UNIVERSIDADE FEDERAL DO PARANÁ

MATHEUS MORAES SANTOS

Grupos algébricos e Álgebras de Hopf

CURITIBA
2021

MATHEUS MORAES SANTOS

Grupos algébricos e Álgebras de Hopf

Trabalho de conclusão apresentado ao curso de Licenciatura em Matemática da Universidade Federal do Paraná como requisito parcial à obtenção do grau de licenciado em Matemática.

Orientador: Prof. Dr. Marcelo Muniz Silva Alves.

CURITIBA
2021

AGRADECIMENTOS

Primeiramente agradeço a Deus, meu criador e formador.

À minha família, em especial aos meus pais, Rosemeri e Carlos, pelo apoio e amor incondicional. Sem eles este trabalho não seria possível.

Aos meus amigos, por me acompanharem nessa jornada em todos os momentos.

A todos os professores que fizeram parte do meu crescimento acadêmico e pessoal, em particular aos professores do curso de Matemática da UFPR.

Por fim ao meu orientador, Professor Marcelo Muniz, pelas incontáveis e valiosas lições durante estes dois anos de orientação.

"Tudo o que temos de decidir é o que fazer com o tempo que nos é dado."
- Gandalf, o Cinzento

RESUMO

A todo grupo algébrico pode-se relacionar duas estruturas distintas: grupos algébricos afins e grupos algébricos projetivos. Neste trabalho apresentamos esses dois tipos de grupos. Inicialmente desenvolvemos um exemplo de grupo algébrico projetivo, o grupo de uma curva elíptica. Em sequência estudamos a teoria geral dos grupos algébricos afins e a sua relação com as álgebras de Hopf. Em especial demonstramos, via a teoria de ações de grupos algébricos e das representações de suas álgebras de funções, que todo grupo algébrico afim pode ser linearizado, isto é, pode ser realizado como um grupo de matrizes. Em conclusão discutimos alguns exemplos de linearização de grupos algébricos afins.

Palavras chave: Grupos algébricos, Álgebras de Hopf, Linearidade dos grupos algébricos afins.

ABSTRACT

To every algebraic group we can associate two distinct structures: affine algebraic groups and projective algebraic groups. In this dissertation we present these two types of groups. We initially develop an example of a projective algebraic group, the group of an elliptic curve. Next, we study the general theory of affine algebraic groups and their relation with Hopf algebras. In particular, we prove, via the theory of actions of algebraic groups and the representations of their algebra of functions, that every affine algebraic group can be linearized, that is, it can be realized as a matrix group. In conclusion we discuss some examples of linearization of affine algebraic groups.

Keywords: Algebraic groups, Hopf Algebras, Linearity of affine algebraic groups.

Lista de Figuras

Sumário

Introdução

Um grupo algébrico é um conjunto equipado de duas estruturas, a de *grupo abstrato* e a de *variedade algébrica*, compatíveis no sentido em que as operações do grupo são morfismos de variedades. Em geometria algébrica existem diversas formulações do conceito de variedade, que, de certo modo, podem ser consideradas como generalizações da seguinte: uma variedade algébrica consiste em um conjunto de pontos, que são soluções de uma quantia finita de equações polinomiais, com coeficientes em um corpo $\mathbb{K}$.

Fixado um corpo $\mathbb{K}$, as variedades algébricas surgem naturalmente em dois espaços geométricos: o espaço afim $\mathbb{A}^n_{\mathbb{K}}$ e o espaço projetivo $\mathbb{P}^n_{\mathbb{K}}$. Nesse sentido os grupos algébricos pertencentes a um espaço afim são denominados *grupos algébricos afins* e aqueles pertencentes a um espaço projetivo são chamados *grupos algébricos projetivos*, ou ainda, *variedades abelianas*, visto que todo grupo dessa forma é necessariamente comutativo.

Há uma conexão notória entre os grupos algébricos afins e as variedades abelianas: todo grupo algébrico conexo G contém um único subgrupo algébrico maximal H que é isomorfo a um grupo algébrico afim, é normal e tal que o quociente G/H é uma variedade abeliana. Esse resultado é conhecido como *Teorema da estrutura de Chevalley-Barsotti* e a partir dele podemos dizer que os grupos algébricos afins e as variedades abelianas são os ingredientes principais de um grupo algébrico. O teorema da estrutura para os grupos algébricos foi desenvolvido independentemente por C. Chevalley e I. Barsotti na década de 50, segundo [4] (Capítulo VI, Seção 2).

Dada uma variedade algébrica afim V, associamos uma *álgebra de funções regulares*, denotada por $\mathbb{K}[V]$. Quando V também possui a estrutura de grupo algébrico, sua álgebra de funções traz uma representação natural do grupo V que satisfaz propriedades importantes para o estudo do grupo, e estas vêm do fato que $\mathbb{K}[V]$ é munida de uma estrutura extra, a estrutura de *álgebra de Hopf*. Em resumo, uma álgebra de Hopf é um espaço vetorial sobre $\mathbb{K}$, munido de duas estruturas formalmente duais: a de álgebra e a de coálgebra, além de um operador linear, chamado antípoda, que generaliza o conceito de inverso em um grupo.

Esse trabalho é dividido em três principais objetivos: desenvolver um exemplo clássico de grupo algébrico projetivo, o grupo de uma curva elíptica; apresentar a teoria geral dos grupos algébricos afins e suas ações, em especial o *Teorema da linearidade*; e descrever a relação entre os grupos algébricos afins e as álgebras de Hopf.

O primeiro capítulo consiste em uma introdução à geometria de curvas no plano projetivo. Desenvolvemos resultados gerais sobre curvas projetivas planas, como a classificação das cônicas em $\mathbb{P}^2_{\mathbb{R}}$ e dois casos particulares do Teorema de Bézout, válidos sobre um corpo arbitrário $\mathbb{K}$, além de construir a estrutura de grupo algébrico em uma curva elíptica.

Os próximos dois capítulos são destinados à construção dos fundamentos necessários para o estudo dos grupos algébricos afins. No Capítulo 2 fazemos um apanhado geral sobre módulos e álgebras sobre um anel comutativo e, em especial, construímos o produto tensorial de módulos. No Capítulo 3 é desenvolvida a teoria clássica de geometria algébrica, em particular demonstramos o *Lema de Normalização de Noether* e uma versão do *Nullstellensatz* de Hilbert.

O último capítulo é dividido em três momentos: inicialmente desenvolvemos um estudo dos grupos algébricos afins e suas ações em variedades. Em seguida apresentamos uma introdução às álgebras de Hopf e demonstramos que a álgebra de funções de um grupo algébrico afim é munida dessa estrutura. Por fim estudamos representações da álgebra de funções de um grupo algébrico afim, os comódulos, e dessa forma demonstramos o *Teorema da linearidade dos grupos algébricos afins*, o qual garante que todo grupo algébrico afim é isomorfo a um subgrupo algébrico de algum *grupo linear geral*, isto é, um subgrupo algébrico de $\mathrm{GL}_n(\mathbb{K})$, para algum natural n. Além disso apresentamos exemplos da linearização de alguns grupos algébricos clássicos, como o *grupo aditivo*, o *grupo multiplicativo* e o *grupo afim*.

Capítulo 1

Grupo de uma curva elíptica

Neste capítulo vamos desenvolver um exemplo de grupo algébrico projetivo, o grupo de uma curva cúbica, mais conhecida como curva elíptica. Durante as próximas seções apresentamos, baseado em [19], um apanhado de definições e resultados que compõem uma introdução à geometria de curvas no espaço projetivo.

1.1 Espaço afim

Definição 1.1.1. O *espaço afim* n-dimensional sobre um corpo $\mathbb{K}$ é o produto cartesiano $\mathbb{K}^n$, o qual denotamos por $\mathbb{A}^n_{\mathbb{K}}$, ou simplesmente $\mathbb{A}^n$.

Observação 1.1.2. Note que o espaço afim $\mathbb{A}^n$ é apenas um conjunto, a priori desvinculado de qualquer estrutura algébrica. Os elementos de $\mathbb{A}^n$ também são chamados de pontos.

Nas próximas seções abordaremos resultados sobre envolvendo espaços afins de dimensão 2, isto é $\mathbb{A}^2_{\mathbb{K}}$, também chamado de *plano afim* sobre $\mathbb{K}$.

1.2 Espaço projetivo

Inicialmente vamos discutir o espaço onde o grupo da cúbica é realizado. Dado um corpo $\mathbb{K}$ definimos o plano projetivo, denotado por $\mathbb{P}^2_{\mathbb{K}}$, como o quociente

$$\mathbb{P}^2_{\mathbb{K}} := (\mathbb{K}^3 - \{0\})/\sim,$$

onde $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$, para todo $\lambda \in \mathbb{K}^*$.

Cada elemento do plano projetivo é uma classe de equivalência de um ponto não nulo (X, Y, Z), denotada por $(X : Y : Z)$.

Podemos estender esta construção para o espaço projetivo de dimensão n, definindo

$$\mathbb{P}^n_{\mathbb{K}} \coloneqq (\mathbb{K}^{n+1} - \{0\})/\sim$$

onde $(X_0, \ldots, X_n) \sim (\lambda X_0, \ldots, \lambda X_n)$ para todo $\lambda \in \mathbb{K}^*$. Em especial para $n = 1$ temos a reta projetiva $\mathbb{P}^1_{\mathbb{K}}$.

Observação 1.2.1. Note que a origem $(0, 0, 0)$ é descartada do plano projetivo, logo não há a classe $(0{:}0{:}0)$.

1.3 Ação do grupo das matrizes

O grupo das matrizes invertíveis $\mathrm{GL}_3(\mathbb{K})$ tem uma ação natural no plano projetivo, dada pela multiplicação: dado um ponto $(a{:}b{:}c) \in \mathbb{P}^2_{\mathbb{K}}$ e uma matriz $M \in \mathrm{GL}_3(\mathbb{K})$ definimos

$$M \cdot (a{:}b{:}c) \coloneqq (M \cdot (a\ b\ c)^t)^t/\sim,$$

ou seja, fazemos a multiplicação de uma matriz 3×3 por uma matriz coluna 3×1, então transpomos este resultado obtendo uma matriz 1×3 cujas entradas são as coordenadas de um representante de $(a{:}b{:}c)$, e por fim tomamos a classe deste elemento.

Esta ação é bem definida, pois se $M \cdot (a{:}b{:}c) = (a'{:}b'{:}c')$, então para qualquer $\lambda \in \mathbb{K}^*$ temos

$$\begin{aligned} M \cdot (\lambda a{:}\lambda b{:}\lambda c) &= (M \cdot (\lambda a\ \lambda b\ \lambda c)^t)^t/\sim \\ &= \lambda (M \cdot (a\ b\ c)^t)^t/\sim \\ &= \lambda (M \cdot (a{:}b{:}c)) \\ &= \lambda (a'{:}b'{:}c'). \end{aligned}$$

Além disso, satisfaz os axiomas de uma ação de grupo abstrato em um conjunto, isto é, $\mathrm{Id}_3 \cdot (a{:}b{:}c) = (a{:}b{:}c)$ e $(MN) \cdot (a{:}b{:}c) = M \cdot (N \cdot (a{:}b{:}c))$, para todas $M, N \in \mathrm{GL}_3(\mathbb{K})$ e $(a{:}b{:}c) \in \mathbb{P}^2_{\mathbb{K}}$.

Observação 1.3.1. A teoria de ações de grupo, em especial dos algébricos, é explorada com detalhes na Seção 4.2.

A multiplicação por matrizes invertíveis atua como as mudanças de coordenadas no plano projetivo. Isso nos sugere a seguinte definição.

Definição 1.3.2. Uma *transformação projetiva* em $\mathbb{P}^2_{\mathbb{K}}$ é uma função $T : \mathbb{P}^2_{\mathbb{K}} \to \mathbb{P}^2_{\mathbb{K}}$ com $T(P) = M \cdot P$, para uma matriz $M \in \mathrm{GL}_3(\mathbb{K})$ e pontos $P = (X{:}Y{:}Z)$.

Teorema 1.3.3. *Sejam $P_1, P_2, P_3, P_4 \in \mathbb{P}^2_{\mathbb{K}}$ pontos três a três não colineares. Existe uma transformação projetiva T tal que $T(P_1) = (1{:}0{:}0)$, $T(P_2) = (0{:}1{:}0), T(P_3) = (0{:}0{:}1)$ e $T(P_4) = (1{:}1{:}1)$.*

Demonstração. Denote $P_i = (X_i{:}Y_i{:}Z_i)$, $i = 1, 2, 3, 4$. Como não há 3 pontos colineares as colunas da matriz

$$M = \begin{pmatrix} X_1 & X_2 & X_3 \\ Y_1 & Y_2 & Y_3 \\ Z_1 & Z_2 & Z_3 \end{pmatrix}$$

são linearmente independentes, portanto M é invertível.

Observe que $M \cdot (1{:}0{:}0) = (X_1{:}Y_1{:}Z_1), M \cdot (0{:}1{:}0) = (X_2{:}Y_2{:}Z_2)$ e $M \cdot (0{:}0{:}1) = (X_3{:}Y_3{:}Z_3)$.

Também pela independência linear entre os $P_i's$ temos que existem $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathbb{K}$ não todos nulos tais que

$$\varepsilon_1 \begin{pmatrix} X_1 \\ Y_1 \\ Z_1 \end{pmatrix} + \varepsilon_2 \begin{pmatrix} X_2 \\ Y_2 \\ Z_2 \end{pmatrix} + \varepsilon_3 \begin{pmatrix} X_3 \\ Y_3 \\ Z_3 \end{pmatrix} = \begin{pmatrix} X_4 \\ Y_4 \\ Z_4 \end{pmatrix}.$$

Logo, tomando os representantes $P_i = (\varepsilon_i X_i{:}\varepsilon_i Y_i{:}\varepsilon_i Z_i)$, $i = 1, 2, 3$ temos a matriz invertível

$$N = \begin{pmatrix} \varepsilon_1 X_1 & \varepsilon_2 X_2 & \varepsilon_3 X_3 \\ \varepsilon_1 Y_1 & \varepsilon_2 Y_2 & \varepsilon_3 Y_3 \\ \varepsilon_1 Z_1 & \varepsilon_2 Z_2 & \varepsilon_3 Z_3 \end{pmatrix}.$$

Definimos $S : \mathbb{P}^2_{\mathbb{K}} \to \mathbb{P}^2_{\mathbb{K}}$ por $S(P) = N \cdot P$. Segue que S tem as seguintes imagens:

$$(1{:}0{:}0) \mapsto P_1,\ (0{:}1{:}0) \mapsto P_2,\ (0{:}0{:}1) \mapsto P_3 \text{ e } (1{:}1{:}1) \mapsto P_4.$$

Portanto a transformação desejada é $T = S^{-1}$, isto é $T : \mathbb{P}^2_{\mathbb{K}} \to \mathbb{P}^2_{\mathbb{K}}$ é dada por $T(P) = N^{-1} \cdot P$. ■

O teorema abaixo tem grande importância na área de geometria projetiva clássica e generaliza o resultado anterior.

Teorema 1.3.4 (Teorema Fundamental da Geometria Projetiva)**.** *Dados dois conjuntos de pontos três a três não colineares $\{A, B, C, D\}, \{A', B', C', D'\} \subset \mathbb{P}^2_{\mathbb{K}}$ existe uma única transformação projetiva que leva*

$$A \mapsto A', B \mapsto B', C \mapsto C', D \mapsto D'.$$

A ideia da demonstração é usar o Teorema 1.3.3 para levar A, B, C, D por uma transformação projetiva no quadrilátero padrão, isto é, nos pontos $(1{:}0{:}0)$, $(0{:}1{:}0)$,

(0:0:1), (1:1:1) e pelo mesmo processo levar o quadrilátero padrão em A', B', C', D'. Assim a transformação projetiva em questão é obtida compondo as duas transformações anteriores. A unicidade segue do fato que as transformações projetivas são invertíveis (veja o Teorema 3 do Capítulo 3 em [6]).

Observação 1.3.5. Perceba que, no caso do plano afim real $\mathbb{A}^2_{\mathbb{R}}$, dados três pontos não colineares existe uma (única) transformação afim, isto é, uma transformação dada por uma matriz invertível, que mapeia estes pontos a outros três fixados (respeitando a não colinearidade). Entretanto a imagem de um quarto ponto por esta mesma transformação é completamente determinada pelos demais. Este resultado é conhecido como *Teorema Fundamental da Geometria Afim* (veja [6], Capítulo 2).

1.4 Cônicas em $\mathbb{A}^2_{\mathbb{R}}$ e $\mathbb{P}^2_{\mathbb{R}}$

As cônicas possuem um papel essencial para os resultados que compõem a estrutura de grupo da cúbica, assim essa seção se dedica à passagem desses elementos do plano real $\mathbb{A}^2_{\mathbb{R}}$ para o projetivo $\mathbb{P}^2_{\mathbb{R}}$, bem como desenvolve alguns teoremas de classificação.

Uma *cônica* em $\mathbb{A}^2_{\mathbb{R}}$ é a curva descrita pelas raízes de um polinômio $q(X, Y) \in \mathbb{R}[X, Y]$, da forma

$$q(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f, \tag{1.1}$$

onde nem todos os escalares $a, \ldots, f \in \mathbb{R}$ são nulos. Ou seja, é um conjunto da forma

$$C = \{(X, Y) \in \mathbb{A}^2_{\mathbb{R}} \mid q(X, Y) = 0\}.$$

Definição 1.4.1. Uma cônica dada por um polinômio $q \in \mathbb{R}[X, Y]$ como em (1.1) é dita *não degenerada* se

$$\begin{vmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{vmatrix} \neq 0.$$

A partir do grupo de transformações euclidianas do plano, isto é, o grupo $E(2) = \{T(\mathbf{x}) = M\mathbf{x} + v : M \in \mathrm{M}_2(\mathbb{R}) \text{ ortogonal}, v \in \mathbb{A}^2_{\mathbb{R}}\}$, podemos classificar as cônicas não degeneradas em:

$$\begin{cases} \text{Parábola} & (Y^2 = aX), \\ \text{Elipse} & \left(\dfrac{X^2}{a^2} + \dfrac{Y^2}{b^2} = 1\right), \\ \text{Hipérbole} & \left(\dfrac{X^2}{a^2} - \dfrac{Y^2}{b^2} = 1\right), \end{cases}$$

onde $a, b \in \mathbb{R}$.

Agora via o grupo de transformações afins em $\mathbb{A}^2_{\mathbb{R}}$, denotado por $A(2) = \{T(\mathbf{x}) = M\mathbf{x} + v : M \in \mathrm{M}_2(\mathbb{R}) \text{ invertível}, v \in \mathbb{A}^2_{\mathbb{R}}\}$, é possível classificar as cônicas em:

$$\text{Não Degeneradas} = \begin{cases} \text{Parábola} & (Y^2 = X), \\ \text{Elipse} & (X^2 + Y^2 = 1), \\ \text{Hipérbole} & (X^2 - Y^2 = 1), \end{cases}$$

e

$$\text{Degeneradas} = \begin{cases} \text{Ponto único} & (X^2 + Y^2 = 0), \\ \text{Conjunto vazio} & (X^2 + Y^2 = -1, X^2 = -1, 1 = 0), \\ \text{Reta} & (X = 0), \\ \text{Par de retas} & (XY = 0), \\ \text{Retas paralelas} & (X(X-1) = 0), \\ \text{Reta dupla} & (X^2 = 0). \end{cases}$$

Para definir curvas, em especial cônicas, no plano projetivo, é preciso considerar equações compatíveis com este espaço, neste sentido definimos:

Definição 1.4.2. Um polinômio $F \in \mathbb{K}[X_1, \ldots, X_n]$ é dito *homogêneo* se todos seus termos não nulos possuem o mesmo grau, ou seja, F é da forma

$$F(X_1, \ldots, X_n) = \sum_{d_1 + \cdots + d_n = d} a_{d_1, \ldots, d_n} X_1^{d_1} \ldots X_n^{d_n},$$

onde $a_{d_1,\ldots,d_n} \in \mathbb{K}$ e d é o grau de F.

Algebricamente é possível obter um polinômio homogêneo a partir de um polinômio qualquer, introduzindo uma nova variável. Esse processo é chamado homogeneização.

Definição 1.4.3. Seja $F \in \mathbb{K}[X_1, \ldots, X_n]$ um polinômio de grau d. A *homogeneização* de F em $n+1$ variáveis é a aplicação

$$\varphi^n : \mathbb{K}[X_1, \ldots, X_n] \longrightarrow \mathbb{K}[X_1, \ldots, X_n, X_{n+1}],$$

dada por

$$F(X_1, \ldots, X_n) \longmapsto X_{n+1}^d F\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Quando não existir possibilidade de confusão denotaremos φ^n simplesmente por φ.

Tomando $\mathbb{K} = \mathbb{R}$, $n = 2$ e $d = 2$ temos que φ^2 leva um polinômio genérico não nulo $q(X, Y) = aX^2 + bXY + cY^2 + dX + eY + f \in \mathbb{R}[X, Y]$ em $Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 \in \mathbb{R}[X, Y, Z]$.

Assim definimos uma cônica projetiva real como um conjunto da forma

$$C = \{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{R}} : Q(X, Y, Z) = 0\},$$

para um polinômio homogêneo de grau dois $Q(X, Y, Z) \in \mathbb{R}[X, Y, Z]$.

De modo geral no plano projetivo sobre um corpo $\mathbb{K}$ definimos curvas:

Definição 1.4.4. Uma *curva projetiva* $D \subset \mathbb{P}^2_{\mathbb{K}}$ é o conjunto de raízes de um polinômio homogêneo $F \in \mathbb{K}[X, Y, Z]$.

Estes conjuntos respeitam a estrutura do plano projetivo, pois se d é o grau de F e $(X:Y:Z) \in D$, então

$$F(\lambda X, \lambda Y, \lambda X) = \lambda^d F(X, Y, Z) = 0,$$

assim D está bem definida, visto que independe da escolha do representante da classe $(X:Y:Z) \in \mathbb{P}^2_{\mathbb{K}}$.

Geometricamente o processo de homogeneização ocorre de maneira natural, tendo em vista que o plano afim $\mathbb{A}^2_{\mathbb{K}}$ está em bijeção com cortes do plano projetivo, por exemplo o subconjunto $\{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{K}} : Z = 1\} \subset \mathbb{P}^2_{\mathbb{K}}$. De fato, a cada ponto $(X, Y) \in \mathbb{A}^2_{\mathbb{K}}$ associamos bijetivamente a classe $(X:Y:1)$, que possui um único representante nesse subconjunto, pois se $(X:Y:1) = (X':Y':1)$ então $X = X'$ e $Y = Y'$. De maneira semelhante temos bijeções de $\mathbb{A}^2_{\mathbb{K}}$ com $\{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{K}} : X = 1\} \subset \mathbb{P}^2_{\mathbb{K}}$ e $\{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{K}} : Y = 1\} \subset \mathbb{P}^2_{\mathbb{K}}$.

Pelo raciocínio anterior é válido escrever o plano afim como

$$\mathbb{A}^2_{\mathbb{K}} = \{(X:Y:1) \in \mathbb{P}^2_{\mathbb{K}} : (X, Y) \in \mathbb{A}^2_{\mathbb{K}}\}. \tag{1.2}$$

Em especial podemos enxergar uma curva afim como parte de uma curva projetiva: começamos com uma curva afim $C = \{(X, Y) \in \mathbb{A}^2_{\mathbb{K}} : f(X, Y) = 0\}$, onde $f \in \mathbb{K}[X, Y]$. Pela aplicação de homogeneização φ obtemos um polinômio homogêneo $\varphi(f) \in \mathbb{K}[X, Y, Z]$, que define uma curva projetiva $D = \{(X:Y:Z) \in \mathbb{P}^2_{\mathbb{R}} : \varphi(f)(X, Y, Z) = 0\}$. Por fim notamos que C pode ser realizada, a partir da identificação (1.2), como a interseção da curva projetiva D com o conjunto projetivo $Z = 1$, isto é

$$C = D \cap \{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{K}} : Z = 1\}.$$

Notação 1.4.5. No decorrer deste capítulo denotaremos

$$\mathcal{V}(F) = \{(X_1 : \ldots : X_{n+1}) \in \mathbb{P}^n_{\mathbb{K}} : F(X_1, \ldots, X_{n+1}) = 0\},$$

para a curva projetiva descrita por um polinômio homogêneo $F \in \mathbb{K}[X_1, \ldots, X_{n+1}]$.

Uma pergunta natural ao se pensar em cônicas projetivas reais é: *Assim como no caso afim, existe uma classificação destes elementos?* A resposta é afirmativa, e para comprovar este fato necessitaremos de resultados sobre formas bilineares em um espaço vetorial.

Com esse resultado provaremos que as cônicas não degeneradas em $\mathbb{A}^2_{\mathbb{R}}$, inseridas no plano projetivo $\mathbb{P}^2_{\mathbb{R}}$ via o processo de homogeneização, são projetivamente equivalentes. A seguir damos uma ideia da demonstração deste resultado para um caso particular. Considere as cônicas não degeneradas, dadas por equações como abaixo.

$$\text{Elipse} = \{(X, Y) \in \mathbb{A}^2_{\mathbb{R}} : X^2 + Y^2 - 1 = 0\},$$

$$\text{Hipérbole} = \{(X, Z) \in \mathbb{A}^2_{\mathbb{R}} : X^2 - Z^2 + 1 = 0\},$$

e

$$\text{Parábola} = \{(X, Y) \in \mathbb{A}^2_{\mathbb{R}} : Y^2 - X = 0\}.$$

Geometricamente essas curvas são representadas por

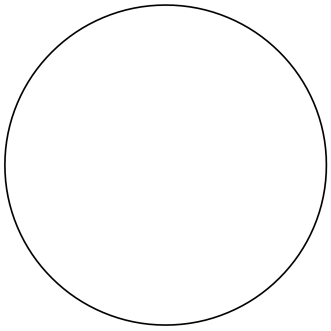


Figura 1.1: Elipse.

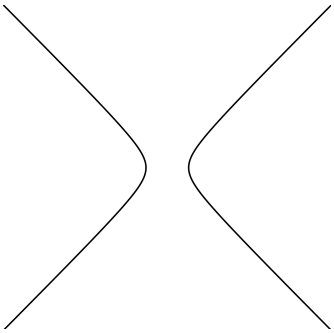


Figura 1.2: Hipérbole.
Fonte: Autoria própria.

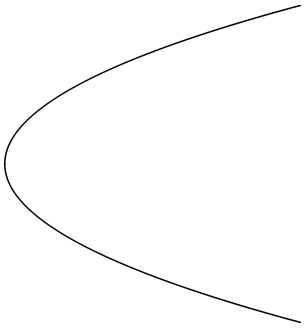


Figura 1.3: Parábola.

