado pode ser encontrada em [3, capítulo 4]. $\square$

Lembremos que, dado um conjunto Γ , o conjunto de todos os subconjuntos de Γ é dito **conjunto das partes** de Γ e é denotado por $\mathcal{P}(\Gamma)$. Neste trabalho, acreditaremos no axioma seguinte, o qual garante a existência de uma função que “escolhe” um elemento de cada subconjunto não vazio de qualquer conjunto dado.

Axioma da Escolha. *Para qualquer conjunto Γ , existe uma função $E: \mathcal{P}(\Gamma) \setminus \{\emptyset\} \rightarrow \Gamma$ tal que $E(S) \in S$ para todo subconjunto não vazio $S \subset \Gamma$.*

Definição 1. *Seja Γ um conjunto. Uma relação $\leq$ em Γ será dita uma **ordem parcial** em Γ se for uma relação reflexiva, antissimétrica e transitiva, ou seja, se, para todos $x, y, z \in \Gamma$, tivermos:*

$$(i) \quad x \leq x;$$

(ii) $x \leq y$ e $y \leq x$ implicam $x = y$;

(iii) $x \leq y$ e $y \leq z$ implicam $x \leq z$.

Um **conjunto parcialmente ordenado** é um par $(\Gamma, \leq)$, onde Γ é um conjunto e $\leq$, uma ordem parcial em Γ .

Seja $(\Gamma, \leq)$ um conjunto parcialmente ordenado e $\mathcal{C}$ um subconjunto de Γ . Diremos que $\mathcal{C}$ é uma **cadeia** em Γ se quaisquer dois de seus elementos forem comparáveis, isto é, se $x, y \in \mathcal{C}$, então $x \leq y$ ou $y \leq x$. Uma **cota superior** de $\mathcal{C}$ é um elemento $s \in \Gamma$ tal que $x \leq s$ para todo $x \in \mathcal{C}$. Um **elemento maximal** de Γ é um elemento $m \in \Gamma$ para o qual $m \leq x$ implica $x = m$ para todo $x \in \Gamma$. Um **elemento minimal** de Γ é um elemento $n \in \Gamma$ para o qual $x \leq n$ implica $x = n$ para todo $x \in \Gamma$. Logicamente, ao acreditarmos no Axioma da Escolha, ganhamos de brinde a validade de sua forma equivalente: o Lema de Zorn.

Lema 1 (Zorn). *Seja $(\Gamma, \leq)$ um conjunto parcialmente ordenado. Se toda cadeia em Γ possuir cota superior, então Γ possuirá um elemento maximal.*

2.2 NOÇÕES DE TOPOLOGIA GERAL

Definição 2. *Seja X um conjunto. Uma **topologia** em X é uma coleção τ de subconjuntos de X , chamados **conjuntos abertos**, com as propriedades seguintes:*

- (i) $\emptyset \in \tau$ e $X \in \tau$ (vazio e todo o espaço são conjuntos abertos);
- (ii) se $U, V \in \tau$, então $U \cap V \in \tau$ (interseção finita de conjuntos abertos é também um conjunto aberto);
- (iii) se $(U_\lambda)_{\lambda \in \Lambda}$ for uma família de elementos de τ , então $\bigcup_{\lambda \in \Lambda} U_\lambda \in \tau$ (união arbitrária de conjuntos abertos é também um conjunto aberto).

Um **espaço topológico** é um par (X, τ) , onde X é um conjunto e τ , uma topologia em X .

Observação 1. *Geralmente, referiremos ao próprio conjunto X como um espaço topológico.*

Consideremos um espaço topológico X e um ponto $x \in X$. Uma **vizinhança aberta** de x é qualquer conjunto aberto contendo x . Notemos que um subconjunto $U \subset X$ será um conjunto aberto em X se, e somente se, todo ponto de U possuir alguma vizinhança aberta contida em U . Um subconjunto $F \subset X$ será dito **conjunto fechado** se seu complementar $X \setminus F$ for um conjunto aberto. Consequentemente:

- (i) $\emptyset$ e X são conjuntos fechados;
- (ii) se F e G forem conjuntos fechados, então a união $F \cup G$ será também um conjunto fechado;

(iii) se $(F_\lambda)_{\lambda \in \Lambda}$ for uma família qualquer de conjuntos fechados, então a interseção $\bigcap_{\lambda \in \Lambda} F_\lambda$ será também um conjunto fechado.

Seja S um subconjunto de X . O menor conjunto fechado de X que contém S é chamado **fecho** de S e é denotado por $\overline{S}$. Se $\overline{S} = X$, então diremos que S é **denso** em X . O lema seguinte convence-nos do fato de que o fecho de S é o conjunto dos pontos de X que estão “arbitrariamente próximos” de S .

Lema 2. *Seja X um espaço topológico. Se S for um subconjunto de X , então*

$$\overline{S} = \{x \in X; \text{ toda vizinhança aberta de } x \text{ possui interseção não vazia com } S\}.$$

Demonstração. Denotemos o conjunto

$$\{x \in X; \text{ toda vizinhança aberta de } x \text{ possui interseção não vazia com } S\}$$

por F . Evidentemente, $S \subset F$.

Primeiramente, mostremos que F é um conjunto fechado em X . Se $x \in X \setminus F$, então existirá uma vizinhança aberta U de x tal que $U \cap S = \emptyset$ e, conseqüentemente, $U \subset X \setminus F$. Assim, $X \setminus F$ é um conjunto aberto em X .

Agora, já sabemos que F é um conjunto fechado contendo S e, logo, resta mostrarmos que F é o menor subconjunto de X com essa propriedade. Seja G um conjunto fechado em X tal que $S \subset G$. Com isso, dado um ponto $y \in X \setminus G$, o próprio conjunto $X \setminus G$ é uma vizinhança aberta de y satisfazendo $(X \setminus G) \cap S = \emptyset$ e, conseqüentemente, $y \in X \setminus F$. Assim, $X \setminus G \subset X \setminus F$ ou, de modo equivalente, $F \subset G$. Isso torna a prova completa. $\square$

Proposição 1. *Seja X um espaço topológico e sejam A e B subconjuntos de X .*

1. $\overline{A \cup B} = \overline{A} \cup \overline{B}$.
2. $\overline{A \cap B} \subset \overline{A} \cap \overline{B}$.

Demonstração.

1. É fácil ver que a união $\overline{A} \cup \overline{B}$ é um conjunto fechado em X contendo $A \cup B$. Logo, $\overline{A \cup B} \subset \overline{A} \cup \overline{B}$.

Sejam $a \in \overline{A} \cup \overline{B}$ e U uma vizinhança aberta de a . Visto que $a \in \overline{A}$ ou $a \in \overline{B}$, temos $U \cap A \neq \emptyset$ ou $U \cap B \neq \emptyset$. Em ambos os casos, temos $U \cap (A \cup B) \neq \emptyset$. Pelo Lema 2, $a \in \overline{A \cup B}$ e concluímos que $\overline{A \cup B} = \overline{A} \cup \overline{B}$.

2. Claramente, a interseção $\overline{A \cap B}$ é um fechado contendo $A \cap B$. Visto que $\overline{A \cap B}$ é o menor subconjunto de X com essa propriedade, $\overline{A \cap B} \subset \overline{A} \cap \overline{B}$.

$\square$

Observação 2. *Notemos que a inclusão $\overline{A} \cap \overline{B} \subset \overline{A \cap B}$ não é válida em geral. Por exemplo, consideremos o espaço topológico $X = \mathbb{R}$ com a topologia usual e seus subconjuntos $A = (0, 1)$ e $B = (1, 2)$. Nesse caso, $\overline{A} \cap \overline{B} = [0, 1] \cap [1, 2] = \{1\}$, enquanto $\overline{A \cap B} = \overline{\emptyset} = \emptyset$.*

Seja (X, τ) um espaço topológico. Se Y for um subconjunto de X , a coleção

$$\tau_Y := \{Y \cap U; U \in \tau\}$$

será uma topologia em Y , a chamada **topologia induzida**. Por consequência, os conjuntos fechados em Y são da forma $Y \cap F$, onde F é um conjunto fechado em X .

Claramente, a teoria sobre espaços topológicos apresentada aqui é apenas uma parte ínfima da Topologia Geral, porém suficiente para o escopo do presente trabalho. Mais informações a respeito dos espaços topológicos podem ser consultadas em [4].

2.3 NOÇÕES DE TEORIA DE ANÉIS

No presente trabalho, o termo **anel** significará sempre anel comutativo com unidade. Além disso, se A e B forem anéis, um **homomorfismo de anéis** $\phi: A \rightarrow B$ deverá sempre satisfazer $\phi(1_A) = 1_B$, além de preservar somas e produtos. Denotaremos o anel dos polinômios nas variáveis $X_1, \dots, X_n$ com coeficientes em A por $A[X_1, \dots, X_n]$.

2.3.1 DOMÍNIOS E CORPOS

Seja A um anel. Um elemento $a \in A$ será chamado:

1. **invertível** se existir $b \in A$ tal que $ab = 1$;
2. **divisor de zero** se existir $b \in A \setminus \{0\}$ tal que $ab = 0$.

O conjunto dos elementos invertíveis em A , com o produto de A , é um grupo abeliano denotado por $A^\times$. Agora, suponhamos que o anel A possua pelo menos dois elementos. Diremos que A é:

1. um **corpo** se todos os seus elementos não nulos forem invertíveis;
2. um **domínio** se 0 for o único divisor de zero em A .

É fácil ver que todo corpo é um domínio. E se D for um domínio, poderemos construir um importante corpo “contendo” D : o **corpo de frações** $\text{Frac}(D)$ de D .

Sobre o conjunto $D \times (D \setminus \{0\})$, definamos a relação de equivalência seguinte:

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

para todos $(a, b), (c, d) \in D \times (D \setminus \{0\})$. Denotando a classe de equivalência de cada par $(a, b) \in D \times (D \setminus \{0\})$ por $\frac{a}{b}$, o corpo $\text{Frac}(D)$ é o conjunto das classes de equivalência com as

operações

$$\begin{aligned} +: \text{Frac}(D) \times \text{Frac}(D) &\rightarrow \text{Frac}(D) & \cdot: \text{Frac}(D) \times \text{Frac}(D) &\rightarrow \text{Frac}(D) \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ad+bc}{bd} & \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ac}{bd}. \end{aligned}$$

Notemos que D pode ser visto como um subanel de seu corpo de frações por meio do homomorfismo injetor de anéis

$$\begin{aligned} \phi: D &\rightarrow \text{Frac}(D) \\ a &\mapsto \frac{a}{1}. \end{aligned}$$

Se K for um corpo, o corpo de frações do domínio $K[X_1, \dots, X_n]$ será denotado por $K(X_1, \dots, X_n)$.

2.3.2 IDEAIS

Seja A um anel. Diremos que um subconjunto não vazio $I \subset A$ é um **ideal** de A se I for fechado por combinações A -lineares, isto é, se tivermos $ax + by \in I$ para todos $a, b \in A$ e $x, y \in I$.

Exemplo 1. *Seja $\phi: A \rightarrow B$ um homomorfismo de anéis. Claramente, $\phi(0) = 0$. Além disso, se k_1 e k_2 forem elementos de A tais que $\phi(k_1) = 0$ e $\phi(k_2) = 0$, então*

$$\phi(a_1k_1 + a_2k_2) = \phi(a_1)\phi(k_1) + \phi(a_2)\phi(k_2) = \phi(a_1) \cdot 0 + \phi(a_2) \cdot 0 = 0$$

para todos $a_1, a_2 \in A$. Assim, o conjunto $\phi^{-1}(\{0\})$ é um ideal de A . Ele é chamado **núcleo** de ϕ e é denotado por $\text{Ker}(\phi)$.

Consideremos um subconjunto S de um anel A . O conjunto de todas as combinações lineares de elementos de S com coeficientes em A

$$\{a_1s_1 + \dots + a_rs_r; r \in \mathbb{N} \setminus \{0\}, a_i \in A \text{ e } s_i \in S\}$$

é o menor ideal de A que contém S , o qual é chamado **ideal gerado** por S . No caso em que S for finito, digamos, $S = \{s_1, \dots, s_n\}$, o ideal gerado por S será denotado por $(s_1, \dots, s_n)$.

Definição 3. *Sejam A um anel e I um ideal de A . Diremos que I é **finitamente gerado** se existirem $n \in \mathbb{N} \setminus \{0\}$ e $a_1, \dots, a_n \in A$ satisfazendo $I = (a_1, \dots, a_n)$. Em particular, se existir $a \in A$ tal que $I = (a)$, diremos que I é um **ideal principal**.*

Sejam I e J ideais de um anel A e $(I_\lambda)_{\lambda \in \Lambda}$ uma família de ideais de A . É fácil ver que a **interseção** $I \cap J$ é um ideal de A . A seguir, definiremos mais algumas “operações” com ideais.

1. O ideal gerado pela união $\bigcup_{\lambda \in \Lambda} I_\lambda$ recebe o nome de **soma** da família $(I_\lambda)_{\lambda \in \Lambda}$ e é denotado

por $\sum_{\lambda \in \Lambda} I_\lambda$. Por consequência,

$$\sum_{\lambda \in \Lambda} I_\lambda = \{a_{\lambda_1} + \cdots + a_{\lambda_r}; r \in \mathbb{N} \setminus \{0\}, \lambda_i \in \Lambda \text{ e } a_{\lambda_i} \in I_{\lambda_i}\}.$$

2. O ideal gerado por todos os produtos da forma ab , onde $a \in I$ e $b \in J$, é denotado por IJ e dito **produto** de I e J . Explicitamente,

$$IJ = \{a_1b_1 + \cdots + a_rb_r; r \in \mathbb{N} \setminus \{0\}, a_i \in I \text{ e } b_i \in J\}.$$

3. O **radical** de I , denotado por $\text{Rad}(I)$, é o seguinte ideal de A :

$$\{a \in A; a^n \in I \text{ para algum } n \in \mathbb{N} \setminus \{0\}\}.$$

No caso em que $I = \text{Rad}(I)$, diremos que I é um **ideal radical**.

Lembremos que um ideal próprio P de A será um **ideal primo** se, para todos $a, b \in A$, $ab \in P$ implicar $a \in P$ ou $b \in P$. Claramente, os ideais primos são exemplos de ideais radicais.

2.3.3 ANEL QUOCIENTE

Sejam A um anel e I um ideal de A . Sobre o conjunto A , definamos a relação de equivalência seguinte:

$$a \sim b \Leftrightarrow a - b \in I$$

para todos $a, b \in A$. Representemos o conjunto das classes de equivalência por A/I e denotemos a classe de equivalência de um elemento $a \in A$ por $\bar{a}$. O **anel quociente** de A por I é o conjunto A/I com as operações

$$\begin{aligned} +: A/I \times A/I &\rightarrow A/I & \text{ e } \quad \cdot: A/I \times A/I &\rightarrow A/I \\ (\bar{a}, \bar{b}) &\mapsto \overline{a+b} & (\bar{a}, \bar{b}) &\mapsto \overline{ab}. \end{aligned}$$

Percebamos que A/I com a operação $+$ definida acima é o grupo quociente de A por I .

Exemplo 2. *Seja n um inteiro positivo. O anel quociente de $\mathbb{Z}$ por (n) é o anel dos inteiros módulo n e é denotado por $\mathbb{Z}_n$.*

Se $\phi: A \rightarrow B$ for um homomorfismo sobrejetor de anéis, ele induzirá o isomorfismo

$$\begin{aligned} \bar{\phi}: A/\text{Ker}(\phi) &\rightarrow B \\ \bar{a} &\mapsto \phi(a). \end{aligned}$$

Lembremos que um ideal P de A será primo se, e somente se, o quociente A/P for um domínio. Desse modo, mostrar que P é primo é equivalente a mostrar que existe um homomorfismo sobrejetor de anéis de A em um domínio D cujo núcleo seja P .

2.3.4 DOMÍNIOS PRINCIPAIS E DOMÍNIOS FATORIAIS

Aqui, veremos algumas propriedades de anéis “parecidos” com o anel dos números inteiros.

Definição 4. *Seja D um domínio.*

1. *Dados elementos $a, b \in D$, diremos que b **divide** a em D se existir $c \in D$ tal que $a = bc$. Nesse caso, dizemos também que b é um **fator** de a em D e escrevemos $b|a$.*
2. *Diremos que dois elementos $a, b \in D$ são **associados** em D se existir um elemento $u \in D^\times$ tal que $a = ub$.*
3. *Um elemento não invertível $a \in D \setminus \{0\}$ será **irredutível** em D se possuir apenas fatoração trivial em D , isto é, se $a = bc$ implicar $b \in D^\times$ ou $c \in D^\times$ para todos $b, c \in D$.*
4. *Diremos que um elemento não invertível $p \in D \setminus \{0\}$ é **primo** em D se o ideal (p) for primo, isto é, se $p|ab$ implicar $p|a$ ou $p|b$ para todos $a, b \in D$.*
5. *Dados elementos $a_1, \dots, a_n \in D \setminus \{0\}$, um elemento $d \in D$ será um **máximo divisor comum** de $a_1, \dots, a_n$ se d dividir os elementos $a_1, \dots, a_n$ e se todo elemento $d' \in D$ que divide os elementos $a_1, \dots, a_n$ dividir também d .*

Sejam D um domínio e $a_1, \dots, a_n$ elementos não nulos de D . É fácil ver que se d e d' forem maiores divisores comuns de $a_1, \dots, a_n$, então d e d' serão associados em D . Por termos essa unicidade (a menos de multiplicação por invertíveis) do máximo divisor comum, denotaremos qualquer máximo divisor comum de $a_1, \dots, a_n$ por $\text{mdc}(a_1, \dots, a_n)$.

É fácil ver que se $p \in D$ for primo, então p será também irredutível, mas a recíproca não é válida em geral. Entretanto, nos tipos de domínios que definiremos a seguir, os termos primo e irredutível são sinônimos.

Definição 5. *Seja D um domínio.*

1. *Se todo ideal de D for principal, diremos que D é um **domínio principal**.*
2. *Diremos que D é um **domínio fatorial** se todo elemento não invertível $d \in D \setminus \{0\}$ puder ser escrito como produto de irredutíveis de maneira única a menos da ordem dos fatores e de elementos associados. Em outras palavras, para cada elemento não invertível $d \in D \setminus \{0\}$:*

(i) *existem irredutíveis $p_1, \dots, p_m \in D$ tais que $d = p_1 \cdots p_m$;*

(ii) *se $d = q_1 \cdots q_n$ for outra fatoração de d em irredutíveis $q_1, \dots, q_n$, então $m = n$ e existirá uma permutação $\sigma: \{1, \dots, m\} \rightarrow \{1, \dots, m\}$ tal que p_i é associado a $q_{\sigma(i)}$ para todo $i \in \{1, \dots, m\}$.*

Seja D um domínio fatorial e sejam $a_1, \dots, a_n$ elementos não nulos de D . Notemos que existem $r \in \mathbb{N}$, irredutíveis $p_1, \dots, p_r \in D$ não associados dois a dois, $u_1, \dots, u_n \in D^\times$ e $e_{11}, \dots, e_{1r}, \dots, e_{n1}, \dots, e_{nr} \in \mathbb{N}$ tais que podemos escrever

$$a_j = u_j \prod_{i=1}^r p_i^{e_{ji}}$$

para cada $j \in \{1, \dots, n\}$. Desse modo, existe um máximo divisor comum de $a_1, \dots, a_n$ e

$$\text{mdc}(a_1, \dots, a_n) = \prod_{i=1}^r p_i^{\min\{e_{1i}, \dots, e_{ni}\}}.$$

Vejamos uma importante caracterização dos domínios principais.

Teorema 2. *Um domínio D será principal se, e somente se, D for um domínio fatorial tal que, para todos $a, b \in D \setminus \{0\}$, existem $e, f \in D$ satisfazendo $\text{mdc}(a, b) = ea + fb$.*

Definição 6. *Seja D um domínio fatorial. Um polinômio não nulo $f \in D[X]$ será dito **primitivo** se 1 for um máximo divisor comum de seus coeficientes não nulos, isto é, se não existir um irredutível $p \in D$ que divida todos os seus coeficientes.*

Seja D um domínio fatorial. Dado um polinômio $f \in D[X]$, o lema seguinte estabelece uma relação entre a irredutibilidade de f em $D[X]$ e a irredutibilidade de f em $K[X]$, onde $K = \text{Frac}(D)$.

Lema 3. (Gauss) *Seja D um domínio, K seu corpo de frações e $f \in D[X]$ um polinômio não constante. O polinômio f será irredutível em $D[X]$ se, e somente se, f for primitivo em $D[X]$ e irredutível em $K[X]$.*

Esse lema é muito útil para demonstrar o teorema seguinte.

Teorema 3. (Gauss) *Se D for um domínio fatorial, então $D[X]$ também será um domínio fatorial.*

Observação 3. *Em particular, se K for um corpo, então $K[X_1, \dots, X_n]$ será um domínio fatorial.*

As demonstrações do Teorema 2, do Lema de Gauss e do Teorema de Gauss podem ser consultadas em [4, capítulo 2]. De modo geral, os livros [1] e [4] são boas referências para aprofundar o conhecimento a respeito de anéis.

3. MÓDULOS

Definidos em conversas cotidianas informais como “espaços vetoriais sobre algum anel”, os módulos são as estrelas deste capítulo. Aqui, veremos suas propriedades elementares e construiremos o produto tensorial de módulos. Ao final, trataremos, brevemente, das estruturas algébricas “resultantes da fusão de um anel com um módulo”: as álgebras. Neste capítulo, as principais referências utilizadas foram [1] e [2].

3.1 MÓDULOS E HOMOMORFISMOS DE MÓDULOS

Definição 7. *Seja A um anel. Um A -módulo é um par (M, μ) , onde M é um grupo abeliano aditivo e a função*

$$\begin{aligned}\mu: A \times M &\rightarrow M \\ (a, m) &\mapsto am\end{aligned}$$

é uma “multiplicação por escalares” que, para todos $a, b \in A$ e $m, n \in M$, satisfaz às condições seguintes:

- (i) $a(m + n) = am + an$;
- (ii) $(a + b)m = am + bm$;
- (iii) $(ab)m = a(bm)$;
- (iv) $1m = m$.

Observação 4. *Geralmente, omitiremos a “multiplicação por escalares” de um A -módulo, escrevendo simplesmente M para denotar um A -módulo (M, μ) .*

Exemplo 3. *Sejam n um inteiro positivo e A um anel.*

1. *O grupo abeliano aditivo $\mathbb{Z}_n$ com a operação*

$$\begin{aligned}\mu: \mathbb{Z} \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n \\ (r, \bar{s}) &\mapsto \overline{rs}\end{aligned}$$

é um $\mathbb{Z}$ -módulo.

2. *Um ideal I de A é um A -módulo. Em particular, o próprio anel A é um A -módulo.*
3. *O anel de polinômios $A[X_1, \dots, X_n]$ é um A -módulo.*

Definição 8. *Sejam M e N A -módulos. Uma função $\phi: M \rightarrow N$ é dita **homomorfismo de A -módulos** ou **A -linear** se*

$$\phi(am_1 + bm_2) = a\phi(m_1) + b\phi(m_2)$$

para todos $a, b \in A$ e $m_1, m_2 \in M$. O conjunto de todos os homomorfismos de A -módulos de M em N será denotado por $\text{Hom}_A(M, N)$.

Exemplo 4. *Sejam M , N e P A -módulos.*

1. *A função identidade*

$$\begin{aligned} \text{id}_M: M &\rightarrow M \\ m &\mapsto m \end{aligned}$$

é um clássico exemplo de homomorfismo de A -módulos.

2. *Para cada $m \in M$, a função*

$$\begin{aligned} \mu_m: A &\rightarrow M \\ a &\mapsto am \end{aligned}$$

é um homomorfismo de A -módulos.