Agora homogeneizamos as equações de cada curva, obtendo: para a elipse $\varphi(X^2 + Y^2 - 1) = X^2 + Y^2 - Z^2$, para hipérbole $\varphi(X^2 - Z^2 + 1) = X^2 + Y^2 - Z^2$ (perceba que nesse caso a homogeneização ocorre na variável Y) e para a parábola $\varphi(Y^2 - X) = Y^2 - XZ$. Nos dois primeiros casos notamos que as equações resultantes coincidem diretamente, e como veremos mais adiante com a Proposição 1.5.16, os polinômios $X^2 + Y^2 - Z^2$ e $Y^2 - XZ$ também descrevem a mesma curva projetiva. Ou seja, observamos algebricamente que a passagem das três cônicas não degeneradas no plano real para o projetivo resulta em uma única curva: $\mathcal{V}(X^2 + Y^2 - Z^2) \subset \mathbb{P}^2_{\mathbb{R}}$.

Este fato possui uma tradução geométrica muito evidente, pois em $\mathbb{A}^3_{\mathbb{R}}$ a equação $X^2 + Y^2 - Z^2 = 0$ descreve um cone duplo e as cônicas planas emergem desta construção a partir de interseções do cone com planos convenientes.

1.5 Classificação das cônicas em $\mathbb{P}^2_{\mathbb{R}}$

Durante essa seção desenvolveremos resultados básicos sobre formas bilineares e formas quadráticas em um espaço vetorial, seguindo as referências [12], [14] e [8]. Esses resultados serão utilizados para classificar as cônicas no plano projetivo real.

Definição 1.5.1. Seja V um $\mathbb{K}$-espaço vetorial. Uma *forma bilinear* em V é uma função $f : V \times V \to \mathbb{K}$ que associa a cada par ordenado de vetores $(u, v) \in V \times V$ um escalar $f(u, v) \in \mathbb{K}$, tal que

$$f(\alpha u + v, w) = \alpha f(u, w) + f(v, w),$$
$$f(u, \alpha v + w) = \alpha f(u, v) + f(u, w),$$

para todos $u, v, w \in V$ e $\alpha \in \mathbb{K}$.

Note que a função nula de $V \times V$ em $\mathbb{K}$ é uma forma bilinear, também qualquer combinação linear de formas bilineares resulta em uma forma bilinear. Deste modo o conjunto de todas as formas bilineares em V é um $\mathbb{K}$-espaço vetorial, que denotamos por $L(V, V, \mathbb{K})$.

Proposição 1.5.2. *Seja V um $\mathbb{K}$-espaço vetorial de dimensão finita. Toda forma bilinear f em V possui uma expressão do tipo $f(u, v) = X^t AY$, com X, Y matrizes coordenadas de u, v em uma base $\mathcal{B}$.*

Demonstração. Seja $\mathcal{B} = \{v_1, \ldots, v_n\}$ base ordenada de V. Suponha $u, v \in V$ com $u = x_1v_1 + \ldots + x_nv_n$ e $v = y_1v_1 + \ldots + y_nv_n$, então

$$\begin{aligned} f(u, v) &= f(\sum_{i=1}^{n} x_i v_i, v) \\ &= \sum_{i=1}^{n} x_i f(v_i, v) \\ &= \sum_{i=1}^{n} x_i f(v_i, \sum_{j=1}^{n} y_j v_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j f(v_i, v_j). \end{aligned}$$

Tome $a_{i,j} = f(v_i, v_j)$ e defina $A = (a_{i,j})$. Assim,

$$\begin{aligned} f(u, v) &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x_i y_j \\ &= X^t AY, \end{aligned}$$

com $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ e $A \in \mathrm{M}_n(\mathbb{K})$.

Então toda forma bilinear em V é do tipo

$$f(u, v) = [u]_{\mathcal{B}}^t A [v]_{\mathcal{B}}. \tag{1.3}$$

Por outro lado, dada $A = (a_{i,j}) \in \mathrm{M}_n(\mathbb{K})$ é fácil ver que a Equação 1.3 define uma forma bilinear em V, tal que $a_{i,j} = f(v_i, v_j)$. ■

Definição 1.5.3. Seja V um $\mathbb{K}$-espaço vetorial de dimensão finita e $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base ordenada de V. Se f é forma bilinear em V a *matriz de f na base $\mathcal{B}$* é $A = (a_{i,j}) \in \mathrm{M}_n(\mathbb{K})$, tal que $a_{i,j} = f(v_i, v_j)$, denotada por $[f]_{\mathcal{B}}$.

Teorema 1.5.4. *Seja V como na definição anterior. Para cada base ordenada $\mathcal{B}$ de V, a função que associa cada forma bilinear $f \in V$ a sua matriz em $\mathcal{B}$ é um isomorfismo de $L(V, V, \mathbb{K})$ em $\mathrm{M}_n(\mathbb{K})$.*

Demonstração. Pela Proposição 1.5.2 esta função é bijetiva. Agora mostraremos que é uma transformação linear. De fato,

$$(cf + g)(v_i, v_j) = cf(v_i, v_j) + g(v_i, v_j)$$

para cada i, j, logo

$$[cf + g]_{\mathcal{B}} = c[f]_{\mathcal{B}} + [g]_{\mathcal{B}}.$$

■

Definição 1.5.5. Seja f uma forma bilinear em V. Dizemos que f é *simétrica* se para todos $u, v \in V$,

$$f(u, v) = f(v, u).$$

Corolário 1.5.6. *Seja $\mathbb{K}$ um corpo e V um $\mathbb{K}$-espaço vetorial. Existe um isomorfismo entre o espaço vetorial das formas bilineares simétricas e o espaço das matrizes $n \times n$ simétricas com entradas em $\mathbb{K}$.*

Demonstração. Por definição a matriz de uma forma bilinear f em V é $[f]_{\mathcal{B}} = (a_{i,j})$, onde $a_{i,j} = f(v_i, v_j)$ para $1 \leq i, j \leq n$ e $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base ordenada de V.

Agora se f é simétrica $f(v_i, v_j) = f(v_j, v_i)$, logo $a_{i,j} = a_{j,i}$, ou seja, a matriz $[f]_{\mathcal{B}}$ é simétrica. Assim segue do Teorema 1.5.4 que há um isomorfismo entre o espaço das formas bilineares simétricas e o espaço das matrizes $n \times n$ simétricas. ■

Definição 1.5.7. Seja V um espaço vetorial sobre um corpo $\mathbb{K}$. Uma *forma quadrática* em V é uma função $q : V \to \mathbb{K}$ tal que

(i) $q(\lambda v) = \lambda^2 q(v)$, para todos $v \in V$ e $\lambda \in \mathbb{K}$;

(ii) a função $f_q : V \times V \to \mathbb{K}$ definida por

$$f_q(u, v) = q(u + v) - q(u) - q(v)$$

é uma forma bilinear simétrica em V.

Os próximos dois resultados indicam a forte relação entre formas quadráticas em um espaço vetorial e polinômios homogêneos de grau dois, fixado um sistema de coordenadas.

Proposição 1.5.8. *Sejam V um $\mathbb{K}$-espaço vetorial e $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base de V. Dado um polinômio homogêneo de grau dois*

$$F(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} c_{i,j} X_i X_j$$

em $\mathbb{K}[X_1, \ldots, X_n]$, a função $q : V \to \mathbb{K}$ dada por

$$q(\sum_{i=1}^{n} \alpha_i v_i) \coloneqq \sum_{1 \leq i \leq j \leq n} c_{i,j} \alpha_i \alpha_j$$

é uma forma quadrática em V.

Demonstração. Sejam $u = \sum_{i=1}^{n} \alpha_i v_i, v = \sum_{i=1}^{n} \beta_i v_i, w = \sum_{i=1}^{n} \gamma_i v_i$ vetores em V e $\lambda \in \mathbb{K}$ um escalar. Então,

(i) $q(\lambda v) = q(\lambda \sum_{i=1}^{n} \alpha_i v_i)$

$$\begin{aligned}
&= q(\sum_{i=1}^{n} (\lambda \alpha_i) v_i) \\
&= \sum_{1 \leq i \leq j \leq n} c_{i,j} (\lambda \alpha_i)(\lambda \alpha_j) \\
&= \lambda^2 \sum_{1 \leq i \leq j \leq n} c_{i,j} \alpha_i \alpha_j \\
&= \lambda^2 q(\sum_{i=1}^{n} \alpha_i v_i) \\
&= \lambda^2 q(v).
\end{aligned}$$

(ii) a função $f_q : V \times V \to \mathbb{K}$ dada por

$$\begin{aligned}
f_q(u, v) &= q(u + v) - q(u) - q(v) \\
&= q(\sum_{i=1}^{n} (\alpha_i + \beta_i) v_i) - q(\sum_{i=1}^{n} \alpha_i v_i) - q(\sum_{i=1}^{n} \beta_i v_i) \\
&= \sum_{1 \leq i \leq j \leq n} c_{i,j} (\alpha_i + \beta_i)(\alpha_j + \beta_j) - \sum_{1 \leq i \leq j \leq n} c_{i,j} \alpha_i \alpha_j - \sum_{1 \leq i \leq j \leq n} c_{i,j} \beta_i \beta_j \\
&= \sum_{1 \leq i \leq j \leq n} c_{i,j} (\alpha_i \alpha_j + \alpha_i \beta_j + \beta_i \alpha_j + \beta_i \beta_j - \alpha_i \alpha_j - \beta_i \beta_j) \\
&= \sum_{1 \leq i \leq j \leq n} c_{i,j} (\alpha_i \beta_j + \beta_i \alpha_j),
\end{aligned}$$

é uma forma bilinear simétrica em V. De fato,

$$\begin{aligned} f_q(\lambda u + v, w) &= \sum_{1\leq i\leq j\leq n} c_{i,j}[(\lambda\alpha_i + \beta_i)\gamma_j + \gamma_i(\lambda\alpha_j + \beta_j)] \\ &= \sum_{1\leq i\leq j\leq n} c_{i,j}[(\lambda\alpha_i\gamma_j + \lambda\gamma_i\alpha_j) + (\beta_i\gamma_j + \gamma_i\beta_j)] \\ &= \lambda \sum_{1\leq i\leq j\leq n} c_{i,j}(\alpha_i\gamma_j + \gamma_i\alpha_j) + \sum_{1\leq i\leq j\leq n} c_{i,j}(\beta_i\gamma_j + \gamma_i\beta_j) \\ &= \lambda f_q(u, w) + f_q(v, w). \end{aligned}$$

De modo análogo prova-se que $f_q(u, \lambda v + w) = \lambda f_q(u, v) + f_q(u, w)$. Por fim, facilmente verificamos que f_q é simétrica

$$\begin{aligned} f_q(u, v) &= \sum_{1\leq i\leq j\leq n} c_{i,j}(\alpha_i\beta_j + \beta_i\alpha_j) \\ &= \sum_{1\leq i\leq j\leq n} c_{i,j}(\beta_i\alpha_j + \alpha_i\beta_j) \\ &= f_q(v, u). \end{aligned}$$

■

Reciprocamente, dada uma forma quadrática em V podemos associar um polinômio homogêneo de grau dois.

Proposição 1.5.9. *Sejam $q : V \to \mathbb{K}$ uma forma quadrática e $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base de V. Então existem escalares $c_{i,j} \in \mathbb{K}$ tais que*

$$q(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{1\leq i\leq j\leq n} c_{i,j}\alpha_i\alpha_j,$$

para todo $v = \sum_{i=1}^{n} \alpha_i v_i \in V$. Em especial, associamos a q o polinômio homogêneo de grau dois $Q(X_1, \ldots, X_n) = \sum_{1\leq i\leq j\leq n} c_{i,j}X_iX_j$.

Demonstração. Vamos proceder por indução na dimensão n do espaço vetorial V.

Para $n = 1$ é evidente, pois pela definição de forma quadrática $q(\alpha_1 v_1) = q(v_1)\alpha_1^2$, e $c_{1,1} = q(v_1)$. Agora para $n = 2$ temos,

$$\begin{aligned} q(\alpha_1 v_1 + \alpha_2 v_2) &= f_q(\alpha_1 v_1, \alpha_2 v_2) + q(\alpha_1 v_1) + q(\alpha_2 v_2) \\ &= f_q(v_1, v_2)\alpha_1\alpha_2 + q(v_1)\alpha_1^2 + q(v_2)\alpha_2^2 \end{aligned}$$

e basta tomar

$$c_{i,j} = \begin{cases} f_q(v_i, v_j), \text{ se } i \neq j \\ q(v_i), \text{ se } i = j \end{cases}. \tag{1.4}$$

Suponha válido para $n = k-1$, isto é,

$$q(\sum_{i=1}^{k-1} \alpha_i v_i) = \sum_{1\leq i<j\leq k-1} f_q(v_i, v_j)\alpha_i\alpha_j + \sum_{i=1}^{k-1} q(v_i)\alpha_i^2.$$

Então dado $v = \sum_{i=1}^{k} \alpha_i v_i$ temos,

$$\begin{aligned}
q(v) &= q(\sum_{i=1}^{k} \alpha_i v_i) \\
&= q(\sum_{i=1}^{k-1} \alpha_i v_i + \alpha_k v_k) \\
&= f_q(\sum_{i=1}^{k-1} \alpha_i v_i, \alpha_k v_k) + q(\sum_{i=1}^{k-1} \alpha_i v_i) + q(\alpha_k v_k) \\
&= \sum_{i=1}^{k-1} \alpha_i\alpha_k f_q(v_i, v_k) + \left(\sum_{1\leq i<j\leq k-1} f_q(v_i, v_j)\alpha_i\alpha_j + \sum_{i=1}^{k-1} q(v_i)\alpha_i^2 \right) + q(v_k)\alpha_k^2 \\
&= \sum_{1\leq i<j\leq k} f_q(v_i, v_j)\alpha_i\alpha_j + \sum_{i=1}^{k} q(v_i)\alpha_i^2.
\end{aligned}$$

o que conclui a indução. Assim é válido escrever

$$q(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{1\leq i\leq j\leq n} c_{i,j}\alpha_i\alpha_j,$$

onde os coeficientes $c_{i,j}$ são dados como na Equação (1.4). ■

Proposição 1.5.10. *Seja $\mathbb{K}$ um corpo com característica diferente de 2. Se V é um $\mathbb{K}$-espaço vetorial de dimensão finita, existe uma bijeção entre formas quadráticas em V e formas bilineares simétricas em V.*

Demonstração. Dada uma forma bilinear simétrica g em V definimos uma forma quadrática $q : V \to \mathbb{K}$ pondo $q(v) = g(v, v)$, para $v \in V$. A função q é de fato uma forma quadrática, pois

(i) $q(\lambda v) = g(\lambda v, \lambda v) = \lambda^2 g(v, v) = \lambda^2 q(v)$, para todo $v \in V$ e $\lambda \in \mathbb{K}$.

(ii) a função $f_q : V \times V \to \mathbb{K}$ dada por

$$\begin{aligned} f_q(u,v) &= q(u+v) - q(u) - q(v) \\ &= g(u+v, u+v) - g(u,u) - g(v,v) \\ &= g(u,u) + g(u,v) + g(v,u) + g(v,v) - g(u,u) - g(v,v) \\ &= 2g(u,v) \end{aligned}$$

é uma forma bilinear simétrica.

Reciprocamente, dada uma forma quadrática $q : V \to \mathbb{K}$ e fixada uma base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V a Proposição 1.5.9 nos permite escrever q como um polinômio homogêneo de grau dois

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} c_{i,j} X_i X_j, \tag{1.5}$$

cujas indeterminadas são as coordenadas de um vetor $v \in V$ na base $\mathcal{B}$, isto é, se $v = \sum_{i=1}^n \alpha_i v_i$ então $q(v) = q(\sum_{i=1}^n \alpha_i v_i) = \sum_{1 \leq i \leq j \leq n} c_{i,j} \alpha_i \alpha_j$. Agora notamos que a Equação (1.5) pode ser representada matricialmente, ou seja, denotando $\mathbf{x}^t = (X_1 \ \cdots \ X_n)$ temos

$$Q(X_1, \ldots, X_n) = \mathbf{x}^t A \mathbf{x},$$

onde $A = (a_{i,j})$ é a matriz simétrica dada por $a_{i,j} = a_{j,i} = c_{i,j}/2$, se $i \neq j$ e $a_{i,i} = c_{i,i}$.

Por fim a Proposição 1.5.2 nos garante que fixada uma base $\mathcal{B}$ de V, uma forma bilinear simétrica f em V é unicamente determinada por sua representação matricial $[f]_{\mathcal{B}}$, logo a forma bilinear simétrica associada à forma quadrática q é f, tal que $[f]_{\mathcal{B}} = A$. ■

Teorema 1.5.11. *Sejam $\mathbb{K}$ um corpo de característica diferente de 2, V um $\mathbb{K}$-espaço vetorial de dimensão finita e f uma forma bilinear simétrica em V. Então existe uma base ordenada para V tal que f é representada por uma matriz diagonal.*

Demonstração. Queremos uma base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V tal que, se $i \neq j$ então

$$f(v_i, v_j) = 0.$$

Se $f = 0$ ou $n = 1$ é evidente. Suponha $f \neq 0$ e $n > 1$. Se $f(u,u) = 0$ para todo $u \in V$, então $q(u) = 0$ e pela fórmula de polarização

$$f(u,v) = \tfrac{1}{4} q(u+v) - \tfrac{1}{4} q(u-v)$$

segue que $f = 0$.

Então existe $w \in V$ tal que $q(w) = f(w,w) \neq 0$. Tome $W = \langle w \rangle$ e $W^\perp$ o subespaço $W^\perp = \{v \in V : f(w,v) = 0\}$. Afirmamos que $V = W \oplus W^\perp$. De fato,

(i) *São independentes*: Tome $\alpha w \in W$, se $\alpha w \in W^{\perp}$ então

$$f(\alpha w, \alpha w) = \alpha^2 f(w, w) = 0,$$

mas $f(w, w) \neq 0$, logo $\alpha = 0$.

(ii) *Todo $v \in V$ é uma soma de vetores em W e $W^{\perp}$*: Considere

$$u = v - \frac{f(v, w)}{f(w, w)} w.$$

Assim temos que

$$f(w, u) = f(w, v) - \frac{f(v, w)}{f(w, w)} f(w, w) = f(w, v) - f(v, w),$$

e como f é simétrica segue que $f(w, u) = 0$. Logo $u \in W^{\perp}$ e

$$v = u + \frac{f(v, w)}{f(w, w)} w$$

mostra que $V = W + W^{\perp}$.

Note que $f|_{W^{\perp}}$ é forma bilinear simétrica em $W^{\perp}$. Como $\dim W^{\perp} = (n-1)$ podemos assumir por indução que $W^{\perp}$ tem uma base $\{v_2, \ldots, v_n\}$ tal que

$$f(v_i, v_j) = 0$$

para todo $2 \leq i \neq j \leq n$. Escolhendo $v_1 = w$ temos uma base $\{v_1, v_2, \ldots, v_n\}$ de V tal que

$$f(v_i, v_j) = 0$$

para todo $1 \leq i \neq j \leq n$. ■

Agora possuímos todos os resultados para classificar as cônicas em $\mathbb{P}^2_{\mathbb{R}}$, mas para isso precisamos definir os critérios de classificação:

Definição 1.5.12. Duas curvas $C = \mathcal{V}(F), C' = \mathcal{V}(G) \subset \mathbb{P}^2_{\mathbb{K}}$ são ditas *projetivamente equivalentes* se existir $M \in \mathrm{GL}_3(\mathbb{K})$ tal que $G(X, Y, Z) = F(U, V, W)$, onde

$$\begin{pmatrix} U \\ V \\ W \end{pmatrix} = M \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Corolário 1.5.13. *A menos de equivalência qualquer cônica de $\mathbb{P}^2_{\mathbb{R}}$ é uma das seguintes:*

(a) *Cônica não degenerada:* $\mathcal{V}(X^2 + Y^2 - Z^2)$;

(b) *Conjunto vazio:* $\mathcal{V}(X^2 + Y^2 + Z^2)$;

(c) *Par de retas:* $\mathcal{V}(X^2 - Y^2)$;

(d) *Ponto único:* $(0{:}0{:}1) = \mathcal{V}(X^2 + Y^2)$;

(e) *Reta dupla:* $\mathcal{V}(X^2)$.

Demonstração. Seja $C = \mathcal{V}(Q) \in \mathbb{P}^2_{\mathbb{R}}$ uma cônica projetiva. Pela Proposição 1.5.8 o polinômio homogêneo de grau dois $Q(X, Y, Z) \in \mathbb{R}[X, Y, Z]$ está associado à uma forma quadrática q em $\mathbb{R}^3$. Deste modo podemos escolher uma base $\mathcal{B} = \{v_1, v_2, v_3\}$ de $\mathbb{R}^3$ como no teorema anterior, isto é, existem escalares $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathbb{K}$ tais que

$$q(\alpha v_1 + \beta v_2 + \gamma v_3) = \varepsilon_1\alpha^2 + \varepsilon_2\beta^2 + \varepsilon_3\gamma^2,$$

para todo $v = \alpha v_1 + \beta v_2 + \gamma v_3 \in \mathbb{R}^3$.

Pela Proposição 1.5.9 associamos q, em relação a essa nova base, ao polinômio homogêneo $Q'(X, Y, Z) = \varepsilon_1 X^2 + \varepsilon_2 Y^2 + \varepsilon_3 Z^2 \in \mathbb{R}[X, Y, Z]$. Perceba que $C = \mathcal{V}(Q)$ é levada em $C' = \mathcal{V}(Q')$ pela matriz mudança de base, que caracteriza uma transformação projetiva.

Agora todo número real ε é 0 ou $\pm$ um quadrado, logo basta considerar Q' onde $\varepsilon_i = 0$ ou ± 1. De fato, caso algum dos ε_i for diferente de 0, 1, ou -1, a relação $\varepsilon_i = \pm\lambda_i^2$ nos dá $Q'(X, Y, Z) = \pm(\lambda_1 X)^2 \pm (\lambda_2 Y)^2 \pm (\lambda_3 Z)^2$ e então por uma simples mudança de coordenadas voltamos aos casos anteriores.

Também como estamos interessados somente em $Q' = 0$ pode-se multiplicar Q' por -1 se necessário. Observando cada caso temos a classificação desejada. ■

Para um corpo $\mathbb{K}$ de característica diferente de 2 é possível obter uma expressão simplificada para uma cônica projetiva não degenerada $C \in \mathbb{P}^2_{\mathbb{K}}$, como mostra a proposição abaixo. Neste contexto uma cônica é dita não degenerada se a sua forma quadrática correspondente é não degenerada. Por sua vez uma forma quadrática é não degenerada quando a sua forma bilinear simétrica é não degenerada. Recordamos abaixo a definição de forma bilinear não degenerada.

Definição 1.5.14. Sejam V um espaço vetorial de dimensão n e f uma forma bilinear em V. Dizemos que f é *não degenerada* se satisfaz as condições equivalentes abaixo.

(i) $\text{rank}[f]_{\mathcal{B}} = n$, para toda base ordenada $\mathcal{B}$ de V.

(ii) Para cada vetor não nulo $u \in V$, existe um vetor $v \in V$ tal que $f(u, v) \neq 0$.

(iii) Para cada vetor não nulo $v \in V$, existe um vetor $u \in V$ tal que $f(u, v) \neq 0$.

Observação 1.5.15. Perceba esta definição é condizente com a definição de cônicas não degeneradas reais (veja a Definição 1.4.1), pois o posto da matriz da forma bilinear associada é completo se, e somente se, esta matriz é invertível.

Proposição 1.5.16. *Sejam $\mathbb{K}$ um corpo de característica diferente de 2, V um espaço vetorial de dimensão 3 sobre $\mathbb{K}$ e $q : V \to \mathbb{K}$ uma forma quadrática não degenerada em V. Se $0 \neq e_1 \in V$ satisfaz $q(e_1) = 0$ então existe uma base $\mathcal{B} = \{e_1, e_2, e_3\}$ de V tal que $q(xe_1 + ye_2 + ze_3) = xz + ay^2$. Em particular, toda cônica não degenerada e não vazia $C \subset \mathbb{P}^2_{\mathbb{K}}$ é projetivamente equivalente à cônica $\mathcal{V}(XZ - Y^2)$.*

Demonstração. Seja f a forma bilinear simétrica associada a q. Como f é não degenerada, existe $v \in V$ tal que $f(e_1, v) \neq 0$ e então tomando $u := \frac{v}{2f(e_1,v)}$ temos $f(e_1, u) = \frac{1}{2}$.

Para obter e_3 precisamos garantir que $f(e_3, e_3) = 0$. Para isso perturbamos u na direção de e_1, obtendo

$$q(u + \lambda e_1) = f(u + \lambda e_1, u + \lambda e_1) = q(u) + 2\lambda f(e_1, u) + \lambda^2 q(e_1) = q(u) + \lambda.$$

Assim, escolhendo $\lambda = -q(u)$ definimos $e_3 = u - q(u)e_1$.

A partir de e_1 e e_3 escolhemos w de forma a completar uma base $\mathcal{C} = \{e_1, e_3, w\}$, onde

$$[f]_{\mathcal{C}} = \begin{pmatrix} 0 & * & \frac{1}{2} \\ * & * & * \\ \frac{1}{2} & * & 0 \end{pmatrix}.$$

Precisamos encontrar e_2 tal que $f(e_1, e_2) = f(e_3, e_2) = 0$, para isso perturbamos w nas direções de e_1 e e_3:

$$e_2 = w + \alpha e_1 + \beta e_3.$$

Aplicando as condições temos,

$$\begin{aligned} f(e_1, w + \alpha e_1 + \beta e_3) &= f(e_1, w) + \alpha f(e_1, e_1) + \beta f(e_1, e_3) \\ 0 &= f(e_1, w) + \frac{\beta}{2} \\ \Rightarrow\ \beta &= -2f(e_1, w), \end{aligned}$$

e

$$\begin{aligned} f(e_3, w + \alpha e_1 + \beta e_3) &= f(e_3, w) + \alpha f(e_3, e_1) + \beta f(e_3, e_3) \\ 0 &= f(e_3, w) + \frac{\alpha}{2} \\ \Rightarrow\ \alpha &= -2f(e_3, w). \end{aligned}$$

De forma análoga obtêm-se $q(e_2) = q(w) + 2\alpha f(w, e_1) + 2\beta f(w, e_3) + \alpha\beta$. Denotamos $q(e_2) = a$.