3. *Se $\phi: M \rightarrow N$ e $\psi: N \rightarrow P$ forem homomorfismos de A -módulos, então a função composta $\psi \circ \phi$ será um homomorfismo de A -módulos de M em P .*

4. *O conjunto $\text{Hom}_A(M, N)$ com as operações*

$$\begin{aligned} +: \text{Hom}_A(M, N) \times \text{Hom}_A(M, N) &\rightarrow \text{Hom}_A(M, N) \\ (\phi, \psi) &\mapsto \phi + \psi: \begin{array}{ccc} M &\rightarrow & N \\ m &\rightarrow & \phi(m) + \psi(m) \end{array} \end{aligned}$$

e

$$\begin{aligned} \mu: A \times \text{Hom}_A(M, N) &\rightarrow \text{Hom}_A(M, N) \\ (a, \phi) &\mapsto a\phi: \begin{array}{ccc} M &\rightarrow & N \\ m &\rightarrow & a\phi(m) \end{array} \end{aligned}$$

é um A -módulo.

Definição 9. *Um homomorfismo de A -módulos $\phi: M \rightarrow N$ será um **isomorfismo** se existir um homomorfismo $\psi: N \rightarrow M$ tal que $\phi \circ \psi = \text{id}_N$ e $\psi \circ \phi = \text{id}_M$. Quando existir um isomorfismo entre dois A -módulos M e N , diremos que M e N são isomorfos.*

Proposição 2. *Seja $\phi: M \rightarrow N$ um homomorfismo de A -módulos. Então, ϕ será um isomorfismo se, e somente se, ϕ for bijetor.*

Demonstração. Suponhamos que ϕ seja um isomorfismo. Como ϕ possui inversa, ϕ é bijetor.

Reciprocamente, suponhamos que ϕ seja bijetor. Basta mostrarmos que sua inversa ϕ^{-1} é um homomorfismo. Consideremos $a, b \in A$ e $n_1, n_2 \in N$ e definamos $m_1 = \phi^{-1}(n_1)$ e $m_2 = \phi^{-1}(n_2)$.

Notemos que

$$\begin{aligned}\phi^{-1}(an_1 + bn_2) &= \phi^{-1}(a\phi(m_1) + b\phi(m_2)) = \phi^{-1}(\phi(am_1 + bm_2)) = am_1 + bm_2 \\ &= a\phi^{-1}(n_1) + b\phi^{-1}(n_2),\end{aligned}$$

o que conclui a prova. $\square$

3.2 SUBMÓDULOS E MÓDULOS QUOCIENTES

Definição 10. *Seja M um A -módulo. Um **submódulo** N de M é um subconjunto não vazio de M que é fechado por combinações A -lineares, isto é, $an_1 + bn_2 \in N$ para todos $a, b \in A$ e $n_1, n_2 \in N$.*

Exemplo 5. *Se M for um A -módulo, então $\{0\}$ e M serão submódulos de M .*

Proposição 3. *Sejam M e N A -módulos e seja $\phi: M \rightarrow N$ um homomorfismo de A -módulos.*

1. *Se M' for um submódulo de M , então $\phi(M')$ será um submódulo de N .*
2. *Se N' for um submódulo de N , então $\phi^{-1}(N')$ será um submódulo de M .*

Demonstração.

1. Sejam $a, b \in A$ e $n_1, n_2 \in \phi(M')$. Assim, existem $m_1, m_2 \in M'$ tais que $n_1 = \phi(m_1)$ e $n_2 = \phi(m_2)$. Notemos que

$$an_1 + bn_2 = a\phi(m_1) + b\phi(m_2) = \phi(am_1 + bm_2) \in \phi(M'),$$

pois $am_1 + bm_2 \in M'$. Logo, $\phi(M')$ é um submódulo de N .

2. Consideremos $a, b \in A$ e $m_1, m_2 \in \phi^{-1}(N')$, ou seja, $\phi(m_1), \phi(m_2) \in N'$. Temos

$$\phi(am_1 + bm_2) = a\phi(m_1) + b\phi(m_2) \in N',$$

isto é, $am_1 + bm_2 \in \phi^{-1}(N')$. Portanto, $\phi^{-1}(N')$ é um submódulo de M . $\square$

Seja $\phi: M \rightarrow N$ um homomorfismo de A -módulos. O submódulo $\phi(M)$ de N é denominado **imagem** de ϕ e é denotado por $\text{Im}(\phi)$. O submódulo $\phi^{-1}(\{0\})$ de M é denominado **núcleo** de ϕ e é denotado por $\text{Ker}(\phi)$. Com o lema seguinte, concluiremos que $\text{Ker}(\phi)$ é um instrumento muito útil para medir a falta de injetividade do homomorfismo ϕ .

Lema 4. *Sejam M e N A -módulos e seja $\phi: M \rightarrow N$ um homomorfismo de A -módulos. O homomorfismo ϕ será injetor se, e somente se, $\text{Ker}(\phi) = \{0\}$.*

Demonstração. Suponhamos que ϕ seja injetor. Claramente, $\{0\} \subset \text{Ker}(\phi)$. Se $m \in \text{Ker}(\phi)$, então $\phi(m) = 0 = \phi(0)$. Visto que ϕ é injetor, temos $m = 0$ e concluímos que $\text{Ker}(\phi) = \{0\}$.

Reciprocamente, suponhamos que $\text{Ker}(\phi) = \{0\}$. Consideremos $m_1, m_2 \in M$ tais que $\phi(m_1) = \phi(m_2)$ ou, equivalentemente, $\phi(m_1 - m_2) = 0$. Assim, $m_1 - m_2 \in \text{Ker}(\phi) = \{0\}$, ou seja, $m_1 = m_2$. Logo, ϕ é um homomorfismo injetor. $\square$

Dados um A -módulo M e um submódulo N de M , o grupo quociente M/N com a operação

$$\begin{aligned} \mu: A \times M/N &\rightarrow M/N \\ (a, \overline{m}) &\mapsto \overline{am} \end{aligned}$$

é um A -módulo, o qual é chamado **módulo quociente** de M por N . Lembremos que, dadas classes de equivalência $\overline{m_1}, \overline{m_2} \in M/N$, temos

$$\overline{m_1} = \overline{m_2} \Leftrightarrow m_1 - m_2 \in N.$$

Além disso, a função que leva cada elemento em sua respectiva classe de equivalência

$$\begin{aligned} \pi: M &\rightarrow M/N \\ m &\mapsto \overline{m} \end{aligned}$$

é um homomorfismo sobrejetor de A -módulos, o qual é denominado **homomorfismo quociente**. Por meio desse homomorfismo, daremos uma importante caracterização do módulo quociente no teorema seguinte.

Teorema 4 (Propriedade Universal do Quociente). *Sejam M um A -módulo, M' um submódulo de M e $\pi: M \rightarrow M/M'$ o homomorfismo quociente. Para qualquer A -módulo N , denotemos o conjunto*

$$\{\phi \in \text{Hom}_A(M, N); M' \subset \text{Ker}(\phi)\}$$

por $\text{Hom}_A^{M'}(M, N)$. Então as funções

$$\begin{aligned} f: \text{Hom}_A(M/M', N) &\rightarrow \text{Hom}_A^{M'}(M, N) \\ \psi &\mapsto \psi \circ \pi \end{aligned}$$

e

$$\begin{aligned} g: \text{Hom}_A^{M'}(M, N) &\rightarrow \text{Hom}_A(M/M', N) \\ \phi &\mapsto \overline{\phi}: \begin{array}{ccc} M/M' &\rightarrow & N \\ \overline{m} &\rightarrow & \phi(m) \end{array} \end{aligned}$$

são bijeções e são inversas uma da outra.

Demonstração. Primeiramente, provemos que f é uma função. Seja $\psi \in \text{Hom}_A(M/M', N)$. Claramente, $\psi \circ \pi$ é um homomorfismo de A -módulos de M em N . Além disso, temos

$$\psi \circ \pi(m') = \psi(\overline{0}) = 0$$

para todo $m' \in M'$. Em outras palavras, $M' \subset \text{Ker}(\psi \circ \pi)$. Logo, $\psi \circ \pi \in \text{Hom}_A^{M'}(M, N)$ e, desse modo, f é uma função.

Agora, mostremos que g é uma função. Consideremos $\phi \in \text{Hom}_A^{M'}(M, N)$. Notemos que $\bar{\phi}$ é uma função bem definida, pois se $\overline{m_1}, \overline{m_2} \in M/M'$, então

$$\overline{m_1} = \overline{m_2} \Leftrightarrow m_1 - m_2 \in M' \Rightarrow \phi(m_1 - m_2) = 0 \Leftrightarrow \phi(m_1) = \phi(m_2).$$

Além disso, se $a, b \in A$ e $\overline{m_1}, \overline{m_2} \in M/M'$, temos

$$\begin{aligned} \bar{\phi}(a\overline{m_1} + b\overline{m_2}) &= \bar{\phi}(\overline{am_1 + bm_2}) = \phi(am_1 + bm_2) = a\phi(m_1) + b\phi(m_2) \\ &= a\bar{\phi}(\overline{m_1}) + b\bar{\phi}(\overline{m_2}). \end{aligned}$$

Assim, $\bar{\phi}$ é um homomorfismo de A -módulos, ou seja, $\bar{\phi} \in \text{Hom}_A(M/M', N)$. Logo, g é uma função.

Finalmente, mostremos que as funções f e g são inversas uma da outra. Temos

$$f \circ g(\phi) = f(\bar{\phi}) = \bar{\phi} \circ \pi \quad \text{e} \quad g \circ f(\psi) = g(\psi \circ \pi) = \overline{\psi \circ \pi}.$$

Notemos que se $m \in M$, então

$$\bar{\phi} \circ \pi(m) = \bar{\phi}(\overline{m}) = \phi(m),$$

ou seja, $\bar{\phi} \circ \pi = \phi$. Além disso, se $\overline{m} \in M/M'$, então

$$\overline{\psi \circ \pi}(\overline{m}) = \psi \circ \pi(m) = \psi(\overline{m}),$$

isto é, $\overline{\psi \circ \pi} = \psi$. Desse modo, concluímos que $f \circ g(\phi) = \phi$ e $g \circ f(\psi) = \psi$. Em outras palavras, $f \circ g = \text{id}_{\text{Hom}_A^{M'}(M, N)}$ e $g \circ f = \text{id}_{\text{Hom}_A(M/M', N)}$. Isso conclui a demonstração. $\square$

Em particular, o teorema anterior nos diz que qualquer homomorfismo de A -módulos $\phi: M \rightarrow N$ satisfazendo $\phi(M') = \{0\}$ “induz” um único homomorfismo de A -módulos $\bar{\phi}: M/M' \rightarrow N$ tal que o diagrama

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \pi \downarrow & \nearrow \exists! \bar{\phi} & \\ M/M' & & \end{array}$$

comuta, isto é, $\phi = \bar{\phi} \circ \pi$.

Teorema 5 (Teorema do Isomorfismo). *Sejam M e N A -módulos e $\phi: M \rightarrow N$ um homomor-*

fismo de A -módulos. Consideremos M' um submódulo de M tal que $M' \subset \text{Ker}(\phi)$ e

$$\begin{aligned}\bar{\phi}: M/M' &\rightarrow N \\ \bar{m} &\mapsto \phi(m)\end{aligned}$$

o homomorfismo induzido por ϕ . Então, $\text{Ker}(\bar{\phi}) = \text{Ker}(\phi)/M'$ e, em particular, $M/\text{Ker}(\phi)$ e $\text{Im}(\phi)$ são isomorfos.

Demonstração. Devido à demonstração do Teorema 4, $\bar{\phi}$ é, realmente, um homomorfismo de A -módulos. Seja $\bar{x} \in \text{Ker}(\bar{\phi})$. Notemos que $\phi(x) = \bar{\phi}(\bar{x}) = 0$, ou seja, $x \in \text{Ker}(\phi)$. Assim, $\bar{x} \in \text{Ker}(\phi)/M'$. Reciprocamente, seja $\bar{y} \in \text{Ker}(\phi)/M'$. Visto que $y \in \text{Ker}(\phi)$, $\bar{\phi}(\bar{y}) = \phi(y) = 0$, isto é, $\bar{y} \in \text{Ker}(\bar{\phi})$. Logo, $\text{Ker}(\bar{\phi}) = \text{Ker}(\phi)/M'$.

Agora, suponhamos que $M' = \text{Ker}(\phi)$. Nesse caso, temos

$$\text{Ker}(\bar{\phi}) = \text{Ker}(\phi)/\text{Ker}(\phi) = \{\bar{0}\}.$$

Pelo Lema 4, $\bar{\phi}$ é injetor e, logo, a função

$$\begin{aligned}\tilde{\phi}: M/M' &\rightarrow \text{Im}(\phi) \\ \bar{m} &\mapsto \bar{\phi}(\bar{m})\end{aligned}$$

é um isomorfismo de A -módulos. □

3.3 OPERAÇÕES SOBRE SUBMÓDULOS

Dado um A -módulo M , podemos definir, de modo natural, o produto de um ideal de A com o módulo M e, ainda, a soma de uma família de submódulos de M .

Proposição 4. *Sejam M um A -módulo, I um ideal de A e $(M_\lambda)_{\lambda \in \Lambda}$ uma família de submódulos de M .*

1. A **interseção** $\bigcap_{\lambda \in \Lambda} M_\lambda$ é um submódulo de M .

2. O **produto**

$$IM := \left\{ \sum_{i=1}^n a_i m_i \in M; n \in \mathbb{N} \setminus \{0\}, a_i \in I \text{ e } m_i \in M \right\}$$

é um submódulo de M .

3. A **soma**

$$\sum_{\lambda \in \Lambda} M_\lambda := \left\{ \sum_{i=1}^n m_{\lambda_i} \in M; n \in \mathbb{N} \setminus \{0\}, \lambda_i \in \Lambda \text{ e } m_{\lambda_i} \in M_{\lambda_i} \right\}$$

é o menor submódulo de M que contém M_λ para cada $\lambda \in \Lambda$.

Demonstração.

1. É fácil ver que $0 \in \bigcap_{\lambda \in \Lambda} M_\lambda$. Sejam $a, b \in A$ e $x, y \in \bigcap_{\lambda \in \Lambda} M_\lambda$. Visto que M_λ é um submódulo de M para cada $\lambda \in \Lambda$, segue que $ax + by \in M_\lambda$ para todo $\lambda \in \Lambda$, isto é, $ax + by \in \bigcap_{\lambda \in \Lambda} M_\lambda$. Logo, $\bigcap_{\lambda \in \Lambda} M_\lambda$ é um submódulo de M .
2. É claro que $0 \in IM$. Sejam $a, b \in A$ e $x, y \in IM$. Então, existem $n_1, n_2 \in \mathbb{N}$, $a_1, \dots, a_{n_1+n_2} \in I$ e $m_1, \dots, m_{n_1+n_2} \in M$ tais que

$$x = \sum_{i=1}^{n_1} a_i m_i \quad \text{e} \quad y = \sum_{i=n_1+1}^{n_1+n_2} a_i m_i.$$

Notemos que

$$\begin{aligned} ax + by &= a \sum_{i=1}^{n_1} a_i m_i + b \sum_{i=n_1+1}^{n_1+n_2} a_i m_i = \sum_{i=1}^{n_1} a(a_i m_i) + \sum_{i=n_1+1}^{n_1+n_2} b(a_i m_i) \\ &= \sum_{i=1}^{n_1} (aa_i) m_i + \sum_{i=n_1+1}^{n_1+n_2} (ba_i) m_i \in IM, \end{aligned}$$

pois $aa_i, ba_i \in I$ para todo $i \in \{1, \dots, n_1 + n_2\}$. Portanto, IM é um submódulo de M .

3. Primeiramente, provemos que $\sum_{\lambda \in \Lambda} M_\lambda$ é um submódulo de M . Claramente, $0 \in \sum_{\lambda \in \Lambda} M_\lambda$. Sejam $a, b \in A$ e $x, y \in \sum_{\lambda \in \Lambda} M_\lambda$. Desse modo, existem $n_1, n_2 \in \mathbb{N}$, $\lambda_1, \dots, \lambda_{n_1+n_2} \in \Lambda$ e $m_{\lambda_i} \in M_{\lambda_i}$ para cada $i \in \{1, \dots, n_1 + n_2\}$ tais que

$$x = \sum_{i=1}^{n_1} m_{\lambda_i} \quad \text{e} \quad y = \sum_{i=n_1+1}^{n_1+n_2} m_{\lambda_i}.$$

Como M_{λ_i} é um submódulo de M para todo $i \in \{1, \dots, n_1 + n_2\}$, temos $am_{\lambda_i}, bm_{\lambda_i} \in M_{\lambda_i}$ para cada $i \in \{1, \dots, n_1 + n_2\}$. Assim,

$$ax + by = a \sum_{i=1}^{n_1} m_{\lambda_i} + b \sum_{i=n_1+1}^{n_1+n_2} m_{\lambda_i} = \sum_{i=1}^{n_1} am_{\lambda_i} + \sum_{i=n_1+1}^{n_1+n_2} bm_{\lambda_i} \in \sum_{\lambda \in \Lambda} M_\lambda.$$

Logo, $\sum_{\lambda \in \Lambda} M_\lambda$ é um submódulo de M .

Evidentemente, $M_\lambda \subset \sum_{\lambda \in \Lambda} M_\lambda$ para todo $\lambda \in \Lambda$. Agora, mostremos que $\sum_{\lambda \in \Lambda} M_\lambda$ é o menor submódulo de M com essa propriedade. Seja M' um submódulo de M tal que $M_\lambda \subset M'$ para todo $\lambda \in \Lambda$. Desse modo, se $s \in \sum_{\lambda \in \Lambda} M_\lambda$, então s será uma soma de elementos de M' e, conseqüentemente, $s \in M'$. Portanto, $\sum_{\lambda \in \Lambda} M_\lambda \subset M'$.

□

Sejam M um A -módulo e m um elemento de M . O conjunto dos “múltiplos” de m

$$Am := \{am \in M; a \in A\}$$

é a imagem do homomorfismo de A -módulos

$$\begin{aligned} \mu_m: A &\rightarrow M \\ a &\mapsto am \end{aligned}$$

e, logo, um submódulo de M . Dado um subconjunto $S \subset M$, a soma

$$\sum_{s \in S} As$$

é o menor submódulo de M que contém S , o qual é chamado **submódulo gerado** por S .

3.4 PRODUTO DIRETO E SOMA DIRETA

Sejam Λ e X conjuntos não vazios. Lembremos que uma **família** de elementos de X com índices em Λ é uma função $x: \Lambda \rightarrow X$. Para cada $\lambda \in \Lambda$, o elemento $x(\lambda)$ é denominado **termo da família** e é denotado por x_λ . A família x é representada pela notação $(x_\lambda)_{\lambda \in \Lambda}$. Agora, se $(X_\lambda)_{\lambda \in \Lambda}$ for uma família de conjuntos não vazios, seu **produto cartesiano** será o conjunto de todas as famílias $(x_\lambda)_{\lambda \in \Lambda}$ de elementos de $\bigcup_{\lambda \in \Lambda} X_\lambda$ com índices em Λ tais que $x_\lambda \in X_\lambda$ para todo $\lambda \in \Lambda$. O produto cartesiano da família $(X_\lambda)_{\lambda \in \Lambda}$ é denotado por $\prod_{\lambda \in \Lambda} X_\lambda$.

Sejam A um anel e $(M_\lambda)_{\lambda \in \Lambda}$ uma família de A -módulos. O produto cartesiano $\prod_{\lambda \in \Lambda} M_\lambda$ com as operações

$$\begin{aligned} +: \prod_{\lambda \in \Lambda} M_\lambda \times \prod_{\lambda \in \Lambda} M_\lambda &\rightarrow \prod_{\lambda \in \Lambda} M_\lambda & \text{e } \mu: A \times \prod_{\lambda \in \Lambda} M_\lambda &\rightarrow \prod_{\lambda \in \Lambda} M_\lambda \\ ((m_\lambda)_{\lambda \in \Lambda}, (n_\lambda)_{\lambda \in \Lambda}) &\mapsto (m_\lambda + n_\lambda)_{\lambda \in \Lambda} & (a, (m_\lambda)_{\lambda \in \Lambda}) &\mapsto (am_\lambda)_{\lambda \in \Lambda} \end{aligned}$$

é um A -módulo, o qual é chamado **produto direto** da família $(M_\lambda)_{\lambda \in \Lambda}$.

Desse A -módulo, destaca-se seu subconjunto constituído de todas as famílias $(m_\lambda)_{\lambda \in \Lambda}$ cujos termos são quase todos nulos, isto é, o subconjunto seguinte:

$$\left\{ (m_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M_\lambda; m^{-1} \left(\bigcup_{\lambda \in \Lambda} (M_\lambda \setminus \{0_{M_\lambda}\}) \right) \text{ é um conjunto finito} \right\},$$

onde 0_{M_λ} é o elemento neutro do grupo aditivo M_λ para cada $\lambda \in \Lambda$. Esse é um submódulo do produto direto $\prod_{\lambda \in \Lambda} M_\lambda$ chamado **soma direta** da família $(M_\lambda)_{\lambda \in \Lambda}$ e é denotado por $\bigoplus_{\lambda \in \Lambda} M_\lambda$.

Notemos que se Λ for finito, então $\prod_{\lambda \in \Lambda} M_\lambda = \bigoplus_{\lambda \in \Lambda} M_\lambda$.

Observação 5. Se N for um A -módulo, $(m_\lambda)_{\lambda \in \Lambda}$ for um elemento de $\bigoplus_{\lambda \in \Lambda} M_\lambda$ e $\phi_\lambda: M_\lambda \rightarrow N$ for um homomorfismo de A -módulos para cada $\lambda \in \Lambda$, a família $(\phi_\lambda(m_\lambda))_{\lambda \in \Lambda}$ de elementos de N

com índices em Λ possuirá apenas uma quantidade finita de termos não nulos. Por simplicidade, denotaremos a soma dos termos não nulos de $(\phi_\lambda(m_\lambda))_{\lambda \in \Lambda}$ por $\sum_{\lambda \in \Lambda} \phi_\lambda(m_\lambda)$. Naturalmente, se todos os termos da família $(\phi_\lambda(m_\lambda))_{\lambda \in \Lambda}$ forem nulos, então $\sum_{\lambda \in \Lambda} \phi_\lambda(m_\lambda) = 0$.

Exemplo 6. Seja $(M_\lambda)_{\lambda \in \Lambda}$ uma família de A -módulos. Para cada índice $\lambda_0 \in \Lambda$, a inclusão da parcela M_{λ_0} na soma direta $\bigoplus_{\lambda \in \Lambda} M_\lambda$

$$\begin{aligned} i_{\lambda_0}: M_{\lambda_0} &\rightarrow \bigoplus_{\lambda \in \Lambda} M_\lambda \\ m &\mapsto i_{\lambda_0}(m): \Lambda \rightarrow \bigcup_{\lambda \in \Lambda} M_\lambda \\ \lambda &\mapsto \begin{cases} m & \text{se } \lambda = \lambda_0 \\ 0_{M_\lambda} & \text{se } \lambda \neq \lambda_0 \end{cases} \end{aligned}$$

é, claramente, um homomorfismo injetor de A -módulos. Também é fácil ver que cada elemento $(m_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} M_\lambda$ pode ser escrito como a “soma de seus termos”, isto é,

$$(m_\lambda)_{\lambda \in \Lambda} = \sum_{\lambda \in \Lambda} i_\lambda(m_\lambda).$$

Definição 11. Sejam A um anel, M um A -módulo e S um subconjunto de M . Diremos que S é um **conjunto de geradores** se todo elemento de M puder ser escrito como combinação linear dos elementos de S com coeficientes em A , ou seja, se o homomorfismo de A -módulos

$$\begin{aligned} \phi: \bigoplus_{s \in S} A &\rightarrow M \\ (a_s)_{s \in S} &\mapsto \sum_{s \in S} a_s s \end{aligned}$$

for sobrejetor. Quando ϕ for também um isomorfismo, diremos que M é um **módulo livre** sobre A e que S é uma **base** de M .