Tomando α e β como acima e $e_2 = w+\alpha e_1+\beta e_3$ obtemos uma base $\mathcal{B} = \{e_1, e_2, e_3\}$ onde

$$[f]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & a & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix},$$

ou seja,

$$q(xe_1 + ye_2 + ze_3) = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & a & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = xz + ay^2.$$

Se $C = \mathcal{V}(Q) \subset \mathbb{P}^2_{\mathbb{K}}$ é uma cônica projetiva não vazia, então existe $(a:b:c) \in \mathbb{P}^2_{\mathbb{K}}$ tal que $Q(a, b, c) = 0$. Pela Proposição 1.5.8 obtemos uma forma quadrática q induzida por Q e fixado um sistema de coordenadas $\{v_1, v_2, v_3\}$ de $\mathbb{K}^3$, segue que o vetor $e_1 = av_1+bv_2+cv_3$ satisfaz $q(e_1) = 0$, portanto os raciocínios anteriores garantem a existência de uma base $\{e_1, e_2, e_3\}$ de $\mathbb{K}^3$ e de um escalar $a \in \mathbb{K}$ tais que

$$q(xe_1 + ye_2 + ze_3) = xz + ay^2.$$

Como no Corolário 1.5.13, pela Proposição 1.5.9 associamos q, em relação a base $\{e_1, e_2, e_3\}$, ao polinômio homogêneo $Q'(X, Y, Z) = XZ + aY^2$. Note que $C = \mathcal{V}(Q)$ e $C' = \mathcal{V}(Q')$ são projetivamente equivalentes, via a matriz invertível de mudança da base $\{v_1, v_2, v_3\}$ para $\{e_1, e_2, e_3\}$. Agora fazendo a mudança de coordenadas $Z \mapsto -aZ$ obtemos a expressão desejada. ■

Observação 1.5.17. Para um corpo $\mathbb{K}$ com característica igual a 2, tomamos $C = \mathcal{V}(XZ - Y^2)$ como a definição de uma cônica não degenerada.

1.6 Parametrização das cônicas

Nesta seção vamos discutir uma caracterização das cônicas não degeneradas em $\mathbb{P}^2_{\mathbb{K}}$ a partir da reta projetiva. Na realidade as aplicações que definem a parametrização discutida a seguir carregam a estrutura algébrica do plano projetivo, isto é, são *isomorfismos* entre as variedades $\mathbb{P}^1_{\mathbb{K}}$ e C.

Como discutido anteriormente, toda cônica não degenerada pode ser levada por uma transformação projetiva em $C = \mathcal{V}(XZ - Y^2)$, dessa forma considere a aplicação

$$\Phi : \mathbb{P}^1_{\mathbb{K}} \longrightarrow C \subset \mathbb{P}^2_{\mathbb{K}},$$

dada por

$$(U:V) \longmapsto (U^2:UV:V^2)$$

que parametriza C em $\mathbb{P}^1_{\mathbb{K}}$.

Vemos que todo elemento $(U^2:UV:V^2) \in \mathbb{P}^2_{\mathbb{K}}$ pertence a C, pois $U^2V^2 = (UV)^2$. Note que Φ possui uma inversa

$$\Psi : C \longrightarrow \mathbb{P}^1_{\mathbb{K}},$$

que é dada por partes

$$(X:Y:Z) \longmapsto \begin{cases} (X:Y), & se\ X \neq 0 \\ (Y:Z), & se\ Z \neq 0 \end{cases}.$$

Na terminologia de geometria algébrica, Ψ é uma *função racional*, e quando considerada com as duas expressões se torna um *morfismo* (veja [19], Capítulo III).

Perceba que Ψ está bem definida, pois se $X \neq 0$ e $Z \neq 0$ temos que, em C:

$$XZ = Y^2 \Rightarrow \frac{X}{Y} = \frac{Y}{Z} \Rightarrow (X:Y) = (Y:Z).$$

Além disso, caso $X = 0$ e $Z = 0$, Ψ não está definida, pois pela expressão de C temos $Y = 0$ e $(0:0:0) \notin \mathbb{P}^2_{\mathbb{K}}$.

Note que Φ e Ψ são de fato inversas:

- $\Phi \circ \Psi$: Suponha, sem perda de generalidade, que $X \neq 0$. Então

  $$(X:Y:Z) \overset{\Psi}{\longmapsto} (X:Y) \overset{\Phi}{\longmapsto} (X^2:XY:Y^2),$$

  e como $(X^2:XY:Y^2) \in C$, segue que $(X^2:XY:Y^2) = (X:Y:\frac{Y^2}{X}) = (X:Y:Z)$.

  Logo, $\Phi \circ \Psi = \mathrm{id}_C$.

- $\Psi \circ \Phi$: De maneira análoga supomos que $X \neq 0$. Desta forma,

  $$(X:Y) \overset{\Phi}{\longmapsto} (X^2:XY:Y^2) \overset{\Psi}{\longmapsto} (X^2:XY) = X(X:Y) = (X:Y),$$

  E também $\Psi \circ \Phi = \mathrm{id}_{\mathbb{P}^1_{\mathbb{K}}}$.

1.7 Multiplicidade de raízes

É bem conhecido que um polinômio $f(U) \in \mathbb{K}[U]$ de grau d possui no máximo d raízes em $\mathbb{K}$ e, se $\mathbb{K}$ é algebricamente fechado, então possui d raízes em $\mathbb{K}$ (contando multiplicidades).

Nesta seção vamos mostrar um resultado semelhante para o número de raízes de um polinômio homogêneo $F(U,V) \in \mathbb{K}[U,V]$ na reta projetiva.

Seja $F(U,V) \in \mathbb{K}[U,V]$ um polinômio homogêneo não nulo de grau d,

$$F(U,V) = a_dU^d + a_{d-1}U^{d-1}V + \ldots + a_0V^d.$$

Gostaríamos de poder relacionar as raízes de F na reta projetiva com as raízes em $\mathbb{K}$ de um polinômio f em uma variável. Para isso considere a seguinte aplicação de anéis

$$\vartheta_U : \mathbb{K}[U,V] \longrightarrow \mathbb{K}[U],$$

dada por

$$F(U,V) \longmapsto F(U,1).$$

Deste modo o polinômio associado a $F(U,V)$ é

$$\vartheta_U(F) = f(U) = a_d U^d + a_{d-1}U^{d-1} + \cdots + a_0.$$

Se $\alpha \in \mathbb{K}$ é uma raiz de f, temos

$$\begin{aligned} f(\alpha) = 0 &\Leftrightarrow (U-\alpha)|f(U) \\ &\Leftrightarrow f(U) = (U-\alpha)g(U) \\ &\Leftrightarrow F(U,V) = (U-\alpha V)G(U,V) \qquad (*) \\ &\Leftrightarrow (U-\alpha V)|F(U,V) \\ &\Leftrightarrow F(\alpha,1) = 0. \end{aligned}$$

A implicação ($\Rightarrow$) de ($*$) é obtida via a aplicação de homogeneização φ^1 da Definição 1.4.3, que neste contexto também denotamos por φ_U (onde o índice U indica o domínio $\mathbb{K}[U]$ da aplicação) e a recíproca ($\Leftarrow$) é dada pela a aplicação ϑ_U definida acima.

Concluímos que raízes de f em $\mathbb{K}$ correspondem a raízes de F em $\mathbb{P}^1_{\mathbb{K}}$, diferentes de $(1:0)$. Agora se F tem raízes no infinito, isto é, no ponto $(1:0)$ então

$$\begin{aligned} F(1,0) = 0 &\Leftrightarrow a_d = 0 \\ &\Leftrightarrow \deg f < d. \end{aligned}$$

Proposição 1.7.1. *A aplicação de homogeneização φ_U é multiplicativa e a aplicação ϑ_U é homomorfismo de anéis. Além disso φ_U e ϑ_U são inversas.*

Demonstração. φ_U *é multiplicativa*: Dados $f, g \in \mathbb{K}[U]$, com $\deg f = d$ e $\deg g = d'$,

temos

$$\begin{aligned}\varphi_U(f\cdot g)(U) &= V^{d+d'}(f\cdot g)\left(\frac{U}{V}\right)\\ &= V^{d+d'}f\left(\frac{U}{V}\right)\cdot g\left(\frac{U}{V}\right)\\ &= V^{d}f\left(\frac{U}{V}\right)\cdot V^{d'}g\left(\frac{U}{V}\right)\\ &= \varphi_U(f)(U)\cdot\varphi_U(g)(U).\end{aligned}$$

ϑ_U *é homomorfismo*: Sejam $F, G \in \mathbb{K}[U,V]$. Então

$$\begin{aligned}\vartheta_U(F+G)(U,V) &= (F+G)(U,1)\\ &= F(U,1)+G(U,1)\\ &= \vartheta_U(F)+\vartheta_U(G),\end{aligned}$$

e

$$\begin{aligned}\vartheta_U(F\cdot G)(U,V) &= (F\cdot G)(U,1)\\ &= F(U,1)\cdot G(U,1)\\ &= \vartheta_U(F)(U,V)\cdot\vartheta_U(G)(U,V).\end{aligned}$$

Facilmente verificamos que φ_U e ϑ_U são inversas. ■

Corolário 1.7.2. *As aplicações*

$$\varphi_V : \mathbb{K}[V] \longrightarrow \mathbb{K}[V,U]$$

e

$$\vartheta_V : \mathbb{K}[V,U] \longrightarrow \mathbb{K}[V],$$

dadas por

$$\varphi_V(f)(V,U) = U^d f\left(\frac{V}{U}\right) \quad e \quad \vartheta_V(F)(V) = F(V,1),$$

satisfazem as mesmas propriedades de φ_U *e* ϑ_U*.*

Demonstração. De fato, temos isomorfismos canônicos:

$$\alpha : \mathbb{K}[U,V] \longrightarrow \mathbb{K}[V,U],\ F(U,V) \longmapsto F(V,U),$$

e

$$\beta : \mathbb{K}[U] \longrightarrow \mathbb{K}[V],\ f(U) \longmapsto f(V).$$

Assim as aplicações φ_V e ϑ_V são dadas, respectivamente, por composições de φ_U

e ϑ_U com esses morfismos. Mais especificamente,

$$\varphi_V = \alpha\varphi_U\beta^{-1} \quad \text{e} \quad \vartheta_V = \beta\vartheta_U\alpha^{-1}.$$

■

Com base nos argumentos anteriores é formulada a seguinte definição:

Definição 1.7.3. Seja $F \in \mathbb{K}[U,V]$ um polinômio homogêneo não nulo de grau d e $f(U) = \vartheta_U(F)$. Definimos a *multiplicidade* de uma raiz $(\alpha:\beta)$ de F em $\mathbb{P}^1_{\mathbb{K}}$ como sendo:

(i) A multiplicidade da raiz $\alpha/\beta \in \mathbb{K}$ em f; ou

(ii) $d - \deg f$ se $(1:0)$ é a raiz.

O item (ii) é justificado pelo seguinte: seja $g(V) = \vartheta_V(F)$. Se $F(1,0) = 0$ então

$$g(V) = V^k h(V), \tag{1.6}$$

para algum polinômio $h \in \mathbb{K}[V]$, onde $h(0) \neq 0$ e $k \geq 1$ representa a multiplicidade da raiz $(1:0)$ em F.

Vamos mostrar que $k = d - \deg f$. Aplicando φ_V em (1.6) temos,

$$F(U,V) = V^k H(U,V), \tag{1.7}$$

com $k = d - \deg H$.

Perceba que ao homogeneizarmos h por φ_V não alteramos seu grau. De fato, se h é da forma $h(V) = a_0 + \cdots + a_r V^r$, com $a_0 \neq 0$ então

$$H(U,V) = \varphi_V(h) = a_0U^r + a_1VU^{r-1} + \cdots + a_rV_r,$$

ou seja, $\deg H = \deg h$.

Por fim, aplicando ϑ_U em (1.7) obtemos

$$f(U) = 1 \cdot \tilde{h}(U) = a_0U^r + a_1U^{r-1} + \cdots + a_r$$

e como $a_0 \neq 0$ temos $\deg \tilde{h} = \deg h = \deg H$, logo $\deg f = \deg H$ e vale que a multiplicidade de $(1:0)$ em F é $k = d - \deg f$.

Proposição 1.7.4. *Seja $F \in \mathbb{K}[U,V]$ um polinômio homogêneo não nulo de grau d. Então F tem no máximo d raízes em $\mathbb{P}^1_{\mathbb{K}}$. Em particular se $\mathbb{K}$ é algebricamente fechado F tem exatamente d raízes (contando as multiplicidades).*

Demonstração. Seja m_∞ a multiplicidade de $(1:0)$ em F e $f(U) = \vartheta_U(F)$ o polinômio associado a F. Então, por definição

$$\deg f = d - m_\infty.$$

Agora como f possui no máximo $\deg f$ raízes, temos que F possui no máximo $d - m_\infty + m_\infty = d$ raízes e se $\mathbb{K}$ for algebricamente fechado F tem exatamente d raízes, contando as multiplicidades. ■

Para a próxima seção será útil relembrar um resultado sobre polinômios que se anulam em um conjunto infinito (veja por exemplo [18]).

Lema 1.7.5. *Sejam $\mathbb{K}$ um corpo infinito e $\Lambda_i \subset \mathbb{K}$, $i = 1, \ldots, n$ conjuntos infinitos. Se $f \in \mathbb{K}[X_1, \ldots, X_n]$ satisfaz $f(\lambda_1, \ldots, \lambda_n) = 0$, para todo $(\lambda_1, \ldots, \lambda_n) \in \Lambda_1 \times \cdots \times \Lambda_n$, então f é o polinômio nulo.*

1.8 Teorema de Bézout

O Teorema de Bézout em sua forma geral - válido sobre um corpo algebricamente fechado $\mathbb{K}$ - afirma que dadas duas curvas $C = \mathcal{V}(F), C' = \mathcal{V}(G) \subset \mathbb{P}^2_\mathbb{K}$ com $\deg F = m$ e $\deg G = n$, o número de pontos da interseção $C \cap C'$ é igual a $m \cdot n$, contando multiplicidades (veja [25], Capítulo 5.3).

Neste trabalho provaremos dois casos particulares do teorema, em que consideraremos a interseção de uma reta e de uma cônica com uma curva qualquer. Cabe destacar que consideraremos um corpo arbitrário.

Teorema 1.8.1 (Bézout para retas e cônicas)**.** *Seja $L \subset \mathbb{P}^2_\mathbb{K}$ uma reta, $C \subset \mathbb{P}^2_\mathbb{K}$ uma cônica não degenerada e $D = \mathcal{V}(G) \subset \mathbb{P}^2_\mathbb{K}$ uma curva, onde G é um polinômio homogêneo de grau d. Se $L \not\subset D$ e $C \not\subset D$, então*

(i) $|L \cap D| \leq d$.

(ii) $|C \cap D| \leq 2d$.

Demonstração. (i) Uma reta em $\mathbb{P}^2_\mathbb{K}$ é da forma $L = \mathcal{V}(R)$ onde $R(X, Y, Z) = aX + bY + cZ$.

A reta L pode ser parametrizada por

$$\xi : \mathbb{P}^1_\mathbb{K} \longrightarrow L \subset \mathbb{P}^2_\mathbb{K},\ (U:V) \longmapsto (R_1(U,V):R_2(U,V):R_3(U,V)),$$

com R_i polinômios homogêneos lineares. Por exemplo, se $c \neq 0$ então $Z = \frac{-aX-bY}{c}$, assim podemos tomar $R_1 = U$, $R_2 = V$ e $R_3 = \frac{-aU-bV}{c}$.

Agora $|L \cap D|$ é dado pelas soluções $(U:V)$ em $\mathbb{P}^1_{\mathbb{K}}$ de

$$F(U,V) = G(R_1(U,V), R_2(U,V), R_3(U,V)) = 0.$$

Como G tem grau d e R tem grau 1, segue que $\deg F = d$. Assim, pela Proposição 1.7.4, $F(U,V)$ tem no máximo d raízes, ou seja, $|L \cap D| \leq d$.

(ii) Da Proposição 1.5.16 sabemos que toda cônica não degenerada é projetivamente equivalente a $\mathcal{V}(XZ - Y^2)$ e como vimos na Seção 1.6 esta curva é parametrizada por $(U^2:UV:V^2)$, portanto se $C = \mathcal{V}(Q(X,Y,Z))$, existe $M \in \mathrm{GL}_3(\mathbb{K})$ tal que

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = M \begin{pmatrix} U^2 \\ UV \\ V^2 \end{pmatrix},$$

ou seja, existem polinômios homogêneos $Q_i(U,V)$ de grau 2, tais que C é dada parametricamente por

$$\eta : \mathbb{P}^1_{\mathbb{K}} \longrightarrow C \subset \mathbb{P}^2_{\mathbb{K}},\ (U:V) \longmapsto (Q_1(U,V):Q_2(U,V):Q_3(U,V)).$$

Analogamente, $|C \cap D|$ é dado pelas soluções $(U:V)$ em $\mathbb{P}^1_{\mathbb{K}}$ de

$$H(U,V) = G(Q_1(U,V), Q_2(U,V), Q_3(U,V)) = 0.$$

Como G tem grau d e Q tem grau 2, então $\deg H = 2d$. Novamente pela Proposição 1.7.4, $H(U,V)$ tem no máximo $2d$ raízes, ou seja, $|C \cap D| \leq 2d$.

■

Corolário 1.8.2. *Se $P_1, \ldots, P_5 \in \mathbb{P}^2_{\mathbb{R}}$ são pontos distintos e ao menos 4 não colineares então existe uma única cônica passando por $P_1, \ldots, P_5$.*

Demonstração. A existência de uma cônica passando pelos pontos $P_1, \ldots, P_5$ é demonstrada no Corolário 1.11.3, que generaliza esse resultado para um corpo infinito $\mathbb{K}$, assim vamos nos restringir a prova da unicidade, utilizando para isso o Teorema de Bézout e a classificação das cônicas.

Suponha por contradição que C_1 e C_2 são cônicas projetivas distintas, tais que

$$C_1 \cap C_2 \supset \{P_1, \ldots, P_5\}.$$

Como C_1 é não vazia, consideramos dois casos:

(i) *C_1 é não degenerada*: Suponha que $C_1 = \mathcal{V}(Q_1)$ e $C_2 = \mathcal{V}(Q_2)$. Como Q_2 é um polinômio de grau 2 e supomos $|C_1 \cap C_2| \geq 5$, pelo Teorema 1.8.1 temos que $C_1 \subset C_2$.

Para mostrar a inclusão contrária usaremos o resultado da Proposição 1.5.16, que garante que C_1 é projetivamente equivalente a $\mathcal{V}(XZ - Y^2)$, cujos pontos são da forma $(U^2{:}UV{:}V^2)$. Vamos mostrar que $Q_2 = \lambda(XZ - Y^2)$, para algum $\lambda \in \mathbb{R}$.

Suponha que $Q_2(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 \in \mathbb{R}[X, Y, Z]$. Podemos rearranjar os monômios de Q_2 de uma forma conveniente, obtendo

$$Q_2(X, Y, Z) = -c(XZ - Y^2) + Y(bX + eZ) + aX^2 + (d + c)XZ + fZ^2.$$

Agora como $C_1 \subset C_2$, temos que $Q_2(U^2, UV, V^2) = 0$, para todo $(U{:}V) \in \mathbb{P}^1_{\mathbb{R}}$, logo

$$\begin{aligned} &- c(U^2V^2 - (UV)^2) + UV(bU^2 + eV^2) + aU^4 + (d + c)U^2V^2 + fV^4 = 0 \\ \implies &bU^3V + eUV^3 + aU^4 + (d + c)U^2V^2 + fV^4 = 0. \end{aligned} \tag{1.8}$$

Por fim notamos que a Equação (1.8) pode ser vista como um polinômio nas variáveis U e V, que se anula em todo $(U{:}V) \in \mathbb{P}^1_{\mathbb{R}}$, que é um conjunto infinito. Deste modo pelo Lema 1.7.5 o polinômio em questão é o nulo, portanto

$$a = b = e = f = 0 \ \text{ e } \ d = -c$$

e pela expressão de Q_2 temos $Q_2 = \lambda(XZ - Y^2)$, onde $\lambda = d$, assim concluímos que $C_1 = C_2$, uma contradição.

(ii) C_1 *é degenerada*: Pela classificação feita no Corolário 1.5.13 a cônica C_1 é um par de retas ou uma reta dupla, logo o Teorema 1.8.1 nos garante que C_2 também é degenerada (caso contrário teríamos $C_2 \subset C_1$ e então C_2 estaria contida em uma cônica degenerada).

Assim podemos escrever C_1 e C_2 como

$$C_1 = L_0 \cup L_1 \text{ e } C_2 = L_0 \cup L_2,$$

onde $L_0, L_1, L_2 \subset \mathbb{P}^2_{\mathbb{R}}$ são retas e $L_1 \neq L_2$. Novamente pelo Teorema 1.8.1 temos $|L_1 \cap L_2| \leq 1$, logo segue que ao menos 4 pontos distintos de $P_1, \ldots, P_5$ estão em L_0, contradição.

■

1.9 Espaço das cônicas

Definição 1.9.1. Seja $S_2 = \{F \in \mathbb{K}[X, Y, Z] : F \text{ homogêneo de grau } 2\} \cup \{0\}$. Dado $P_0 = (X_0{:}Y_0{:}Z_0) \in \mathbb{P}^2_{\mathbb{K}}$ define-se o conjunto de polinômios $Q \in S_2$ tais que $P_0 \in \mathcal{V}(Q)$, ou

seja

$$S_2(P_0) = \{Q \in S_2 : Q(P_0) = 0\}.$$

Note que, se $Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$ e $Q \in S_2(P_0)$, então

$$aX_0^2 + bX_0Y_0 + cY_0^2 + dX_0Z_0 + eY_0Z_0 + fZ_0^2 = 0.$$

Logo consideramos a transformação linear

$$\sigma : S_2 \longrightarrow \mathbb{K},$$

dada por

$$Q \longmapsto aX_0^2 + \ldots + fZ_0^2.$$

Pelo teorema do núcleo e imagem temos,

$$\begin{array}{rrcl} & \dim \mathrm{Ker}(\sigma) + \dim \mathrm{Im}(\sigma) & = & \dim S_2 \\ \Rightarrow & \dim \mathrm{Ker}(\sigma) & = & 6 - \dim \mathrm{Im}(\sigma) \\ \Rightarrow & \dim \mathrm{Ker}(\sigma) & = & 5. \end{array}$$

Como $\mathrm{Ker}(\sigma) = S_2(P_0)$, temos que $S_2(P_0) \cong \mathbb{K}^5$ é um hiperplano de dimensão 5.

Analogamente para n pontos $P_1, ..., P_n \in \mathbb{P}^2_{\mathbb{K}}$ definimos:

Definição 1.9.2. $S_2(P_1, \ldots, P_n) = \{Q \in S_2 : Q(P_i) = 0, \text{ para } i = 1, \ldots, n\}$.

Teorema 1.9.3. $\dim S_2(P_1, \ldots, P_n) \geq 6 - n$.

Demonstração. Para $i = 1, \ldots, n$ denote $P_i = (X_i : Y_i : Z_i) \in \mathbb{P}^2_{\mathbb{K}}$. Considere a aplicação,

$$\psi : \mathbb{K}^6 \longrightarrow \mathbb{K}^n,$$

dada por

$$\begin{pmatrix} a \\ \vdots \\ f \end{pmatrix} \longmapsto \begin{pmatrix} X_1^2 & X_1Y_1 & \cdots & Z_1^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_n^2 & X_nY_n & \cdots & Z_n^2 \end{pmatrix} \begin{pmatrix} a \\ \vdots \\ f \end{pmatrix}.$$

É fácil ver que ψ é uma transformação linear, agora pelo teorema do núcleo e imagem temos,

$$\dim \mathrm{Ker}(\psi) + \dim \mathrm{Im}(\psi) = \dim \mathbb{K}^6.$$

Note que $\dim \mathrm{Ker}(\psi) = \dim S_2(P_1, \ldots, P_n)$ e como $\dim \mathrm{Im}(\psi) \leq n$, segue que

$$\dim S_2(P_1, \ldots, P_n) = 6 - \dim \mathrm{Im}(\psi) \geq 6 - n.$$

■

Corolário 1.9.4. *Seja $\mathbb{K}$ um corpo infinito. Se $n \leq 5$ e ao menos 4 dos pontos $P_1, \ldots, P_n \in \mathbb{P}^2_{\mathbb{K}}$ não são colineares então,*

$$\dim S_2(P_1, \ldots, P_n) = 6 - n.$$

Demonstração. No caso de $\mathbb{K} = \mathbb{R}$ se $n = 5$ o Corolário 1.8.2 garante que existe uma única cônica passando por $P_1, \ldots, P_n$, isto é, existe um único polinômio homogêneo de grau 2 (a menos de múltiplos escalares) que se anula em $P_1, \ldots, P_n$. Veremos adiante, no Corolário 1.11.3, que esse resultado ainda se mantém verdadeiro para um corpo infinito $\mathbb{K}$, assim

$$\dim S_2(P_1, \ldots, P_5) = 1. \tag{1.9}$$

Se $n \leq 4$ podemos adicionar $P_{n+1}, \ldots, P_5$ pontos respeitando a condição de não colinearidade. Isto implica o aumento de $5 - n$ linhas na matriz

$$A = \begin{pmatrix} X_1^2 & X_1Y_1 & \cdots & Z_1^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_n^2 & X_nY_n & \cdots & Z_n^2 \end{pmatrix},$$

ou seja, o posto de A aumenta no máximo $5 - n$. Sejam ψ_n e ψ_5 as respectivas transformações com n e 5 pontos, pelo argumento anterior temos que,

$$\begin{array}{rcl} \dim \mathrm{Im}(\psi_5) - \dim \mathrm{Im}(\psi_n) & \leq & 5 - n \\ \Rightarrow \qquad \dim \mathrm{Im}(\psi_5) & \leq & \dim \mathrm{Im}(\psi_n) + (5 - n). \end{array}$$

Logo, por (1.9) e pelo Teorema do núcleo e imagem, segue que

$$\begin{array}{rcl} 1 = \dim S_2(P_1, \ldots, P_5) & = & 6 - \dim \mathrm{Im}(\psi_5) \\ & \geq & 6 - \dim \mathrm{Im}(\psi_n) - (5 - n) \\ & = & \dim S_2(P_1, \ldots, P_n) - (5 - n) \\ \Rightarrow \qquad \dim S_2(P_1, \ldots, P_n) & \leq & 6 - n. \end{array}$$

Por fim o teorema anterior garante que

$$\dim S_2(P_1, \ldots, P_n) = 6 - n.$$

■

Até agora construímos resultados apenas acerca de cônicas e retas, logo nestas próximas seções abordamos a estrutura (muito similar) das curvas de grau d, em especial sobre as cúbicas.

1.10 Sistemas lineares

Definição 1.10.1. Seja $S_d = \{F \in \mathbb{K}[X,Y,Z] : F \text{ homogêneo de grau } d\} \cup \{0\}$.

Todo $F \in S_d$ pode ser escrito de modo único como uma soma de monômios de mesmo grau:

$$F(X,Y,Z) = \sum_{i+j+k=d} a_{i,j,k} X^i Y^j Z^k,$$

onde $a_{i,j,k} \in \mathbb{K}$ e i,j,k são inteiros positivos. Também podemos considerar S_d como um $\mathbb{K}$-espaço vetorial, cuja base canônica é

$$\begin{array}{ccccc} & & Z^d & & \\ & XZ^{d-1} & & YZ^{d-1} & \\ \iddots & & \vdots & & \ddots \\ X^{d-1}Z & X^{d-2}YZ & \dots & Y^{d-1}Z & \\ X^d & X^{d-1}Y & X^{d-2}Y^2 & \dots & Y^d \end{array}$$

Podemos obter a dimensão de S_d analisando o número de elementos de cada linha do arranjo acima, onde é fixada a potência da variável Z em cada monômio. Deste modo temos

$$\dim S_d = 1 + 2 + \cdots + d + (d+1) = \binom{d+2}{2}.$$

Analogamente às curvas de grau 2, dados $P_1, \dots, P_n \in \mathbb{P}^2_{\mathbb{K}}$ definimos

$$S_d(P_1, \dots, P_n) = \{F \in S_d : F(P_i) = 0 \text{ para } i = 1, \dots, n\} \subset S_d.$$

Além disso, cada ponto P_i impõe uma condição linear em F, logo $S_d(P_1, \dots, P_n)$ é um espaço vetorial com dimensão maior ou igual $\binom{d+2}{2} - n$.

1.11 Divisibilidade de curvas

O resultado a seguir traduz um fato geométrico sobre curvas, para a álgebra de polinômios associada, isto é, veremos que, nos casos em que estamos interessados, se $\mathcal{V}(G) \subset \mathcal{V}(F)$ então $F = G \cdot H$ para algum polinômio H.

Lema 1.11.1. *Sejam $\mathbb{K}$ um corpo infinito e $F \in S_d$.*

(1) *Seja $L = \mathcal{V}(H) \subset \mathbb{P}^2_{\mathbb{K}}$ uma reta, se $F(X,Y,Z) = 0$ para todo $(X:Y:Z) \in L$, então F é divisível em $\mathbb{K}[X,Y,Z]$ por H, isto é, $F = H \cdot F'$, onde $F' \in S_{d-1}$.*

(2) *Seja $C = \mathcal{V}(Q) \subset \mathbb{P}^2_{\mathbb{K}}$ uma cônica não degenerada, se $F(X,Y,Z) = 0$ para todo $(X:Y:Z) \in C$, então F é divisível em $\mathbb{K}[X,Y,Z]$ por Q, isto é, $F = Q \cdot F''$, onde*

$F'' \in S_{d-2}$.

Demonstração. (1) Seja $H(X,Y,Z) = aX + bY + cZ$ a equação definindo L. Ao menos um dos coeficientes de H é não nulo, logo sem perda de generalidade suponha $a \neq 0$. Faremos uma mudança de coordenadas tal que $L = \mathcal{V}(H')$, onde $H'(X',Y',Z') = X'$. De fato, a transformação em questão é dada por:

$$\begin{pmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} \Rightarrow \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} aX + bY + cZ \\ Y \\ Z \end{pmatrix}.$$

Logo $aX = X' - bY' - cZ'$ e então com estas coordenadas $H'(X',Y',Z') = X' - bY' - cZ' + bY' + cZ' = X'$. Para facilitar a notação retiramos as linhas das variáveis, ou seja, $L = \mathcal{V}(H'(X,Y,Z))$ onde $H'(X,Y,Z) = X$.

Escreva $F(X,Y,Z) = \sum_{i+j+k=d} a_{i,j,k} X^i Y^j Z^k$. Isolando X^i temos,

$$\begin{aligned} F(X,Y,Z) &= \sum_{i=0}^{d} X^i \left(\sum_{j+k=d-i} a_{i,j,k} Y^j Z^k \right) \\ &= \sum_{j+k=d} a_{0,j,k} Y^j Z^k + \sum_{i=1}^{d} X^i \left(\sum_{j+k=d-i} a_{i,j,k} Y^j Z^k \right) \\ &= G(Y,Z) + X \cdot F'(X,Y,Z). \end{aligned} \tag{1.10}$$

Agora como $F(X,Y,Z) = 0$ para todo $(X:Y:Z) \in L = \mathcal{V}(X)$, temos que $F(0,Y,Z) = 0$ para todo $(0:Y:Z) \in \mathbb{P}^2_{\mathbb{K}}$. Desta forma concluímos pela Equação (1.10) que $G(Y,Z) = 0$ para todo $(Y:Z) \in \mathbb{P}^1_{\mathbb{K}}$.

Como $\mathbb{K}$ é infinito $\mathbb{P}^1_{\mathbb{K}}$ também é, logo pelo Lema 1.7.5 segue que $G(Y,Z)$ é o polinômio nulo.

Assim, segue que $F(X,Y,Z) = X \cdot F'(X,Y,Z)$, com $F' \in S_{d-1}$.

(2) Sabemos que C é projetivamente equivalente a $\mathcal{V}(XZ - Y^2)$, logo por uma mudança de coordenadas podemos assumir $Q(X,Y,Z) = XZ - Y^2$. Isolando Y^j em $F(X,Y,Z)$ temos,

$$\begin{aligned} F(X,Y,Z) &= \sum_{i+j+k=d} a_{i,j,k} X^i Y^j Z^k \\ &= \sum_{j=0}^{d} Y^j \left(\sum_{i+k=d-j} a_{i,j,k} X^i Z^k \right) \\ &= F_0 + Y \cdot F_1 + Y^2 \cdot F_2 + Y^3 \cdot F_3 + \cdots + Y^d \cdot F_d, \end{aligned} \tag{1.11}$$

onde $F_j = F_j(X, Z) \in S_{d-j}$, para $j = 0, \ldots, d$.

Por (1.11) escrevemos F como

$$F(X, Y, Z) = F_0 + Y \cdot G(X, Y, Z). \tag{1.12}$$

Afirmação: Todo polinômio homogêneo $F \in S_d$, com $d \geq 2$, possui uma expressão da forma

$$F(X, Y, Z) = R(X, Y, Z) \cdot Q + Y \cdot S(X, Z) + T(X, Z).$$

com $R \in S_{d-2}$, $S \in S_{d-1}$ e $T \in S_d$.

Vamos proceder por indução no grau de F. Para $\deg F = 2$ temos uma expressão da forma

$$F(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2,$$

e para obter

$$F(X, Y, Z) = \lambda \cdot Q + Y \cdot S(X, Z) + T(X, Z)$$

basta tomar

$$\lambda = -c,\ S(X, Z) = bX + eZ \ \text{ e } \ T(X, Z) = aX^2 + (d + c)XZ + fZ^2.$$

Suponha válido para $\deg F = d - 1$. Dado um polinômio F homogêneo de grau d, pela Equação (1.12) temos

$$F(X, Y, Z) = F_0 + Y \cdot G(X, Y, Z),$$

onde $\deg G = d - 1$, e então existem $\widetilde{R} \in S_{d-3}$, $\widetilde{S} \in S_{d-2}$ e $\widetilde{T} \in S_{d-1}$ tais que

$$\begin{aligned}
F(X, Y, Z) &= F_0 + Y(\widetilde{R}(X, Y, Z) \cdot Q + Y \cdot \widetilde{S}(X, Z) + \widetilde{T}(X, Z)) \\
&= F_0 + Y \cdot \widetilde{R}(X, Y, Z) \cdot Q + Y^2 \cdot \widetilde{S}(X, Z) + Y \cdot \widetilde{T}(X, Z) \\
&= F_0 + Y \cdot \widetilde{R}(X, Y, Z) \cdot Q + (XZ - Q) \cdot \widetilde{S}(X, Z) + Y \cdot \widetilde{T}(X, Z) \\
&= (Y \cdot \widetilde{R}(X, Y, Z) - \widetilde{S}(X, Z)) \cdot Q + Y \cdot \widetilde{T}(X, Z) + \\
&\quad + (F_0 + XZ \cdot \widetilde{S}(X, Z)) \\
&= R(X, Y, Z) \cdot Q + Y \cdot S(X, Z) + T(X, Z),
\end{aligned}$$

onde $R(X, Y, Z) = Y\widetilde{R}(X, Y, Z) - \widetilde{S}(X, Z)$, $S(X, Z) = \widetilde{T}(X, Z)$ e $T(X, Z) = F_0 + XZ \cdot \widetilde{S}(X, Z)$, o que conclui a indução.

Da Seção 1.6 sabemos que os pontos de C são da forma $(U^2 : UV : V^2) \in \mathbb{P}^2_{\mathbb{K}}$ para

razões $(U:V) \in \mathbb{P}^1_{\mathbb{K}}$. Desta forma segue que

$$\begin{aligned} F(U^2,UV,V^2) = 0 \Leftrightarrow\ & R(U^2,UV,V^2)\cdot Q(U^2,UV,V^2) + UV\cdot S(U^2,V^2) + \\ & + T(U^2,V^2) = 0 \\ \Leftrightarrow\ & R(U^2,UV,V^2)\cdot 0 + UV\cdot S(U^2,V^2) + T(U^2,V^2) = 0 \\ \Leftrightarrow\ & UV\cdot S(U^2,V^2) + T(U^2,V^2) = 0. \end{aligned} \tag{1.13}$$

Como $S \in S_{d-1}$ e $T \in S_d$ temos expressões da forma,

$$Y\cdot S(X,Z) = \sum_{i+k=d-1} s_{i,k} Y X^i Z^k \ \text{ e } \ T(X,Z) = \sum_{i+k=d} t_{i,k} X^i Z^k.$$

Portanto na Equação (1.13) temos

$$\begin{aligned} & UV \sum_{i+k=d-1} s_{i,k}(U^2)^i(V^2)^k + \sum_{i+k=d} t_{i,k}(U^2)^i(V^2)^k = 0 \\ \Leftrightarrow\ & \sum_{i+k=d-1} s_{i,k} U^{2i+1}V^{2k+1} + \sum_{i+k=d} t_{i,k} U^{2i}V^{2k} = 0. \end{aligned}$$

Perceba que o lado esquerdo da equação acima representa um polinômio homogêneo de grau $2d$ nas variáveis U e V, onde cada monômio é distinto pela paridade do grau das variáveis. Também notamos que ao avaliar este polinômio em qualquer razão $(U:V) \in \mathbb{P}^1_{\mathbb{K}}$, que é um conjunto infinito (pois $\mathbb{K}$ o é), obtemos $0 \in \mathbb{K}$. Assim, pelo Lema 1.7.5 o polinômio em questão deve ser o nulo, isto é, $s_{i,k} = t_{i,k} = 0$, para cada i,k correspondente.

Finalmente, concluímos que $F(X,Y,Z) = Q(X,Y,Z)\cdot F''(X,Y,Z)$, onde $F'' = R \in S_{d-2}$.

■

Corolário 1.11.2. *Seja $L = \mathcal{V}(H) \subset \mathbb{P}^2_{\mathbb{K}}$ uma reta e $C = \mathcal{V}(Q) \subset \mathbb{P}^2_{\mathbb{K}}$ uma cônica não degenerada. Dados $P_1,\ldots,P_n \in \mathbb{P}^2_{\mathbb{K}}$ considere $S_d(P_1,\ldots,P_n)$, para algum d fixo.*

(i) *Se $P_1,\ldots,P_a \in L,\ P_{a+1},\ldots,P_n \notin L$ e $a > d$, então*

$$S_d(P_1,\ldots,P_n) = H\cdot S_{d-1}(P_{a+1},\ldots,P_n).$$

(ii) *Se $P_1,\ldots,P_a \in C,\ P_{a+1},\ldots,P_n \notin C$ e $a > 2d$, então*

$$S_d(P_1,\ldots,P_n) = Q\cdot S_{d-2}(P_{a+1},\ldots,P_n).$$

Demonstração. (i) Seja $F \in S_d(P_1,\ldots,P_n)$ definindo a curva $D = \mathcal{V}(F)$. Se $D \cap L =$

$\{P_1, \ldots, P_a\}$ e $a > d$, então pela negação do Teorema 1.8.1 devemos ter $L \subset D$, logo

$$F(X, Y, Z) = 0 \text{ para todo } (X:Y:Z) \in L.$$

Agora pelo Lema 1.11.1 temos,

$$F = H \cdot F', \text{ com } F' \in S_{d-1} \text{ e } D' = \mathcal{V}(F').$$

Por hipótese $P_{a+1}, \ldots, P_n \notin L$, então devemos ter $P_{a+1}, \ldots, P_n \in D'$, assim $F' \in S_{d-1}(P_{a+1}, \ldots, P_n)$.

(ii) Analogamente seja $F \in S_d(P_1, \ldots, P_n)$ o polinômio definindo a curva $D = \mathcal{V}(F)$. Se $D \cap C = \{P_1, \ldots, P_a\}$ e $a > 2d$, então pela negação do Teorema 1.8.1 devemos ter $C \subset D$, logo $F(X, Y, Z) = 0$ para todo $(X:Y:Z) \in C$ e pelo Lema 1.11.1, $F = Q \cdot F''$, com $F'' \in S_{d-2}$ e $D'' = \mathcal{V}(F'')$.

Por hipótese $P_{a+1}, \ldots, P_n \notin C$, então $P_{a+1}, \ldots, P_n \in D''$, o que implica $F'' \in S_{d-2}(P_{a+1}, \ldots, P_n)$.

■

Corolário 1.11.3. *Seja $\mathbb{K}$ um corpo infinito. Se $P_1, \ldots, P_5 \in \mathbb{P}^2_{\mathbb{K}}$ são pontos distintos e ao menos 4 não colineares então existe uma única cônica passando por $P_1, \ldots, P_5$.*

Demonstração. Considere os dois possíveis casos:

(i) *Existem 3 pontos colineares entre os $P_i's$.* Seja $C = \mathcal{V}(F) \subset \mathbb{P}^2_{\mathbb{K}}$ uma cônica passando pelos cinco pontos. Neste caso a cônica C é unicamente determinada, pois se P_1, P_2 e P_3 são colineares o teorema de Bézout garante que a reta $P_1P_2P_3 = \mathcal{V}(H)$ está contida em C, deste modo $F(P) = 0$, para todo $P \in \mathcal{V}(H)$ e pelo Lema 1.11.1 temos que $F = H \cdot G$ para algum polinômio $G \in \mathbb{K}[X, Y, Z]$. Logo devemos ter $P_4, P_5 \in \mathcal{V}(G)$ e assim $C = P_1P_2P_3 \cup P_4P_5$.

(ii) *Não há pontos três a três colineares.* Iremos provar que toda cônica passando pelos $P_i's$ é projetivamente equivalente à

$$C = \mathcal{V}(\gamma(\beta - \alpha)XY + \beta(\alpha - \gamma)XZ + \alpha(\gamma - \beta)YZ),$$

onde $(\alpha:\beta:\gamma) \in \mathbb{P}^2_{\mathbb{K}}$ é um ponto fixo a ser determinado. Procedemos como no Exemplo 7.16 de [7].

Seja $C = \mathcal{V}(Q) \subset \mathbb{P}^2_{\mathbb{K}}$ uma cônica passando pelos $P_i's$, onde $Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$.

Pelo Teorema 1.3.3 existe uma transformação projetiva T tal que $T(P_1) = (1{:}0{:}0)$, $T(P_2) = (0{:}1{:}0), T(P_3) = (0{:}0{:}1)$ e $T(P_4) = (1{:}1{:}1)$. A imagem do quinto ponto é determinado pelos demais, e denotamos $T(P_5) = (\alpha{:}\beta{:}\gamma)$.

A transformação T discutida acima leva a cônica C em $C' = \mathcal{V}(Q')$, onde

$$Q'(X, Y, Z) = a'X^2 + b'XY + c'Y^2 + d'XZ + e'YZ + f'Z^2.$$

Como $(1{:}0{:}0)$, $(0{:}1{:}0)$, $(0{:}0{:}1)$, $(1{:}1{:}1) \in C'$ devemos ter $a' = c' = f' = 0$ e $b' + d' + e' = 0$, logo obtemos $Q'(X, Y, Z) = b'XY + d'XZ + e'YZ$. A última condição é que $b'\alpha\beta + d'\alpha\gamma + e'\beta\gamma = 0$, pois $(\alpha{:}\beta{:}\gamma) \in C'$.

Para determinar os coeficientes b', d' e e' resolvemos o seguinte sistema linear:

$$\begin{cases} b' + d' + e' &= 0 \\ b'\alpha\beta + d'\alpha\gamma + e'\beta\gamma &= 0 \end{cases}.$$

Observe que, como não há 3 pontos colineares, devemos ter $\alpha \neq 0$, $\beta \neq 0$ e $\beta \neq \gamma$ (é fácil verificar que se ocorresse uma dessas situações encontraríamos 3 pontos colineares). Então podemos dividir a segunda equação por $\alpha\beta$:

$$\begin{cases} b' + d' + e' &= 0 \\ b' + d'\dfrac{\gamma}{\beta} + e'\dfrac{\gamma}{\alpha} &= 0 \end{cases}.$$

Subtraindo a primeira equação da segunda temos,

$$\begin{aligned} & d'\left(\frac{\gamma}{\beta} - 1\right) + e'\left(\frac{\gamma}{\alpha} - 1\right) = 0 \\ \Leftrightarrow \quad & d'\frac{(\gamma - \beta)}{\beta} + e'\frac{(\gamma - \alpha)}{\alpha} = 0 \\ \Leftrightarrow \quad & d'\alpha(\gamma - \beta) + e'\beta(\gamma - \alpha) = 0 \\ \Leftrightarrow \quad & d' = -e'\frac{\beta(\gamma - \alpha)}{\alpha(\gamma - \beta)} \\ \Leftrightarrow \quad & d' = e'\frac{\beta(\alpha - \gamma)}{\alpha(\gamma - \beta)}. \end{aligned}$$

De forma análoga,

$$\begin{aligned} b' &= -d' - e' \\ &= e'\frac{\beta(\gamma - \alpha)}{\alpha(\gamma - \beta)} - e' \\ &= e'\left(\frac{\beta(\gamma - \alpha) - \alpha(\gamma - \beta)}{\alpha(\gamma - \beta)}\right) \\ &= e'\frac{\gamma(\beta - \alpha)}{\alpha(\gamma - \beta)}. \end{aligned}$$

Portando a equação de Q' é:

$$Q'(X,Y,Z) = e'\frac{\gamma(\beta-\alpha)}{\alpha(\gamma-\beta)}XY + e'\frac{\beta(\alpha-\gamma)}{\alpha(\gamma-\beta)}XZ + e'YZ.$$

O coeficiente e' é não nulo, caso contrário teríamos $Q'(X,Y,Z) = b'XY + d'XZ = X(b'Y + d'Z)$ e assim $C' = \mathcal{V}(X) \cup \mathcal{V}(b'Y + d'Z)$ seria a união de duas retas, o que implicaria ao menos 3 pontos colineares.

Desta forma podemos multiplicar Q por $\varepsilon = \frac{\alpha(\gamma-\beta)}{e'}$, obtendo finalmente

$$\varepsilon Q'(X,Y,Z) = \gamma(\beta-\alpha)XY + \beta(\alpha-\gamma)XZ + \alpha(\gamma-\beta)YZ.$$

Veja que $C' = \mathcal{V}(Q') = \mathcal{V}(\varepsilon Q')$ para todo $\varepsilon \neq 0 \in \mathbb{K}$, além disso tomar um representante $(\lambda\alpha : \lambda\beta : \lambda\gamma)$ para P_5 nos dá a mesma cônica C', logo a menos de equivalências existe uma única cônica pelos 5 pontos padrões, o que nos garante uma única cônica passando pelos $P_i's$.

■

1.12 Cúbicas por 8 pontos

Pode ser útil classificar, a menos de equivalência, as curvas projetivas que passam por um conjunto de pontos desejado. Esta abordagem foi utilizada anteriormente no Corolário 1.11.3, onde mostramos que dados cinco pontos, com algumas condições, existe uma única cônica passando por eles, a menos de equivalência.

Outra forma de obter uma classificação é usar a estrutura algébrica do espaço vetorial dos polinômios homogêneos, como fizemos no Corolário 1.9.4, onde a partir da dimensão do espaço $S_2(P_1,\ldots,P_n)$, $1 \leq n \leq 5$, especificamos o número de polinômios linearmente independentes que geram todas as cônicas passando pelos pontos $P_1,\ldots,P_n$.

O resultado a seguir conduz-se na segunda linha de raciocínio, onde mostramos que dados oito pontos "suficientemente genéricos" em $\mathbb{P}^2_{\mathbb{K}}$, existem duas cúbicas, cujos polinômios são linearmente independentes, passando por eles.

Teorema 1.12.1. *Seja $\mathbb{K}$ um corpo infinito e $P_1,\ldots,P_8 \in \mathbb{P}^2_{\mathbb{K}}$ pontos distintos. Suponha que não há 4 dos pontos $P_1,\ldots,P_8$ colineares e nem 7 em uma cônica não degenerada, então*

$$\dim S_3(P_1,\ldots,P_8) = 2.$$

Demonstração. Dizemos que um conjunto de pontos são concônicos se pertencem a uma cônica não degenerada. Como discutido na Seção 1.10

$$\dim S_d(P_1,\ldots,P_n) \geq \binom{d+2}{2} - n,$$

assim,

$$\begin{aligned}\dim S_3(P_1,\ldots,P_8) &\geq \binom{5}{2} - 8\\ &\geq 2.\end{aligned}$$

Resta mostrar que $\dim S_3(P_1,\ldots,P_8) \leq 2$. Dividimos essa prova em três casos:

Caso principal: *Não há 3 pontos colineares e nem 6 concônicos.*

Suponha por contradição que $\dim S_3(P_1,\ldots,P_8) \geq 3$ e sejam P_9, P_{10} pontos distintos da reta $L = P_1P_2$. Desta forma

$$\dim S_3(P_1,\ldots,P_{10}) \geq \dim S_3(P_1,\ldots,P_8) - 2 \geq 1$$

e então existe $F \neq 0 \in S_3(P_1,\ldots,P_{10})$. Pelo Corolário 1.11.2 $F = H \cdot Q$, com $Q \in S_2(P_3,\ldots,P_8)$. Assim temos uma contradição na suposição feita neste caso, pois se $C = \mathcal{V}(Q)$ é não degenerada então os 6 pontos $P_3,\ldots,P_8$ são concônicos, e se C é degenerada então é uma união de retas e no mínimo 3 pontos são colineares.

Caso degenerado 1: *Suponha $P_1, P_2, P_3 \in L = \mathcal{V}(H)$ pontos colineares.*

Seja P_9 um quarto ponto na reta L. Então pelo Corolário 1.11.2,

$$S_3(P_1,\ldots,P_9) = H \cdot S_2(P_4,\ldots,P_8).$$

Também como não há 4 pontos de $P_4,\ldots,P_8$ colineares, pelo Corolário 1.11.3

$$\dim S_2(P_4,\ldots,P_8) = 1 \text{ e então } \dim S_3(P_1,\ldots,P_9) = 1,$$

o que implica $S_3(P_1,\ldots,P_8) \leq 2$.

Caso degenerado 2: *Suponha $P_1,\ldots,P_6 \in C = \mathcal{V}(Q)$ pontos concônicos.*

Escolha $P_9 \in C$ distinto de $P_1,\ldots,P_6$. Novamente pelo Corolário 1.11.2,

$$S_3(P_1,\ldots,P_9) = Q \cdot S_1(P_7,P_8)$$

e a reta $L = P_7P_8$ é única, assim $S_3(P_1,\ldots,P_9)$ tem dimensão 1, gerado por $Q \cdot H$ e portanto $\dim S_3(P_1,\ldots,P_8) \leq 2$. ■

Como um corolário do teorema anterior temos o resultado abaixo, que relaciona 9 pontos em duas cúbicas projetivas.

Corolário 1.12.2. *Sejam $C_1 = \mathcal{V}(F_1), C_2 = \mathcal{V}(F_2) \subset \mathbb{P}^2_{\mathbb{K}}$ duas curvas cúbicas cuja interseção consiste em 9 pontos distintos, $C_1 \cap C_2 = \{P_1, \ldots, P_9\}$. Então uma cúbica D passando por $P_1, \ldots, P_8$ também passa por P_9.*

Demonstração. Se 4 dos pontos $P_1, \ldots, P_8$ pertencem a uma reta L então C_1 e C_2 encontram L em 4 ou mais pontos e pelo Corolário 1.11.2 contêm L, contradizendo a hipótese de $C_1 \cap C_2$ ser um conjunto finito. Do mesmo modo não pode haver 7 pontos concônicos. Agora que as condições da Proposição 1.12.1 são satisfeitas temos

$$\dim S_3(P_1, \ldots, P_8) = 2,$$

ou seja, F_1 e F_2 formam uma base de $S_3(P_1, \ldots, P_8)$ e então $D = \mathcal{V}(G)$, onde $G = \lambda_1 F_1 + \lambda_2 F_2$. Portanto como F_1 e F_2 se anulam em P_9, também G se anula. ■

1.13 Estrutura de grupo em uma cúbica projetiva plana

Após o desenvolvimento teórico realizado nas seções anteriores, estamos em condições de definir o grupo algébrico de uma cúbica projetiva plana.

Considere $\mathbb{K}$ um corpo infinito e $F \in \mathbb{K}[X, Y, Z]$ um polinômio homogêneo de grau 3 definindo a curva cúbica não vazia $\mathcal{C} = \mathcal{V}(F) \subset \mathbb{P}^2_{\mathbb{K}}$. É necessário ainda que $\mathcal{C}$ satisfaça as seguintes condições:

(a) F é irredutível;

(b) Para todo ponto $P \in \mathcal{C}$ existe uma única reta $L = \mathcal{V}(H) \in \mathbb{P}^2_{\mathbb{K}}$ tal que P é raiz múltipla de $F|_L$, isto é, tratando $F \circ H$ parametricamente como no Teorema 1.8.1, $P \in L \cap \mathcal{C}$ tem multiplicidade 2 ou 3;

(c) A curva $\mathcal{C}$ possui um ponto O de inflexão, ou seja, a reta do item anterior possui multiplicidade 3 em O na interseção com $\mathcal{C}$.

O item (a) nos garante que $\mathcal{C}$ não é a união de uma reta e uma cônica, (b) implica que todo ponto possui uma tangente bem definida, ou seja, $\mathcal{C}$ não possui singularidades (a reta L também é denotada por $T_P\mathcal{C}$) e (c) é uma hipótese necessária para a nossa abordagem da associatividade.

Tome uma cúbica $\mathcal{C} = V(F)$ nessas condições e fixe um ponto de inflexão O na curva. Vamos definir uma operação na cúbica por meio das seguintes construções:

Dados pontos $A, B \in \mathcal{C}$,

(I) Seja R o terceiro ponto de interseção de $\mathcal{C}$ com a reta AB;

(II) Seja agora $\overline{R}$ o terceiro ponto de interseção de $\mathcal{C}$ com a reta OR. Defina $A+B \coloneqq \overline{R}$.