Além disso, se M possuir um conjunto finito de geradores, diremos que M é **finitamente gerado** sobre A .

Vejamos que quocientes de módulos finitamente gerados por seus submódulos são também finitamente gerados.

Proposição 5. Sejam M um A -módulo, N um submódulo de M e $\pi: M \rightarrow M/N$ o homomorfismo quociente. Se S for um conjunto de geradores de M , então $\pi(S)$ será um conjunto de geradores de M/N . Em particular, se M for finitamente gerado, então M/N será também finitamente gerado.

Demonstração. Consideremos S um conjunto de geradores de M . Se $m \in M$, então existirão $n \in \mathbb{N}$, $a_1, \dots, a_n \in A$ e $s_1, \dots, s_n \in S$ tais que

$$m = a_1 s_1 + \dots + a_n s_n$$

e, por consequência,

$$\overline{m} = \overline{a_1 s_1 + \cdots + a_n s_n} = a_1 \overline{s_1} + \cdots + a_n \overline{s_n}.$$

Logo, $\pi(S)$ é um conjunto de geradores de M/N . $\square$

Consideremos um anel A . Agora, nosso objetivo é simplificar a notação dos elementos da soma direta $\bigoplus_{\lambda \in \Lambda} A$. A nova notação que obteremos aqui será útil para a construção do produto tensorial de módulos na próxima seção.

Definamos o conjunto

$$S = \left\{ (s_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} A; \text{ existe } \lambda_0 \in \Lambda \text{ tal que } s_{\lambda_0} = 1 \text{ e } s_\lambda = 0 \text{ para todo } \lambda \neq \lambda_0 \right\}.$$

É fácil ver que S é uma base da soma direta $\bigoplus_{\lambda \in \Lambda} A$. Além disso, como a função

$$\begin{aligned} i: \Lambda &\rightarrow \bigoplus_{\lambda \in \Lambda} A \\ \lambda_0 &\mapsto i(\lambda_0): \Lambda \rightarrow A \\ \lambda &\mapsto \begin{cases} 1 & \text{se } \lambda = \lambda_0 \\ 0 & \text{se } \lambda \neq \lambda_0 \end{cases} \end{aligned}$$

é injetora e sua imagem é a base S , podemos identificar Λ com a imagem de i e escrever $\Lambda \subset \bigoplus_{\lambda \in \Lambda} A$. Desse modo, podemos ver $\bigoplus_{\lambda \in \Lambda} A$ como um A -módulo com base Λ . Com isso, todo elemento dessa soma direta pode ser escrito como uma combinação linear formal dos elementos de Λ com coeficientes em A . Explicitamente, um elemento não nulo $(a_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} A$ pode ser

escrito como $\sum_{i=1}^n a_{\lambda_i} \cdot \lambda_i$, onde $a^{-1}(A \setminus \{0\}) = \{\lambda_1, \dots, \lambda_n\}$ e $\lambda_j \neq \lambda_k$ quando $j \neq k$.

As duas proposições seguintes resgatam um velho fato conhecido em Álgebra Linear: para saber o que uma aplicação linear faz com cada elemento de seu domínio, basta saber as imagens dos elementos de certo conjunto de geradores.

Proposição 6. *Sejam M e N A -módulos e seja S um conjunto de geradores de M . Se $\phi, \psi: M \rightarrow N$ forem homomorfismos de A -módulos que coincidem em S , isto é, $\phi|_S = \psi|_S$, então $\phi = \psi$.*

Demonstração. Seja m um elemento de M . Como S é um conjunto de geradores de M , existem $n \in \mathbb{N}$, $a_1, \dots, a_n \in A$ e $s_1, \dots, s_n \in S$ tais que

$$m = \sum_{i=1}^n a_i s_i.$$

Visto que $\phi(s_i) = \psi(s_i)$ para cada $i \in \{1, \dots, n\}$, temos

$$\phi(m) = \phi\left(\sum_{i=1}^n a_i s_i\right) = \sum_{i=1}^n a_i \phi(s_i) = \sum_{i=1}^n a_i \psi(s_i) = \psi\left(\sum_{i=1}^n a_i s_i\right) = \psi(m).$$

Logo, os homomorfismos ϕ e ψ são iguais. □

Proposição 7. *Sejam Λ um conjunto não vazio e P um A -módulo. Para qualquer função $\phi: \Lambda \rightarrow P$, sua extensão*

$$\begin{aligned} \Phi: \bigoplus_{\lambda \in \Lambda} A &\rightarrow P \\ \sum_{i=1}^n a_i \cdot \lambda_i &\mapsto \sum_{i=1}^n a_i \phi(\lambda_i) \end{aligned}$$

é um homomorfismo de A -módulos.

Demonstração. Consideremos $a, b \in A$ e $x, y \in \bigoplus_{\lambda \in \Lambda} A$. Então, existem $n_1, n_2 \in \mathbb{N}$, $a_1, \dots, a_{n_1+n_2} \in A$ e $\lambda_1, \dots, \lambda_{n_1+n_2} \in \Lambda$ tais que

$$x = \sum_{i=1}^{n_1} a_i \cdot \lambda_i \quad \text{e} \quad y = \sum_{i=n_1+1}^{n_1+n_2} a_i \cdot \lambda_i.$$

Observemos que

$$\begin{aligned} \Phi(ax + by) &= \Phi \left(\sum_{i=1}^{n_1} a(a_i \cdot \lambda_i) + \sum_{i=n_1+1}^{n_1+n_2} b(a_i \cdot \lambda_i) \right) = \Phi \left(\sum_{i=1}^{n_1} aa_i \cdot \lambda_i + \sum_{i=n_1+1}^{n_1+n_2} ba_i \cdot \lambda_i \right) \\ &= \sum_{i=1}^{n_1} (aa_i) \phi(\lambda_i) + \sum_{i=n_1+1}^{n_1+n_2} (ba_i) \phi(\lambda_i) = \sum_{i=1}^{n_1} a(a_i \phi(\lambda_i)) + \sum_{i=n_1+1}^{n_1+n_2} b(a_i \phi(\lambda_i)) \\ &= a \sum_{i=1}^{n_1} a_i \phi(\lambda_i) + b \sum_{i=n_1+1}^{n_1+n_2} a_i \phi(\lambda_i) = a \Phi(x) + b \Phi(y). \end{aligned}$$

Portanto, Φ é um homomorfismo de A -módulos. □

3.5 PRODUTO TENSORIAL DE MÓDULOS

Definição 12. *Seja A um anel e sejam M, N e P A -módulos. Um **mapa A -bilinear** é uma função $\phi: M \times N \rightarrow P$ tal que, para todos $m_0 \in M$ e $n_0 \in N$, as funções*

$$\begin{aligned} \phi(m_0, _): N &\rightarrow P & \text{e} & \phi(_, n_0): M \rightarrow P \\ n &\mapsto \phi(m_0, n) & & m \mapsto \phi(m, n_0) \end{aligned}$$

são A -lineares, isto é,

$$\phi(am_1 + bm_2, n_0) = a\phi(m_1, n_0) + b\phi(m_2, n_0) \quad \text{e} \quad \phi(m_0, an_1 + bn_2) = a\phi(m_0, n_1) + b\phi(m_0, n_2)$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N$. O conjunto de todos os mapas bilineares entre $M \times N$ e P será denotado por $\text{Bil}_A(M \times N, P)$.

Construiremos um A -módulo T de modo que exista uma bijeção natural entre os conjuntos $\text{Bil}_A(M \times N, P)$ e $\text{Hom}_A(T, P)$ para todo A -módulo P . O teorema seguinte reescreve isso de um modo mais preciso.

Teorema 6 (Propriedade Universal do Produto Tensorial). *Sejam M e N A -módulos. Então, existe um par (T, τ) , consistindo em um A -módulo T e em um mapa A -bilinear $\tau: M \times N \rightarrow T$, que possui a propriedade seguinte: dados qualquer A -módulo P e qualquer mapa A -bilinear $\phi: M \times N \rightarrow P$, existe um único mapa A -linear $\bar{\phi}: T \rightarrow P$ tal que o diagrama*

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & T \\ \phi \downarrow & \swarrow \exists! \bar{\phi} & \\ P & & \end{array}$$

comuta, isto é, $\phi = \bar{\phi} \circ \tau$. Em outras palavras, todo mapa A -bilinear em $M \times N$ fatora-se através de T . Além disso, se (S, δ) for outro par com essa propriedade, então existirá um único isomorfismo $\beta: T \rightarrow S$ tal que $\delta = \beta \circ \tau$.

Demonstração. Primeiramente, provemos a existência de um par satisfazendo as condições supracitadas.

Seja C a soma direta $\bigoplus_{(m,n) \in M \times N} A$. Definamos os quatro subconjuntos de C seguintes:

- (i) $D_1 = \{(m_1 + m_2, n) - (m_1, n) - (m_2, n) \in C; m_1, m_2 \in M \text{ e } n \in N\}$;
- (ii) $D_2 = \{(m, n_1 + n_2) - (m, n_1) - (m, n_2) \in C; m \in M \text{ e } n_1, n_2 \in N\}$;
- (iii) $D_3 = \{(am, n) - a(m, n) \in C; a \in A, m \in M \text{ e } n \in N\}$;
- (iv) $D_4 = \{(m, an) - a(m, n) \in C; a \in A, m \in M \text{ e } n \in N\}$.

Seja D o submódulo gerado pela união $D_1 \cup D_2 \cup D_3 \cup D_4$ e seja T o módulo quociente C/D . Considerando o homomorfismo quociente $\pi: C \rightarrow T$, denotaremos $\pi(m, n)$ por $m \otimes n$ para cada $(m, n) \in M \times N$. Definamos τ por $\pi|_{M \times N}$, isto é,

$$\begin{aligned} \tau: M \times N &\rightarrow T \\ (m, n) &\mapsto m \otimes n. \end{aligned}$$

Sabemos que $M \times N$ é um conjunto gerador de C . Pela Proposição 5, T é gerado pelos elementos da forma $m \otimes n$. Agora, vejamos algumas propriedades da “operação” $\otimes$. Para todos $a \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N$, temos:

- (i) $(m_1 + m_2) \otimes n = \overline{(m_1 + m_2, n)} = \overline{(m_1, n)} + \overline{(m_2, n)} = m_1 \otimes n + m_2 \otimes n$;
- (ii) $m \otimes (n_1 + n_2) = \overline{(m, n_1 + n_2)} = \overline{(m, n_1)} + \overline{(m, n_2)} = m \otimes n_1 + m \otimes n_2$;
- (iii) $(am) \otimes n = \overline{(am, n)} = a\overline{(m, n)} = a(m \otimes n)$;
- (iv) $m \otimes (an) = \overline{(m, an)} = a\overline{(m, n)} = a(m \otimes n)$.

Com isso,

$$\begin{aligned}\tau(am_1 + bm_2, n_1) &= (am_1 + bm_2) \otimes n_1 = (am_1) \otimes n_1 + (bm_2) \otimes n_1 \\ &= a(m_1 \otimes n_1) + b(m_2 \otimes n_1) = a\tau(m_1, n_1) + b\tau(m_2, n_1)\end{aligned}$$

e

$$\begin{aligned}\tau(m_1, an_1 + bn_2) &= m_1 \otimes (an_1 + bn_2) = m_1 \otimes (an_1) + m_1 \otimes (bn_2) \\ &= a(m_1 \otimes n_1) + b(m_1 \otimes n_2) = a\tau(m_1, n_1) + b\tau(m_1, n_2)\end{aligned}$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N$. Logo, τ é um mapa A -bilinear.

Consideremos um A -módulo P e um mapa A -bilinear $\phi: M \times N \rightarrow P$. Pela Proposição 7, a extensão

$$\begin{aligned}\Phi: C &\rightarrow P \\ \sum_{i=1}^r a_i \cdot (m_i, n_i) &\mapsto \sum_{i=1}^r a_i \phi(m_i, n_i)\end{aligned}$$

é um homomorfismo de A -módulos. Como ϕ é A -bilinear, para todos $a \in A$, $m, m_1, m_2 \in M$ e $n, n_1, n_2 \in N$, temos:

- (i) $\Phi((m_1 + m_2, n) - (m_1, n) - (m_2, n)) = \phi(m_1 + m_2, n) - \phi(m_1, n) - \phi(m_2, n) = 0$;
- (ii) $\Phi((m, n_1 + n_2) - (m, n_1) - (m, n_2)) = \phi(m, n_1 + n_2) - \phi(m, n_1) - \phi(m, n_2) = 0$;
- (iii) $\Phi((am, n) - a(m, n)) = \phi(am, n) - a\phi(m, n) = 0$;
- (iv) $\Phi((m, an) - a(m, n)) = \phi(m, an) - a\phi(m, n) = 0$.

Em outras palavras, Φ anula-se em todos os geradores de D e, logo, $D \subset \text{Ker}(\Phi)$. Pelo Teorema 4, existe um único homomorfismo de A -módulos $\bar{\Phi}: T \rightarrow P$ tal que $\Phi = \bar{\Phi} \circ \pi$. Desse modo,

$$\bar{\Phi} \circ \tau(m, n) = \bar{\Phi} \circ \pi(m, n) = \Phi(m, n) = \phi(m, n)$$

para todos $(m, n) \in M \times N$, isto é, $\phi = \bar{\Phi} \circ \tau$.

Agora, mostremos que $\bar{\Phi}$ é o único mapa A -linear de T em P com essa propriedade. Consideremos $\rho: T \rightarrow P$ um mapa A -linear tal que $\phi = \rho \circ \tau$. Se $c \in C$, então existirão $r \in \mathbb{N}$, $a_1, \dots, a_r \in A$ e $(x_1, y_1), \dots, (x_r, y_r) \in M \times N$ tais que $c = \sum_{i=1}^r a_i \cdot (x_i, y_i)$. Assim,

$$\rho \circ \pi(c) = \sum_{i=1}^r a_i \rho \circ \pi(x_i, y_i) = \sum_{i=1}^r a_i \rho \circ \tau(x_i, y_i) = \sum_{i=1}^r a_i \phi(x_i, y_i) = \Phi(c).$$

Logo, $\Phi = \rho \circ \pi$. Visto que $\bar{\Phi}$ é o único mapa A -linear de T em P satisfazendo $\Phi = \bar{\Phi} \circ \pi$, concluímos que $\rho = \bar{\Phi}$. Portanto, o par (T, τ) construído satisfaz a condição seguinte: para qualquer A -módulo P e qualquer mapa A -bilinear $\phi: M \times N \rightarrow P$, existe um único mapa A -linear $\bar{\Phi}: T \rightarrow P$ tal que $\phi = \bar{\Phi} \circ \tau$.

Finalmente, seja (S, δ) um par que possui essa mesma propriedade. Assim, considerando o A -módulo T e o mapa A -bilinear τ , existe um único mapa A -linear $\alpha: S \rightarrow T$ tal que $\tau = \alpha \circ \delta$.

Agora, utilizando a propriedade do par (T, τ) para o A -módulo S e para o mapa A -bilinear δ , obtemos que existe um único mapa A -linear $\beta: T \rightarrow S$ tal que $\delta = \beta \circ \tau$. Desse modo,

$$\tau = (\alpha \circ \beta) \circ \tau \quad \text{e} \quad \delta = (\beta \circ \alpha) \circ \delta.$$

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau} & T \\ \tau \downarrow & \searrow \alpha \circ \beta & \nearrow \text{id}_T \\ T & & \end{array} \qquad \begin{array}{ccc} M \times N & \xrightarrow{\delta} & S \\ \delta \downarrow & \searrow \beta \circ \alpha & \nearrow \text{id}_S \\ S & & \end{array}$$

Por outro lado, a propriedade do par (T, τ) fornece que id_T é o único mapa A -linear tal que $\tau = \text{id}_T \circ \tau$ enquanto a propriedade do par (S, δ) fornece que id_S é o único mapa A -linear que satisfaz $\delta = \text{id}_S \circ \delta$. Logo, $\alpha \circ \beta = \text{id}_T$ e $\beta \circ \alpha = \text{id}_S$. Por consequência, β é um isomorfismo. $\square$

Observação 6. O A -módulo T construído na demonstração do teorema anterior é chamado **produto tensorial** de M e N sobre A e é denotado por $M \otimes_A N$. E τ é o mapa A -bilinear correspondente ao produto tensorial $M \otimes_A N$.

Exemplo 7. Consideremos um anel A e inteiros positivos m e n .

1. Mostremos que o produto tensorial $A[X] \otimes_A A[Y]$ é isomorfo a $A[X, Y]$.

Pela Propriedade Universal do Produto Tensorial, o mapa A -bilinear

$$\begin{aligned} \phi: \quad A[X] \times A[Y] &\rightarrow A[X, Y] \\ \left(\sum_{i=0}^r a_i X^i, \sum_{j=0}^s b_j Y^j \right) &\mapsto \left(\sum_{i=0}^r a_i X^i \right) \left(\sum_{j=0}^s b_j Y^j \right) \end{aligned}$$

induz o mapa A -linear

$$\begin{aligned} \bar{\Phi}: \quad A[X] \otimes_A A[Y] &\rightarrow A[X, Y] \\ \left(\sum_{i=0}^r a_i X^i \right) \otimes \left(\sum_{j=0}^s b_j Y^j \right) &\mapsto \left(\sum_{i=0}^r a_i X^i \right) \left(\sum_{j=0}^s b_j Y^j \right). \end{aligned}$$

Definamos o mapa A -linear

$$\begin{aligned} \bar{\Psi}: \quad A[X, Y] &\rightarrow A[X] \otimes_A A[Y] \\ \sum_{i=0}^r \sum_{j=0}^s a_{ij} X^i Y^j &\mapsto \sum_{i=0}^r \sum_{j=0}^s a_{ij} (X^i \otimes Y^j). \end{aligned}$$

Consideremos $f_0 \in A[X, Y]$, $g_0 \in A[X]$ e $h_0 \in A[Y]$. Então, existem $r, s \in \mathbb{N}$ e $a_{00}, \dots, a_{0s}, \dots, a_{r0}, \dots, a_{rs}, a_0, \dots, a_r, b_0, \dots, b_s \in A$ tais que

$$f_0(X, Y) = \sum_{i=0}^r \sum_{j=0}^s a_{ij} X^i Y^j, \quad g_0(X) = \sum_{i=0}^r a_i X^i \quad \text{e} \quad h_0(Y) = \sum_{j=0}^s b_j Y^j.$$

Notemos que

$$\overline{\Phi} \circ \overline{\Psi}(f_0) = \overline{\Phi} \left(\sum_{i=0}^r \sum_{j=0}^s a_{ij} (X^i \otimes Y^j) \right) = \sum_{i=0}^r \sum_{j=0}^s a_{ij} \overline{\Phi}(X^i \otimes Y^j) = f_0$$

e

$$\begin{aligned} \overline{\Psi} \circ \overline{\Phi}(g_0 \otimes h_0) &= \overline{\Psi} \left(\left(\sum_{i=0}^r a_i X^i \right) \left(\sum_{j=0}^s b_j Y^j \right) \right) = \overline{\Psi} \left(\sum_{i=0}^r \sum_{j=0}^s a_i b_j X^i Y^j \right) \\ &= \sum_{i=0}^r \sum_{j=0}^s a_i b_j (X^i \otimes Y^j) = \sum_{i=0}^r \sum_{j=0}^s (a_i X^i) \otimes (b_j Y^j) \\ &= \sum_{i=0}^r (a_i X^i) \otimes \left(\sum_{j=0}^s b_j Y^j \right) = g_0 \otimes h_0. \end{aligned}$$

Desse modo, $\overline{\Phi} \circ \overline{\Psi} = \text{id}_{A[X,Y]}$ e $\overline{\Psi} \circ \overline{\Phi}|_S = \text{id}_{A[X] \otimes_A A[Y]|_S}$, onde

$$S = \{g \otimes h; g \in A[X] \text{ e } h \in A[Y]\}.$$

A Proposição 6 fornece que $\overline{\Psi} \circ \overline{\Phi} = \text{id}_{A[X] \otimes_A A[Y]}$, uma vez que S é um conjunto de geradores de $A[X] \otimes_A A[Y]$. Assim, concluímos que $\overline{\Phi}$ é um isomorfismo.

2. Seja d o inteiro positivo tal que $d = \text{mdc}(m, n)$. Provemos que o produto tensorial $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ é isomorfo a $\mathbb{Z}_d$.

Sejam $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ tais que $m|r_1 - r_2$ e $n|s_1 - s_2$. Notemos que $d|r_1 s_1 - r_2 s_2$, pois

$$r_1 s_1 - r_2 s_2 = r_1 s_1 - r_2 s_1 + r_2 s_1 - r_2 s_2 = (r_1 - r_2) s_1 + r_2 (s_1 - s_2).$$

Isso mostra que a função

$$\begin{aligned} \phi: \mathbb{Z}_m \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_d \\ (\bar{r}, \bar{s}) &\mapsto \overline{r s} \end{aligned}$$

está bem definida. É fácil ver que ϕ é um mapa $\mathbb{Z}$ -bilinear. Pela Propriedade Universal do Produto Tensorial, ϕ induz o mapa $\mathbb{Z}$ -linear

$$\begin{aligned} \overline{\Phi}: \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n &\rightarrow \mathbb{Z}_d \\ \bar{r} \otimes \bar{s} &\mapsto \overline{r s}. \end{aligned}$$

Agora, definamos a função

$$\begin{aligned} \overline{\Psi}: \mathbb{Z}_d &\rightarrow \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \\ \bar{t} &\mapsto t(\bar{1} \otimes \bar{1}). \end{aligned}$$

Verifiquemos que essa função está, de fato, bem definida. Visto que $\mathbb{Z}$ é um domínio principal, existem $e, f \in \mathbb{Z}$ tais que $d = em + fn$. Sejam $t_1, t_2 \in \mathbb{Z}$ tais que $d|t_1 - t_2$, ou

seja, existe $c \in \mathbb{Z}$ tal que

$$t_1 - t_2 = dc = (em + fn)c.$$

Com isso, obtemos

$$\begin{aligned}\overline{\Psi}(\overline{t_1}) &= (t_2 + emc + fnc)(\overline{1} \otimes \overline{1}) \\ &= t_2(\overline{1} \otimes \overline{1}) + emc(\overline{1} \otimes \overline{1}) + fnc(\overline{1} \otimes \overline{1}) \\ &= t_2(\overline{1} \otimes \overline{1}) + (\overline{emc} \otimes \overline{1}) + (\overline{1} \otimes \overline{fnc}) \\ &= t_2(\overline{1} \otimes \overline{1}) + (\overline{0} \otimes \overline{1}) + (\overline{1} \otimes \overline{0}) \\ &= \overline{\Psi}(\overline{t_2}).\end{aligned}$$

Claramente, $\overline{\Psi}$ é um mapa $\mathbb{Z}$ -linear. Além disso, temos

$$\overline{\Phi} \circ \overline{\Psi}(\overline{t}) = \overline{\Phi}(t(\overline{1} \otimes \overline{1})) = \overline{\Phi}(\overline{t} \otimes \overline{1}) = \overline{t}$$

e

$$\overline{\Psi} \circ \overline{\Phi}(\overline{r} \otimes \overline{s}) = \overline{\Psi}(\overline{rs}) = rs(\overline{1} \otimes \overline{1}) = \overline{r} \otimes \overline{s}$$

para todos $\overline{r} \in \mathbb{Z}_m$, $\overline{s} \in \mathbb{Z}_n$ e $\overline{t} \in \mathbb{Z}_d$. Desse modo, $\overline{\Phi} \circ \overline{\Psi} = \text{id}_{\mathbb{Z}_d}$ e $\overline{\Psi} \circ \overline{\Phi}|_{S'} = \text{id}_{\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n}|_{S'}$, onde

$$S' = \{\overline{r} \otimes \overline{s}; \overline{r} \in \mathbb{Z}_m \text{ e } \overline{s} \in \mathbb{Z}_n\}.$$

Como S' é um conjunto de geradores de $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$, temos $\overline{\Psi} \circ \overline{\Phi} = \text{id}_{\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n}$. Portanto, $\overline{\Phi}$ é um isomorfismo.