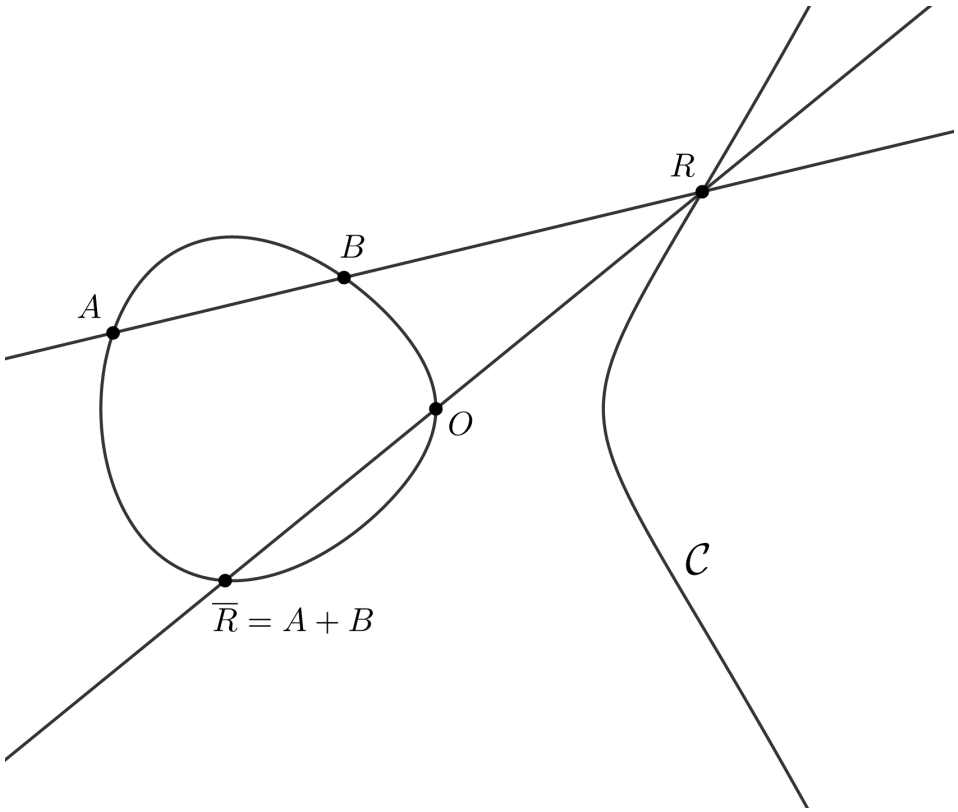


Figura 1.4: Construção da operação do grupo.
Fonte: Autoria própria.

Teorema 1.13.1. *A cúbica $\mathcal{C}$ munida com a operação $+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, dada por $A+B = \overline{R}$ como definido acima é um grupo algébrico abeliano, com O o elemento neutro.*

Demonstração. Vamos proceder verificando os axiomas da estrutura de grupo e visto que a associatividade é o mais trabalhoso deixamos esta discussão para a próxima seção.

Primeiramente é preciso que a operação "+" e o conceito de elemento inverso estejam bem definidos.

Dados $P, Q \in \mathcal{C}$ temos dois casos: $P \neq Q$ e $L = PQ \subset \mathbb{P}^2_{\mathbb{K}}$ é unicamente determinada ou $P = Q$ e por (b) existe uma única reta $L = T_P\mathcal{C} \subset \mathbb{P}^2_{\mathbb{K}}$ tal que P é raiz múltipla de $F|_L$. Em qualquer caso $F|_L$ é um polinômio cúbico em duas variáveis (U e V, veja a demonstração do Teorema 1.8.1), que possui duas raízes em $\mathbb{K}$, logo $F|_L$ se fatora como o produto de três fatores lineares, portanto o terceiro ponto de interseção R é definido e tem coordenadas em $\mathbb{K}$.

(i) (Elemento neutro) Como O, A e $\overline{A}$ são colineares a construção $O + A$ consiste em tomar a reta $L = OA$ encontrando $\overline{A}$ e usando a mesma reta voltamos a A finalizando a soma, então de fato O é elemento neutro.

(ii) (Inverso) Seja $L = T_O\mathcal{C}$ a reta tangente em O. Como O é ponto de inflexão o terceiro ponto de interseção entre L e $\mathcal{C}$ é $\overline{O} = O$. Desta forma para cada ponto $A \in \mathcal{C}$ definimos $-A$ como o terceiro ponto de interseção da reta $A\overline{O}$ e $\mathcal{C}$. Facilmente vemos que $A + (-A) = O$, logo todo elemento possui inverso.

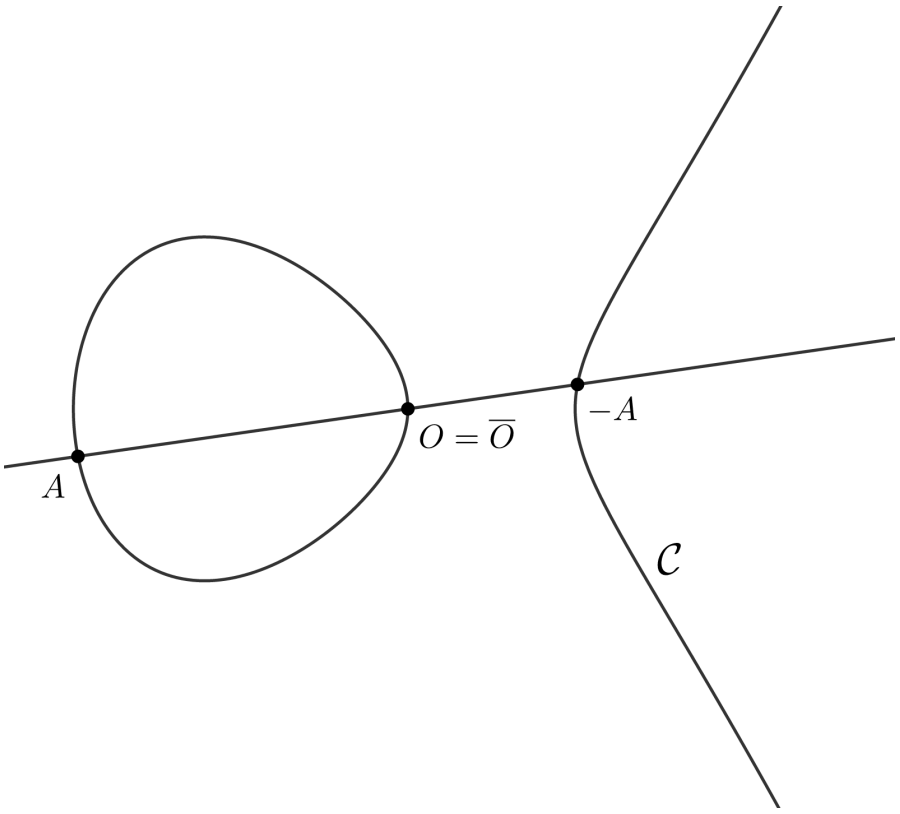


Figura 1.5: Elemento inverso.
Fonte: Autoria própria.

(iii) (Comutatividade) Basta notar que $L = AB = BA$, ou seja, as retas coincidem, então se R é o terceiro ponto de interseção de L com $\mathcal{C}$ temos que $A + B = B + A = \overline{R}$.

■

1.14 Associatividade

Primeiramente vamos provar, com os resultados que desenvolvemos, um caso suficientemente geral da associatividade, isto é, quando os oito pontos que compõem a construção $(A + B) + C$ são distintos.

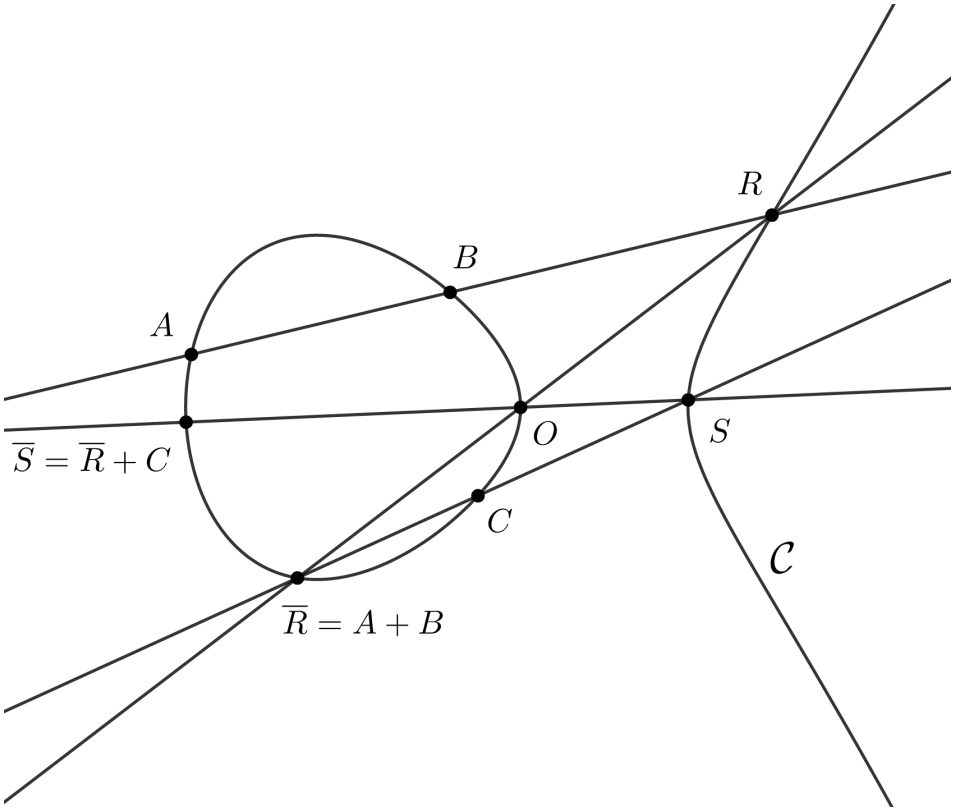


Figura 1.6: Construção de $(A + B) + C = \overline{S}$.
Fonte: Autoria própria.

Suponha $A, B, C \in \mathcal{C}$ então a construção $(A + B) + C = \overline{S}$ usa quatro retas:

$$L_1 = ABR,\ L_2 = RO\overline{R},\ L_3 = C\overline{R}S \text{ e } L_4 = SO\overline{S}.$$

A construção $(B + C) + A = \overline{T}$ usa outras quatro retas:

$$M_1 = BCQ,\ M_2 = QO\overline{Q},\ M_3 = A\overline{Q}T \text{ e } M_4 = TO\overline{T}.$$

Para mostrar que $\overline{S} = \overline{T}$ basta mostrar que $S = T$, e para isso considere as duas cúbicas,

$$D_1 = L_1 \cup M_2 \cup L_3 \quad \text{e} \quad D_2 = M_1 \cup L_2 \cup M_3.$$

Então, por construção

$$\mathcal{C} \cap D_1 = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, S\},$$
$$\mathcal{C} \cap D_2 = \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, T\}.$$

Agora como os nove pontos $A, \ldots, S$ são distintos, $\mathcal{C}$ e D_1 satisfazem as condições do Corolário 1.12.2, logo D_2 deve passar por S e assim $S = T$.

1.15 Associatividade geral

Para garantir que se pode tomar pontos A, B, C quaisquer na cúbica e obter $(A + B) + C = A + (B + C)$ é necessário uma abordagem que foge do escopo desse trabalho, desta forma citaremos uma fonte onde é apresentada esta demonstração.

As condições da construção do grupo (itens (a), (b) e (c)) garantem que $\mathcal{C}$ é projetivamente equivalente a uma *curva elíptica*, dada por uma equação da forma:

$$-Y^2Z + X^3 + aXZ^2 + bZ^3 = 0.$$

Essa equivalência é feita com detalhes em [3], Teorema 3.1.

Assumindo $\mathcal{C}$ uma curva elíptica, a referência [23], Proposição 3.4, demonstra por meio da teoria dos divisores que existe uma bijeção entre o grupo de Picard de grau zero de $\mathcal{C}$, que é abeliano, e a curva $\mathcal{C}$, bem como mostra que as operações dos grupos coincidem, o que implica na associatividade do *grupo geométrico* definido anteriormente.

Capítulo 2

Fundamentos da Teoria de Módulos e Álgebras

Apresentamos, ao longo das próximas seções, um apanhado geral da teoria de módulos e álgebras. Nesse texto todos os anéis são considerados associativos e com unidade. Para esse capítulo, a menos de menção contrária, k denota um anel comutativo.

2.1 Módulos sobre anéis

Definição 2.1.1. Seja A um anel. Um A-módulo à esquerda é um par (M, μ) onde M é um grupo abeliano e $\mu : A \times M \to M$ é uma aplicação cuja ação em (a, x) é denotada por $\mu(a, x) = ax$, e satisfaz

$$\begin{aligned} a(x+y) &= ax + ay, \\ (a+b)x &= ax + bx, \\ (ab)x &= a(bx), \\ 1x &= x, \end{aligned}$$

para todos $a, b \in A$ e $x, y \in M$.

Analogamente, há o conceito de A-módulo à direita.

Definição 2.1.2. Seja A um anel. Um A-módulo à direita é um par (M, μ) onde M é um grupo abeliano e $\mu : M \times A \to M$ é uma aplicação $(x, a) \mapsto xa$ que satisfaz

$$\begin{aligned} (x+y)a &= xa + ya, \\ x(a+b) &= xa + xb, \\ x(ab) &= (xa)b, \\ x1 &= x, \end{aligned}$$

para todos $a, b \in A$ e $x, y \in M$.

Neste texto, salvo menção em contrário, por "A-módulo" entenderemos um A-módulo à esquerda. Na ocorrência de um A-módulo N à esquerda e um A-módulo M à direita usaremos as identificações ${}_AN$ e M_A.

Definição 2.1.3. Sejam A e B anéis. Se um grupo abeliano M possui estrutura de A-módulo à esquerda e estrutura de B módulo à direita, o chamamos de $(A-B)$-*bimódulo* e denotamos ${}_AM_B$.

Exemplos 2.1.4. Alguns módulos:

(1) Todo espaço vetorial sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo.

(2) Todo grupo abeliano G é um $\mathbb{Z}$-módulo com $\mu : \mathbb{Z} \times G \to G$ dada por: se $n > 0$ $(n, g) \mapsto n \cdot g = g + g + \cdots + g$ (n vezes); se $n = 0$, $(0, g) \mapsto 0 \cdot g = 0_G$; se $n < 0$ então $(n, g) \mapsto -((-n) \cdot g)$.

(3) Todo anel A é um módulo sobre si mesmo. Todo ideal à esquerda de A é um A-módulo à esquerda, e todo ideal à direita de A é um A-módulo à direita. Em particular, todo ideal de A é um A-módulo (à esquerda e à direita).

(4) Se A é um subanel de B, então B é um A-módulo com $(a, b) \mapsto a \cdot b$ sendo a multiplicação em B. Em particular $A[X_1, \ldots, X_n]$ e $A[X]$ são A-módulos.

(5) Sejam A e B anéis e $\varphi : A \to B$ um homomorfismo de anéis. Então todo B-módulo M induz um A-módulo, definindo $am \coloneqq \varphi(a)m$, para $a \in A, b \in B$ e $m \in M$.

(6) Seja $T : V \to V$ uma transformação linear, onde V é um espaço vetorial de dimensão finita sobre o corpo $\mathbb{K}$. Então V pode ser visto como um $\mathbb{K}[X]$-módulo, se definirmos a multiplicação por escalar $\mathbb{K}[X] \times V \to V$ por

$$f(X)v = (\sum_{i=0}^{n} c_i X^i)v \coloneqq \sum_{i=0}^{n} c_i T^i(v),$$

onde $f(X) = \sum_{i=0}^{n} c_i X^i \in \mathbb{K}[X]$, T^0 é a transformação identidade de V e T^i é a composta de T com T i vezes se $i \geq 1$.

Observação 2.1.5. Quando A é um anel comutativo não há diferença entre A-módulos à esquerda e à direita. Mais precisamente, se M é um A-módulo à esquerda então podemos definir uma estrutura de A-módulo à direita em M por $x \cdot a = ax$ para $a \in A$ e $x \in M$; reciprocamente, cada A-módulo à direita tem uma estrutura natural de A-módulo à esquerda.

Isso não é verdade para um anel não-comutativo por conta do terceiro axioma. Gostaríamos de mostrar que $(x \cdot a) \cdot b = x \cdot (ab)$ para todo $x \in M$ e $a, b \in A$, mas neste caso teríamos

$$(x \cdot a) \cdot b = b(ax) = (ba)x = x \cdot (ba).$$

Obeserve que ficamos com $(x \cdot a) \cdot b = x \cdot (ba)$ e, como A não é comutativo, não podemos afirmar que $x \cdot (ba) = x \cdot (ab)$.

A partir daqui trabalharemos com módulos à esquerda, entretanto todos os resultados e as definições valem para módulos à direita, feitas as devidas alterações.

Definição 2.1.6. Sejam M e N dois A-módulos. Uma aplicação $\phi : M \to N$ é um *homomorfismo* de A-módulos ou um A-*homomorfismo* se

$$\phi(m + m') = \phi(m) + \phi(m'),$$
$$\phi(am) = a\phi(m),$$

para todo $a \in A$ e $m, m' \in M$. O homomorfismo $\phi : M \to N$ é um isomorfismo de A-módulos se existe um A-homomorfismo $\psi : N \to M$ tal que $\psi \circ \phi = I_M$ e $\phi \circ \psi = I_N$, onde I_M e I_N são os homomorfismos identidade em M e N, respectivamente.

Exemplo 2.1.7. Alguns homomorfismos:

(1) Se $\mathbb{K}$ é corpo, então $\mathbb{K}$-módulos são espaços vetoriais e $\mathbb{K}$-homomorfismos são transformações lineares.

(2) Todo homomorfismo de grupos abelianos é um $\mathbb{Z}$-homomorfismo, pois se $n > 0$,

$$\varphi(ng) = \varphi(g + g + \cdots + g) = \varphi(g) + \varphi(g) + \cdots + \varphi(g) = n\varphi(g);$$

se $n = 0$

$$\varphi(ng) = \varphi(0) = n\varphi(g);$$

e se $n < 0$

$$\varphi(ng) = \varphi(-((-n) \cdot g)) = -(\varphi(g) + \varphi(g) + \cdots + \varphi(g)) = -(-n)\varphi(g) = n\varphi(g).$$

(3) Se A é um anel comutativo, M um A-módulo e $f \in A$, então a multiplicação por f, $\mu_f : M \to N$ dada por $m \mapsto fm$ é um A-homomorfismo. De fato, A é comutativo, logo $\mu_f(am) = f(am) = (fa)m = (af)m = a(fm) = a\mu_f(m)$.

Definição 2.1.8. Um *submódulo* M' de M é um subgrupo de M que é fechado em relação à multiplicação por elementos de A.

Observação 2.1.9. Todo submódulo de um A-módulo também é um A-módulo.

Definição 2.1.10. Se M' é um A-submódulo do A-módulo M, o grupo abeliano M/M' tem estrutura de A-módulo, definida por $a(m + M') = am + M'$. Dizemos que M/M' é o A-módulo *quociente* de M por M'.

Exemplo 2.1.11. Seja M um A-módulo e $(M_\lambda)_{\lambda\in\Lambda}$ uma família de submódulos de M, a *interseção* $\bigcap_{\lambda\in\Lambda} M_\lambda$ é um A-módulo. De fato, esse conjunto é um submódulo de M e portanto um A-módulo.

Definição 2.1.12. Seja M um A-módulo e $(M_\lambda)_{\lambda\in\Lambda}$ uma família de submódulos de M. Definimos

(i) A *soma* $\sum_{\lambda\in\Lambda} M_\lambda$ como o conjunto de todas as somas finitas $\sum_{\lambda\in\Lambda} m_\lambda$, onde $m_\lambda \in M_\lambda$, para todo $\lambda \in \Lambda$ e quase todos os m_λ são nulos. A soma é o menor submódulo de M que contém todos os M_λ.

(ii) Se I é um ideal de A e M um A-módulo definimos o *submódulo produto* IM como sendo o conjunto de todas as somas finitas $\sum_j a_j m_j$, com $a_j \in I$ e $m_j \in M$.

O kernel a imagem de um homomorfismo de módulos ainda são submódulos, como indica a proposição abaixo (veja a Proposição 2.3 em [20]).

Proposição 2.1.13. (1) *O kernel* $\operatorname{Ker}\varphi \subset M$ *e a imagem* $\operatorname{Im}\varphi \subset N$ *de um homomorfismo de A-módulos $\varphi : M \to N$ são submódulos.*

(2) *Se $N \subset M$ é um submódulo dado, existem um módulo quociente M/N e uma aplicação sobrejetiva $\pi : M \to M/N$ tais que* $\operatorname{Ker}\pi = N$.

Por fim enunciamos os Teoremas do isomorfismo para a estrutura de módulos (veja o Teorema 2.3 em [20]).

Teorema 2.1.14 (Teoremas do isomorfismo)**.**

(1°) *Sejam M e N A-módulos e $\varphi : M \to N$ homomorfismo, então* $M/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

(2°) *Se N é um A-módulo e $L, M \subset N$ são submódulos, então*

$$(M + L)/L \cong M/(M \cap L).$$

(3°) *Se $L \subset M \subset N$ são submódulos, então*

$$N/M \cong (N/L)/(M/L).$$

2.2 Álgebras

Os anéis mais importantes neste trabalho são os anéis de polinômios em n indeterminadas $k[X_1, \ldots, X_n]$, onde k é um anel comutativo, e seus anéis quocientes. Esses anéis possuem uma estrutura extra, a estrutura de k-álgebra.

Definição 2.2.1. Uma *k-álgebra* é um anel A junto com um homomorfismo de anéis $\phi : k \to A$ tal que $\phi(\lambda)a = a\phi(\lambda)$, para cada $a \in A$ e $\lambda \in k$.

Observação 2.2.2. Há várias definições equivalentes de k-álgebra. Uma segunda definição mais prática é: uma k-álgebra A é um anel A, com uma estrutura de k-módulo, tal que o produto de A é uma aplicação k-bilinear. Note que, pela bilinearidade, se $\lambda \in k$ e $a \in A$ então

$$\lambda \cdot a = \lambda \cdot (1_A a) = (\lambda \cdot 1_A)a.$$

Pode-se mostrar que $\phi : k \to A$ dado por $\phi(\lambda) = \lambda \cdot 1_A$ é um homomorfismo de anéis e (novamente pela bilinearidade) vale que $\phi(\lambda)a = a\phi(\lambda)$ para cada $a \in A$ e $\lambda \in k$.

Reciprocamente, se A é um anel e $\phi : k \to A$ é um homomorfismo de anéis tal que $\phi(\lambda)a = a\phi(\lambda)$ para cada $a \in A$ e $\lambda \in k$, pode-se verificar que A tem estrutura de k-módulo por

$$\lambda \cdot a = \phi(\lambda)a$$

e que o produto em A é k-bilinear.

Uma terceira forma de compreender k-álgebras é apresentada na Proposição 2.6.9, via o produto tensorial.

Definição 2.2.3. Se A é uma k-álgebra,

(i) uma subálgebra de A é um subanel B de A que também é um k-submódulo de A.

(ii) um ideal da k-álgebra A é um ideal do anel A.

Exemplos 2.2.4. Sejam k um anel comutativo e A uma k-álgebra.

(1) O anel de polinômios $A[X_1, \ldots, X_n]$ é uma k-álgebra para qualquer inteiro positivo n. Em particular, $k[X_1, \ldots, X_n]$ é uma k-álgebra comutativa.

(2) Se I é um ideal de A então I é também um k-submódulo de A, e com isso o anel quociente A/I tem uma estrutura canônica de k-módulo, e também tem estrutura de k-álgebra.

Definição 2.2.5. Sejam A e B duas k-álgebras. Uma aplicação $f : A \to B$ é um *homomorfismo de k-álgebras* se é um homomorfismo de anéis e também um homomorfismo de k-módulos.

Observação 2.2.6. Módulos à esquerda (à direita) sobre uma álgebra A são módulos à esquerda (à direita) sobre o anel A. Cada A-módulo possui uma estrutura natural de k-módulo.

2.3 Categorias

Nesta seção reunimos definições e resultados básicos de categorias e funtores, além de alguns exemplos.

Definição 2.3.1. Uma *categoria* $\mathcal{C}$ é uma tripla (Ob, $\mathrm{Hom}_{\mathcal{C}}$, $\circ$) definida por:

(i) Uma classe $\mathrm{Ob}\,\mathcal{C}$, chamada classe de *objetos* de $\mathcal{C}$.

(ii) Para cada par (X, Y) de objetos de $\mathcal{C}$, um conjunto denotado $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, cujos elementos são morfismos de X em Y tais que, se $(X, Y) \neq (X', Y')$, então $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap \mathrm{Hom}_{\mathcal{C}}(X', Y') = \varnothing$.

(iii) Para cada tripla de objetos (X, Y, Z) de $\mathcal{C}$, uma aplicação

$$\circ : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z),$$

onde a imagem do par (g, f) é denotada por $g \circ f$ ou gf, chamada *composição de morfismos* e satisfaz as duas condições a seguir:

(C_1) Se $f \in \mathrm{Hom}_{\mathcal{C}}(U, V)$, $g \in \mathrm{Hom}_{\mathcal{C}}(V, W)$ e $h \in \mathrm{Hom}_{\mathcal{C}}(W, X)$, então

$$h(gf) = (hg)f.$$

(C_2) Para cada objeto X de $\mathcal{C}$ existe um morfismo $1_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$, chamado *identidade em* X tal que, se $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ e $g \in \mathrm{Hom}_{\mathcal{C}}(W, X)$ então,

$$f1_X = f \quad \text{e} \quad 1_X g = g.$$

Exemplos 2.3.2. (1) A categoria Ens ou Set tem por objetos conjuntos, por morfismos funções e a composição usual.

(2) Gr é a categoria de grupos, os morfismos são homomorfismos de grupos e a composição é a usual.

(3) Top é a categoria dos espaços topológicos, os morfismos são funções contínuas e a composição é a usual.

(4) Seja k um anel comutativo. A categoria $\mathrm{Alg}\,k$ das k-álgebras tem como morfismos os homomorfismos de k-álgebras e a composição usual.

(5) Seja A uma k-álgebra. A categoria $\operatorname{Mod} A$ de A-módulos à esquerda tem como morfismos as aplicações A-lineares e a composição é a usual.

(6) Seja G um monóide. Definimos a categoria $\mathcal{C}$ de G por um único objeto X e $\operatorname{Hom}_{\mathcal{C}}(X, X) = G$.

(7) Um conjunto parcialmente ordenado X pode ser considerado como uma categoria $\mathcal{C} = PO(X)$ cujos objetos são elementos de X e $\operatorname{Hom}_{\mathcal{C}}(a, b)$ é um conjunto com um elemento ρ_b^a se $a \preceq b$ e vazio caso contrário. Da transitividade da ordem parcial em X segue que $\rho_b^a \rho_c^b = \rho_c^a$, o que define a composição.

(8) Seja $\mathbb{K}$ um corpo. Considere a classe ε de todas as triplas (E, F, f) onde E, F são $\mathbb{K}$-espaços vetoriais e $f : E \to F$ é $\mathbb{K}$-linear. Consideramos a categoria onde a classe de objetos é ε e um morfismo $(E, F, f) \to (E', F', f')$ é um par (u, v) onde $u : E \to E'$ e $v : F \to F'$ são $\mathbb{K}$-lineares tais que $f'u = vf$.

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ E' & \xrightarrow[f']{} & F' \end{array}$$

Se definirmos a composição dos morfismos $(u, v) : (E, F, f) \to (E', F', f')$ e $(u', v') : (E', F', f') \to (E'', F'', f'')$ por $(u', v')(u, v) = (u'u, v'v)$, obtemos uma categoria.

(9) Seja $\mathbb{K}$ um corpo algebricamente fechado. Definimos a categoria das variedades algébricas $\mathrm{VA}(\mathbb{K})$ cujos objetos são variedades algébricas em $\mathbb{A}^n$, para algum $n \geq 1$ e os morfismos são funções polinomiais (veja as Seções 3.4 e 3.8).

(10) Seja $\mathbb{K}$ um corpo. A categoria $\mathrm{AlgAf}(\mathbb{K})$ tem por objetos $\mathbb{K}$-álgebras afins, isto é, álgebras comutativas, sem elementos nilpotentes e finitamente geradas sobre $\mathbb{K}$. Um morfismo nesta categoria é um homomorfismo de $\mathbb{K}$-álgebras.

Na Seção 3.8 exploramos a relação entre as categorias $\mathrm{VA}(\mathbb{K})$ e $\mathrm{AlgAf}(\mathbb{K})$.

Definição 2.3.3. Seja $\mathcal{C}$ uma categoria e $f : X \to Y$ um morfismo de $\mathcal{C}$. Dizemos que f é um *isomorfismo* se existe um morfismo $g : Y \to X$ tal que $g \circ f = 1_X$ e $f \circ g = 1_Y$.

Definição 2.3.4. Sejam $\mathcal{C}$, $\mathcal{D}$ duas categorias. Dizemos que $\mathcal{D}$ é uma *subcategoria* de $\mathcal{C}$ se todo objeto de $\mathcal{D}$ é um objeto de $\mathcal{C}$, se todo morfismo de $\mathcal{D}$ é um morfismo de $\mathcal{C}$ e se a composição coincide. Assim, se X, Y são dois objetos de $\mathcal{D}$, temos

$$\operatorname{Hom}_{\mathcal{D}}(X, Y) \subseteq \operatorname{Hom}_{\mathcal{C}}(X, Y).$$

Se esta inclusão for uma igualdade para todos X, Y em $\mathcal{D}$, ou seja, se todo morfismo $X \to Y$ de $\mathcal{C}$ é morfismo de $\mathcal{D}$, dizemos que $\mathcal{D}$ é uma *subcategoria plena*.

Uma subcategoria de Ens é chamada de *categoria concreta*. Alguns exemplos são: Gr, Ab, Top, $\operatorname{Mod} A$, $\operatorname{Alg} k$.

Definição 2.3.5. Sejam $\mathcal{C}, \mathcal{D}$ duas categorias.

(I) Um *funtor covariante* $F : \mathcal{C} \to \mathcal{D}$ é uma função que associa a cada objeto X de $\mathcal{C}$ um objeto $F(X)$ ou FX de $\mathcal{D}$ e para cada morfismo $f : X \to Y$ de $\mathcal{C}$ um morfismo $F(f)$ ou $Ff : FX \to FY$ de $\mathcal{D}$ tal que

(F_1) Se gf é definido em $\mathcal{C}$, então $F(g)F(f)$ é definido em $\mathcal{D}$ e $F(gf) = F(g)F(f)$.

(F_2) Para todo objeto X de $\mathcal{C}$, $F(1_X) = 1_{FX}$.

(II) Um *funtor contravariante* $F : \mathcal{C} \to \mathcal{D}$ é uma função que associa a cada objeto X de $\mathcal{C}$ um objeto $F(X)$ ou FX de $\mathcal{D}$ e para cada morfismo $f : X \to Y$ de $\mathcal{C}$ um morfismo $F(f)$ ou $Ff : FY \to FX$ de $\mathcal{D}$ tal que

(F_1) Se gf é definido em $\mathcal{C}$, então $F(f)F(g)$ é definido em $\mathcal{D}$ e $F(gf) = F(f)F(g)$.

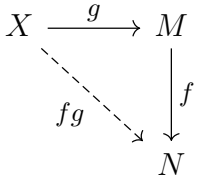
(F_2) Para todo objeto X de $\mathcal{C}$, $F(1_X) = 1_{FX}$.

Exemplos 2.3.6. (1) Seja $\mathcal{C}$ uma subcategoria de $\mathcal{D}$. Existe um funtor canônico, denominado inclusão, $J : \mathcal{C} \to \mathcal{D}$ definido para cada objeto X de $\mathcal{C}$ por $J(X) = X$ e para todo morfismo f de $\mathcal{C}$ por $J(f) = f$. Se $\mathcal{C} = \mathcal{D}$ o funtor inclusão é chamado identidade e denotado $1_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$.

(2) Se $\mathcal{C} = \mathrm{Gr}, \mathrm{Ab}, \operatorname{Mod} A, \operatorname{Alg} k$ existe um funtor $U : \mathcal{C} \to \mathrm{Ens}$, chamado *funtor esquecimento*, que associa a cada objeto seu conjunto correspondente e a cada morfismo a aplicação correspondente. Da mesma forma, se A é uma k-álgebra existe um funtor esquecimento $U : \operatorname{Mod} A \to \operatorname{Mod} k$.

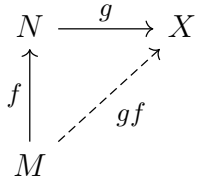
(3) Sejam $\mathcal{C}, \mathcal{D}, \mathcal{E}$ três categorias e $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{E}$ dois funtores. O *funtor composto* $G \circ F$ ou GF de $\mathcal{C}$ em $\mathcal{E}$ é definido por $(GF)(X) = G(F(X))$ para todo objeto X de $\mathcal{C}$ e $(GF)(f) = G(F(f))$ para todo morfismo f de $\mathcal{C}$.

(4) Sejam $\mathcal{C}$ uma categoria e X um objeto de $\mathcal{C}$. O funtor $\operatorname{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to \mathrm{Ens}$ associa a cada objeto M de $\mathcal{C}$ o conjunto $\operatorname{Hom}_{\mathcal{C}}(X, M)$ e a cada morfismo $f : M \to N$ a aplicação $\operatorname{Hom}_{\mathcal{C}}(X, f) : \operatorname{Hom}_{\mathcal{C}}(X, M) \to \operatorname{Hom}_{\mathcal{C}}(X, N)$ dada por $\operatorname{Hom}_{\mathcal{C}}(X, f)(g) = fg$.



Esse funtor é covariante.

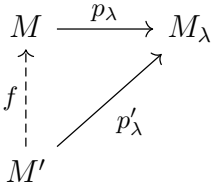
(5) Sejam $\mathcal{C}$ uma categoria e X um objeto de $\mathcal{C}$. O funtor $\mathrm{Hom}_{\mathcal{C}}(-, X) : \mathcal{C} \to \mathrm{Ens}$ associa a cada objeto M de $\mathcal{C}$ o conjunto $\mathrm{Hom}_{\mathcal{C}}(M, X)$ e a cada morfismo $f : M \to N$ a aplicação $\mathrm{Hom}_{\mathcal{C}}(f, X) : \mathrm{Hom}_{\mathcal{C}}(N, X) \to \mathrm{Hom}_{\mathcal{C}}(M, X)$ dada por $\mathrm{Hom}_{\mathcal{C}}(f, X)(g) = gf$.



Esse funtor é contravariante.

2.4 Produtos e Somas Diretas

Definição 2.4.1. Seja $(M_\lambda)_{\lambda\in\Lambda}$ uma família de objetos de uma categoria $\mathcal{C}$. Um *produto* desta família é um par $(M, (p_\lambda)_{\lambda\in\Lambda})$, dado por um objeto M e por uma família de morfismos $(p_\lambda : M \to M_\lambda)_{\lambda\in\Lambda}$ tal que, se $(M', (p'_\lambda)_{\lambda\in\Lambda})$ é um par de outro objeto M' e outra família $(p'_\lambda : M' \to M_\lambda)_{\lambda\in\Lambda}$, então existe um único morfismo $f : M' \to M$ tal que $p_\lambda f = p'_\lambda$ para todo $\lambda \in \Lambda$.



A condição da unicidade pode ser reformulada como: se f e g são dois morfismos tais que $p_\lambda f = p_\lambda g$ para todo $\lambda \in \Lambda$, então $f = g$.

Lema 2.4.2. *Se uma família de objetos $(M_\lambda)_{\lambda\in\Lambda}$ admite um produto, esse é único a menos de isomorfismo.*

Demonstração. Veja [2], Lema 2.1. ■

Por abuso de linguagem dizemos que M, se existe, é o produto da família $(M_\lambda)_{\lambda\in\Lambda}$, e denotamos $M = \prod_{\lambda\in\Lambda} M_\lambda$. Se $\Lambda = \{1, 2, \ldots, n\}$ denotamos $M = \prod_{i=1}^{n} M_i$ ou $M = M_1 \times \cdots \times M_n$. Se todos os M_λ são iguais a N, denotamos $M = N^\Lambda$. Os morfismos $(p_\lambda : M \to M_\lambda)_{\lambda\in\Lambda}$ são chamados *projeções canônicas*.

Teorema 2.4.3. *Seja A uma k-álgebra. Toda família $(M_\lambda)_{\lambda\in\Lambda}$ de A-módulos admite um produto em* Mod A.

Demonstração. Dados dois conjuntos não vazios M e Λ, o produto cartesiano M^Λ é o conjunto das funções de Λ em M. Por abuso de linguagem denotamos um elemento m de M^Λ por $(m_\lambda)_{\lambda\in\Lambda}$, onde $m_\lambda = m(\lambda)$.

Dada uma família de A-módulos $(M_\lambda)_{\lambda\in\Lambda}$, considere o conjunto $M = \bigcup_{\lambda\in\Lambda} M_\lambda$ e o produto cartesiano M^Λ. Este conjunto tem uma estrutura canônica de A-módulo dada por

$$(m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} = (m_\lambda + n_\lambda)_{\lambda\in\Lambda}, \quad a(m_\lambda)_{\lambda\in\Lambda} = (am_\lambda)_{\lambda\in\Lambda}.$$

Pode-se mostrar que o submódulo

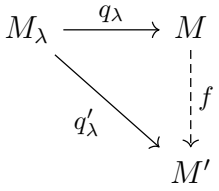
$$P = \{(m_\lambda)_{\lambda\in\Lambda} \in M^\Lambda \ : \ m_\lambda \in M_\lambda, \ \forall\ \lambda \in \Lambda\}$$

é um produto direto da família $(M_\lambda)_{\lambda\in\Lambda}$ com a família de morfismos

$$p_\mu : P \to M_\mu, \quad (m_\lambda)_{\lambda\in\Lambda} \mapsto m_\mu.$$

■

Definição 2.4.4. Seja $(M_\lambda)_{\lambda\in\Lambda}$ uma família de objetos de uma categoria $\mathcal{C}$. Uma *soma direta* ou *coproduto* desta família é um par $(M, (q_\lambda)_{\lambda\in\Lambda})$ onde M é um objeto e $(q_\lambda : M_\lambda \to M)_{\lambda\in\Lambda}$ uma família de morfismos tal que, se $(M', (q'_\lambda)_{\lambda\in\Lambda})$ é um par de outro objeto M' e outra família $(q'_\lambda : M_\lambda \to M')_{\lambda\in\Lambda}$, então existe um único morfismo $f : M \to M'$ tal que $fq_\lambda = q'_\lambda$ para todo $\lambda \in \Lambda$.



A condição da unicidade pode ser reformulada como: se f e g são dois morfismos tais que $fq_\lambda = gq_\lambda$ para todo $\lambda \in \Lambda$, então $f = g$.

Dizemos que M, se existe, é a *soma direta* ou *coproduto* da família $(M_\lambda)_{\lambda\in\Lambda}$. Denotamos $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ ou $\coprod_{\lambda\in\Lambda} M_\lambda$. Se $\Lambda = \{1, 2, \ldots, n\}$ denotamos $M = \bigoplus_{i=1}^n M_i$, $M = \coprod_{i=1}^n M_i$ ou $M = M_1 \oplus \cdots \oplus M_n$. Por fim se $M_\lambda = N$, para todo $\lambda \in \Lambda$, então denotamos $M = N^{(\Lambda)}$. Os morfismos $(q_\lambda : M_\lambda \to M)_{\lambda\in\Lambda}$ são chamados *inclusões canônicas*.

Lema 2.4.5. *Se uma família de objetos admite uma soma direta, essa é única a menos de isomorfismo.*

Demonstração. Veja [2], Lema 2.3. ■

Teorema 2.4.6. *Seja A uma k-álgebra. Toda família $(M_\lambda)_{\lambda\in\Lambda}$ de A-módulos admite uma soma direta em* Mod A.

Demonstração. Como antes, sejam $M = \bigcup_{\lambda\in\Lambda} M_\lambda$ e

$$\prod_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \in M^\Lambda : m_\lambda \in M_\lambda, \ \forall\ \lambda \in \Lambda\}.$$

Dado $(m_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda$, dizemos que seu suporte é

$$\operatorname{supp}((m_\lambda)_{\lambda\in\Lambda}) = \{\lambda \in \Lambda : m_\lambda \neq 0\}.$$

Considere o conjunto

$$S = \{(m_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda : |\operatorname{supp}((m_\lambda)_{\lambda\in\Lambda})| < \infty\}.$$

Então S é um A-módulo pois é um A-submódulo de $\prod_{\lambda\in\Lambda} M_\lambda$, e é uma soma direta da família $(M_\lambda)_{\lambda\in\Lambda}$ com os morfismos

$$q_\mu : M_\mu \to S, \quad m \mapsto (m_\lambda)_{\lambda\in\Lambda}$$

em que $m_\mu = m$ e $m_\lambda = 0$ se $\lambda \neq \mu$. ■

Observação 2.4.7. Se o conjunto Λ é finito então o produto direto e a soma direta da família de A-módulos $(M_\lambda)_{\lambda\in\Lambda}$ coincidem.

Definição 2.4.8 (soma direta interna)**.** Seja $(M_\lambda)_{\lambda\in\Lambda}$ uma família de submódulos de um A-módulo M. Diremos que a soma $\sum_{\lambda\in\Lambda} M_\lambda$ é direta se é isomorfa à soma direta $\bigoplus_{\lambda\in\Lambda} M_\lambda$.

A próxima proposição estende caracterizações conhecidas de uma soma direta (interna) no contexto de espaços vetoriais de dimensão finita para módulos sobre uma álgebra.

Proposição 2.4.9. *Seja $(M_\lambda)_{\lambda\in\Lambda}$ uma família de submódulos de um A-módulo M. As condições abaixo são equivalentes:*

(1) *A soma $\sum_{\lambda\in\Lambda} M_\lambda$ é direta.*

(2) *Para todo $\lambda \in \Lambda$, temos $M_\lambda \cap \sum_{\mu\neq\lambda} M_\mu = 0$.*

(3) *Se $\sum_{\lambda\in\Lambda} x_\lambda = 0$, onde $(x_\lambda)_{\lambda\in\Lambda}$ é uma família com suporte finito tal que $x_\lambda \in M_\lambda$, para todo $\lambda \in \Lambda$ então $x_\lambda = 0$ para todo $\lambda \in \Lambda$.*

(4) *Todo $x \in \sum_{\lambda\in\Lambda} M_\lambda$ se escreve de modo único na forma $x = \sum_{\lambda\in\Lambda} x_\lambda$, onde $(x_\lambda)_{\lambda\in\Lambda}$ é uma família com suporte finito tal que $x_\lambda \in M_\lambda, \forall\ \lambda \in \Lambda$.*

2.5 Módulos livres

Sejam A uma k-álgebra e M módulo sobre A. Um subconjunto X de M é dito *livre* ou *linearmente independente* se, para toda família $(x_\lambda)_{\lambda\in\Lambda}$ de elementos de X cujo

suporte é finito, a relação $\sum_{\lambda\in\Lambda} a_\lambda x_\lambda = 0$, com a_λ elementos de A, implica $a_\lambda = 0$ para todo $\lambda \in \Lambda$. Um conjunto X que não é livre é dito *linearmente dependente*.

Um *conjunto gerador* para M, ou um conjunto de geradores de M, é um conjunto $X \subset M$ tal que todo elemento de M se escreve com combinação linear de elementos de X. Um A-módulo M é finitamente gerado se possui um conjunto gerador finito.

Uma *base* de um módulo M é por definição uma família livre de elementos de M que o gera. Nem todo módulo tem base, por exemplo: se G é um grupo abeliano finito de ordem n então G não contém nenhum subconjunto livre sobre $\mathbb{Z}$ (pois $n \cdot x = 0$ para todo $x \in G$).

Exemplo 2.5.1. Se A é um domínio de integridade, $0 \neq f \in A$ e $\operatorname{Frac} A$ é seu corpo de frações, então

$$A[1/f] = A + Af^{-1} + Af^{-2} + \cdots$$

é um A-submódulo de $\operatorname{Frac} A$ que normalmente não é finitamente gerado como A-módulo. Note que $\{1, f^{-1}, f^{-2}, \ldots\}$ é um conjunto de geradores infinito para $A[1/f]$.

Considere, por exemplo, o caso em que $A = \mathbb{Z}$ e $f \geq 2$. Se existe um conjunto gerador finito X para $\mathbb{Z}[1/f]$ então $X \subset \mathbb{Z} + \mathbb{Z}f^{-1} + \cdots + \mathbb{Z}f^{-n}$ para algum $n \geq 0$. Mas

$$\frac{1}{f^{n+1}} \notin \mathbb{Z} + \mathbb{Z}f^{-1} + \cdots + \mathbb{Z}f^{-n},$$

pois se

$$\frac{1}{f^{n+1}} = a_0 + \frac{a_1}{f} + \cdots + \frac{a_n}{f^n}$$

então teremos

$$1 = a_0 f^{n+1} + a_1 f^n + \cdots + a_n f = df$$

com d inteiro, portanto $f \geq 2$ divide 1 em $\mathbb{Z}$, absurdo.

Exemplos 2.5.2. Seja A um anel.

(1) O anel de polinômios $A[X]$ tem o conjunto

$$1, X, X^2, \ldots$$

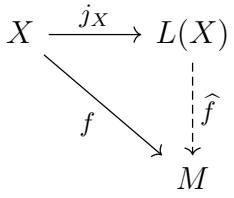
como conjunto gerador. Pela construção de $A[X]$ este conjunto é uma base, pois se

$$a_0 + a_1 X + \cdots + a_n X^n = 0,$$

então $a_0 = a_1 = \cdots = a_n = 0$. Mais ainda, $A[X]$ não é um A-módulo finitamente gerado. De fato, se $B \subset A[X]$ é um conjunto finito de polinômios e o grau máximo de um elemento de B é n então X^{n+1} não se escreve como combinação linear de elementos de B.

(2) Seja I um ideal do anel A. O A-módulo A/I é gerado por $1+I$, mas o conjunto $\{1+I\}$ *não* é livre se $I \neq 0$, pois se $f \in I$ então $f(1+I) = 0$. Portanto A/I é finitamente gerado e não é livre.

Definição 2.5.3. Seja X um conjunto. Um *A-módulo livre* sobre X é um A-módulo $L(X)$ junto de uma aplicação $j_X : X \to L(X)$ tal que, se M é um A-módulo e $f : X \to M$ uma aplicação, então existe um único morfismo de A-módulos $\widehat{f} : L(X) \to M$ tal que $\widehat{f} j_X = f$.



Teorema 2.5.4. *Para todo conjunto X, existe um A-módulo livre sobre X, único a menos de isomorfismo.*

Demonstração. Mostraremos a existência deste A-módulo.

Dado um conjunto X podemos considerar a soma direta da família $(A_\lambda)_{\lambda \in X}$, onde $A_\lambda = A$ para cada $\lambda \in X$,

$$A^{(X)} = \bigoplus_{\lambda \in X} A_\lambda = \{(a_\lambda)_{\lambda \in X} : \text{apenas finitos } a_\lambda \neq 0\}.$$

Vejamos que $A^{(X)}$ é um módulo livre sobre X. A aplicação $j_X : X \to A^{(X)}$ é dada por $\lambda \mapsto e_\lambda$, onde $e_\lambda = (\delta_{\lambda,\mu} 1_A)_{\mu \in X}$ e $\delta_{\lambda,\mu}$ denota a função Delta de Kronecker.

Cada elemento a de $A^{(X)}$ se escreve de modo único como

$$a = \sum_{\lambda \in X} a_\lambda e_\lambda = \sum_{\lambda \in \mathrm{supp}(a)} a_\lambda e_\lambda,$$

o que mostra que o conjunto $B = \{e_\lambda\}_{\lambda \in X}$ é uma base de $A^{(X)}$ sobre A. Com isso podemos mostrar que a propriedade universal é satisfeita: dado um A-módulo M e uma função $f : X \to M$, podemos definir a aplicação $\widehat{f} : A^{(X)} \to M$ da seguinte forma: dado

$$a = \sum_{\lambda \in \mathrm{supp}(a)} a_\lambda e_\lambda$$

em $A^{(X)}$, tomamos

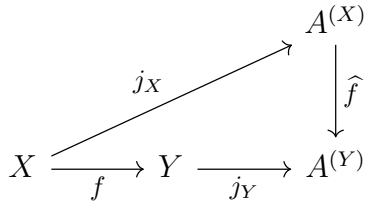
$$\widehat{f}(a) = \sum_{\lambda \in \mathrm{supp}(a)} a_\lambda f_\lambda.$$

Como B é uma base de $A^{(X)}$ a função $\widehat{f}$ está bem definida, pois a expressão para a em termos de elementos de B é única. Pode-se verificar que $\widehat{f}$ é A-linear, e também que é a única aplicação A-linear de $A^{(X)}$ em M tal que $\widehat{f} j_X = f$. ∎

Teorema 2.5.5. *Um módulo é livre se, e somente se, possui uma base.*

Observação 2.5.6. É fácil construir módulos que não são livres: como já visto, se I é um ideal de A então o A-módulo A/I não é livre, pois para cada $x+I$ em A/I e cada $a \in I$ tem-se que $a \cdot (x+I) = 0$. Portanto, se todos os módulos de um anel são livres é necessário que este anel não possua ideais não triviais. Quando A é um anel comutativo isso equivale a pedir que A seja um corpo. O caso não-comutativo é um pouco mais complicado, pois é preciso garantir que não existam ideais à esquerda. Isso é o que ocorre em *anéis de divisão*, isto é, anéis onde todo elemento não nulo admite inverso para o produto.

Observação 2.5.7. A construção do A-módulo livre $A^{(X)}$ fornece um funtor da categoria dos conjuntos na categoria dos A-módulos, que em objetos é dado por $X \mapsto A^{(X)}$, e em morfismos é definido da seguinte forma: se $f : X \to Y$ é uma função, então o morfismo $\widehat{f} : A^{(X)} \to A^{(Y)}$ é o único morfismo que completa o diagrama



Nas bases canônicas temos $\widehat{f}(e_x) = e_{f(x)} \in A^{(Y)}$.

2.6 Produto Tensorial

Para esta seção A denota uma k-álgebra, onde k é um anel comutativo.

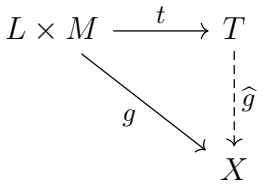
Sejam L_A e ${}_AM$ dois A-módulos. Uma aplicação g do k-módulo produto $L \times M$ em um k-módulo X é dita A-bilinear se

$$\begin{aligned} g(\alpha_1 x_1 + \alpha_2 x_2, y) &= \alpha_1 g(x_1, y) + \alpha_2 g(x_2, y), \\ g(x, \beta_1 y_1 + \beta_2 y_2) &= \beta_1 g(x, y_1) + \beta_2 g(x, y_2), \\ g(xa, y) &= g(x, ay), \end{aligned}$$

para todos $x, x_1, x_2 \in L$, $y, y_1, y_2 \in M$, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in k$ e $a \in A$.

Definição 2.6.1. Um *produto tensorial* de L_A e ${}_AM$ é um par (T, t), onde T é um k-módulo e $t : L \times M \to T$ é uma aplicação A-bilinear tal que, para todo par (X, g) onde X é um k-módulo e $g : L \times M \to X$ uma aplicação A-bilinear, existe uma única aplicação

k-linear $\widehat{g} : T \to X$, tal que $\widehat{g}t = g$.



Teorema 2.6.2. *Sejam L_A e ${}_AM$ dois A-módulos, então existe em* Mod k *um produto tensorial de L e M, único a menos de isomorfismo.*

Demonstração. Indicamos a existência desse k-módulo.

Seja $k^{(L\times M)}$ o k-módulo livre sobre o conjunto $L \times M$. Os elementos de $k^{(L\times M)}$ são combinações lineares da forma

$$\sum_{(x,y)\in L\times M} \alpha_{(x,y)}(x, y),$$

onde $x \in L$, $y \in M$ e $(\alpha_{(x,y)})_{(x,y)\in L\times M}$ é uma família de elementos de k, cujo suporte é finito.

Seja R o submódulo de $k^{(L\times M)}$ gerado pelos elementos da forma

$$\begin{gathered}(\alpha_1 x_1 + \alpha_2 x_2, y) - \alpha_1(x_1, y) - \alpha_2(x_2, y),\\ (x, \beta_1 y_1 + \beta_2 y_2) - \beta_1(x, y_1) - \beta_2(x, y_2),\\ (xa, y) - (x, ay),\end{gathered}$$

para todos $x, x_1, x_2 \in L$, $y, y_1, y_2 \in M$, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in k$ e $a \in A$. Definimos $T = k^{(L\times M)}/R$ e a aplicação t como a composição da inclusão $j : L \times M \to k^{(L\times M)}$ e a projeção $p : k^{(L\times M)} \to T$, canônicas.

Pela definição de R facilmente verifica-se que t é A-bilinear e também que o par (T, t) satisfaz a propriedade universal do produto tensorial. ■

Notação 2.6.3. O produto tensorial T de dois A-módulos L_A, ${}_AM$ é denotado por $L\otimes_A M$ ou, quando não há perigo de confusão, simplesmente por $L\otimes M$ e a classe de um elemento $(x, y) \in L \times M$ pela aplicação t, é denotada por $t(x, y) = x \otimes y$. Perceba que um elemento genérico de $L \otimes M$ é da forma

$$\sum_{\lambda\in\Lambda} \alpha_\lambda(x_\lambda \otimes y_\lambda),$$

onde $x_\lambda \in L$, $y_\lambda \in M$ e $(\alpha_\lambda)_{\lambda\in\Lambda}$ é uma família de elementos de k, cujo suporte é finito.