Lema 5. *Sejam M , N e P A -módulos.*

1. *Todo elemento de $M \otimes_A N$ é uma soma de elementos da forma $m \otimes n$, onde $m \in M$ e $n \in N$.*
2. *Todo elemento de $(M \otimes_A N) \otimes_A P$ é uma soma de elementos da forma $(m \otimes n) \otimes p$, onde $m \in M$, $n \in N$ e $p \in P$. Em particular,*

$$S_1 = \{(m \otimes n) \otimes p; m \in M, n \in N \text{ e } p \in P\}$$

é um conjunto de geradores de $(M \otimes_A N) \otimes_A P$.

3. *Todo elemento de $M \otimes_A (N \otimes_A P)$ é uma soma de elementos da forma $m \otimes (n \otimes p)$, onde $m \in M$, $n \in N$ e $p \in P$. Em particular,*

$$S_2 = \{m \otimes (n \otimes p); m \in M, n \in N \text{ e } p \in P\}$$

é um conjunto de geradores de $M \otimes_A (N \otimes_A P)$.

Demonstração.

1. Seja $t \in M \otimes_A N$. Da construção feita no teorema anterior, sabemos que $M \otimes_A N$ é gerado por elementos da forma $m \otimes n$, onde $m \in M$ e $n \in N$. Desse modo, existem $r \in \mathbb{N}$, $a_1, \dots, a_r \in A$, $m_1, \dots, m_r \in M$ e $n_1, \dots, n_r \in N$ tais que

$$t = \sum_{i=1}^r a_i(m_i \otimes n_i) = \sum_{i=1}^r (a_i m_i) \otimes n_i.$$

Claramente, $a_i m_i \in M$ para todo $i \in \{1, \dots, r\}$ e, logo, escrevemos t da maneira desejada.

2. Consideremos $t \in (M \otimes_A N) \otimes_A P$. Pelo item anterior, existem $r \in \mathbb{N}$, $t_1, \dots, t_r \in M \otimes_A N$ e $p_1, \dots, p_r \in P$ tais que

$$t = \sum_{i=1}^r t_i \otimes p_i.$$

Para cada $i \in \{1, \dots, r\}$, o item anterior também fornece que existem $s_i \in \mathbb{N}$, $m_{i1}, \dots, m_{is_i} \in M$ e $n_{i1}, \dots, n_{is_i} \in N$ satisfazendo

$$t_i = \sum_{j=1}^{s_i} m_{ij} \otimes n_{ij}.$$

Com isso, podemos reescrever o elemento t da maneira seguinte

$$t = \sum_{i=1}^r \left(\sum_{j=1}^{s_i} m_{ij} \otimes n_{ij} \right) \otimes p_i = \sum_{i=1}^r \sum_{j=1}^{s_i} ((m_{ij} \otimes n_{ij}) \otimes p_i).$$

3. A demonstração deste item é similar à prova do item anterior.

□

Proposição 8. *Sejam M e N A -módulos. Se S_1 e S_2 forem conjuntos de geradores de M e N , respectivamente, então*

$$S := \{m \otimes n \in M \otimes_A N; m \in S_1 \text{ e } n \in S_2\}$$

será um conjunto de geradores de $M \otimes_A N$. Em particular, se M e N forem finitamente gerados, então $M \otimes_A N$ será também finitamente gerado.

Demonstração. Seja $x \in M \otimes_A N$. Pelo primeiro item do Lema 5, existem $r \in \mathbb{N}$, $x_1, \dots, x_r \in M$ e $y_1, \dots, y_r \in N$ tais que

$$x = \sum_{i=1}^r x_i \otimes y_i.$$

Desse modo, para cada $i \in \{1, \dots, r\}$, existem $r_i, t_i \in \mathbb{N}$, $a_{i1}, \dots, a_{ir_i}, a'_{i1}, \dots, a'_{it_i} \in A$, $s_{i1}, \dots, s_{ir_i} \in S_1$ e $s'_{i1}, \dots, s'_{it_i} \in S_2$ tais que

$$x_i = \sum_{j=1}^{r_i} a_{ij} s_{ij} \quad \text{e} \quad y_i = \sum_{k=1}^{t_i} a'_{ik} s'_{ik}.$$

Assim,

$$\begin{aligned}
 x &= \sum_{i=1}^r \left(\sum_{j=1}^{r_i} a_{ij} s_{ij} \right) \otimes \left(\sum_{k=1}^{t_i} a'_{ik} s'_{ik} \right) = \sum_{i=1}^r \sum_{j=1}^{r_i} (a_{ij} s_{ij}) \otimes \left(\sum_{k=1}^{t_i} a'_{ik} s'_{ik} \right) \\
 &= \sum_{i=1}^r \sum_{j=1}^{r_i} \sum_{k=1}^{t_i} (a_{ij} s_{ij}) \otimes (a'_{ik} s'_{ik}) = \sum_{i=1}^r \sum_{j=1}^{r_i} \sum_{k=1}^{t_i} a_{ij} (s_{ij} \otimes a'_{ik} s'_{ik}) \\
 &= \sum_{i=1}^r \sum_{j=1}^{r_i} \sum_{k=1}^{t_i} a_{ij} a'_{ik} (s_{ij} \otimes s'_{ik}),
 \end{aligned}$$

ou seja, x é uma combinação linear de elementos de S com coeficientes em A . Portanto, S é um conjunto de geradores de $M \otimes_A N$. $\square$

No teorema seguinte, veremos que o produto tensorial possui propriedades familiares.

Teorema 7. *Sejam M , N e P A -módulos e seja $(N_\lambda)_{\lambda \in \Lambda}$ uma família de A -módulos.*

1. *O produto tensorial é comutativo, isto é, $M \otimes_A N$ é isomorfo a $N \otimes_A M$.*
2. *O produto tensorial é associativo, isto é, $(M \otimes_A N) \otimes_A P$ é isomorfo a $M \otimes_A (N \otimes_A P)$.*
3. *O produto tensorial possui distributividade com relação à soma direta, isto é, $M \otimes_A \left(\bigoplus_{\lambda \in \Lambda} N_\lambda \right)$ é isomorfo a $\bigoplus_{\lambda \in \Lambda} (M \otimes_A N_\lambda)$.*
4. *O A -módulo A é o elemento neutro do produto tensorial, isto é, $A \otimes_A M$ é isomorfo a M .*

Demonstração.

1. Consideremos a função

$$\begin{aligned}
 \phi: M \times N &\rightarrow N \otimes_A M \\
 (m, n) &\mapsto n \otimes m.
 \end{aligned}$$

Observemos que

$$\begin{aligned}
 \phi(am_1 + bm_2, n_1) &= n_1 \otimes (am_1 + bm_2) = a(n_1 \otimes m_1) + b(n_1 \otimes m_2) \\
 &= a\phi(m_1, n_1) + b\phi(m_2, n_1)
 \end{aligned}$$

e

$$\begin{aligned}
 \phi(m_1, an_1 + bn_2) &= (an_1 + bn_2) \otimes m_1 = a(n_1 \otimes m_1) + b(n_2 \otimes m_1) \\
 &= a\phi(m_1, n_1) + b\phi(m_1, n_2)
 \end{aligned}$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N$, isto é, ϕ é um mapa A -bilinear. Pela Propriedade Universal do Produto Tensorial, ϕ induz o mapa A -linear

$$\begin{aligned}
 \bar{\Phi}: M \otimes_A N &\rightarrow N \otimes_A M \\
 m \otimes n &\mapsto n \otimes m.
 \end{aligned}$$

De maneira análoga, o mapa

$$\begin{aligned}\psi: N \times M &\rightarrow M \otimes_A N \\ (n, m) &\mapsto m \otimes n\end{aligned}$$

é A -bilinear e induz o mapa A -linear

$$\begin{aligned}\bar{\Psi}: N \otimes_A M &\rightarrow M \otimes_A N \\ n \otimes m &\mapsto m \otimes n.\end{aligned}$$

Definindo os conjuntos

$$S = \{m \otimes n; m \in M \text{ e } n \in N\} \text{ e } S' = \{n \otimes m; m \in M \text{ e } n \in N\},$$

temos $\bar{\Phi} \circ \bar{\Psi}|_{S'} = \text{id}_{N \otimes_A M}|_{S'}$ e $\bar{\Psi} \circ \bar{\Phi}|_S = \text{id}_{M \otimes_A N}|_S$. Além disso, sabemos que S e S' são conjuntos de geradores de $M \otimes_A N$ e de $N \otimes_A M$, respectivamente. Pela Proposição 6, $\bar{\Phi} \circ \bar{\Psi} = \text{id}_{N \otimes_A M}$ e $\bar{\Psi} \circ \bar{\Phi} = \text{id}_{M \otimes_A N}$. Portanto, $\bar{\Phi}$ é um isomorfismo.

2. Para cada $p \in P$, definamos o mapa

$$\begin{aligned}\phi_p: M \times N &\rightarrow M \otimes_A (N \otimes_A P) \\ (m, n) &\mapsto m \otimes (n \otimes p),\end{aligned}$$

o qual é A -bilinear. De fato, para cada $p \in P$, temos

$$\begin{aligned}\phi_p(am_1 + bm_2, n_1) &= (am_1 + bm_2) \otimes (n_1 \otimes p) = a(m_1 \otimes (n_1 \otimes p)) + b(m_2 \otimes (n_1 \otimes p)) \\ &= a\phi_p(m_1, n_1) + b\phi_p(m_2, n_1)\end{aligned}$$

e

$$\begin{aligned}\phi_p(m_1, an_1 + bn_2) &= m_1 \otimes ((an_1 + bn_2) \otimes p) = m_1 \otimes (a(n_1 \otimes p) + b(n_2 \otimes p)) \\ &= a(m_1 \otimes (n_1 \otimes p)) + b(m_1 \otimes (n_2 \otimes p)) \\ &= a\phi_p(m_1, n_1) + b\phi_p(m_1, n_2)\end{aligned}$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N$. Pela Propriedade Universal do Produto Tensorial, ϕ_p induz o mapa A -linear

$$\begin{aligned}\bar{\Phi}_p: M \otimes_A N &\rightarrow M \otimes_A (N \otimes_A P) \\ m \otimes n &\mapsto m \otimes (n \otimes p)\end{aligned}$$

para cada $p \in P$. Agora, definamos o mapa

$$\begin{aligned}\phi: (M \otimes_A N) \times P &\rightarrow M \otimes_A (N \otimes_A P) \\ (t, p) &\mapsto \bar{\Phi}_p(t),\end{aligned}$$

o qual é A -bilinear, pois $\phi(_, p) = \overline{\Phi}_p$ é A -linear para cada $p \in P$ e

$$\begin{aligned}
 \phi\left(\sum_{i=1}^r m_i \otimes n_i, ap_1 + bp_2\right) &= \overline{\Phi}_{ap_1+bp_2}\left(\sum_{i=1}^r m_i \otimes n_i\right) \\
 &= \sum_{i=1}^r m_i \otimes (n_i \otimes (ap_1 + bp_2)) \\
 &= \sum_{i=1}^r a(m_i \otimes (n_i \otimes p_1)) + b(m_i \otimes (n_i \otimes p_2)) \\
 &= a \sum_{i=1}^r \phi(m_i \otimes n_i, p_1) + b \sum_{i=1}^r \phi(m_i \otimes n_i, p_2) \\
 &= a\phi\left(\sum_{i=1}^r m_i \otimes n_i, p_1\right) + b\phi\left(\sum_{i=1}^r m_i \otimes n_i, p_2\right)
 \end{aligned}$$

para todos $a, b \in A$, $r \in \mathbb{N} \setminus \{0\}$, $m_1, \dots, m_r \in M$, $n_1, \dots, n_r \in N$ e $p_1, p_2 \in P$. Pela Propriedade Universal do Produto Tensorial, ϕ induz o mapa A -linear

$$\begin{aligned}
 \overline{\Phi}: (M \otimes_A N) \otimes_A P &\rightarrow M \otimes_A (N \otimes_A P) \\
 (m \otimes n) \otimes p &\mapsto m \otimes (n \otimes p).
 \end{aligned}$$

Analogamente, para cada $m \in M$, o mapa

$$\begin{aligned}
 \psi_m: N \times P &\rightarrow (M \otimes_A N) \otimes_A P \\
 (n, p) &\mapsto (m \otimes n) \otimes p
 \end{aligned}$$

é A -bilinear e induz o mapa A -linear

$$\begin{aligned}
 \overline{\Psi}_m: N \otimes_A P &\rightarrow (M \otimes_A N) \otimes_A P \\
 n \otimes p &\mapsto (m \otimes n) \otimes p.
 \end{aligned}$$

Ainda de modo similar, o mapa

$$\begin{aligned}
 \psi: M \times (N \otimes_A P) &\rightarrow (M \otimes_A N) \otimes_A P \\
 (m, t) &\mapsto \overline{\Psi}_m(t)
 \end{aligned}$$

é A -bilinear e induz o mapa A -linear

$$\begin{aligned}
 \overline{\Psi}: M \otimes_A (N \otimes_A P) &\rightarrow (M \otimes_A N) \otimes_A P \\
 m \otimes (n \otimes p) &\mapsto (m \otimes n) \otimes p.
 \end{aligned}$$

Definamos os conjuntos

$$S = \{(m \otimes n) \otimes p; m \in M, n \in N \text{ e } p \in P\} \text{ e } S' = \{m \otimes (n \otimes p); m \in M, n \in N \text{ e } p \in P\}.$$

Claramente, $\bar{\Phi} \circ \bar{\Psi}|_{S'} = \text{id}_{M \otimes_A (N \otimes_A P)}|_{S'}$ e $\bar{\Psi} \circ \bar{\Phi}|_S = \text{id}_{(M \otimes_A N) \otimes_A P}|_S$. Visto que S e S' são conjuntos de geradores de $(M \otimes_A N) \otimes_A P$ e $M \otimes_A (N \otimes_A P)$, respectivamente, temos $\bar{\Phi} \circ \bar{\Psi} = \text{id}_{M \otimes_A (N \otimes_A P)}$ e $\bar{\Psi} \circ \bar{\Phi} = \text{id}_{(M \otimes_A N) \otimes_A P}$. Portanto, $\bar{\Phi}$ é um isomorfismo.

3. Consideremos a função

$$\begin{aligned} \phi: M \times \bigoplus_{\lambda \in \Lambda} N_\lambda &\rightarrow \bigoplus_{\lambda \in \Lambda} (M \otimes_A N_\lambda) \\ (m, (n_\lambda)_{\lambda \in \Lambda}) &\mapsto (m \otimes n_\lambda)_{\lambda \in \Lambda}. \end{aligned}$$

Notemos que

$$\begin{aligned} \phi(am_1 + bm_2, (n_\lambda)_{\lambda \in \Lambda}) &= ((am_1 + bm_2) \otimes n_\lambda)_{\lambda \in \Lambda} = (a(m_1 \otimes n_\lambda) + b(m_2 \otimes n_\lambda))_{\lambda \in \Lambda} \\ &= a(m_1 \otimes n_\lambda)_{\lambda \in \Lambda} + b(m_2 \otimes n_\lambda)_{\lambda \in \Lambda} \\ &= a\phi(m_1, (n_\lambda)_{\lambda \in \Lambda}) + b\phi(m_2, (n_\lambda)_{\lambda \in \Lambda}) \end{aligned}$$

e

$$\begin{aligned} \phi(m_1, a(n_\lambda)_{\lambda \in \Lambda} + b(n'_\lambda)_{\lambda \in \Lambda}) &= \phi(m_1, (an_\lambda + bn'_\lambda)_{\lambda \in \Lambda}) = (m_1 \otimes (an_\lambda + bn'_\lambda))_{\lambda \in \Lambda} \\ &= (a(m_1 \otimes n_\lambda) + b(m_1 \otimes n'_\lambda))_{\lambda \in \Lambda} \\ &= a(m_1 \otimes n_\lambda)_{\lambda \in \Lambda} + b(m_1 \otimes n'_\lambda)_{\lambda \in \Lambda} \\ &= a\phi(m_1, (n_\lambda)_{\lambda \in \Lambda}) + b\phi(m_1, (n'_\lambda)_{\lambda \in \Lambda}) \end{aligned}$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $(n_\lambda)_{\lambda \in \Lambda}, (n'_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} N_\lambda$, ou seja, ϕ é um mapa A -bilinear. Pela Propriedade Universal do Produto Tensorial, ϕ induz o mapa A -linear

$$\begin{aligned} \bar{\Phi}: M \otimes_A \bigoplus_{\lambda \in \Lambda} N_\lambda &\rightarrow \bigoplus_{\lambda \in \Lambda} (M \otimes_A N_\lambda) \\ m \otimes (n_\lambda)_{\lambda \in \Lambda} &\mapsto (m \otimes n_\lambda)_{\lambda \in \Lambda}. \end{aligned}$$

Para cada $\lambda_0 \in \Lambda$, definamos o mapa

$$\begin{aligned} \psi_{\lambda_0}: M \times N_{\lambda_0} &\rightarrow M \otimes_A \bigoplus_{\lambda \in \Lambda} N_\lambda \\ (m, n) &\mapsto m \otimes i_{\lambda_0}(n), \end{aligned}$$

onde i_{λ_0} é o homomorfismo de inclusão da parcela N_{λ_0} na soma direta $\bigoplus_{\lambda \in \Lambda} N_\lambda$, isto é,

$$\begin{aligned} i_{\lambda_0}: N_{\lambda_0} &\rightarrow \bigoplus_{\lambda \in \Lambda} N_\lambda \\ n &\mapsto i_{\lambda_0}(n): \Lambda \rightarrow \bigcup_{\lambda \in \Lambda} N_\lambda \\ \lambda &\mapsto \begin{cases} n & \text{se } \lambda = \lambda_0 \\ 0_{N_\lambda} & \text{se } \lambda \neq \lambda_0. \end{cases} \end{aligned}$$

Para cada $\lambda_0 \in \Lambda$, observemos que

$$\psi_{\lambda_0}(am_1 + bm_2, n_1) = (am_1 + bm_2) \otimes i_{\lambda_0}(n_1) = a\psi_{\lambda_0}(m_1, n_1) + b\psi_{\lambda_0}(m_2, n_1)$$

e

$$\begin{aligned} \psi_{\lambda_0}(m_1, an_1 + bn_2) &= m_1 \otimes i_{\lambda_0}(an_1 + bn_2) = m_1 \otimes (ai_{\lambda_0}(n_1) + bi_{\lambda_0}(n_2)) \\ &= a\psi_{\lambda_0}(m_1, n_1) + b\psi_{\lambda_0}(m_1, n_2) \end{aligned}$$

para todos $a, b \in A$, $m_1, m_2 \in M$ e $n_1, n_2 \in N_{\lambda_0}$, ou seja, ψ_{λ_0} é um mapa A -bilinear. Pela Propriedade Universal do Produto Tensorial, ψ_{λ_0} induz o mapa A -linear

$$\begin{aligned} \bar{\Psi}_{\lambda_0}: M \otimes_A N_{\lambda_0} &\rightarrow M \otimes_A \bigoplus_{\lambda \in \Lambda} N_{\lambda} \\ m \otimes n &\mapsto m \otimes i_{\lambda_0}(n) \end{aligned}$$

para cada $\lambda_0 \in \Lambda$. Agora, definamos o mapa

$$\begin{aligned} \bar{\Psi}: \bigoplus_{\lambda \in \Lambda} (M \otimes_A N_{\lambda}) &\rightarrow M \otimes_A \bigoplus_{\lambda \in \Lambda} N_{\lambda} \\ (t_{\lambda})_{\lambda \in \Lambda} &\mapsto \sum_{\lambda \in \Lambda} \bar{\Psi}_{\lambda}(t_{\lambda}). \end{aligned}$$

É fácil ver que $\bar{\Psi}$ é A -linear. Além disso, $\bar{\Phi} \circ \bar{\Psi} = \text{id}_{\bigoplus_{\lambda \in \Lambda} (M \otimes_A N_{\lambda})}$. De fato, se $(t_{\lambda})_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} (M \otimes_A N_{\lambda})$, então, para cada $\lambda \in \Lambda$, existem $r_{\lambda} \in \mathbb{N}$, $m_{\lambda 1}, \dots, m_{\lambda r_{\lambda}} \in M$ e $n_{\lambda 1}, \dots, n_{\lambda r_{\lambda}} \in N_{\lambda}$ tais que $t_{\lambda} = \sum_{i=1}^{r_{\lambda}} m_{\lambda i} \otimes n_{\lambda i}$ e, consequentemente,

$$\begin{aligned} \bar{\Phi} \circ \bar{\Psi}((t_{\lambda})_{\lambda \in \Lambda}) &= \bar{\Phi} \left(\sum_{\lambda \in \Lambda} \bar{\Psi}_{\lambda} \left(\sum_{i=1}^{r_{\lambda}} m_{\lambda i} \otimes n_{\lambda i} \right) \right) = \bar{\Phi} \left(\sum_{\lambda \in \Lambda} \sum_{i=1}^{r_{\lambda}} \bar{\Psi}_{\lambda}(m_{\lambda i} \otimes n_{\lambda i}) \right) \\ &= \bar{\Phi} \left(\sum_{\lambda \in \Lambda} \sum_{i=1}^{r_{\lambda}} (m_{\lambda i} \otimes i_{\lambda}(n_{\lambda i})) \right) = \sum_{\lambda \in \Lambda} \sum_{i=1}^{r_{\lambda}} \bar{\Phi}(m_{\lambda i} \otimes i_{\lambda}(n_{\lambda i})) \\ &= \sum_{\lambda \in \Lambda} \sum_{i=1}^{r_{\lambda}} i_{\lambda}(m_{\lambda i} \otimes n_{\lambda i}) = \sum_{\lambda \in \Lambda} i_{\lambda} \left(\sum_{i=1}^{r_{\lambda}} m_{\lambda i} \otimes n_{\lambda i} \right) \\ &= \left(\sum_{i=1}^{r_{\lambda}} m_{\lambda i} \otimes n_{\lambda i} \right)_{\lambda \in \Lambda} = (t_{\lambda})_{\lambda \in \Lambda}. \end{aligned}$$

Notemos que

$$\begin{aligned} \bar{\Psi} \circ \bar{\Phi}(m \otimes (n_{\lambda})_{\lambda \in \Lambda}) &= \bar{\Psi}((m \otimes n_{\lambda})_{\lambda \in \Lambda}) = \sum_{\lambda \in \Lambda} \bar{\Psi}_{\lambda}(m \otimes n_{\lambda}) \\ &= \sum_{\lambda \in \Lambda} m \otimes i_{\lambda}(n_{\lambda}) = m \otimes \sum_{\lambda \in \Lambda} i_{\lambda}(n_{\lambda}) \\ &= m \otimes (n_{\lambda})_{\lambda \in \Lambda} \end{aligned}$$

para todos $m \in M$ e $(n_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} N_\lambda$. Definindo

$$S = \left\{ m \otimes (n_\lambda)_{\lambda \in \Lambda}; \ m \in M \text{ e } (n_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} N_\lambda \right\},$$

vale $\bar{\Psi} \circ \bar{\Phi}|_S = \text{id}_{M \otimes_A \bigoplus_{\lambda \in \Lambda} N_\lambda}|_S$. Como S é um conjunto de geradores de $M \otimes_A \bigoplus_{\lambda \in \Lambda} N_\lambda$, temos $\bar{\Psi} \circ \bar{\Phi} = \text{id}_{M \otimes_A \bigoplus_{\lambda \in \Lambda} N_\lambda}$. Portanto, $\bar{\Phi}$ é um isomorfismo.

4. Seja ϕ a operação de “multiplicação por escalares” do A -módulo M , isto é,

$$\begin{aligned} \phi: \ A \times M &\rightarrow M \\ (a, m) &\mapsto am. \end{aligned}$$

Evidentemente, ϕ é A -bilinear. Pela Propriedade Universal do Produto Tensorial, ϕ induz o mapa A -linear

$$\begin{aligned} \bar{\Phi}: \ A \otimes_A M &\rightarrow M \\ a \otimes m &\mapsto am. \end{aligned}$$

Agora, definamos o mapa

$$\begin{aligned} \bar{\Psi}: \ M &\rightarrow A \otimes_A M \\ m &\mapsto 1 \otimes m. \end{aligned}$$

É fácil ver que $\bar{\Psi}$ é A -linear. Notemos que

$$\bar{\Phi} \circ \bar{\Psi}(m) = \bar{\Phi}(1 \otimes m) = 1m = m$$

e

$$\bar{\Psi} \circ \bar{\Phi}(a \otimes m) = \bar{\Psi}(am) = 1 \otimes (am) = a(1 \otimes m) = a \otimes m$$

para todos $a \in A$ e $m \in M$. Assim, $\bar{\Phi} \circ \bar{\Psi} = \text{id}_M$ e $\bar{\Psi} \circ \bar{\Phi}|_S = \text{id}_{A \otimes_A M}|_S$, onde

$$S = \{a \otimes m; \ a \in A \text{ e } m \in M\}.$$

Visto que S é um conjunto de geradores de $A \otimes_A M$, temos $\bar{\Psi} \circ \bar{\Phi} = \text{id}_{A \otimes_A M}$. Finalmente, concluímos que $\bar{\Phi}$ é um isomorfismo.

□

3.6 ÁLGEBRAS

Sejam A e B anéis e seja $\phi: A \rightarrow B$ um homomorfismo de anéis. De modo natural, esse homomorfismo induz a “multiplicação por escalares” seguinte:

$$\begin{aligned}\mu: A \times B &\rightarrow B \\ (a, b) &\mapsto \phi(a)b.\end{aligned}$$

É fácil ver que (B, μ) é um A -módulo. Como sempre, denotaremos $\mu(a, b)$ por, simplesmente, ab . Desse modo, B possui tanto uma estrutura de anel quanto uma estrutura de A -módulo, as quais são compatíveis no sentido de que satisfazem à condição seguinte:

$$a(b_1b_2) = (ab_1)b_2 = b_1(ab_2)$$

para todos $a \in A$ e $b_1, b_2 \in B$.

Definição 13. *Seja A um anel. Uma A -álgebra é um par (B, ϕ) , onde B é um anel e $\phi: A \rightarrow B$ é um homomorfismo de anéis. Além disso, chamamos ϕ de **homomorfismo base**.*

Observação 7. *Quando o homomorfismo ϕ estiver claro pelo contexto, referiremos ao próprio anel B como uma A -álgebra.*

Exemplo 8. *Seja A um anel.*

1. *O anel A é uma $\mathbb{Z}$ -álgebra com o homomorfismo natural*

$$\begin{aligned}\phi: \mathbb{Z} &\rightarrow A \\ n &\mapsto n1_A,\end{aligned}$$

onde 1_A denota o elemento neutro com respeito ao produto de A .

2. *O anel de polinômios $A[X_1, \dots, X_n]$ é uma A -álgebra com o homomorfismo inclusão*

$$\begin{aligned}i: A &\rightarrow A[X_1, \dots, X_n] \\ a &\mapsto a.\end{aligned}$$

Definição 14. *Seja A um anel e sejam (B, ϕ) e (C, ψ) A -álgebras. Um **homomorfismo de A -álgebras** é um homomorfismo de anéis $\alpha: B \rightarrow C$ compatível com os homomorfismos base $\phi: A \rightarrow B$ e $\psi: A \rightarrow C$, isto é, tal que $\alpha \circ \phi = \psi$.*

$$\begin{array}{ccc} B & \xrightarrow{\alpha} & C \\ \phi \swarrow & & \searrow \psi \\ & A & \end{array}$$

Proposição 9. *Seja A um anel e sejam (B, ϕ) e (C, ψ) A -álgebras. Um mapa $\alpha: B \rightarrow C$ será um homomorfismo de A -álgebras se, e somente se, for tanto um homomorfismo de anéis quanto um homomorfismo de A -módulos.*

Demonstração. Suponhamos que α seja um homomorfismo de A -álgebras. Em particular, α é um homomorfismo de anéis. Visto que $\alpha \circ \phi = \psi$, temos

$$\begin{aligned}\alpha(a_1b_1 + a_2b_2) &= \alpha(\phi(a_1)b_1 + \phi(a_2)b_2) = \alpha(\phi(a_1))\alpha(b_1) + \alpha(\phi(a_2))\alpha(b_2) \\ &= \psi(a_1)\alpha(b_1) + \psi(a_2)\alpha(b_2) = a_1\alpha(b_1) + a_2\alpha(b_2)\end{aligned}$$

para todos $a_1, a_2 \in A$ e $b_1, b_2 \in B$. Logo, α é também um homomorfismo de A -módulos.

Reciprocamente, suponhamos que α seja tanto um homomorfismo de anéis quanto um homomorfismo de A -módulos. Assim, para mostrar que α é um homomorfismo de A -álgebras, basta verificar que $\alpha \circ \phi = \psi$. E essa igualdade é, de fato, válida, pois

$$\alpha \circ \phi(a) = \alpha(\phi(a)1_B) = \alpha(a1_B) = a\alpha(1_B) = a1_C = \psi(a)1_C = \psi(a)$$

para todo $a \in A$. □

Exemplo 9. Sejam A um anel, B uma A -álgebra e $\lambda_1, \dots, \lambda_n \in B$. O mapa de avaliação

$$\begin{aligned}\alpha: A[X_1, \dots, X_n] &\rightarrow B \\ f(X_1, \dots, X_n) &\mapsto f(\lambda_1, \dots, \lambda_n)\end{aligned}$$

é um homomorfismo de A -álgebras.

Definição 15. Sejam A um anel e B uma A -álgebra. Uma **A -subálgebra** de B é um subconjunto C de B que é tanto um subanel quanto um A -módulo. Além disso, se Λ for um subconjunto qualquer de B , a menor A -subálgebra de B contendo Λ será chamada **A -subálgebra gerada** por Λ e será denotada por $A[\Lambda]$.

Observação 8. No caso em que Λ for finito, digamos, $\Lambda = \{\lambda_1, \dots, \lambda_n\}$, a A -subálgebra gerada por Λ será denotada por $A[\lambda_1, \dots, \lambda_n]$.

Proposição 10. Sejam A um anel, B uma A -álgebra e Λ um subconjunto de B . Temos

$$A[\Lambda] = \{f(\lambda_1, \dots, \lambda_r) \in B; r \in \mathbb{N} \setminus \{0\}, f \in A[X_1, \dots, X_r] \text{ e } \lambda_1, \dots, \lambda_r \in \Lambda\}.$$

Demonstração. Denotemos o conjunto

$$\{f(\lambda_1, \dots, \lambda_r) \in B; r \in \mathbb{N} \setminus \{0\}, f \in A[X_1, \dots, X_r] \text{ e } \lambda_1, \dots, \lambda_r \in \Lambda\}$$

por S . É fácil ver que S é uma A -subálgebra de B contendo Λ e, logo, $A[\Lambda] \subset S$.

Consideremos $s \in S$. Então, existem $n, r \in \mathbb{N}$, $m_{11}, \dots, m_{1r}, \dots, m_{n1}, \dots, m_{nr} \in \mathbb{N}$, $a_1, \dots, a_n \in A$ e $\lambda_1, \dots, \lambda_r \in \Lambda$ tais que $s = \sum_{i=1}^n a_i \prod_{j=1}^r \lambda_j^{m_{ij}}$. Visto que $A[\Lambda]$ é um subanel de B contendo Λ , o produto $\prod_{j=1}^r \lambda_j^{m_{ij}}$ é um elemento de $A[\Lambda]$ para todo $i \in \{1, \dots, n\}$. Além disso, como $A[\Lambda]$ é um submódulo de B , a combinação A -linear $\sum_{i=1}^n a_i \prod_{j=1}^r \lambda_j^{m_{ij}}$ pertence também a $A[\Lambda]$. Assim, $S \subset A[\Lambda]$, o que conclui a prova. □

Observação 9. No caso em que Λ for finito, digamos, $\Lambda = \{\lambda_1, \dots, \lambda_n\}$, teremos

$$A[\lambda_1, \dots, \lambda_n] = \{f(\lambda_1, \dots, \lambda_n) \in B; f \in A[X_1, \dots, X_n]\}.$$

Definição 16. Seja A um anel. Uma A -álgebra B será dita **finitamente gerada** se existir um subconjunto finito $\{\lambda_1, \dots, \lambda_n\} \subset B$ tal que $B = A[\lambda_1, \dots, \lambda_n]$.

Proposição 11. Seja A um anel. Uma A -álgebra B será finitamente gerada se, e somente se, existir um homomorfismo sobrejetor de A -álgebras $\alpha: A[X_1, \dots, X_n] \rightarrow B$ para algum inteiro positivo n .

Demonstração. Suponhamos que B seja uma A -álgebra finitamente gerada, isto é, $B = A[\lambda_1, \dots, \lambda_m]$ para certos $m \in \mathbb{N} \setminus \{0\}$ e $\lambda_1, \dots, \lambda_m \in B$. Definamos o homomorfismo avaliação

$$\begin{aligned} \beta: A[X_1, \dots, X_m] &\rightarrow B \\ f(X_1, \dots, X_m) &\mapsto f(\lambda_1, \dots, \lambda_m). \end{aligned}$$

Notemos que

$$\beta(A[X_1, \dots, X_m]) = \{f(\lambda_1, \dots, \lambda_m) \in B; f \in A[X_1, \dots, X_m]\} = A[\lambda_1, \dots, \lambda_m] = B,$$

isto é, β é um homomorfismo sobrejetor de A -álgebras.

Reciprocamente, suponhamos que $\alpha: A[X_1, \dots, X_n] \rightarrow B$ seja um homomorfismo sobrejetor de A -álgebras para determinado inteiro positivo n . Mostremos que $B = A[\alpha(X_1), \dots, \alpha(X_n)]$. Claramente, temos a inclusão $A[\alpha(X_1), \dots, \alpha(X_n)] \subset B$. Visto que α é sobrejetor, dado $b \in B$, existe $f \in A[X_1, \dots, X_n]$ tal que $b = \alpha(f)$. Por sua vez, existem $r \in \mathbb{N}$, $m_{11}, \dots, m_{1n}, \dots, m_{r1}, \dots, m_{rn} \in \mathbb{N}$ e $a_1, \dots, a_r \in A$ tais que $f(X_1, \dots, X_n) = \sum_{i=1}^r a_i \prod_{j=1}^n X_j^{m_{ij}}$. Desse modo,

$$\begin{aligned} b &= \alpha \left(\sum_{i=1}^r a_i \prod_{j=1}^n X_j^{m_{ij}} \right) = \sum_{i=1}^r a_i \alpha \left(\prod_{j=1}^n X_j^{m_{ij}} \right) \\ &= \sum_{i=1}^r a_i \prod_{j=1}^n \alpha(X_j)^{m_{ij}} = f(\alpha(X_1), \dots, \alpha(X_n)), \end{aligned}$$

ou seja, $b \in A[\alpha(X_1), \dots, \alpha(X_n)]$. Logo, $B = A[\alpha(X_1), \dots, \alpha(X_n)]$ é uma A -álgebra finitamente gerada. $\square$

3.7 PRODUTO TENSORIAL DE ÁLGEBRAS

Consideremos um anel A e sejam B e C A -álgebras. Nesta seção, veremos que o produto tensorial $B \otimes_A C$ admite uma estrutura de A -álgebra. Primeiramente, nosso objetivo é definir um produto em $B \otimes_A C$.

Para cada par $(b, c) \in B \times C$, definamos o mapa

$$\begin{aligned}\phi_{(b,c)}: B \times C &\rightarrow B \otimes_A C \\ (b', c') &\mapsto bb' \otimes cc',\end{aligned}$$

o qual é A -bilinear, pois

$$\begin{aligned}\phi_{(b,c)}(a_1b'_1 + a_2b'_2, c'_1) &= b(a_1b'_1 + a_2b'_2) \otimes cc'_1 = (b(a_1b'_1) + b(a_2b'_2)) \otimes cc'_1 \\ &= (a_1(bb'_1) + a_2(bb'_2)) \otimes cc'_1 = a_1(bb'_1 \otimes cc'_1) + a_2(bb'_2 \otimes cc'_1) \\ &= a_1\phi_{(b,c)}(b'_1, c'_1) + a_2\phi_{(b,c)}(b'_2, c'_1)\end{aligned}$$

e

$$\begin{aligned}\phi_{(b,c)}(b'_1, a_1c'_1 + a_2c'_2) &= bb'_1 \otimes c(a_1c'_1 + a_2c'_2) = bb'_1 \otimes (c(a_1c'_1) + c(a_2c'_2)) \\ &= bb'_1 \otimes (a_1(cc'_1) + a_2(cc'_2)) = a_1(bb'_1 \otimes cc'_1) + a_2(bb'_1 \otimes cc'_2) \\ &= a_1\phi_{(b,c)}(b'_1, c'_1) + a_2\phi_{(b,c)}(b'_1, c'_2)\end{aligned}$$

para todos $a_1, a_2 \in A$, $b'_1, b'_2 \in B$ e $c'_1, c'_2 \in C$. Pela Propriedade Universal do Produto Tensorial, o mapa A -bilinear $\phi_{(b,c)}$ induz o homomorfismo de A -módulos

$$\begin{aligned}\bar{\Phi}_{(b,c)}: B \otimes_A C &\rightarrow B \otimes_A C \\ b' \otimes c' &\mapsto bb' \otimes cc'\end{aligned}$$

para cada $(b, c) \in B \times C$. Isso nos permite definir o mapa seguinte:

$$\begin{aligned}\psi: B \times C &\rightarrow \text{Hom}_A(B \otimes_A C, B \otimes_A C) \\ (b, c) &\mapsto \bar{\Phi}_{(b,c)}.\end{aligned}$$

Notemos que, para todos $a_1, a_2 \in A$, $b_1, b_2, b' \in B$ e $c_1, c_2, c' \in C$, temos

$$\begin{aligned}\psi(a_1b_1 + a_2b_2, c_1)(b' \otimes c') &= (a_1b_1 + a_2b_2)b' \otimes c_1c' \\ &= a_1(b_1b' \otimes c_1c') + a_2(b_2b' \otimes c_1c') \\ &= a_1(\psi(b_1, c_1)(b' \otimes c')) + a_2(\psi(b_2, c_1)(b' \otimes c')) \\ &= (a_1\psi(b_1, c_1) + a_2\psi(b_2, c_1))(b' \otimes c')\end{aligned}$$

e

$$\begin{aligned}\psi(b_1, a_1c_1 + a_2c_2)(b' \otimes c') &= b_1b' \otimes (a_1c_1 + a_2c_2)c' \\ &= a_1(b_1b' \otimes c_1c') + a_2(b_1b' \otimes c_2c') \\ &= a_1(\psi(b_1, c_1)(b' \otimes c')) + a_2(\psi(b_1, c_2)(b' \otimes c')) \\ &= (a_1\psi(b_1, c_1) + a_2\psi(b_1, c_2))(b' \otimes c').\end{aligned}$$

Em outras palavras, para todos $a_1, a_2 \in A$, $b_1, b_2 \in B$ e $c_1, c_2 \in C$, valem

$$\psi(a_1b_1 + a_2b_2, c_1)|_S = (a_1\psi(b_1, c_1) + a_2\psi(b_2, c_1))|_S$$

e

$$\psi(b_1, a_1c_1 + a_2c_2)|_S = (a_1\psi(b_1, c_1) + a_2\psi(b_1, c_2))|_S,$$

onde $S = \{b \otimes c; b \in B \text{ e } c \in C\}$. Visto que S é um conjunto de geradores do produto tensorial $B \otimes_A C$, temos

$$\psi(a_1b_1 + a_2b_2, c_1) = a_1\psi(b_1, c_1) + a_2\psi(b_2, c_1) \quad \text{e} \quad \psi(b_1, a_1c_1 + a_2c_2) = a_1\psi(b_1, c_1) + a_2\psi(b_1, c_2)$$

para todos $a_1, a_2 \in A$, $b_1, b_2 \in B$ e $c_1, c_2 \in C$, ou seja, o mapa ψ é A -bilinear. Pela Propriedade Universal do Produto Tensorial, esse mapa induz o homomorfismo de A -módulos

$$\begin{aligned} \bar{\Psi}: B \otimes_A C &\rightarrow \text{Hom}_A(B \otimes_A C, B \otimes_A C) \\ b \otimes c &\mapsto \bar{\Phi}_{(b,c)}. \end{aligned}$$

Finalmente, definamos o produto em $B \otimes_A C$ da maneira seguinte:

$$\begin{aligned} \cdot: (B \otimes_A C) \times (B \otimes_A C) &\rightarrow B \otimes_A C \\ (t_1, t_2) &\mapsto \bar{\Psi}(t_1)(t_2). \end{aligned}$$

Explicitamente, temos

$$(b_1 \otimes c_1) \cdot (b_2 \otimes c_2) = \bar{\Psi}(b_1 \otimes c_1)(b_2 \otimes c_2) = \bar{\Phi}_{(b_1, c_1)}(b_2 \otimes c_2) = b_1b_2 \otimes c_1c_2$$

para todos $b_1, b_2 \in B$ e $c_1, c_2 \in C$. E, de modo geral,

$$\begin{aligned} \left(\sum_{i=1}^m b_i \otimes c_i \right) \cdot \left(\sum_{j=1}^n b'_j \otimes c'_j \right) &= \bar{\Psi} \left(\sum_{i=1}^m b_i \otimes c_i \right) \left(\sum_{j=1}^n b'_j \otimes c'_j \right) = \left(\sum_{i=1}^m \bar{\Phi}_{(b_i, c_i)} \right) \left(\sum_{j=1}^n b'_j \otimes c'_j \right) \\ &= \sum_{i=1}^m \bar{\Phi}_{(b_i, c_i)} \left(\sum_{j=1}^n b'_j \otimes c'_j \right) = \sum_{i=1}^m \sum_{j=1}^n \bar{\Phi}_{(b_i, c_i)}(b'_j \otimes c'_j) \\ &= \sum_{i=1}^m \sum_{j=1}^n b_i b'_j \otimes c_i c'_j \end{aligned}$$

para todos $m, n \in \mathbb{N} \setminus \{0\}$, $b_1, \dots, b_m, b'_1, \dots, b'_n \in B$ e $c_1, \dots, c_m, c'_1, \dots, c'_n \in C$.

Agora, verifiquemos que $(B \otimes_A C, +, \cdot)$ é um anel. Já sabemos que $(B \otimes_A C, +)$ é um grupo abeliano. Além disso, dados $t_1, t_2, t_3 \in B \otimes_A C$, existem $m, n, p \in \mathbb{N}$, $b_1, \dots, b_{m+n+p} \in B$ e $c_1, \dots, c_{m+n+p} \in C$ tais que

$$t_1 = \sum_{i=1}^m b_i \otimes c_i, \quad t_2 = \sum_{j=1}^n b_{m+j} \otimes c_{m+j} \quad \text{e} \quad t_3 = \sum_{k=1}^p b_{m+n+k} \otimes c_{m+n+k}.$$

Isso nos permite concluir que o produto é associativo:

$$\begin{aligned}
 (t_1 \cdot t_2) \cdot t_3 &= \left(\sum_{i=1}^m \sum_{j=1}^n b_i b_{m+j} \otimes c_i c_{m+j} \right) \cdot \left(\sum_{k=1}^p b_{m+n+k} \otimes c_{m+n+k} \right) \\
 &= \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^p (b_i b_{m+j}) b_{m+n+k} \otimes (c_i c_{m+j}) c_{m+n+k} \\
 &= \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^p b_i (b_{m+j} b_{m+n+k}) \otimes c_i (c_{m+j} c_{m+n+k}) \\
 &= \left(\sum_{i=1}^m b_i \otimes c_i \right) \cdot \left(\sum_{j=1}^n \sum_{k=1}^p b_{m+j} b_{m+n+k} \otimes c_{m+j} c_{m+n+k} \right) \\
 &= t_1 \cdot (t_2 \cdot t_3).
 \end{aligned}$$

O produto é também comutativo:

$$t_1 \cdot t_2 = \sum_{i=1}^m \sum_{j=1}^n b_i b_{m+j} \otimes c_i c_{m+j} = \sum_{j=1}^n \sum_{i=1}^m b_{m+j} b_i \otimes c_{m+j} c_i = t_2 \cdot t_1.$$

O produto é distributivo com relação à soma:

$$\begin{aligned}
 t_1 \cdot (t_2 + t_3) &= \left(\sum_{i=1}^m b_i \otimes c_i \right) \cdot \left(\sum_{j=1}^{n+p} b_{m+j} \otimes c_{m+j} \right) \\
 &= \sum_{i=1}^m \sum_{j=1}^{n+p} b_i b_{m+j} \otimes c_i c_{m+j} \\
 &= \sum_{i=1}^m \left(\left(\sum_{j=1}^n b_i b_{m+j} \otimes c_i c_{m+j} \right) + \left(\sum_{k=n+1}^{n+p} b_i b_{m+k} \otimes c_i c_{m+k} \right) \right) \\
 &= \sum_{i=1}^m \sum_{j=1}^n b_i b_{m+j} \otimes c_i c_{m+j} + \sum_{i=1}^m \sum_{k=1}^p b_i b_{m+n+k} \otimes c_i c_{m+n+k} \\
 &= t_1 \cdot t_2 + t_1 \cdot t_3.
 \end{aligned}$$

E, por fim, $1_B \otimes 1_C$ é o elemento neutro com respeito ao produto:

$$t_1 \cdot (1_B \otimes 1_C) = \sum_{i=1}^m b_i 1_B \otimes c_i 1_C = t_1.$$

Logo, $(B \otimes_A C, +, \cdot)$ é, de fato, um anel. Para vermos esse anel como uma A -álgebra, resta definirmos um homomorfismo de anéis de A em $B \otimes_A C$. Para tal, consideremos o mapa

$$\begin{aligned}
 \varphi: A &\rightarrow B \otimes_A C \\
 a &\mapsto (a 1_B) \otimes 1_C.
 \end{aligned}$$

Observemos que, para todos $a_1, a_2 \in A$, temos:

- (i) $\varphi(a_1 + a_2) = ((a_1 + a_2)1_B) \otimes 1_C = (a_1 1_B + a_2 1_B) \otimes 1_C = \varphi(a_1) + \varphi(a_2);$
- (ii) $\varphi(a_1 a_2) = ((a_1 a_2)(1_B 1_B)) \otimes 1_C = ((a_1 1_B)(a_2 1_B)) \otimes 1_C = \varphi(a_1) \cdot \varphi(a_2);$
- (iii) $\varphi(1_A) = (1_A 1_B) \otimes 1_C = 1_B \otimes 1_C.$

Portanto, φ é um homomorfismo de anéis e $B \otimes_A C$ é uma A -álgebra com esse homomorfismo.