Construímos, de modo natural, o produto tensorial de duas aplicações A-lineares $f : L_A \to L'_A$ e $g : {}_AM \to {}_AM'$. Considere a aplicação

$$f \times g : L_A \times {}_AM \to L'_A \times {}_AM',$$

dada por

$$(f \times g)(x, y) = (f(x), g(y)).$$

Também definimos $t' : L' \times M' \to L' \otimes M'$ como a aplicação do tensor. Note que a composição $t'(f \times g)$ é uma aplicação A-bilinear. De fato, basta mostrar que respeita a compatibilidade, isto é,

$$\begin{aligned}(t'(f \times g))(ax, y) &= t'(f(ax), g(y)) \\ &= t'(af(x), g(y)) \\ &= t'(f(x), ag(y)) \\ &= t'(f(x), g(ay)) \\ &= (t'(f \times g))(x, ay).\end{aligned}$$

Portanto, pela propriedade universal do produto tensorial $L \otimes M$, existe uma única aplicação k-linear $f \otimes g : L \otimes M \to L' \otimes M'$ tornando o diagrama abaixo comutativo,

$$\begin{array}{ccc} L \times M & \xrightarrow{\quad t \quad} & L \otimes M \\ {\scriptstyle f \times g}\downarrow & & \downarrow{\scriptstyle f \otimes g} \\ L' \times M' & \xrightarrow[\quad t' \quad]{} & L' \otimes M' \end{array}$$

assim essa aplicação é dada por $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

A proposição a seguir demonstra que o produto tensorial de módulos é "comutativo" e "associativo".

Proposição 2.6.4. (1) *Seja A uma k-álgebra comutativa e L, M dois A-módulos. Então a aplicação k-linear*

$$\varphi : L \otimes_A M \to M \otimes_A L,$$

dada por

$$x \otimes y \mapsto y \otimes x,$$

é um isomorfismo de k-módulos.

(2) *Sejam A, B duas k-álgebras e $L_A, {}_AM_B, {}_BN$ três módulos. Então a aplicação*

$$\varphi : L \otimes_A (M \otimes_B N) \to (L \otimes_A M) \otimes_B N,$$

dada por

$$x \otimes_A (y \otimes_B z) \mapsto (x \otimes_A y) \otimes_B z,$$

é um isomorfismo de k-módulos.

Observação 2.6.5. Por construção o produto tensorial de dois módulos sobre uma k-álgebra é um *k-módulo*. Veremos que se os módulos possuem estruturas extras, o produto tensorial pode ser visto como um módulo sobre uma álgebra.

Sejam A, B e C três k-álgebras, ${}_BL_A$ um $(B-A)$-bimódulo e ${}_AL_C$ um $(A-C)$-bimódulo. Então o produto tensorial $L \otimes_A M$ possui uma estrutura natural de $(B-C)$-bimódulo, dada nos geradores por

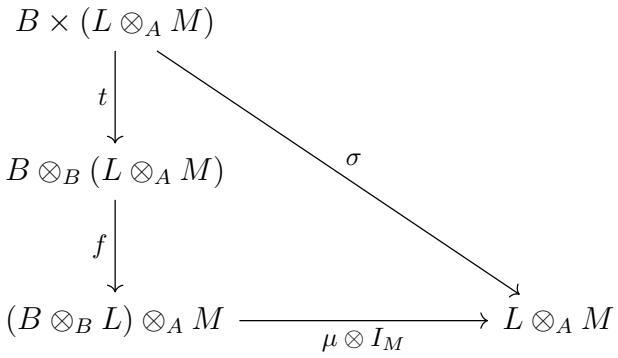
$$b \cdot (x \otimes y) \cdot c = (bx) \otimes (yc),$$

para todos $b \in B, x \in L, y \in M$ e $c \in C$.

Basta verificar que as aplicações definindo as novas estruturas de módulos estão bem definidas e que respeitam a soma em $L \otimes_A M$, visto que os outros axiomas são evidentemente satisfeitos. Além disso, abordamos apenas a estrutura de B-módulo à esquerda, o outro lado é análogo.

O B-módulo L pode ser visto como um k-módulo por $\lambda \cdot x \coloneqq (\lambda 1_B)x$ e então a multiplicação externa de B em L é uma aplicação k-bilinear, assim induz uma única aplicação k-linear $\mu : B \otimes_B L \to L$, dada por $\mu(b \otimes x) = bx$.

Agora considere o diagrama,



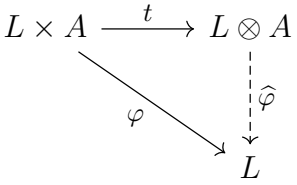
onde t é a aplicação do tensor, f é o isomorfismo da Proposição 2.6.4 e σ é a composição $\sigma = (\mu \otimes I_M) \circ f \circ t$, ou seja, $\sigma(b, x \otimes y) = (bx) \otimes y$. Portanto σ está bem definida e é linear em $L \otimes_A M$.

Teorema 2.6.6. *Seja A uma k-álgebra. Para todos A-módulos L_A e ${}_AM$ temos isomorfismos de A-módulos,*

$$L \otimes_A A \xrightarrow{\sim} L_A \quad e \quad A \otimes_A M \xrightarrow{\sim} {}_AM.$$

Demonstração. Denotando por $\varphi : L \times A \to A$ a aplicação A-bilinear definindo o módulo L, temos pela propriedade universal de $L \otimes A$ que existe uma única aplicação k-linear $\widehat{\varphi}$

tornando o diagrama abaixo comutativo.



Assim $\widehat{\varphi} : L \otimes A \to L$ é dada por $\widehat{\varphi}(x \otimes a) = xa$. Perceba que munindo $L \otimes A$ com a estrutura de A-módulo à direita (veja a Observação 2.6.5), $\widehat{\varphi}$ é claramente A-linear. Por outro lado definimos a aplicação A-linear $\psi : L \to L \otimes A$ por $\psi(x) = x \otimes 1$. É fácil ver que $\widehat{\varphi}$ e ψ são mutuamente inversas, o que conclui o isomorfismo.

O outro isomorfismo é realizado de maneira análoga. ■

O produto tensorial "respeita" somas diretas, como indica o teorema a seguir. Uma interpretação informal desse resultado é que há uma "propriedade distributiva" para produtos tensoriais, análoga a conhecida para números.

Teorema 2.6.7. *Sejam $(L_\lambda)_{\lambda\in\Lambda}$ uma família de A-módulos à direita e $(M_\sigma)_{\sigma\in\Sigma}$ uma família de A-módulos à esquerda. Então temos um isomorfismo de k-módulos,*

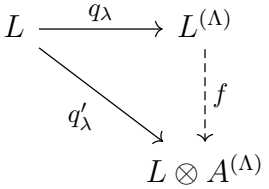
$$\left(\bigoplus_{\lambda\in\Lambda} L_\lambda\right) \bigotimes \left(\bigoplus_{\sigma\in\Sigma} M_\sigma\right) \xrightarrow{\sim} \bigoplus_{(\lambda,\sigma)\in\Lambda\times\Sigma} (L_\lambda \otimes M_\sigma).$$

Corolário 2.6.8. *Sejam L_A, ${}_AM$ dois A-módulos e Λ um conjunto. Temos isomorfismos de A-módulos,*

$$L \otimes_A A^{(\Lambda)} \xrightarrow{\sim} L_A^{(\Lambda)} \quad e \quad A^{(\Lambda)} \otimes_A M \xrightarrow{\sim} {}_AM^{(\Lambda)}.$$

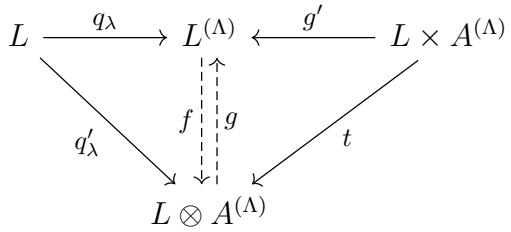
Demonstração. A demonstração desse resultado segue diretamente do teorema anterior, bastando notar que os isomorfismos acima também são A-lineares. Apresentamos outra solução, a partir da teoria desenvolvida nesse capítulo.

Sejam $(q_\lambda : L \to L^{(\Lambda)})_{\lambda\in\Lambda}$ as inclusões canônicas da soma direta e considere as aplicações $(q'_\lambda : L \to L \otimes A^{(\Lambda)})_{\lambda\in\Lambda}$ dadas por $q'_\lambda(x) = x \otimes e_\lambda$, onde $e_\lambda = (\delta_{\lambda,\mu}1_A)_{\mu\in\Lambda}$. As aplicações $(q'_\lambda)_{\lambda\in\Lambda}$ são evidentemente A-lineares, logo pela propriedade universal da soma direta $L^{(\Lambda)}$, induzem uma única aplicação A-linear $f : L^{(\Lambda)} \to L \otimes A^{(\Lambda)}$ tornando o diagrama comutativo,



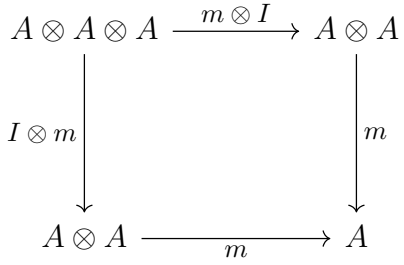
ou seja, $f((x_\lambda)_{\lambda\in\Lambda}) = \sum_{\lambda\in\Lambda} x_\lambda \otimes e_\lambda$ (perceba que essa soma é finita, pois $(x_\lambda)_{\lambda\in\Lambda}$ possui suporte finito).

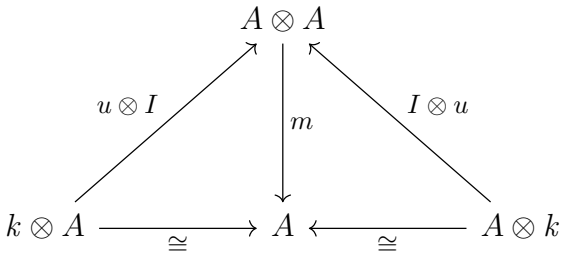
Por outro lado considere $L^{(\Lambda)}$ como um k-módulo. Definimos uma aplicação A-bilinear $g' : L \times A^{(\Lambda)} \to L^{(\Lambda)}$ por $g'(x, (a_\lambda)_{\lambda\in\Lambda}) = (xa_\lambda)_{\lambda\in\Lambda}$. Pela propriedade universal de $L \otimes A^{(\Lambda)}$ existe uma única aplicação k-linear $g : L \otimes A^{(\Lambda)} \to L^{(\Lambda)}$ completando o diagrama à direita,



logo g é dada por $g(x\otimes(a_\lambda)_{\lambda\in\Lambda}) = (xa_\lambda)_{\lambda\in\Lambda}$. Perceba que g também é A-linear e facilmente vemos que f e g são mutuamente inversas, o que conclui o isomorfismo. ■

Proposição 2.6.9. *A toda estrutura de k-álgebra estabelecida na Definição 2.2.1, isto é, um anel A junto de um homomorfismo de anéis $\phi : k \to A$ satisfazendo $\phi(\lambda)a = a\phi(\lambda)$, podemos associar uma tripla (A, m, u) onde A é um k-módulo e $m : A \otimes_k A \to A$, $u : k \to A$ são aplicações k-lineares satisfazendo os diagramas comutativos:*

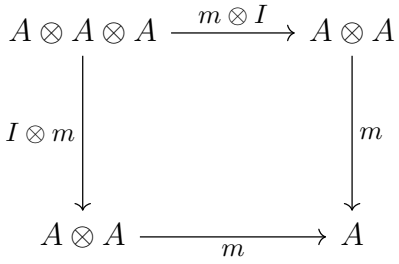




Reciprocamente, a cada tripla (A, m, u) satisfazendo os diagramas acima, podemos associar uma k-álgebra como na definição citada. Isso mostra que (A, m, u) é uma definição equivalente de álgebra.

Demonstração. Como na Observação 2.2.2 o anel A pode ser visto como um k-módulo por $\lambda \cdot a \coloneqq \phi(\lambda)a$, e assim a multiplicação interna do anel A é uma aplicação k-bilinear. Deste modo induz uma única aplicação k-linear $m : A\otimes A \to A$ por $m(a\otimes b) = ab$. Como

a multiplicação de A é associativa, temos o diagrama



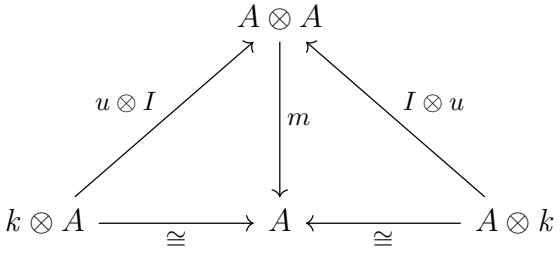
Para o segundo diagrama basta tomar $u = \phi$. De fato, denotando $\varphi_l : k \otimes A \to A$ e $\varphi_r : A \otimes k \to A$ os isomorfismos canônicos, temos

$$\begin{aligned}(m(u \otimes I))(\lambda \otimes a) &= m(u(\lambda) \otimes I(a)) \\ &= m(\phi(\lambda) \otimes a) \\ &= \phi(\lambda)a \\ &= \lambda \cdot a \\ &= \varphi_l(\lambda \otimes a),\end{aligned}$$

e analogamente

$$(m(I \otimes u))(a \otimes \lambda) = \varphi_r(a \otimes \lambda).$$

Portanto o diagrama



é comutativo.

Por outro lado, dada uma tripla (A, m, u) nas condições do enunciado basta definir $a \cdot b = m(a \otimes b)$ para o produto interno do anel A, cuja unidade é dada por $u(1_k)$, e $\phi = u$ para o homomorfismo de anéis da estrutura de k-álgebra. ■

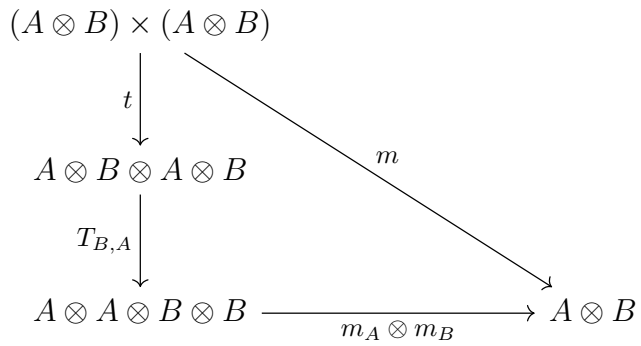
Teorema 2.6.10. *Sejam A, B duas k-álgebras. Então $A \otimes_k B$ é munido de uma estrutura natural de k-álgebra, dada por*

$$(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb').$$

Além disso, quando k é um corpo a k-álgebra $A \otimes_k B$ é comutativa se, e somente se, A e B são.

Demonstração. Vamos proceder mostrando que a operação está bem definida, visto que os axiomas são evidentemente satisfeitos.

Denote por $T_{B,A} : B \otimes A \to A \otimes B$ o isomorfismo de k-módulos da Proposição 2.6.4, ou seja, $T_{B,A}$ é dado por $T_{B,A}(b \otimes a) = a \otimes b$. A multiplicação da k-álgebra pode ser compreendida como a aplicação $m : (A \otimes B) \times (A \otimes B) \to A \otimes B$ dada pelo diagrama



onde $m_A : A \otimes A \to A$ e $m_B : B \otimes B \to B$ são as multiplicações de A e B, respectivamente. Portanto m é bem definida. ■

Exemplo 2.6.11. Sejam $A = \mathbb{K}[X_1, \ldots, X_n]$ e $B = \mathbb{K}[Y_1, \ldots, Y_m]$ duas álgebras de polinômios sobre $\mathbb{K}$. Vamos mostrar que o produto tensorial de A e B sobre $\mathbb{K}$ ainda é uma álgebra de polinômios, mais concretamente, existe um isomorfismo de $\mathbb{K}$-álgebras

$$A \otimes B \cong \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m].$$

Primeiramente note que a aplicação

$$\theta : A \times B \to \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m],$$

dada por

$$\theta(f, g) = fg,$$

é $\mathbb{K}$-bilinear. Deste modo θ induz uma única aplicação $\mathbb{K}$-linear

$$\widehat{\theta} : A \otimes B \to \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m],$$

dada por

$$\widehat{\theta}(f \otimes g) = fg.$$

A aplicação $\widehat{\theta}$ é um homomorfismo de $\mathbb{K}$-álgebras, pois

$$\begin{aligned}\widehat{\theta}((f\otimes g)(f'\otimes g')) &= \widehat{\theta}(ff'\otimes gg')\\ &= (ff')(gg')\\ &= (fg)(f'g')\\ &= \widehat{\theta}(f\otimes g)\widehat{\theta}(f'\otimes g').\end{aligned}$$

Agora definimos o homomorfismo de $\mathbb{K}$-álgebras

$$\varphi : \mathbb{K}[X_1,\ldots,X_n,Y_1,\ldots,Y_m]\to A\otimes B,$$

dado nos geradores por

$$\begin{aligned}X_i &\mapsto X_i\otimes 1,\\ Y_j &\mapsto 1\otimes Y_j.\end{aligned}$$

É fácil ver que $\widehat{\theta}$ e φ são mutuamente inversos.

Desenvolvemos um resultado análogo ao exemplo anterior na Proposição 3.9.1 (3).

Capítulo 3

Fundamentos de Geometria Algébrica

Esse capítulo é dedicado a construção de resultados básicos da teoria de geometria algébrica clássica. As principais referências são [19], [20] e [22]. No que segue $\mathbb{K}$ denota um corpo algebricamente fechado.

3.1 Integridade de anéis

Durante esta seção todos os anéis são comutativos.

Definição 3.1.1. Seja $A \subset B$ uma extensão de anéis, isto é, A é um subanel de B. Dizemos que $x \in B$ é *inteiro* sobre A se satisfaz uma equação polinomial com coeficientes em A e coeficiente líder 1, isto é, se existem um inteiro positivo m e elementos $a_{m-1}, \ldots, a_0 \in A$ tais que,

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = 0.$$

Definição 3.1.2. Seja $A \subset B$ uma extensão de anéis. Então B é *inteiro sobre* A se todo elemento de B é inteiro sobre A. O conjunto de elementos de B que são inteiros sobre A é chamado de *fecho inteiro*, ou *normalização* de A em B e denotado por $\tilde{A}$, ou ainda $\mathcal{F}(A, B)$.

Exemplos 3.1.3. Alguns exemplos de elementos inteiros e não inteiros.

(1) $\mathbb{Z}[1/3]$ não é inteiro sobre $\mathbb{Z}$, pois todo polinômio com coeficientes inteiros e coeficiente líder 1, avaliado em $1/3$, resulta em uma expressão da forma

$$\frac{1}{3^m} + a_{m-1}\frac{1}{3^{m-1}} + \cdots + a_0,$$

que se anula se, e somente se,

$$1 + 3a_{m-1} + \cdots + 3^m a_0 = 0,$$

isto é, se

$$1 = 3 \cdot r$$

para algum $r \in \mathbb{Z}$, o que é impossível pois o único invertível em $\mathbb{Z}$ é o 1.

Compare com o Exemplo 2.5.1; o $\mathbb{Z}$-módulo $\mathbb{Z}[1/3]$ não é finitamente gerado.

Por um raciocínio análogo mostra-se que dado um polinômio irredutível $f \in \mathbb{K}[X]$ a extensão $\mathbb{K}[X] \subset \mathbb{K}[X][1/f]$ não é inteira. Mais geralmente, se A é um DFU e $\operatorname{Frac} A$ é o seu corpo de frações, então todo elemento de $\operatorname{Frac} A \setminus A$ não é inteiro sobre A.

(2) $\mathbb{K}[X^2] \subset \mathbb{K}[X]$ é uma extensão inteira, pois X satisfaz a equação mônica $Y^2 - X^2 = 0$.

(3) A razão áurea $\phi = \frac{1+\sqrt{5}}{2}$ é um elemento inteiro sobre $\mathbb{Z}$, isto é, $\mathbb{Z} \subset \mathbb{Z}[\phi]$ é uma extensão inteira. De fato, ϕ satisfaz a relação $\phi^2 - \phi - 1 = 0$.

Proposição 3.1.4. *Seja $A \subset B$ uma extensão de anéis. São equivalentes:*

(1) *$x \in B$ é inteiro sobre A.*

(2) *$A \subset A[x]$ é uma extensão finita, isto é, $A[x]$ é um A-módulo finitamente gerado.*

Demonstração. Veja a Proposição 4.2 em [20]. ■

Observação 3.1.5. Note que do resultado anterior concluímos que toda extensão finita $A \subset B$ de anéis também é inteira.

Definição 3.1.6. Um domínio de integridade A é dito *integralmente fechado* ou *normal*, se $A = \mathcal{F}(A, \operatorname{Frac} A)$, isto é, se o fecho inteiro de A sobre seu anel de frações coincide com o próprio A.

Exemplos 3.1.7. Seja $A = \mathbb{K}[X, Y]/(f)$, onde f é um polinômio irredutível de $\mathbb{K}[X, Y]$. Perceba que A é um domínio de integridade, pois (f) é um ideal primo. Denotamos $x = X + (f)$ e $y = Y + (f)$ para as classes de X e Y. Veremos um exemplo onde A é normal e outro onde não é.

(1) Se $f(X, Y) = Y^2 - X^2 - X^3$ então A não é normal. De fato, o elemento $t = y/x \in \operatorname{Frac} A$ é inteiro sobre A, pois satisfaz a relação $t^2 - x - 1 = 0$, então $A[t] \subset \tilde{A}$. Entretanto $t \notin A$: se $t = h(x, y)$ então $y = xh(x, y)$, o que ocorre se, e somente se, $Y - Xh(X, Y) \in (Y^2 - X^2 - X^3)$, ou seja, deveríamos ter $Y - Xh(X, Y) = g(X, Y)(Y^2 - X^2 - X^3)$ para algum polinômio $g(X, Y) \in \mathbb{K}[X, Y]$. Agora notamos que o lado direito da equação pode possuir monômios em Y somente com grau maior ou igual a 2, entretando do lado esquerdo possui o termo Y com grau 1, dessa forma $Y - Xh(X, Y) \notin (Y^2 - X^2 - X^3)$.

(2) Se $f(X, Y) = Y^2 - X$ então mostra-se que A é integralmente fechado.

A proposição a seguir explora algumas propriedades essenciais das extensões inteiras (veja [20], Seção 4.3).

Proposição 3.1.8. *Sejam $A \subset B \subset C$ extensões de anéis.*

(1) *O fecho inteiro $\mathcal{F}(A, B)$ é um anel.*

(2) *Se C é uma B-álgebra finitamente gerada e B uma A-álgebra finitamente gerada, então C é uma A-álgebra finitamente gerada.*

(3) *Se C é inteiro sobre B e B inteiro sobre A, então C é inteiro sobre A.*

3.2 Anéis noetherianos

Nesta seção exploramos algumas boas propriedades dos anéis noetherianos, em particular notamos que os anéis de polinômios sobre um corpo $\mathbb{K}$ são noetherianos.

Definição 3.2.1. Um anel A satisfazendo as seguintes propriedades equivalentes é chamado *noetheriano*.

(i) Toda cadeia de ideais $I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$ de A estabiliza, ou seja, existe um inteiro positivo m tal que, se $n > m$ então $I_n = I_m$.

(ii) Todo conjunto de ideais de A possui elemento maximal.

(iii) Todo ideal de A é finitamente gerado.

A seguir temos alguns exemplos de anéis noetherianos.

Exemplo 3.2.2. (1) Todo corpo é um anel noetheriano, visto que seus únicos ideais $(0_{\mathbb{K}})$ e $\mathbb{K}$, são finitamente gerados.

(2) Todo domínio de ideais principais é noetheriano, pois todo ideal é gerado por um único elemento.

(3) Pelo item anterior o anel dos inteiros $\mathbb{Z}$ é noetheriano.

A propriedade de um anel ser noetheriano é preservada por quocientes, isto é,

Proposição 3.2.3. *Seja A um anel noetheriano e I um ideal de A, então o anel quociente A/I é noetheriano.*

Demonstração. Pelo Teorema da correspondência para ideais de um anel, temos que uma cadeia

$$\overline{I}_1 \subset \overline{I}_2 \subset \cdots \subset \overline{I}_k \subset \cdots$$

de ideais de A/I corresponde a uma cadeia

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$

de ideais de A tais que I_n contém I, para todo n. Como A é noetheriano a cadeia acima estabiliza, isto é, existe um inteiro positivo m tal que, se $n > m$ então $I_n = I_m$. Agora como essa correspondência preserva ordem, segue que $\overline{I}_n = \overline{I}_m$, para todo $n > m$. ■

O próximo resultado garante que a condição de um anel A ser noetheriano é preservada ao tomar o anel de polinômios em uma indeterminada com coeficientes em A.

Teorema 3.2.4 (da Base de Hilbert)**.** *Se A é noetheriano então o anel de polinômios $A[X]$ e o anel das séries formais $A[[X]]$ também são noetherianos.*

Demonstração. Veja [20], Teorema 3.6. ■

Procedendo por indução no teorema anterior obtemos o seguinte resultado.

Corolário 3.2.5. *Se A é um anel noetheriano, então $A[X_1, \ldots, X_n]$ também é noetheriano. Em particular, se $\mathbb{K}$ é corpo então $\mathbb{K}[X_1, \ldots, X_n]$ é noetheriano.*

Será útil para a Seção 3.9 o seguinte lema:

Lema 3.2.6. *Sejam A um anel noetheriano e $I \subset J$ ideais de A. Se $A/I \cong A/J$, então $I = J$.*

Demonstração. Supondo por contradição $I \subsetneq J$, mostramos a existência de uma cadeia ascendente infinita de ideais de A.

Denote $L_0 = I$ e $L_1 = J$, então $L_0 \subsetneq L_1$ e $A/L_0 \cong A/L_1$. Suponha que para $n = k$ existem ideais L_k, L_{k+1} de A, tais que $L_k \subsetneq L_{k+1}$ e $A/L_k \cong A/L_{k+1}$. Pelo isomorfismo anterior temos que o ideal não trivial L_{k+1}/L_k corresponde a um ideal $L_{k+2}/L_{k+1} \subset A/L_{k+1}$, onde L_{k+2} é um ideal de A com $L_{k+1} \subsetneq L_{k+2}$.