Observação 10. Notemos que a “multiplicação por escalares” induzida pelo homomorfismo φ em $B \otimes_A C$ coincide com a “multiplicação por escalares” da estrutura de A -módulo que $B \otimes_A C$ possui como produto tensorial de A -módulos. De fato, para todo $a \in A$, vale

$$\begin{aligned} \varphi(a) \cdot t_1 &= ((a 1_B) \otimes 1_C) \cdot \left(\sum_{i=1}^m b_i \otimes c_i \right) = \sum_{i=1}^m ((a 1_B) b_i) \otimes (1_C c_i) \\ &= \sum_{i=1}^m (a(1_B b_i)) \otimes c_i = \sum_{i=1}^m a(b_i \otimes c_i) = a t_1. \end{aligned}$$

Exemplo 10. Sejam B e C A -álgebras. Os mapas

$$\begin{array}{ccc} \alpha: B & \rightarrow & B \otimes_A C \quad \text{e} \quad \beta: C & \rightarrow & B \otimes_A C \\ b & \mapsto & b \otimes 1_C & & c & \mapsto & 1_B \otimes c \end{array}$$

são homomorfismos de A -álgebras. De fato, para todos $a_1, a_2 \in A$, $b_1, b_2 \in B$ e $c_1, c_2 \in C$, temos:

- (i) $\alpha(a_1 b_1 + a_2 b_2) = (a_1 b_1 + a_2 b_2) \otimes 1_C = ((a_1 b_1) \otimes 1_C) + ((a_2 b_2) \otimes 1_C) = a_1 \alpha(b_1) + a_2 \alpha(b_2);$
- (ii) $\alpha(b_1 b_2) = (b_1 b_2) \otimes 1_C = (b_1 \otimes 1_C) \cdot (b_2 \otimes 1_C) = \alpha(b_1) \cdot \alpha(b_2);$
- (iii) $\alpha(1_B) = 1_B \otimes 1_C;$
- (iv) $\beta(a_1 c_1 + a_2 c_2) = 1_B \otimes (a_1 c_1 + a_2 c_2) = (1_B \otimes (a_1 c_1)) + (1_B \otimes (a_2 c_2)) = a_1 \beta(c_1) + a_2 \beta(c_2);$
- (v) $\beta(c_1 c_2) = 1_B \otimes (c_1 c_2) = (1_B \otimes c_1) \cdot (1_B \otimes c_2) = \beta(c_1) \cdot \beta(c_2);$
- (vi) $\beta(1_C) = 1_B \otimes 1_C.$

Por meio desses homomorfismos, poderemos apresentar uma importante propriedade do produto tensorial de álgebras no próximo teorema. Para isso, precisaremos do lema seguinte.

Lema 6. Sejam B e C A -álgebras, S um conjunto de geradores do A -módulo B e $\phi: B \rightarrow C$ um homomorfismo de A -módulos tal que $\phi(1_B) = 1_C$. Se $\phi(s_1 s_2) = \phi(s_1) \phi(s_2)$ para todos $s_1, s_2 \in S$, então ϕ será um homomorfismo de A -álgebras.

Demonstração. Sejam b_1 e b_2 elementos de B . Então, existem $a_1, \dots, a_m, a'_1, \dots, a'_n \in A$ e $s_1, \dots, s_m, s'_1, \dots, s'_n \in S$ tais que

$$b_1 = \sum_{i=1}^m a_i s_i \quad \text{e} \quad b_2 = \sum_{j=1}^n a'_j s'_j.$$

Notemos que

$$\begin{aligned}
 \phi(b_1 b_2) &= \phi \left(\left(\sum_{i=1}^m a_i s_i \right) \left(\sum_{j=1}^n a'_j s'_j \right) \right) = \phi \left(\sum_{i=1}^m (a_i s_i) \left(\sum_{j=1}^n a'_j s'_j \right) \right) \\
 &= \phi \left(\sum_{i=1}^m \sum_{j=1}^n (a_i s_i) (a'_j s'_j) \right) = \phi \left(\sum_{i=1}^m \sum_{j=1}^n (a_i a'_j) (s_i s'_j) \right) \\
 &= \sum_{i=1}^m \sum_{j=1}^n (a_i a'_j) \phi(s_i s'_j) = \sum_{i=1}^m \sum_{j=1}^n (a_i a'_j) (\phi(s_i) \phi(s'_j)) \\
 &= \sum_{i=1}^m \sum_{j=1}^n (a_i \phi(s_i)) (a'_j \phi(s'_j)) = \sum_{i=1}^m (a_i \phi(s_i)) \left(\sum_{j=1}^n a'_j \phi(s'_j) \right) \\
 &= \left(\sum_{i=1}^m a_i \phi(s_i) \right) \left(\sum_{j=1}^n a'_j \phi(s'_j) \right) = \phi \left(\sum_{i=1}^m a_i s_i \right) \phi \left(\sum_{j=1}^n a'_j s'_j \right) \\
 &= \phi(b_1) \phi(b_2).
 \end{aligned}$$

Logo, ϕ é um homomorfismo de A -álgebras. □

Teorema 8. *Sejam B e C A -álgebras e consideremos os homomorfismos de A -álgebras*

$$\begin{aligned}
 \alpha: B &\rightarrow B \otimes_A C & \text{e} & \quad \beta: C \rightarrow B \otimes_A C \\
 b &\mapsto b \otimes 1_C & & \quad c \mapsto 1_B \otimes c.
 \end{aligned}$$

Seja D uma A -álgebra qualquer. Dados homomorfismos de A -álgebras $\phi: B \rightarrow D$ e $\psi: C \rightarrow D$, existe um único homomorfismo de A -álgebras $\bar{\Gamma}: B \otimes_A C \rightarrow D$ tal que o diagrama

$$\begin{array}{ccccc}
 & & B \otimes_A C & & \\
 & \nearrow \alpha & \downarrow \exists! \bar{\Gamma} & \nwarrow \beta & \\
 B & \xrightarrow{\phi} & D & \xleftarrow{\psi} & C \\
 & \nwarrow & \uparrow & \nearrow & \\
 & & A & &
 \end{array}$$

comuta, isto é, $\bar{\Gamma} \circ \alpha = \phi$ e $\bar{\Gamma} \circ \beta = \psi$.

Demonstração. Primeiramente, mostremos a existência de um homomorfismo de A -álgebras com essa propriedade. Sejam $\phi: B \rightarrow D$ e $\psi: C \rightarrow D$ homomorfismos de A -álgebras. Pela Propriedade Universal do Produto Tensorial, o mapa A -bilinear

$$\begin{aligned}
 \gamma: B \times C &\rightarrow D \\
 (b, c) &\mapsto \phi(b)\psi(c)
 \end{aligned}$$

induz o homomorfismo de A -módulos

$$\begin{aligned}
 \bar{\Gamma}: B \otimes_A C &\rightarrow D \\
 b \otimes c &\mapsto \phi(b)\psi(c).
 \end{aligned}$$

Notemos que

$$\bar{\Gamma}(1_B \otimes 1_C) = \phi(1_B)\psi(1_C) = 1_D 1_D = 1_D$$

e

$$\begin{aligned} \bar{\Gamma}((b_1 \otimes c_1) \cdot (b_2 \otimes c_2)) &= \bar{\Gamma}(b_1 b_2 \otimes c_1 c_2) = \phi(b_1 b_2)\psi(c_1 c_2) = \phi(b_1)\psi(c_1)\phi(b_2)\psi(c_2) \\ &= \bar{\Gamma}(b_1 \otimes c_1)\bar{\Gamma}(b_2 \otimes c_2) \end{aligned}$$

para todos $b_1, b_2 \in B$ e $c_1, c_2 \in C$. Pelo Lema 6, $\bar{\Gamma}$ é também um homomorfismo de A -álgebras. Além disso, para todos $b \in B$ e $c \in C$, temos

$$\bar{\Gamma} \circ \alpha(b) = \bar{\Gamma}(b \otimes 1_C) = \phi(b)\psi(1_C) = \phi(b)1_D = \phi(b)$$

e

$$\bar{\Gamma} \circ \beta(c) = \bar{\Gamma}(1_B \otimes c) = \phi(1_B)\psi(c) = 1_D\psi(c) = \psi(c),$$

ou seja, $\bar{\Gamma} \circ \alpha = \phi$ e $\bar{\Gamma} \circ \beta = \psi$.

Agora, mostremos que $\bar{\Gamma}$ é o único homomorfismo de A -álgebras que faz o diagrama anterior comutar. Seja $\delta: B \otimes_A C \rightarrow D$ um homomorfismo de A -álgebras tal que $\delta \circ \alpha = \phi$ e $\delta \circ \beta = \psi$. Observemos que

$$\delta(b \otimes c) = \delta((b \otimes 1_C) \cdot (1_B \otimes c)) = \delta(b \otimes 1_C)\delta(1_B \otimes c) = \delta(\alpha(b))\delta(\beta(c)) = \phi(b)\psi(c) = \bar{\Gamma}(b \otimes c)$$

para todos $b \in B$ e $c \in C$. Em outras palavras, $\delta|_S = \bar{\Gamma}|_S$, onde

$$S = \{b \otimes c; b \in B \text{ e } c \in C\}.$$

Visto que S é um conjunto de geradores do A -módulo $B \otimes_A C$, a Proposição 6 fornece que $\delta = \bar{\Gamma}$. Isso conclui a prova. $\square$

4. VARIEDADES ALGÉBRICAS AFINS

Os espaços afins e as variedades algébricas afins são os principais ingredientes deste capítulo. Inicialmente, trataremos das propriedades básicas das variedades algébricas afins e de seus ideais correspondentes. Em seguida, apresentaremos o Teorema da Base de Hilbert e a Topologia de Zariski nos espaços afins. Ao final deste capítulo, essas duas ferramentas serão essenciais para provarmos que é possível escrever qualquer variedade algébrica afim como a união finita de suas componentes irredutíveis. As principais referências utilizadas neste capítulo foram [2] e [6].

Ao longo deste capítulo, L denotará um corpo e K um subcorpo de L .

4.1 VARIEDADES ALGÉBRICAS AFINS E SEUS RESPECTIVOS IDEAIS

Definição 17. *Seja n um inteiro positivo.*

1. O conjunto L^n é chamado **espaço afim** de dimensão n sobre L e é denotado por $\mathbb{A}^n(L)$.
2. Um subconjunto $V \subset \mathbb{A}^n(L)$ será chamado **K -variedade algébrica afim** se existirem polinômios $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ de modo que V seja o conjunto solução do sistema de equações

$$\begin{cases} f_1(X_1, \dots, X_n) = 0 \\ f_2(X_1, \dots, X_n) = 0 \\ \vdots \\ f_m(X_1, \dots, X_n) = 0 \end{cases}$$

em $\mathbb{A}^n(L)$. Esse sistema é dito **sistema de equações que define V** .

Observação 11.

1. Por simplicidade, escreveremos apenas K -variedade para nos referirmos a uma K -variedade algébrica afim. Além disso, escreveremos simplesmente

$$f_i(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, m\})$$

para representar o sistema do segundo item da definição anterior.

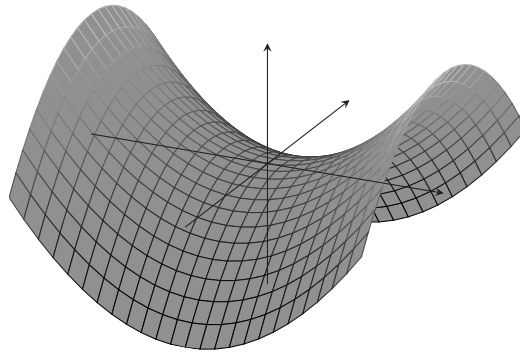
2. Uma K -variedade V é também uma K' -variedade para qualquer subcorpo $K' \subset L$ que contém todos os coeficientes de um sistema de equações que define V . Isso ocorre, por exemplo, se tivermos $K \subset K'$.

Em nosso cotidiano, é comum nos depararmos com K -variedades. Vejamos dois exemplos bem familiares.

Exemplo 11.

1. Em $\mathbb{A}^n(L)$, os conjuntos que são solução de sistemas de equações lineares com coeficientes em K , popularizados pela Álgebra Linear, são as K -variedades lineares.
2. Em $\mathbb{A}^n(L)$, o conjunto dos zeros de um polinômio não constante $f \in K[X_1, \dots, X_n]$ é uma K -hipersuperfície. Em particular, K -hipersuperfícies em $\mathbb{A}^2(L)$ recebem o nome de curvas algébricas planas. Por definição, toda K -variedade V em $\mathbb{A}^n(L)$, com $V \neq \mathbb{A}^n(L)$, é a interseção de uma quantidade finita de K -hipersuperfícies.

Figura 4.1: $\mathbb{Q}$ -hipersuperfície definida pela equação $X_1^2 - X_2^2 - X_3 = 0$ em $\mathbb{A}^3(\mathbb{R})$



Lema 7. A união e a interseção de duas K -variedades de $\mathbb{A}^n(L)$ são também K -variedades de $\mathbb{A}^n(L)$.

Demonstração. Sejam V_1 e V_2 K -variedades definidas pelos sistemas

$$f_i(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, r\})$$

e

$$f_j(X_1, \dots, X_n) = 0 \quad (j \in \{r+1, \dots, r+s\}),$$

respectivamente. É fácil ver que a interseção $V_1 \cap V_2$ é a K -variedade definida pelo sistema

$$f_i(X_1, \dots, X_n) \quad (i \in \{1, \dots, r+s\}).$$

Agora, mostremos que a união $V_1 \cup V_2$ é a K -variedade definida pelo sistema

$$f_i(X_1, \dots, X_n)f_j(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, r\} \text{ e } j \in \{r+1, \dots, r+s\}).$$

Seja $x \in V_1 \cup V_2$, isto é, x é zero dos polinômios $f_1, \dots, f_r$ ou x é zero dos polinômios $f_{r+1}, \dots, f_{r+s}$. Em ambos os casos, x é solução do sistema

$$f_i(X_1, \dots, X_n)f_j(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, r\} \text{ e } j \in \{r+1, \dots, r+s\}).$$

Reciprocamente, seja y uma solução do sistema acima. Suponhamos que $y \notin V_1$, isto é, existe $i \in \{1, \dots, r\}$ tal que $f_i(y) \neq 0$. Por hipótese, para cada $j \in \{r+1, \dots, r+s\}$, temos $f_i(y)f_j(y) = 0$ e, por consequência, vale $f_j(y) = 0$. Logo, $y \in V_1 \cup V_2$, o que conclui a prova. $\square$

Nos espaços afins de dimensão $n \geq 2$ sobre o corpo $\mathbb{R}$, uma K -hipersuperfície pode ser vazia ou consistir em um único ponto. Por exemplo, as equações $X_1^2 + \dots + X_n^2 + 1 = 0$ e $X_1^2 + \dots + X_n^2 = 0$ definem as $\mathbb{Q}$ -hipersuperfícies $\emptyset$ e $\{0\}$, respectivamente. Entretanto, existem corpos imunes a esse fenômeno: os corpos algebricamente fechados.

Definição 18. Diremos que L é um **corpo algebricamente fechado** se todo polinômio não constante $f \in L[X]$ possuir uma raiz $a \in L$.

Observação 12. Todo corpo algebricamente fechado é infinito. De fato, se L for finito, digamos, $L = \{a_1, \dots, a_r\}$, então o polinômio não constante $(X-a_1)(X-a_2)\dots(X-a_r)+1 \in L[X]$ não possuirá raiz em L .

Na proposição seguinte, veremos, em particular, que existem infinitos pontos “dentro” e “fora” das hipersuperfícies que habitam espaços afins de dimensão $n \geq 2$ sobre corpos algebricamente fechados.

Proposição 12.

1. Se L for infinito e $n \geq 1$, então o complementar de qualquer K -hipersuperfície em $\mathbb{A}^n(L)$ conterá infinitos pontos. Em particular, o complementar de qualquer K -variedade V em $\mathbb{A}^n(L)$, com $V \neq \mathbb{A}^n(L)$, conterá infinitos pontos.
2. Se L for algebricamente fechado e $n \geq 2$, então toda K -hipersuperfície em $\mathbb{A}^n(L)$ conterá infinitos pontos.

Demonstração.

1. Provemos a primeira afirmação utilizando indução sobre n .

Seja f um polinômio não constante em $K[X_1]$. Visto que L é infinito e f possui uma quantidade finita de zeros em L , existem infinitos elementos em $\mathbb{A}^1(L)$ que não são zeros de f . Logo, a afirmação é verdadeira quando $n = 1$.

Suponhamos que o complementar de qualquer K -hipersuperfície em $\mathbb{A}^{n-1}(L)$ possua infinitos pontos, onde $n-1$ é determinado inteiro positivo, e provemos que a afirmação é válida para n . Seja g um polinômio não constante em $K[X_1, \dots, X_n]$. Com isso,

$$g = g_0 + g_1X_n + \dots + g_rX_n^r$$

para certos $r \in \mathbb{N}$ e $g_0, \dots, g_r \in K[X_1, \dots, X_{n-1}]$, com $g_r \neq 0$. Pela hipótese de indução, existe $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}(L)$ tal que $g_r(a_1, \dots, a_{n-1}) \neq 0$. Desse modo, $g(a_1, \dots, a_{n-1}, X_n)$ é um polinômio não nulo em $L[X_n]$. Como ele possui uma quantidade finita de zeros no corpo infinito L , o conjunto

$$\{(a_1, \dots, a_{n-1}, a_n) \in \mathbb{A}^n(L); g(a_1, \dots, a_{n-1}, a_n) \neq 0\}$$

é infinito e está contido no complementar da K -hipersuperfície definida pela equação $g(X_1, \dots, X_n) = 0$ em $\mathbb{A}^n(L)$. Pelo Princípio de Indução Finita, a afirmação é válida para todo inteiro positivo n .

2. Sejam $n \geq 2$, h um polinômio não constante em $K[X_1, \dots, X_n]$ e H a K -hipersuperfície definida pela equação $h(X_1, \dots, X_n) = 0$ em $\mathbb{A}^n(L)$. Sem perda de generalidade, suponha que seja possível escrever

$$h = h_0 + h_1 X_n + \dots + h_s X_n^s$$

para certos $s \in \mathbb{N} \setminus \{0\}$ e $h_0, \dots, h_s \in K[X_1, \dots, X_{n-1}]$, com $h_s \neq 0$. Pelo item anterior, o conjunto

$$B := \{(b_1, \dots, b_{n-1}) \in \mathbb{A}^{n-1}(L); h_s(b_1, \dots, b_{n-1}) \neq 0\}$$

é infinito. Notemos que, para cada $(b'_1, \dots, b'_{n-1}) \in B$, $h(b'_1, \dots, b'_{n-1}, X_n)$ é um polinômio não constante em $L[X_n]$ e, como L é algebricamente fechado, existe $b'_n \in L$ tal que $h(b'_1, \dots, b'_{n-1}, b'_n) = 0$. Portanto, o conjunto

$$\{(b_1, \dots, b_{n-1}, b_n) \in \mathbb{A}^n(L); (b_1, \dots, b_{n-1}) \in B \text{ e } h(b_1, \dots, b_{n-1}, b_n) = 0\}$$

é infinito e está contido em H .

□

É claro que, para um subconjunto $V \subset \mathbb{A}^n(L)$, o polinômio $0 \in K[X_1, \dots, X_n]$ anula-se em todos os pontos de V . Além disso, se $f, g \in K[X_1, \dots, X_n]$ forem polinômios que se anulam em todos os pontos de V , então

$$(af + bg)(x) = a(x)f(x) + b(x)g(x) = a(x) \cdot 0 + b(x) \cdot 0 = 0$$

para todos $a, b \in K[X_1, \dots, X_n]$ e $x \in V$. Portanto, o conjunto de todos os polinômios em $K[X_1, \dots, X_n]$ que se anulam em V é um ideal desse anel, fazendo jus à definição seguinte.

Definição 19. *Seja V um subconjunto de $\mathbb{A}^n(L)$. O conjunto*

$$\{f \in K[X_1, \dots, X_n]; f(x) = 0 \text{ para todo } x \in V\}$$

*é chamado **ideal de V em $K[X_1, \dots, X_n]$** e é denotado por $\mathcal{I}(V)$.*

Proposição 13. *Sejam L um corpo algebricamente fechado e $n \geq 1$. Consideremos um polinômio não constante $f \in K[X_1, \dots, X_n]$ e H a K -hipersuperfície em $\mathbb{A}^n(L)$ definida pela equação $f(X_1, \dots, X_n) = 0$. Seja $f = u f_1^{\alpha_1} f_2^{\alpha_2} \cdots f_r^{\alpha_r}$ a decomposição de f em um produto de potências de polinômios irredutíveis $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ que são dois a dois não associados, onde $u \in K^\times$. Então, $\mathcal{I}(H) = (f_1 f_2 \cdots f_r)$.*

Demonstração. Primeiramente, mostremos que o polinômio $f_1 f_2 \cdots f_r$ anula-se em todos os pontos de H . Se $x \in H$, então

$$u f_1^{\alpha_1}(x) f_2^{\alpha_2}(x) \cdots f_r^{\alpha_r}(x) = f(x) = 0.$$

Desse modo, existe $j \in \{1, \dots, r\}$ tal que $f_j(x) = 0$ e, assim,

$$(f_1 f_2 \cdots f_r)(x) = f_j(x) \cdot \prod_{\substack{i=1 \\ i \neq j}}^r f_i(x) = 0 \cdot \prod_{\substack{i=1 \\ i \neq j}}^r f_i(x) = 0.$$

Logo, $f_1 f_2 \cdots f_r \in \mathcal{I}(H)$ e, conseqüentemente, $(f_1 f_2 \cdots f_r) \subset \mathcal{I}(H)$.

Seja $g \in \mathcal{I}(H)$. Como $K[X_1, \dots, X_n]$ é um domínio fatorial e $f_1, \dots, f_r$ são polinômios irredutíveis que são dois a dois não associados, para mostrar que $g \in (f_1 f_2 \cdots f_r)$, basta provar que $f_i \mid g$ em $K[X_1, \dots, X_n]$ para todo $i \in \{1, \dots, r\}$. Suponhamos, por absurdo, que exista $k \in \{1, \dots, r\}$ tal que f_k não seja um divisor de g em $K[X_1, \dots, X_n]$. Como f_k é um polinômio não constante, podemos supor, sem perda de generalidade, que seja possível escrever

$$f_k = h_0 + h_1 X_n + \cdots + h_s X_n^s$$

para determinados $s \in \mathbb{N} \setminus \{0\}$ e $h_0, \dots, h_s \in K[X_1, \dots, X_{n-1}]$, com $h_s \neq 0$.

Suponhamos, por absurdo, que f_k seja um divisor de g em $K(X_1, \dots, X_{n-1})[X_n]$. Assim, existem $c_1 \in K[X_1, \dots, X_n]$ e $c_2 \in K[X_1, \dots, X_{n-1}]$ tais que $c_1 f_k = c_2 g$. Visto que f_k é primo e f_k não divide g em $K[X_1, \dots, X_n]$, temos $f_k \mid c_2$ em $K[X_1, \dots, X_n]$, o que contradiz o fato de que X_n ocorre em f_k mas não em c_2 . Com isso, concluímos que f_k não é um divisor de g também em $K(X_1, \dots, X_{n-1})[X_n]$. Além disso, o Lema de Gauss fornece que f_k é irredutível em $K(X_1, \dots, X_{n-1})[X_n]$. Desse modo, $\text{mdc}(f_k, g) = 1$ em $K(X_1, \dots, X_{n-1})[X_n]$. Como $K(X_1, \dots, X_{n-1})[X_n]$ é um domínio principal, existem polinômios $a, b \in K[X_1, \dots, X_n]$ e $d \in K[X_1, \dots, X_{n-1}] \setminus \{0\}$ tais que

$$d = a f_k + b g.$$

Pelo primeiro item da Proposição 12, existe $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}(L)$ satisfazendo

$$d(a_1, \dots, a_{n-1}) h_s(a_1, \dots, a_{n-1}) \neq 0.$$

Visto que $f_k(a_1, \dots, a_{n-1}, X_n)$ é um polinômio não constante em $L[X_n]$, existe $a_n \in L$ tal que $f_k(a_1, \dots, a_{n-1}, a_n) = 0$. Assim, $(a_1, \dots, a_n) \in H$ e, por conseqüência, $g(a_1, \dots, a_n) = 0$.

Isso contradiz o fato de que $d(a_1, \dots, a_{n-1}) \neq 0$. Logo, $g \in (f_1 f_2 \cdots f_r)$ e concluimos que $\mathcal{I}(H) = (f_1 f_2 \cdots f_r)$. $\square$

Observação 13. Na demonstração da proposição anterior, convençionemos que tanto $K[X_1, \dots, X_{n-1}]$ quanto $K(X_1, \dots, X_{n-1})$ representam o corpo K quando $n = 1$.

Definição 20. Seja I um ideal de $K[X_1, \dots, X_n]$. O conjunto dos zeros comuns a todos os polinômios de I é dito **conjunto algébrico afim** definido por I e é denotado por $\mathcal{V}(I)$, isto é,

$$\mathcal{V}(I) = \{x \in \mathbb{A}^n(L); f(x) = 0 \text{ para todo } f \in I\}.$$

Observação 14.

1. Se I e J forem ideais de $K[X_1, \dots, X_n]$ satisfazendo $I \subset J$, então, tomando os conjuntos algébricos afins correspondentes, teremos a reversão dessa inclusão: $\mathcal{V}(I) \supset \mathcal{V}(J)$.
2. No caso em que I for um ideal finitamente gerado, digamos, $I = (f_1, \dots, f_m)$, utilizaremos também a notação $\mathcal{V}(f_1, \dots, f_m)$ para nos referirmos ao conjunto algébrico afim definido por I , o qual é a K -variedade definida pelo sistema de equações

$$f_i(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, m\}).$$

Desse modo, percebemos que toda K -variedade é um conjunto algébrico afim.

Vejamos algumas propriedades das “operações” $\mathcal{I}$ e $\mathcal{V}$.

Proposição 14. Consideremos um subconjunto $V \subset \mathbb{A}^n(L)$, duas K -variedades V_1 e V_2 de $\mathbb{A}^n(L)$ e uma família de K -variedades $(V_\lambda)_{\lambda \in \Lambda}$ de $\mathbb{A}^n(L)$.

1. Se L for infinito, então $\mathcal{I}(\mathbb{A}^n(L)) = (0)$.
2. $\mathcal{I}(\emptyset) = (1)$.
3. $\mathcal{I}(V) = \text{Rad}(\mathcal{I}(V))$.
4. $\mathcal{V}(\mathcal{I}(V_1)) = V_1$.
5. $V_1 \subset V_2$ se, e somente se, $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$, onde ocorrerá a igualdade $V_1 = V_2$ se, e somente se, $\mathcal{I}(V_1) = \mathcal{I}(V_2)$.
6. $\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$.
7. $V_1 \cup V_2 = \mathcal{V}(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2))$.
8. $\bigcap_{\lambda \in \Lambda} V_\lambda = \mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right)$.

Demonstração. Notemos que é possível escrever $V_1 = \mathcal{V}(f_1, \dots, f_r)$ e $V_2 = \mathcal{V}(g_1, \dots, g_s)$ para certos polinômios $f_1, \dots, f_r, g_1, \dots, g_s \in K[X_1, \dots, X_n]$.

1. Claramente, $(0) \subset \mathcal{I}(\mathbb{A}^n(L))$. Pelo primeiro item da Proposição 12, se f for um polinômio não nulo, então existirá $x \in \mathbb{A}^n(L)$ satisfazendo $f(x) \neq 0$. De modo equivalente, se $f \in \mathcal{I}(\mathbb{A}^n(L))$, então $f = 0$. Assim, concluímos que $\mathcal{I}(\mathbb{A}^n(L)) = (0)$.
2. Para todos $f \in K[X_1, \dots, X_n]$ e $x \in \mathbb{A}^n(L)$, a proposição

$$x \in \emptyset \Rightarrow f(x) = 0$$

é verdadeira. Logo, $\mathcal{I}(\emptyset) = K[X_1, \dots, X_n] = (1)$.

3. Como sempre, $\mathcal{I}(V) \subset \text{Rad}(\mathcal{I}(V))$. Consideremos $f \in \text{Rad}(\mathcal{I}(V))$, ou seja, existe um inteiro positivo m tal que $f^m \in \mathcal{I}(V)$. Se $x \in V$, então $(f(x))^m = 0$ e, por consequência, $f(x) = 0$. Portanto, $f \in \mathcal{I}(V)$ e concluímos que $\mathcal{I}(V) = \text{Rad}(\mathcal{I}(V))$.
4. É fácil ver que $V_1 \subset \mathcal{V}(\mathcal{I}(V_1))$. Como $(f_1, \dots, f_r) \subset \mathcal{I}(V_1)$, temos

$$\mathcal{V}(\mathcal{I}(V_1)) \subset \mathcal{V}(f_1, \dots, f_r) = V_1.$$

Logo, $\mathcal{V}(\mathcal{I}(V_1)) = V_1$.

5. Evidentemente, se $V_1 \subset V_2$, então $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$. Reciprocamente, supondo a inclusão $\mathcal{I}(V_2) \subset \mathcal{I}(V_1)$, podemos revertê-la tomando os conjuntos algébricos afins correspondentes: $\mathcal{V}(\mathcal{I}(V_1)) \subset \mathcal{V}(\mathcal{I}(V_2))$. Isso, pelo item anterior, significa que $V_1 \subset V_2$.
Além disso, é claro que $V_1 = V_2$ implica $\mathcal{I}(V_1) = \mathcal{I}(V_2)$. Agora, assumindo a igualdade $\mathcal{I}(V_1) = \mathcal{I}(V_2)$, temos $\mathcal{V}(\mathcal{I}(V_1)) = \mathcal{V}(\mathcal{I}(V_2))$, o que o item anterior traduz em $V_1 = V_2$.
6. É fácil ver que $\mathcal{I}(V_1) \cap \mathcal{I}(V_2) \subset \mathcal{I}(V_1 \cup V_2)$. Visto que $V_1 \subset V_1 \cup V_2$ e $V_2 \subset V_1 \cup V_2$, temos $\mathcal{I}(V_1 \cup V_2) \subset \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$ devido ao Lema 7 e ao item anterior. Desse modo, $\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$.
7. Seja $x \in V_1 \cup V_2$. Se $f \in \mathcal{I}(V_1) \cdot \mathcal{I}(V_2)$, então existirão polinômios $p_1, \dots, p_m \in \mathcal{I}(V_1)$ e $q_1, \dots, q_m \in \mathcal{I}(V_2)$ tais que

$$f = p_1 q_1 + \dots + p_m q_m.$$

Além disso, temos $x \in V_1$ ou $x \in V_2$. Em particular, x é zero dos polinômios $p_1, \dots, p_m$ ou x é zero dos polinômios $q_1, \dots, q_m$. Em ambos os casos, o ponto x é zero de f . Logo, $x \in \mathcal{V}(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2))$.

Reciprocamente, consideremos $y \in \mathcal{V}(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2))$. Suponhamos que $y \notin V_1$, ou seja, existe $i \in \{1, \dots, r\}$ tal que $f_i(y) \neq 0$. Seja $j \in \{1, \dots, s\}$ qualquer. Claramente, $f_i g_j \in \mathcal{I}(V_1) \cdot \mathcal{I}(V_2)$ e, consequentemente,

$$f_i(y) g_j(y) = f_i g_j(y) = 0.$$

O fato de que $f_i(y) \neq 0$ implica $g_j(y) = 0$. Portanto, $y \in V_1 \cup V_2$ e concluímos que $V_1 \cup V_2 = \mathcal{V}(\mathcal{I}(V_1) \cdot \mathcal{I}(V_2))$.

8. Notemos que, para todo $\lambda_0 \in \Lambda$, temos a inclusão

$$\mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right) \subset \mathcal{V}(\mathcal{I}(V_{\lambda_0})) = V_{\lambda_0}$$

obtida por meio da reversão da familiar inclusão $\mathcal{I}(V_{\lambda_0}) \subset \sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)$. Assim,

$$\mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right) \subset \bigcap_{\lambda \in \Lambda} V_\lambda.$$

Sejam $x \in \bigcap_{\lambda \in \Lambda} V_\lambda$ e $f \in \sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)$. Desse modo, existem $\lambda_1, \dots, \lambda_m \in \Lambda$ e $f_{\lambda_i} \in \mathcal{I}(V_{\lambda_i})$, para cada $i \in \{1, \dots, m\}$, satisfazendo

$$f = f_{\lambda_1} + \dots + f_{\lambda_m}.$$

Visto que o ponto x é zero dos polinômios $f_{\lambda_1}, \dots, f_{\lambda_m}$, esse ponto também é zero do polinômio f . Portanto, $x \in \mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right)$ e concluímos que $\mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right) = \bigcap_{\lambda \in \Lambda} V_\lambda$.

□

Em particular, as propriedades acima mostram que o mapa

$$\begin{array}{ccc} \mathcal{I}: \{K\text{-variedades } V \subset \mathbb{A}^n(L)\} & \rightarrow & \{\text{ideais radicais } I \subset K[X_1, \dots, X_n]\} \\ V & \mapsto & \mathcal{I}(V) \end{array}$$

reverte a relação de inclusão de variedades e é injetivo, pois possui o mapa inverso à esquerda

$$\begin{array}{ccc} \mathcal{V}: \{\text{ideais radicais } I \subset K[X_1, \dots, X_n]\} & \rightarrow & \{K\text{-variedades } V \subset \mathbb{A}^n(L)\} \\ I & \mapsto & \mathcal{V}(I). \end{array}$$

Definição 21. Uma K -variedade $V \subset \mathbb{A}^n(L)$ será dita **irredutível** se, para quaisquer K -variedades V_1 e V_2 de $\mathbb{A}^n(L)$ tais que $V = V_1 \cup V_2$, tivermos $V = V_1$ ou $V = V_2$.

Proposição 15. Uma K -variedade $V \subset \mathbb{A}^n(L)$ será irredutível se, e somente se, seu ideal $\mathcal{I}(V)$ for primo.

Demonstração. Suponhamos que V seja irredutível. Sejam $f_1, f_2 \in K[X_1, \dots, X_n]$ polinômios tais que $f_1 f_2 \in \mathcal{I}(V)$. Pelo Lema 7, as interseções $V \cap \mathcal{V}(f_1)$ e $V \cap \mathcal{V}(f_2)$ são K -variedades de $\mathbb{A}^n(L)$. Mostremos que V é a união dessas duas K -variedades.

Seja $x \in V$ tal que $x \notin \mathcal{V}(f_1)$. Notemos que $f_1(x) \neq 0$, enquanto $f_1 f_2(x) = 0$. Isso implica $f_2(x) = 0$ e, por consequência, $x \in \mathcal{V}(f_2)$. Logo, temos a decomposição

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

Por hipótese, $V = V \cap \mathcal{V}(f_1)$ ou $V = V \cap \mathcal{V}(f_2)$. Visto que $V \subset \mathcal{V}(f_1)$ ou $V \subset \mathcal{V}(f_2)$, temos $f_1 \in \mathcal{I}(V)$ ou $f_2 \in \mathcal{I}(V)$. Desse modo, o ideal $\mathcal{I}(V)$ é primo.

Reciprocamente, suponhamos que o ideal $\mathcal{I}(V)$ seja primo. Sejam V_1 e V_2 duas K -variedades de $\mathbb{A}^n(L)$ tais que $V = V_1 \cup V_2$. Suponhamos, por absurdo, que $V \neq V_1$ e $V \neq V_2$. A Proposição 14 fornece que $\mathcal{I}(V) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$, $\mathcal{I}(V) \subsetneq \mathcal{I}(V_1)$ e $\mathcal{I}(V) \subsetneq \mathcal{I}(V_2)$. Desse modo, existem polinômios $g_1 \in \mathcal{I}(V_1)$ e $g_2 \in \mathcal{I}(V_2)$ tais que $g_1, g_2 \notin \mathcal{I}(V)$. Claramente,

$$g_1 g_2 \in \mathcal{I}(V_1) \cap \mathcal{I}(V_2) = \mathcal{I}(V)$$

e, como $\mathcal{I}(V)$ é primo, $g_1 \in \mathcal{I}(V)$ ou $g_2 \in \mathcal{I}(V)$, o que é uma contradição. Logo, a K -variedade V é irredutível. $\square$

4.2 O TEOREMA DA BASE DE HILBERT

Nesta seção, veremos que ideais em anéis de polinômios com coeficientes em um corpo são finitamente gerados. Como consequência, provaremos que conjuntos algébricos afins podem ser sempre definidos por uma quantidade finita de polinômios.

Definição 22. *Um anel A será dito **noetheriano** se todos os seus ideais forem finitamente gerados.*

Notemos que todo domínio principal é um anel noetheriano. Em particular, $\mathbb{Z}$, K e $K[X]$ são exemplos de anéis noetherianos.

Proposição 16. *Seja A um anel. Então, são equivalentes:*

1. A é noetheriano;
2. qualquer cadeia ascendente de ideais de A é estacionária, isto é, se

$$I_1 \subset I_2 \subset \cdots \subset I_m \subset \cdots$$

for uma cadeia ascendente de ideais de A , então existe $m \in \mathbb{N}$ tal que $I_k = I_m$ para todos $k \geq m$;

3. todo conjunto Γ não vazio de ideais de A possui um elemento maximal com respeito à inclusão, isto é, existe um ideal $M \in \Gamma$ tal que, para todo $I \in \Gamma$, $M \subset I$ implica $I = M$.

Demonstração.

$1 \Rightarrow 2$. Suponhamos que A seja noetheriano e seja

$$I_1 \subset I_2 \subset \cdots \subset I_m \subset \cdots$$

uma cadeia ascendente de ideais de A . Então, a união $I := \bigcup_{k \in \mathbb{N} \setminus \{0\}} I_k$ é um ideal de A e, conseqüentemente, existem $a_1, \dots, a_r \in A$ tais que $I = (a_1, \dots, a_r)$. Para cada $i \in \{1, \dots, r\}$, existe $m_i \in \mathbb{N}$ tal que $a_i \in I_{m_i}$. Definindo $m = \max\{m_1, \dots, m_r\}$, temos

$$I = (a_1, \dots, a_r) \subset I_m \subset I_k \subset I$$

para todo $k \geq m$. Isso mostra que $I_k = I = I_m$ para todo $k \geq m$. Logo, a cadeia ascendente de ideais é estacionária.

$2 \Rightarrow 3$. Suponhamos que exista um conjunto não vazio Γ de ideais de A que não possua um elemento maximal com respeito à inclusão. Então, para cada $I \in \Gamma$, o conjunto

$$S_I := \{J \in \Gamma; I \subsetneq J\}$$

é não vazio. Pelo Axioma da Escolha, existe uma função $E: \mathcal{P}(\Gamma) \setminus \{\emptyset\} \rightarrow \Gamma$ tal que $E(S) \in S$ para cada subconjunto não vazio $S \subset \Gamma$. Definamos a função

$$\begin{aligned} f: \Gamma &\rightarrow \Gamma \\ I &\mapsto E(S_I). \end{aligned}$$

Evidentemente, $I \subsetneq f(I)$ para todo $I \in \Gamma$. Tomemos um elemento I_0 em Γ . Pelo Teorema da Recursão em $\mathbb{N}$, existe uma função $h: \mathbb{N} \rightarrow \Gamma$ tal que $h(0) = I_0$ e $h(n+1) = f(h(n))$ para todo $n \in \mathbb{N}$. Desse modo,

$$h(n) \subsetneq f(h(n)) = h(n+1)$$

para qualquer $n \in \mathbb{N}$. Logo, a cadeia ascendente de ideais

$$h(1) \subsetneq h(2) \subsetneq \dots \subsetneq h(n) \subsetneq \dots$$

não é estacionária.

$3 \Rightarrow 1$. Suponhamos que todo conjunto não vazio de ideais de A possua um elemento maximal com respeito à inclusão. Seja I um ideal de A . Definamos o conjunto

$$\Gamma = \{J \subset I; J \text{ é um ideal finitamente gerado de } A\}.$$

Notemos que $\Gamma \neq \emptyset$, uma vez que $(0) \in \Gamma$. Seja M um elemento maximal de Γ . Claramente, $M \subset I$ e M é finitamente gerado, digamos, $M = (a_1, \dots, a_r)$ para certos $a_1, \dots, a_r \in A$. Notemos que $I \subset M$, pois, caso contrário, existiria um elemento $a_{r+1} \in I \setminus M$ e, assim, teríamos

$$M \subsetneq (a_1, \dots, a_r, a_{r+1}) \subset I,$$

contradizendo a maximalidade de M em Γ . Logo, $I = M$ é finitamente gerado.

□

Teorema 9 (Teorema da Base de Hilbert). *Se A for um anel noetheriano, então $A[X_1, \dots, X_n]$ será também noetheriano.*

Demonstração. Basta mostrarmos a proposição seguinte:

$$A \text{ noetheriano} \Rightarrow A[X] \text{ noetheriano.}$$

Fazendo indução sobre n , o fato de que, para todo inteiro positivo n , A noetheriano implica $A[X_1, \dots, X_n]$ noetheriano decorrerá dessa proposição.

Suponhamos que A seja um anel noetheriano. Seja I um ideal de $A[X]$. Mostremos que I é finitamente gerado. Claramente, podemos supor $I \neq (0)$. Para cada $k \in \mathbb{N}$, definamos o conjunto

$$J_k = \{a \in A; \text{ existem } f \in I \text{ e } a_0, \dots, a_{k-1} \in A \text{ tais que } f(X) = aX^k + a_{k-1}X^{k-1} + \dots + a_0\}.$$

É fácil ver que J_k é um ideal de A para todo $k \in \mathbb{N}$. Além disso, $J_k \subset J_{k+1}$ para todo $k \in \mathbb{N}$. De fato, sejam $k_0 \in \mathbb{N}$ e $a_{k_0} \in J_{k_0}$. Então existem $p \in I$ e $a_0, \dots, a_{k_0-1} \in A$ satisfazendo $p(X) = a_{k_0}X^{k_0} + a_{k_0-1}X^{k_0-1} + \dots + a_0$. Visto que

$$a_{k_0}X^{k_0+1} + a_{k_0-1}X^{k_0} + \dots + a_0X = Xp(X) \in I,$$

temos $a_{k_0} \in J_{k_0+1}$.

Como A é noetheriano, a cadeia ascendente de ideais de A

$$J_0 \subset J_1 \subset \dots \subset J_m \subset \dots$$

é estacionária, isto é, existe $m \in \mathbb{N}$ tal que $J_k = J_m$ para todo $k \geq m$. Em adição a isso, os ideais $J_0, \dots, J_m$ são finitamente gerados, ou seja, existem $a_{k1}, a_{k2}, \dots, a_{kn_k} \in A$ tais que

$$J_k = (a_{k1}, a_{k2}, \dots, a_{kn_k})$$

para cada $k \in \{0, \dots, m\}$. Evidentemente, para todos $k \in \{0, \dots, m\}$ e $j \in \{1, \dots, n_k\}$, existe $f_{kj} \in I$ tal que podemos escrever

$$f_{kj}(X) = a_{kj}X^k + a_{k,j,k-1}X^{k-1} + \dots + a_{k,j,0}$$

para certos $a_{k,j,0}, \dots, a_{k,j,k-1} \in A$. Definamos o ideal

$$I' = (\{f_{kj} \in I; k \in \{0, \dots, m\} \text{ e } j \in \{1, \dots, n_k\}\})$$

e mostremos que $I = I'$.

A inclusão $I' \subset I$ é óbvia. Para mostrar que $I \subset I'$, basta provar a afirmação seguinte utilizando indução sobre k .

AFIRMAÇÃO: Para todos $k \in \mathbb{N}$ e $f \in A[X] \setminus \{0\}$, se $f \in I$ e $\text{grau}(f) = k$, então $f \in I'$.

Seja $f \in I$ um polinômio constante, isto é, $f(X) = a$ para algum $a \in A$. Assim, $a \in J_0$ e, por consequência, existem $b_1, \dots, b_{n_0} \in A$ tais que

$$f(X) = a = b_1 a_{01} + \dots + b_{n_0} a_{0n_0} = b_1 f_{01}(X) + \dots + b_{n_0} f_{0n_0}(X) \in I'.$$

Logo, a afirmação é verdadeira quando $k = 0$.

Agora, suponhamos que, para determinado inteiro positivo k e para todos $h \in A[X] \setminus \{0\}$, se $h \in I$ com $\text{grau}(h) < k$, então $h \in I'$. Seja $g \in I$ um polinômio de grau k . Escrevamos

$$g(X) = c_k X^k + c_{k-1} X^{k-1} + \dots + c_0$$

para certos $c_0, \dots, c_k \in A$. Temos dois casos.

CASO 1: Suponhamos que $k \leq m$. Nesse caso, $c_k \in J_k$ e, desse modo, existem $d_1, \dots, d_{n_k} \in A$ tais que

$$c_k = d_1 a_{k1} + \dots + d_{n_k} a_{kn_k}.$$

Definindo

$$h(X) = g(X) - (d_1 f_{k1}(X) + \dots + d_{n_k} f_{kn_k}(X)),$$

temos $h \in I$ e, além disso, $h = 0$ ou $\text{grau}(h) < k$. Em ambos os casos, $h \in I'$. De fato, se $h \neq 0$, a hipótese de indução fornecerá que $h \in I'$. Logo,

$$g(X) = h(X) + (d_1 f_{k1}(X) + \dots + d_{n_k} f_{kn_k}(X)) \in I'.$$

CASO 2: Suponhamos que $k > m$. Nesse caso, $c_k \in J_k = J_m$ e, logo, é possível escrever

$$c_k = d_1 a_{m1} + \dots + d_{n_m} a_{mn_m}$$

para certos $d_1, \dots, d_{n_m} \in A$. Definamos o polinômio

$$h(X) = g(X) - X^{k-m}(d_1 f_{m1}(X) + \dots + d_{n_m} f_{mn_m}(X)).$$

Notemos que $h \in I$, onde $h = 0$ ou $\text{grau}(h) < k$. De qualquer forma, analogamente ao caso anterior, temos $h \in I'$ e concluímos que

$$g(X) = h(X) + X^{k-m}(d_1 f_{m1}(X) + \dots + d_{n_m} f_{mn_m}(X)) \in I'.$$

Pelo Princípio de Indução Finita, a afirmação é válida para todo $k \in \mathbb{N}$. Portanto, $I = I'$ é finitamente gerado e $A[X]$ é noetheriano. $\square$

Corolário 1. *Qualquer cadeia descendente de K -variedades de $\mathbb{A}^n(L)$ é estacionária, isto é, se*

$$V_1 \supset V_2 \supset \cdots \supset V_m \supset \cdots$$

for uma cadeia descendente de K -variedades de $\mathbb{A}^n(L)$, então existe $m \in \mathbb{N}$ tal que $V_k = V_m$ para todos $k \geq m$.

Demonstração. Consideremos

$$V_1 \supset V_2 \supset \cdots \supset V_m \supset \cdots$$

uma cadeia descendente de K -variedades de $\mathbb{A}^n(L)$. Pelo quinto item da Proposição 14, tomando o ideal correspondente a cada K -variedade, obtemos a seguinte cadeia ascendente de ideais do anel $K[X_1, \dots, X_n]$:

$$\mathcal{I}(V_1) \subset \mathcal{I}(V_2) \subset \cdots \subset \mathcal{I}(V_m) \subset \cdots$$

Pelo Teorema da Base de Hilbert, $K[X_1, \dots, X_n]$ é noetheriano e, em particular, existe $m \in \mathbb{N}$ tal que $\mathcal{I}(V_k) = \mathcal{I}(V_m)$ para todo $k \geq m$. Recorrendo novamente ao quinto item da Proposição 14, obtemos $V_k = V_m$ para cada $k \geq m$, o que conclui a prova. $\square$

No segundo item da Observação 14, vimos que toda K -variedade em $\mathbb{A}^n(L)$ é um conjunto algébrico afim. Com auxílio do Teorema da Base de Hilbert, podemos mostrar a parte que falta para concluirmos que K -variedade e conjunto algébrico afim são sinônimos.

Corolário 2. *Se I for um ideal de $K[X_1, \dots, X_n]$, então $\mathcal{V}(I)$ será uma K -variedade em $\mathbb{A}^n(L)$.*

Demonstração. Notemos que existem $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ tais que $I = (f_1, \dots, f_m)$, uma vez que o Teorema da Base de Hilbert fornece que $K[X_1, \dots, X_n]$ é noetheriano. Desse modo, $\mathcal{V}(I) = \mathcal{V}(f_1, \dots, f_m)$ é o conjunto solução do sistema de equações

$$f_i(X_1, \dots, X_n) = 0 \quad (i \in \{1, \dots, m\}).$$

$\square$

4.3 DECOMPOSIÇÃO DE VARIEDADES EM COMPONENTES IRREDUTÍVEIS

Começemos esta seção introduzindo uma topologia nos espaços afins e, por consequência, nas K -variedades.

Lema 8 (Topologia de Zariski). *Em $\mathbb{A}^n(L)$, temos as propriedades seguintes:*

1. *o espaço afim $\mathbb{A}^n(L)$ e o conjunto vazio são K -variedades;*
2. *união finita de K -variedades é uma K -variedade;*

3. interseção arbitrária de K -variedades é uma K -variedade.

Desse modo, as K -variedades são os conjuntos fechados de uma topologia em $\mathbb{A}^n(L)$, a chamada **topologia de Zariski com respeito a K** .

Demonstração.

1. É fácil ver que $\mathbb{A}^n(L) = \mathcal{V}(0)$ e $\emptyset = \mathcal{V}(1)$. Assim, $\mathbb{A}^n(L)$ e $\emptyset$ são K -variedades.
2. Conforme vimos no Lema 7, união finita de K -variedades é uma K -variedade.
3. Seja $(V_\lambda)_{\lambda \in \Lambda}$ uma família de K -variedades de $\mathbb{A}^n(L)$. Pelo oitavo item da Proposição 14, temos $\bigcap_{\lambda \in \Lambda} V_\lambda = \mathcal{V}\left(\sum_{\lambda \in \Lambda} \mathcal{I}(V_\lambda)\right)$. Pelo Corolário 2, $\bigcap_{\lambda \in \Lambda} V_\lambda$ é uma K -variedade.

□

Observação 15. Seja V uma K -variedade em $\mathbb{A}^n(L)$. A topologia de Zariski no espaço afim $\mathbb{A}^n(L)$ com respeito a K induz uma topologia em V , a chamada **topologia de Zariski em V com respeito a K** . Notemos que os conjuntos fechados dessa topologia são as K -variedades contidas em V . De fato, se $W \subset V$ for uma K -variedade, então W é um conjunto fechado em $\mathbb{A}^n(L)$ e, por consequência, $W = V \cap W$ é um conjunto fechado em V . Reciprocamente, se F for um conjunto fechado em V , poderemos escrever $F = V \cap G$ para certo conjunto fechado G em $\mathbb{A}^n(L)$. Como V e G são K -variedades, F é uma K -variedade contida em V .

Definição 23. Seja X um espaço topológico. Diremos que X é **irredutível** se, para quaisquer conjuntos fechados F_1 e F_2 em X tais que $X = F_1 \cup F_2$, tivermos $X = F_1$ ou $X = F_2$. Um subconjunto Y de X será irredutível se Y for irredutível como um espaço topológico com a topologia induzida.

Observação 16. A Observação 15 esclarece o fato de que uma K -variedade será irredutível no sentido da Definição 21 se, e somente se, ela for irredutível como espaço topológico com a topologia de Zariski com respeito a K .

Lema 9. Seja X um espaço topológico. Então, são equivalentes:

1. X é irredutível;
2. se U_1 e U_2 forem conjuntos abertos não vazios em X , então $U_1 \cap U_2 \neq \emptyset$;
3. qualquer conjunto aberto não vazio em X é denso em X .

Demonstração.

$1 \Rightarrow 2$. Suponhamos que X seja irredutível e sejam U_1 e U_2 conjuntos abertos não vazios em X . Suponhamos, por absurdo, que $U_1 \cap U_2 = \emptyset$. Isso nos fornece a seguinte decomposição de X como união de conjuntos fechados:

$$X = (X \setminus U_1) \cup (X \setminus U_2).$$

Visto que X é irredutível, temos $X = X \setminus U_1$ ou $X = X \setminus U_2$. Em outras palavras, $U_1 = \emptyset$ ou $U_2 = \emptyset$, o que é uma contradição. Logo, a interseção $U_1 \cap U_2$ é não vazia.

$2 \Rightarrow 3$. Suponhamos que quaisquer dois conjuntos abertos não vazios em X possuem interseção não vazia. Seja U um conjunto aberto não vazio em X . Por hipótese, para cada $x \in X$, a interseção de U com qualquer conjunto aberto em X contendo o ponto x é não vazia. Logo, $\overline{U} = X$.

$3 \Rightarrow 1$. Suponhamos que todo conjunto aberto não vazio em X seja denso em X . Sejam F_1 e F_2 conjuntos fechados em X tais que $X = F_1 \cup F_2$. Suponhamos que $X \neq F_1$. Desse modo, $X \setminus F_1$ é um conjunto aberto não vazio em X . Por hipótese, X é o menor conjunto fechado em X contendo $X \setminus F_1$. Visto que F_2 é um conjunto fechado em X contendo $X \setminus F_1$, temos $X = F_2$, o que conclui a prova.

□

Corolário 3. *Seja Y um subconjunto de um espaço topológico X . Então, são equivalentes:*

1. Y é irredutível;
2. se U_1 e U_2 forem conjuntos abertos em X tais que $U_1 \cap Y \neq \emptyset$ e $U_2 \cap Y \neq \emptyset$, então $U_1 \cap U_2 \cap Y \neq \emptyset$;
3. o fecho $\overline{Y}$ é irredutível.

Demonstração.

$1 \Leftrightarrow 2$. A equivalência entre as afirmações 1 e 2 é uma consequência do Lema 9.

$1 \Rightarrow 3$. Suponhamos que Y seja irredutível. Sejam F_1 e F_2 conjuntos fechados em $\overline{Y}$ tais que $\overline{Y} = F_1 \cup F_2$. Em particular, F_1 e F_2 são fechados em X , uma vez que $\overline{Y}$ é fechado em X . Assim, $Y \cap F_1$ e $Y \cap F_2$ são fechados em Y satisfazendo

$$Y = (Y \cap F_1) \cup (Y \cap F_2).$$

Por hipótese, $Y = Y \cap F_1$ ou $Y = Y \cap F_2$. Isso significa que $Y \subset F_1$ ou $Y \subset F_2$. Logo, $\overline{Y} = F_1$ ou $\overline{Y} = F_2$.

$3 \Rightarrow 1$. Suponhamos que $\overline{Y}$ seja irredutível. Sejam G_1 e G_2 conjuntos fechados em Y tais que $Y = G_1 \cup G_2$. Pelo primeiro item da Proposição 1, temos a seguinte decomposição de $\overline{Y}$ como união de dois de seus conjuntos fechados:

$$\overline{Y} = \overline{G_1} \cup \overline{G_2}.$$

Por hipótese, $\overline{Y} = \overline{G_1}$ ou $\overline{Y} = \overline{G_2}$. Sem perda de generalidade, suponhamos que $\overline{Y} = \overline{G_1}$.

Notemos que existe um conjunto fechado F em X satisfazendo $G_1 = Y \cap F$. Pelo segundo item da Proposição 1, $\overline{G_1} \subset \overline{Y \cap F} = \overline{Y} \cap F$ e, por consequência,

$$G_1 \subset Y \cap \overline{G_1} \subset (Y \cap \overline{Y}) \cap F = Y \cap F = G_1.$$

Com isso, $G_1 = Y \cap \overline{G_1} = Y \cap \overline{Y} = Y$ e, portanto, Y é irredutível.

□

Definição 24. *Seja X um espaço topológico. Uma **componente irredutível** de X é um subconjunto irredutível de X que é maximal com respeito à inclusão.*

Observação 17. *Pelo terceiro item do Corolário 3, qualquer componente irredutível em um espaço topológico é um conjunto fechado nesse espaço. De fato, se Y for uma componente irredutível de um espaço topológico X , então o fecho $\overline{Y}$ será um subconjunto irredutível. Visto que $Y \subset \overline{Y}$, a maximalidade de Y fornece que $Y = \overline{Y}$.*

Proposição 17. *Seja X um espaço topológico.*

1. *Seja $\mathcal{C}$ uma cadeia de subconjuntos irredutíveis de X com relação à inclusão, isto é,*

$$W_1, W_2 \in \mathcal{C} \Rightarrow W_1 \subset W_2 \text{ ou } W_2 \subset W_1.$$

Então, $Y := \bigcup_{W \in \mathcal{C}} W$ é também um subconjunto irredutível de X .

2. *Qualquer subconjunto irredutível de X está contido em uma componente irredutível de X .*
3. *X é a união de suas componentes irredutíveis.*

Demonstração.

1. Sejam U_1 e U_2 conjuntos abertos em X tais que $U_1 \cap Y \neq \emptyset$ e $U_2 \cap Y \neq \emptyset$. Assim, existem subconjuntos irredutíveis $W_1, W_2 \in \mathcal{C}$ tais que $U_1 \cap W_1 \neq \emptyset$ e $U_2 \cap W_2 \neq \emptyset$. Sem perda de generalidade, suponhamos que $W_2 \subset W_1$. Com isso, $U_2 \cap W_1 \neq \emptyset$. Pelo Corolário 3, $U_1 \cap U_2 \cap W_1 \neq \emptyset$ e, a fortiori, $U_1 \cap U_2 \cap Y \neq \emptyset$. Recorrendo novamente ao Corolário 3, concluímos que Y é irredutível.
2. Seja Z um subconjunto irredutível de X . Utilizaremos o Lema de Zorn para mostrar a existência de uma componente maximal contendo Z . Definamos o conjunto

$$\Gamma = \{W \subset X; W \text{ é um subconjunto irredutível de } X \text{ tal que } Z \subset W\}.$$

Notemos que $\Gamma \neq \emptyset$, pois $Z \in \Gamma$. Além disso, Γ é um conjunto parcialmente ordenado pela inclusão e, de acordo com o item anterior, toda cadeia em Γ possui cota superior. Pelo Lema de Zorn, existe um elemento maximal $M \in \Gamma$. Evidentemente, M é um subconjunto

irredutível de X contendo Z . Resta mostrarmos que M é uma componente irredutível de X .

Se N for um subconjunto irredutível de X tal que $M \subset N$, então N conterá Z e, por consequência, teremos $N \in \Gamma$. Pela maximalidade de M em Γ , temos $M = N$. Logo, M é uma componente irredutível de X .

3. É fácil ver que, para cada $x \in X$, $\{x\}$ é um subconjunto irredutível de X e, pelo item anterior, existe uma componente irredutível M_x de X contendo $\{x\}$. Desse modo,

$$X = \bigcup_{x \in X} \{x\} = \bigcup_{x \in X} M_x.$$

Isso torna a prova completa.

□

Definição 25. Um espaço topológico X será dito **noetheriano** se toda cadeia descendente de conjuntos fechados em X for estacionária, isto é, se

$$F_1 \supset F_2 \supset \cdots \supset F_m \supset \cdots$$

for uma cadeia descendente de conjuntos fechados em X , então existirá $m \in \mathbb{N}$ tal que $F_k = F_m$ para todo $k \geq m$.

Exemplo 12. Conforme vimos no Corolário 1, qualquer K -variedade V de $\mathbb{A}^n(L)$ com a topologia de Zariski é um espaço topológico noetheriano.

Lema 10. Um espaço topológico X será noetheriano se, e somente se, todo conjunto Γ não vazio de subconjuntos fechados em X possuir um elemento minimal com relação à inclusão.

Demonstração. Suponhamos que X seja noetheriano. Seja Γ um conjunto não vazio de subconjuntos fechados em X . Suponhamos, por absurdo, que Γ não possua um elemento minimal com relação à inclusão. Isso significa que, para cada $F \in \Gamma$, o conjunto

$$S_F := \{G \in \Gamma; G \subsetneq F\}$$

é não vazio. Pelo Axioma da Escolha, existe uma função $E: \mathcal{P}(\Gamma) \setminus \{\emptyset\} \rightarrow \Gamma$ tal que $E(S) \in S$ para cada subconjunto não vazio $S \subset \Gamma$. Definamos a função

$$\begin{aligned} f: \Gamma &\rightarrow \Gamma \\ F &\mapsto E(S_F). \end{aligned}$$

É fácil ver que $f(F) \subsetneq F$ para cada $F \in \Gamma$. Consideremos um elemento $F_0 \in \Gamma$. Pelo Teorema da Recursão em $\mathbb{N}$, existe uma função $h: \mathbb{N} \rightarrow \Gamma$ tal que $h(0) = F_0$ e $h(n+1) = f(h(n))$ para todo $n \in \mathbb{N}$. Com isso,

$$h(n) \supsetneq f(h(n)) = h(n+1)$$

para cada $n \in \mathbb{N}$. Desse modo, construímos a seguinte cadeia descendente de conjuntos fechados em X :

$$h(1) \supsetneq h(2) \supsetneq \cdots \supsetneq h(n) \supsetneq \cdots .$$

Isso contradiz o fato de que X é noetheriano. Logo, Γ possui um elemento minimal.

Reciprocamente, suponhamos que todo conjunto não vazio de conjuntos fechados em X possua um elemento minimal com relação à inclusão. Seja

$$F_1 \supset F_2 \supset \cdots \supset F_m \supset \cdots$$

uma cadeia descendente de conjuntos fechados em X . Por hipótese, existe $m \in \mathbb{N}$ tal que F_m é um elemento minimal do conjunto

$$\{F_i \subset X; i \in \mathbb{N} \setminus \{0\}\}.$$

Assim, $F_k = F_m$ para todo $k \geq m$ e, portanto, X é noetheriano. $\square$

Proposição 18. *Todo espaço topológico noetheriano possui apenas uma quantidade finita de componentes irredutíveis e nenhuma componente está contida na união das outras.*

Demonstração. Sejam X um espaço topológico noetheriano e Γ o conjunto de todos os subconjuntos fechados de X que não podem ser escritos como uma união finita de subconjuntos irredutíveis de X .

Suponhamos, por absurdo, que Γ seja não vazio. Pelo Lema 10, existe um elemento minimal $Y \in \Gamma$. Visto que Y não é irredutível, existem conjuntos fechados Y_1, Y_2 em Y tais que $Y = Y_1 \cup Y_2$, $Y_1 \subsetneq Y$ e $Y_2 \subsetneq Y$. Visto que Y é minimal em Γ , $Y_1 \notin \Gamma$ e $Y_2 \notin \Gamma$. Com isso, Y_1 e Y_2 são uniões finitas de subconjuntos irredutíveis de X e, consequentemente, o mesmo pode ser dito sobre Y , o que é uma contradição.

Como $\Gamma = \emptyset$, todo conjunto fechado em X , em particular o próprio X , pode ser escrito como união finita de subconjuntos irredutíveis de X . Pelo segundo item da Proposição 17, existem componentes irredutíveis, distintas duas a duas, $X_1, \dots, X_m$ de X tais que

$$X = X_1 \cup \cdots \cup X_m.$$

Seja W uma componente irredutível qualquer de X . Pela Observação 17, $(W \cap X_i)$ é um conjunto fechado em W para todo $i \in \{1, \dots, m\}$. Além disso,

$$W = \bigcup_{i=1}^m (W \cap X_i).$$

Como W é irredutível, existe $j \in \{1, \dots, m\}$ tal que $W = W \cap X_j$. Visto que $W \subset X_j$ e W é uma componente irredutível de X , $W = X_j$. Logo, $X_1, \dots, X_m$ são todas as componentes irredutíveis de X .

Finalmente, suponhamos, por absurdo, que exista $k \in \{1, \dots, m\}$ tal que $X_k \subset \bigcup_{\substack{i=1 \\ i \neq k}}^m X_i$.

Nesse caso, temos a seguinte decomposição de X_k como união de conjuntos fechados em X_k :

$$X_k = \bigcup_{\substack{i=1 \\ i \neq k}}^m (X_k \cap X_i).$$

De modo similar ao ocorrido anteriormente, $X_k = X_k \cap X_l$ para algum $l \in \{1, \dots, m\} \setminus \{k\}$ e, conseqüentemente, $X_k = X_l$, o que é uma contradição. Portanto, nenhuma componente irredutível de X está contida na união das outras componentes irredutíveis de X . $\square$

Corolário 4. *Qualquer K -variedade V de $\mathbb{A}^n(L)$ possui apenas uma quantidade finita de componentes irredutíveis $V_1, \dots, V_m$. Além disso, temos $V = V_1 \cup \dots \cup V_m$ e, nessa representação, nenhum V_i é supérfluo.*

Demonstração. Esse resultado segue imediatamente da proposição anterior e do terceiro item da Proposição 17. $\square$

Exemplo 13. *Mostremos que a $\mathbb{Q}$ -variedade $\mathcal{V}(XY)$ de $\mathbb{A}^2(\mathbb{R})$ possui apenas duas componentes irredutíveis, a saber, $\mathcal{V}(X)$ e $\mathcal{V}(Y)$.*

Primeiramente, notemos que

$$\mathcal{V}(X) = \{(0, y) \in \mathbb{A}^2(\mathbb{R}); y \in \mathbb{R}\}, \quad \mathcal{V}(Y) = \{(x, 0) \in \mathbb{A}^2(\mathbb{R}); x \in \mathbb{R}\} \text{ e } \mathcal{V}(XY) = \mathcal{V}(X) \cup \mathcal{V}(Y).$$

Dado $g \in \mathbb{Q}[X, Y]$, existem $r, s \in \mathbb{N}$ e $a_{00}, \dots, a_{0s}, \dots, a_{r0}, \dots, a_{rs} \in \mathbb{Q}$ tais que

$$\begin{aligned} g(X, Y) &= \sum_{j=0}^s \sum_{i=0}^r a_{ij} X^i Y^j = \sum_{j=0}^s \left(a_{0j} Y^j + \sum_{i=1}^r a_{ij} X^i Y^j \right) \\ &= \sum_{j=0}^s a_{0j} Y^j + X \sum_{i=1}^r \sum_{j=0}^s a_{ij} X^{i-1} Y^j. \end{aligned}$$

Desse modo, se $g \in \mathcal{I}(\mathcal{V}(X))$, então

$$\sum_{j=0}^s a_{0j} y^j = 0$$

para todo $y \in \mathbb{R}$, ou seja, o polinômio $\sum_{j=0}^s a_{0j} Y^j$ é nulo. Por consequência,

$$g(X, Y) = X \sum_{i=1}^r \sum_{j=0}^s a_{ij} X^{i-1} Y^j \in (X).$$

Isso mostra que $\mathcal{I}(\mathcal{V}(X)) \subset (X)$. Evidentemente, temos a inclusão $(X) \subset \mathcal{I}(\mathcal{V}(X))$. Logo, $\mathcal{I}(\mathcal{V}(X)) = (X)$ e, de modo análogo, conclui-se que $\mathcal{I}(\mathcal{V}(Y)) = (Y)$.

É fácil ver que

$$\begin{aligned}\phi: \mathbb{Q}[X, Y] &\rightarrow \mathbb{Q}[Z] & \text{e } \psi: \mathbb{Q}[X, Y] &\rightarrow \mathbb{Q}[Z] \\ f(X, Y) &\mapsto f(0, Z) & f(X, Y) &\mapsto f(Z, 0)\end{aligned}$$

são homomorfismos sobrejetores de anéis. Além disso, $\text{Ker}(\phi) = (X)$ e $\text{Ker}(\psi) = (Y)$. Visto que $\mathbb{Q}[Z]$ é um domínio, os ideais (X) e (Y) são primos em $\mathbb{Q}[X, Y]$. Pela Proposição 15, as $\mathbb{Q}$ -variedades $\mathcal{V}(X)$ e $\mathcal{V}(Y)$ são subconjuntos irredutíveis de $\mathcal{V}(XY)$.

Seja W um subconjunto irredutível de $\mathcal{V}(XY)$ tal que $\mathcal{V}(X) \subset W$. Claramente, $\mathcal{V}(X)$ e $W \cap \mathcal{V}(Y)$ são conjuntos fechados em W satisfazendo

$$W = \mathcal{V}(X) \cup (W \cap \mathcal{V}(Y)).$$

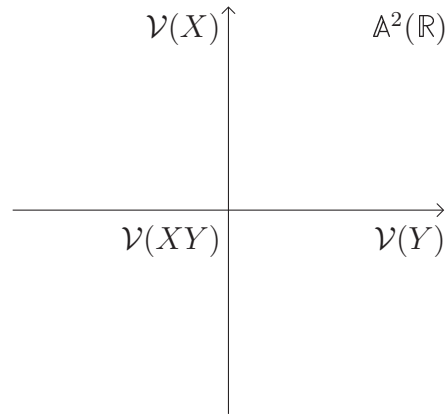
Como $W \neq W \cap \mathcal{V}(Y)$, temos $W = \mathcal{V}(X)$. Isso significa que $\mathcal{V}(X)$ é uma componente irredutível de $\mathcal{V}(XY)$. Similarmente, prova-se que $\mathcal{V}(Y)$ é também uma componente irredutível de $\mathcal{V}(XY)$.

Portanto,

$$\mathcal{V}(XY) = \mathcal{V}(X) \cup \mathcal{V}(Y)$$

é uma decomposição de $\mathcal{V}(XY)$ como união de duas de suas componentes irredutíveis. O Corolário 4 garante que $\mathcal{V}(X)$ e $\mathcal{V}(Y)$ são as únicas componentes irredutíveis de $\mathcal{V}(XY)$, uma vez que qualquer componente irredutível de $\mathcal{V}(XY)$ está contida na união $\mathcal{V}(X) \cup \mathcal{V}(Y)$.

Figura 4.2: Decomposição da curva algébrica plana definida pela equação $XY = 0$



5. CONCLUSÕES

De acordo com o exposto, a estrutura dos módulos é bastante rica por generalizar ideias a respeito de anéis e de espaços vetoriais. Além disso, as variedades algébricas afins são os exemplos mais simples de variedades algébricas. Por essa razão, elas são um bom ponto de partida para compreendermos a motivação para a fundamentação atual da Geometria Algébrica, devida a Grothendieck.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ATIYAH, M. F.; MACDONALD, I. G. **Introduction to commutative algebra**. Reading, Massachusetts: Addison-Wesley, 1969.
- [2] BORGES, H.; TENGAN, E. **Álgebra comutativa em quatro movimentos**. Rio de Janeiro: IMPA, 2015.
- [3] ENDERTON, H. B. **Elements of set theory**. New York: Academic Press, 1977.
- [4] GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. 6. ed. Rio de Janeiro: IMPA, 2013.
- [5] HALMOS, P. R. **Teoria ingênua dos conjuntos**. Rio de Janeiro: Editora Ciência Moderna, 2001.
- [6] KUNZ, E. **Introduction to commutative algebra and algebraic geometry**. Boston: Birkhäuser, 1985.
- [7] MUNKRES, J. R. **Topology**. 2. ed. Upper Saddle River, New Jersey: Prentice Hall, 2000.
- [8] SHAFAREVICH, I. R. **Basic algebraic geometry 1: varieties in projective space**. 2. ed. Berlin: Springer-Verlag, 1994.