Agora pelo terceiro Teorema do isomorfismo para anéis temos,

$$\frac{A}{L_{k+1}} \cong \frac{(A/L_k)}{(L_{k+1}/L_k)} \overset{(*)}{\cong} \frac{(A/L_{k+1})}{(L_{k+2}/L_{k+1})} \cong \frac{A}{L_{k+2}},$$

onde $(*)$ é obtido por extensão do isomorfismo $\varphi : A/L_k \xrightarrow{\sim} A/L_{k+1}$, isto é, definindo $\overline{\varphi} : A/L_k \xrightarrow{\sim} (A/L_{k+1})/(L_{k+2}/L_{k+1})$ por $\overline{\varphi}(\overline{a}) = \varphi(\overline{a}) + (L_{k+2}/L_{k+1})$, mostra-se que $\operatorname{Ker}\overline{\varphi} = L_{k+1}/L_k$. De fato,

$$\begin{aligned} \overline{a} \in \operatorname{Ker}\overline{\varphi} &\Leftrightarrow \overline{\varphi}(\overline{a}) = \overline{0} + L_{k+2}/L_{k+1} \\ &\Leftrightarrow \varphi(\overline{a}) \in L_{k+2}/L_{k+1} \\ &\Leftrightarrow \overline{a} \in L_{k+1}/L_k. \end{aligned}$$

Assim a indução mostra que a cadeia ascendente de ideais

$$L_0 \subset L_1 \subset \cdots \subset L_k \subset \cdots$$

não estabiliza, o que é uma contradição no fato de A ser noetheriano. ■

3.3 Normalização de Noether

Como resultado principal demonstramos, a partir de dois lemas auxiliares, o *Lema de normalização de Noether*, que é essencial na demonstração do *Nullstellensatz Fraco* (Teorema 3.3.6) e, por consequência, essencial para o *Nullstellensatz* (Teorema 3.4.6).

Definição 3.3.1. Sejam $\mathbb{K}$ um corpo e A uma $\mathbb{K}$-álgebra. Dizemos que os elementos $y_1, \ldots, y_n \in A$ são *algebricamente independentes* sobre $\mathbb{K}$ se a sobrejeção natural

$$\varphi : \mathbb{K}[Y_1, \ldots, Y_n] \twoheadrightarrow \mathbb{K}[y_1, \ldots, y_n]$$

é um isomorfismo. Ou seja, não existem relações polinomiais com coeficientes em $\mathbb{K}$ tais que

$$F(y_1, \ldots, y_n) = 0.$$

Os dois próximos lemas são utilizados na demonstração do Teorema 3.3.4.

Lema 3.3.2. *Dado um conjunto finito $Y = \{Y_1^{m_1} \cdots Y_n^{m_n}\}$ de monômios em $Y_1, \ldots, Y_n$, existe um sistema de inteiros positivos $r_1, \ldots, r_{n-1}, r_n = 1$, chamados pesos, tais que o peso de um monômio*

$$\rho(Y_1^{m_1} \cdots Y_n^{m_n}) \coloneqq \sum_{i=1}^{n} r_i m_i$$

distingue o monômio, ou seja,

$$(m_1, \ldots, m_n) \neq (m_1', \ldots, m_n') \Rightarrow \rho(Y_1^{m_1} \cdots Y_n^{m_n}) \neq \rho(Y_1^{m_1'} \cdots Y_n^{m_n'}).$$

Demonstração. Usaremos indução no número de variáveis. Para $n = 1$ é evidente, basta tomar $r_1 = 1$. Para $n = 2$ temos $Y = \{Y_1^{m_1} Y_2^{m_2}\}$, assim escolhemos $r_2 = 1$ e $r_1 > \max\{m_2 : Y_1^{m_1} Y_2^{m_2} \in Y, \text{ para algum } m_1\}$. Suponha por contradição que existam $(m_1, m_2) \neq (m_1', m_2')$ tais que $\rho(Y_1^{m_1} Y_2^{m_2}) = \rho(Y_1^{m_1'} Y_2^{m_2'})$, isto é

$$r_1 m_1 + m_2 = r_1 m_1' + m_2'.$$

Se $m_2' = m_2$ não há o que provar, logo podemos supor, sem perda de generalidade, que $m_2' > m_2$. Assim temos

$$r_1(m_1 - m_1') = m_2' - m_2 > 0,$$

logo segue que $m_1 - m_1' > 0$ e então

$$r_1 \leq r_1(m_1 - m_1') = m_2' - m_2 < m_2'$$

é uma contradição na escolha de r_1.

Suponha válido para $n = k - 1$ variáveis. Dado um conjunto finito de monômios $Y = \{Y_1^{m_1} \cdots Y_k^{m_k}\}$, escrevemos todo elemento de Y como $Y_1^{m_1}(Y_2^{m_2} \cdots Y_k^{m_k})$, onde $Y_2^{m_2} \cdots Y_k^{m_k}$ pertence a um conjunto finito Y'.

Pela hipótese de indução existem inteiros positivos $r_2, \ldots, r_{k-1}, r_k = 1$ tais que

$$(m_2, \ldots, m_k) \neq (m_2', \ldots, m_k') \Rightarrow \rho(Y_2^{m_2} \cdots Y_k^{m_k}) \neq \rho(Y_2^{m_2'} \cdots Y_k^{m_k'}).$$

Agora escolha $r_1 > \max\{\rho(Y_2^{m_2} \cdots Y_k^{m_k}) = \sum_{i=2}^k r_i m_i : Y_2^{m_2} \cdots Y_k^{m_k} \in Y'\}$. Suponha por contradição que existam $(m_1, \ldots, m_n) \neq (m_1', \ldots, m_n')$ tais que

$$\begin{aligned} &\rho(Y_1^{m_1} \cdots Y_n^{m_n}) = \rho(Y_1^{m_1'} \cdots Y_n^{m_n'}) \\ \Rightarrow\ & r_1 m_1 + \sum_{i=2}^k r_i m_i = r_1 m_1' + \sum_{i=2}^k r_i m_i'. \end{aligned}$$

Se $\sum_{i=2}^k r_i m_i = \sum_{i=2}^k r_i m_i'$ não há o que provar, então suponha, sem perda de generalidade, que $\sum_{i=2}^k r_i m_i < \sum_{i=2}^k r_i m_i'$. Assim

$$r_1 \leq r_1(m_1 - m_1') = \sum_{i=2}^k r_i m_i' - \sum_{i=2}^k r_i m_i < \sum_{i=2}^k r_i m_i'$$

gera uma contradição na maximalidade de r_1, o que completa a indução. ■

Lema 3.3.3. *Suponha que $A = \mathbb{K}[y_1, \ldots, y_n]$ e que $0 \neq F \in \mathbb{K}[Y_1, \ldots, Y_n]$ é tal que $F(y_1, \ldots, y_n) = 0$. Então existem $y_1^*, \ldots, y_{n-1}^* \in A$ tais que y_n é inteiro sobre $A^* = \mathbb{K}[y_1^*, \ldots, y_{n-1}^*]$ e $A = A^*[y_n]$.*

Demonstração. Definimos novas variáveis Y_i^*, para $i < n$, como

$$Y_i^* = Y_i - Y_n^{r_i},$$

onde $r_i \in \mathbb{Z}$ são inteiros positivos a serem escolhidos mais adiante. Também definimos um polinômio $G \in \mathbb{K}[Y_1^*, \ldots, Y_{n-1}^*, Y_n]$ como

$$G(Y_1^*, \ldots, Y_{n-1}^*, Y_n) = F(Y_1^* + Y_n^{r_1}, \ldots, Y_{n-1}^* + Y_n^{r_{n-1}}, Y_n). \tag{3.1}$$

Note que pela Equação (3.1), ao avaliar F em $y_1, \ldots, y_n$ obtemos uma relação polinomial $G(y_1^*, \ldots, y_{n-1}^*, y_n) = 0$, onde $y_i^* = y_i - y_n^{r_i}$, para $i < n$. Vamos proceder

mostrando que esta equação dá origem a uma relação mônica em y_n para uma escolha conveniente de $r_1, \ldots, r_{n-1}$.

Como $F \in \mathbb{K}[Y_1, \ldots, Y_n]$ escrevemos:

$$F(Y_1, \ldots, Y_n) = \sum_{m_1,\ldots,m_n} a_{m_1,\ldots,m_n} \prod_{i=1}^{n} Y_i^{m_i},$$

onde todo coeficiente $a_{m_1,\ldots,m_n}$ é não nulo. Assim,

$$G(Y_1^*, \ldots, Y_{n-1}^*, Y_n) = \sum_{m_1,\ldots,m_n} a_{m_1,\ldots,m_n} \prod_{i=1}^{n-1} (Y_i^* + Y_n^{r_i})^{m_i} Y_n^{m_n}.$$

Ao expandir a expressão acima, temos que cada termo

$$a_{m_1,\ldots,m_n} \prod_{i=1}^{n-1} (Y_i^* + Y_n^{r_i})^{m_i} Y_n^{m_n}$$

presente na soma, possui um monômio de maior grau em Y_n, isto é, um monômio da forma

$$a_{m_1,\ldots,m_n} Y_n^{\sum_{i=1}^{n-1} r_i m_i + m_n}.$$

Agora pelo Lema 3.3.2, existem inteiros positivos $r_1, \ldots, r_{n-1}, r_n = 1$ tais que,

$$(m_1, \ldots, m_n) \neq (m_1', \ldots, m_n') \Rightarrow \sum_{i=1}^{n} r_i m_i \neq \sum_{i=1}^{n} r_i m_i'.$$

Então,

$$M = \sum_{i=1}^{n} r_i \overline{m}_i = \max\{\sum_{i=1}^{n} r_i m_i : a_{m_1,\ldots,m_n} Y_n^{\sum r_i m_i} \text{ é um termo de } G\}$$

é a maior potência de Y_n e só aparece uma vez, logo não pode haver cancelamentos e o termo de maior ordem em Y_n ocorrendo em G é $a_{\overline{m}_1,\ldots,\overline{m}_n} Y_n^M$. Portanto podemos escrever G como

$$G(Y_1^*, \ldots, Y_{n-1}^*, Y_n) = a_{\overline{m}_1,\ldots,\overline{m}_n} \cdot H,$$

com $H \in \mathbb{K}[Y_1^*, \ldots, Y_{n-1}^*][Y_n]$ da forma

$$H = \sum_{k=0}^{M} b_k(Y_1^*, \ldots, Y_{n-1}^*) Y_n^k.$$

Por fim definimos o polinômio $h \in A^*[Y_n]$, advindo de uma "avaliação parcial" do

polinômio H em $y_1^*, \ldots, y_{n-1}^*$, isto é

$$h(Y_n) = \sum_{k=0}^{M} b_k(y_1^*, \ldots, y_{n-1}^*) Y_n^k.$$

Assim,

$$\begin{aligned} h(y_n) &= \sum_{k=0}^{M} b_k(y_1^*, \ldots, y_{n-1}^*) y_n^k \\ &= H(y_1^*, \ldots, y_{n-1}^*, y_n) \\ &= \frac{1}{a_{\overline{m}_1,\ldots,\overline{m}_n}} G(y_1^*, \ldots, y_{n-1}^*, y_n) \\ &= 0, \end{aligned}$$

o que implica y_n inteiro em A^* e, por construção, $A = A^*[y_n]$. ■

Teorema 3.3.4 (Lema de Normalização de Noether)**.** *Sejam $\mathbb{K}$ um corpo e A uma $\mathbb{K}$-álgebra finitamente gerada, então existem elementos $z_1, \ldots, z_m \in A$ tais que,*

(i) *$z_1, \ldots, z_m$ são algebricamente independentes sobre $\mathbb{K}$.*

(ii) *A é um B-módulo finitamente gerado, onde $B = \mathbb{K}[z_1, \ldots, z_m]$. Ou seja, toda extensão finita $A \supset \mathbb{K}$ pode ser escrita como*

$$\mathbb{K} \subset B \subset A.$$

Demonstração. Vamos proceder por indução no número de geradores de A. Se $n = 0$ não há o que mostrar. Se $n > 0$ e os geradores $y_1, \ldots, y_n$ são algebricamente independentes sobre $\mathbb{K}$, novamente não há o que mostrar. Suponha $y_1, \ldots, y_n$ algebricamente dependentes sobre $\mathbb{K}$, e tome um polinômio não nulo $F \in \mathbb{K}[Y_1, \ldots, Y_n]$ tal que $F(y_1, \ldots, y_n) = 0$. Então pelo Lema 3.3.3 existem $y_1^*, \ldots, y_{n-1}^* \in A$ tais que y_n é inteiro sobre $A^* = \mathbb{K}[y_1^*, \ldots, y_{n-1}^*]$ e $A = A^*[y_n]$.

Agora, aplicando a hipótese de indução em A^*, temos que existem elementos $z_1, \ldots, z_m \in A^*$ que são algebricamente independentes sobre $\mathbb{K}$ e com A^* finito sobre $B = \mathbb{K}[z_1, \ldots, z_m]$. Por fim basta notar que, como y_n é inteiro sobre A^*, pela Proposição 3.1.4 a extensão $A^* \subset A^*[y_n]$ é finita, e portanto as extensões de anéis

$$B \subset A^* \subset A^*[y_n] = A$$

são finitas. ■

3.3.1 Nullstellensatz Fraco

Proposição 3.3.5. *Seja $A \subset B$ uma extensão inteira de um domínio de integridade. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração. ($\Rightarrow$) Se $x \in B$ é não nulo, então existe uma relação mônica

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

com $a_i \in A$ e podemos supor $a_0 \neq 0$. Como A é corpo, $a_0^{-1} \in A$, logo

$$\begin{aligned} & x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) + a_0 = 0 \\ \Rightarrow & -a_0^{-1}(x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)) - a_0^{-1}a_0 = 0 \\ \Rightarrow & x(-a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)) = 1 \\ \Rightarrow & x^{-1} = -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in B, \end{aligned}$$

e portanto B é corpo.
($\Leftarrow$) Seja $0 \neq x \in A$. Como B é corpo, então $x^{-1} \in B$ e assim satisfaz uma relação inteira sobre A

$$(x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \cdots + a_0 = 0.$$

Multiplicando ambos os lados da equação anterior por x^{n-1}, obtemos

$$\begin{aligned} & x^{n-1}((x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \cdots + a_0) = 0 \\ \Rightarrow & x^{-1} + a_{n-1} + \cdots + a_0x^{n-1} = 0 \\ \Rightarrow & x^{-1} = -a_{n-1} - \cdots - a_0x^{n-1} \in A, \end{aligned}$$

o que implica A ser corpo. ■

Teorema 3.3.6 (Nullstellensatz Fraco)**.** *Sejam $\mathbb{K}$ um corpo e $\mathbb{L}$ uma $\mathbb{K}$-álgebra finitamente gerada que também é um corpo. Então a extensão de corpos $\mathbb{K} \subset \mathbb{L}$ é uma extensão finita.*

Demonstração. Suponha que a extensão $\mathbb{K} \subset \mathbb{L}$ não seja finita. Pelo Lema de Normalização de Noether (Teorema 3.3.4), existem elementos $z_1, \ldots, z_m \in \mathbb{L}$ que são algebricamente independentes sobre $\mathbb{K}$ e $A = \mathbb{K}[z_1, \ldots, z_m] \subset \mathbb{L}$ é uma extensão finita. Sabemos da Proposição 3.1.4 que toda extensão finita é inteira, logo pela Proposição 3.3.5 como $\mathbb{L}$ é corpo, A também deve ser. Agora note que o ideal $(z_1, \ldots, z_n)$ de $A = \mathbb{K}[z_1, \ldots, z_m]$ é não trivial, o que é uma contradição no fato de A ser corpo. Assim, $A = \mathbb{K}$ e a extensão de corpos $\mathbb{K} \subset \mathbb{L}$ é finita. ■

Como consequência do teorema acima temos o seguinte resultado, que caracteriza os ideais maximais de $\mathbb{K}[X_1, \ldots, X_n]$.

Corolário 3.3.7. *Suponha $\mathbb{K}$ algebricamente fechado. Então todo ideal maximal de $A = \mathbb{K}[X_1, \ldots, X_n]$ é da forma*

$$m = (X_1 - a_1, \ldots, X_n - a_n),$$

para algum $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$.

Demonstração. Seja $m \in A$ um ideal maximal e denote $B = A/m$. Considere o homomorfismo de $\mathbb{K}$-álgebras

$$\varphi : \mathbb{K} \to B,$$

dado pela composição da projeção canônica $\pi : A \to B$ e da inclusão $j : \mathbb{K} \to A$, ou seja, $\varphi = \pi \circ j$. Como m é maximal segue que B é corpo, mais ainda, é uma $\mathbb{K}$-álgebra finitamente gerada (pelos elementos $X_i + m$).

Pelo Nullstellensatz Fraco (Teorema 3.3.6) a extensão $\mathbb{K} \subset B$ é finita, em particular é uma extensão algébrica. Agora como $\mathbb{K}$ é um corpo algebricamente fechado isso implica que φ é um isomorfismo.

Escreva $b_i = \pi(X_i) \in B$. Como φ é isomorfismo existe um único $a_i \in \mathbb{K}$ tal que $\varphi(a_i) = b_i$, portanto $\pi(a_i) = b_i$, ou seja, $X_i - a_i \in \operatorname{Ker} \pi = m$. Deste modo existem únicos escalares $a_1, \ldots, a_n \in \mathbb{K}$ tais que $(X_1 - a_1, \ldots, X_n - a_n) \subset m$. Para a inclusão contrária basta notar que $(X_1 - a_1, \ldots, X_n - a_n)$ é um ideal maximal. De fato, considere o homomorfismo sobrejetor de anéis $\theta : A \to \mathbb{K}$, dado pela avaliação em $(a_1, \ldots, a_n)$, isto é

$$\theta(f) = f(a_1, \ldots, a_n).$$

Pode-se mostrar que $\operatorname{Ker} \theta = (X_1 - a_1, \ldots, X_n - a_n)$ e então pelo Teorema do isomorfismo para anéis temos

$$\frac{A}{(X_1 - a_1, \ldots, X_n - a_n)} \cong \mathbb{K},$$

o que implica $(X_1 - a_1, \ldots, X_n - a_n)$ maximal. ∎

3.4 Variedades algébricas afins

Nesta seção vamos definir formalmente o conceito de variedade algébrica em um *espaço afim* (veja a Definição 1.1.1).

Seja $\mathcal{V}$ a função entre a família de subconjuntos de $\mathbb{K}[X_1, \ldots, X_n]$ e a família de subconjuntos de $\mathbb{A}^n$, dada por

$$\mathcal{V}(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n : f(a_1, \ldots, a_n) = 0, \forall\ f \in S\}.$$

Perceba que o subconjunto $S \subset \mathbb{K}[X_1, \ldots, X_n]$ e o ideal gerado por ele (S) em $\mathbb{K}[X_1, \ldots, X_n]$, possuem a mesma imagem pela aplicação $\mathcal{V}$. De fato, por um lado $S \subset (S)$, logo

$$\begin{aligned} a \in \mathcal{V}((S)) &\Rightarrow f(a) = 0, \forall\ f \in (S) \\ &\Rightarrow f(a) = 0, \forall\ f \in S \\ &\Rightarrow a \in \mathcal{V}(S). \end{aligned}$$

Por outro lado,

$$\begin{aligned} a \in \mathcal{V}(S) &\Rightarrow f(a) = 0, \forall\ f \in S \\ &\Rightarrow g(a)f(a) = 0, \forall\ g \in \mathbb{K}[X_1, \ldots, X_n], f \in S \\ &\Rightarrow h(a) = 0, \forall\ h \in (S) \\ &\Rightarrow a \in \mathcal{V}((S)). \end{aligned}$$

Deste modo definimos o conceito de variedade algébrica afim.

Definição 3.4.1. Um conjunto $X \subset \mathbb{A}^n$ é chamado de *variedade algébrica afim*, ou somente *variedade afim*, se $X = \mathcal{V}(I)$ para algum ideal I de $\mathbb{K}[X_1, \ldots, X_n]$. De modo natural, um subconjunto $Y \subset X$ é dito uma *subvariedade* de X se existe um ideal J de $\mathbb{K}[X_1, \ldots, X_n]$ tal que $Y = \mathcal{V}(J)$.

Notação 3.4.2. Note que, como os anéis de polinômios sobre $\mathbb{K}$ são noetherianos, todo ideal $I \subset \mathbb{K}[X_1, \ldots, X_n]$ é finitamente gerado, logo dada uma variedade $\mathcal{V}(I) \subset \mathbb{A}^n$, existem polinômios $f_1, \ldots, f_r \in \mathbb{K}[X_1, \ldots, X_n]$ tais que

$$\mathcal{V}(I) = \mathcal{V}((f_1, \ldots, f_r)).$$

Para evitar parênteses duplos, convencionamos a notação

$$\mathcal{V}(f_1, \ldots, f_r) \coloneqq \mathcal{V}((f_1, \ldots, f_r)).$$

Observação 3.4.3. O conceito de variedade algébrica pode ser abstraído, no sentido em que elimina-se a dependência entre o conjunto definindo a variedade e o espaço afim (veja a Definição 1.4.17 em [22]). Neste texto o termo *variedade afim*, ou simplesmente *variedade*, sempre denotará um subconjunto de $\mathbb{A}^n$, para algum inteiro positivo n, cujos pontos satisfazem um sistema finito de equações polinomiais.

Agora fazemos uma construção no sentido contrário, isto é, a cada subconjunto de $\mathbb{A}^n$ associamos um ideal de $\mathbb{K}[X_1, \ldots, X_n]$.

Dado $X \subset \mathbb{A}^n$ considere o subconjunto

$$\mathcal{I}(X) = \{f \in \mathbb{K}[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0, \forall\ (a_1, \ldots, a_n) \in X\}$$

de $\mathbb{K}[X_1, \ldots, X_n]$. É facil ver que $\mathcal{I}(X)$ é um ideal de $\mathbb{K}[X_1, \ldots, X_n]$.

Enunciamos sem demonstração algumas propriedades das aplicações $\mathcal{V}$ e $\mathcal{I}$ (veja [22], Lema 3.4).

Proposição 3.4.4. *As aplicações $\mathcal{V}, \mathcal{I}$ satisfazem:*

(1) $X \subset \mathcal{V}(\mathcal{I}(X))$, *para todo subconjunto* $X \in \mathbb{A}^n$.

(2) $I \subset \mathcal{I}(\mathcal{V}(I))$, *para todo ideal* I *de* $\mathbb{K}[X_1, \ldots, X_n]$.

(3) *Se* $S \subset T \subset \mathbb{K}[X_1, \ldots, X_n]$, *então* $\mathcal{V}(T) \subset \mathcal{V}(S)$.

(4) *Se* $X \subset Y \subset \mathbb{A}^n$, *então* $\mathcal{I}(Y) \subset \mathcal{I}(X)$.

(5) *Se* $I, J \subset \mathbb{K}[X_1, \ldots, X_n]$ *são ideais, então*

$$\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J).$$

(6) *Se* $\{I_\lambda\}_{\lambda \in \Lambda}$ *é uma família de ideais de* $\mathbb{K}[X_1, \ldots, X_n]$, *então*

$$\bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda) = \mathcal{V}\left(\sum_{\lambda \in \Lambda} I_\lambda\right).$$

Observação 3.4.5. Quando X é uma variedade algébrica, digamos $X = \mathcal{V}(J)$ para algum ideal J de $\mathbb{K}[X_1, \ldots, X_n]$, obtemos a igualdade $X = \mathcal{V}(I(X))$, ou ainda, $\mathcal{V}(J) = \mathcal{V}(\mathcal{I}(\mathcal{V}(J)))$. De fato, por (1) basta mostrar que $\mathcal{V}(\mathcal{I}(\mathcal{V}(J))) \subset \mathcal{V}(J)$. Se $a \in \mathcal{V}(\mathcal{I}(\mathcal{V}(J)))$ então $f(a) = 0$, para todo $f \in \mathcal{I}(\mathcal{V}(J))$ e por (2) $J \subset \mathcal{I}(\mathcal{V}(J))$, logo temos em particular $f(a) = 0$, para todo $f \in J$, assim $a \in X = \mathcal{V}(J)$.

A inclusão $I \subset \mathcal{I}(\mathcal{V}(I))$ nem sempre é uma igualdade. Tome, por exemplo, o ideal $I = (X^2) \subset \mathbb{K}[X]$. Então $V(I) = \{a \in \mathbb{K} : X^2(a) = 0\} = \{0\}$, logo

$$\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\{0\}) = (X) \not\subset (X^2).$$

O *Teorema dos zeros de Hilbert*, mais conhecido como *Nullstellensatz*, garante que a inclusão contrária é verdadeira sempre que o ideal I de $\mathbb{K}[X_1, \ldots, X_n]$ é radical, isto é, se

$$I = \operatorname{rad} I = \{f \in \mathbb{K}[X_1, \ldots, X_n] : f^n \in I, \text{ para algum } n \in \mathbb{Z}^+\}.$$

Teorema 3.4.6 (Nullstellensatz)**.** *Seja* $\mathbb{K}$ *um corpo algebricamente fechado e* I *um ideal de* $\mathbb{K}[X_1, \ldots, X_n]$.

(1) *Se* $I \subsetneq \mathbb{K}[X_1, \ldots, X_n]$, *então* $\mathcal{V}(I) \neq \varnothing$.

(2) $\mathcal{I}(\mathcal{V}(I)) = \operatorname{rad} I$.

Demonstração. Vamos demonstrar apenas o item (1), para mais detalhes consulte, por exemplo, a Seção 5.6 de [20].
(1) Se $I \subsetneq \mathbb{K}[X_1, \ldots, X_n]$ é um ideal próprio, ou é maximal ou está contido em um ideal maximal. Agora pelo Corolário 3.3.7 todo ideal maximal é da forma $m = (X_1 - a_1, \ldots, X_n - a_n)$, logo em ambos os casos temos $\mathcal{V}(m) \subset \mathcal{V}(I)$, ou seja, $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. ■

3.5 Topologia de Zariski

O espaço afim $\mathbb{A}^n$ pode ser munido de uma topologia, conhecida como topologia de Zariski, cujos conjuntos fechados são variedades. De fato,

(i) $\varnothing = \mathcal{V}(1)$ e $\mathbb{A}^n = \mathcal{V}(0)$ são variedades.

(ii) Pela Proposição 3.4.4, item (5), a união de duas variedades ainda é um variedade, onde
$$\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J).$$

(iii) Novamente pela Proposição 3.4.4, item (6), temos que se $\{X_\lambda\}_{\lambda \in \Lambda}$ é uma família de variedades, dada por uma família de ideais $\{I_\lambda\}_{\lambda \in \Lambda} \subset \mathbb{K}[X_1, \ldots, X_n]$, então a interseção desta família ainda é uma variedade,
$$\bigcap_{\lambda \in \Lambda} X_\lambda = \bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda) = \mathcal{V}\left(\sum_{\lambda \in \Lambda} I_\lambda\right).$$

Observação 3.5.1. Note que a topologia de Zariski é "fraca"comparada, por exemplo, com a topologia euclidiana em $\mathbb{R}$. Os fechados da topologia de Zariski neste espaço são apenas conjuntos finitos de pontos, dados pelos zeros de polinômios em $\mathbb{R}[X]$, já a topologia euclidiana admite todos os intervalos fechados da reta real.

De maneira natural podemos considerar a topologia de Zariski restrita a uma variedade $X \subset \mathbb{A}^n$. Neste caso os fechados são subvariedades $Y \subset X$.

Observação 3.5.2. Um espaço topológico X é dito *noetheriano* se seus subconjuntos fechados satisfazem a condição de cadeia descendente (c.c.d.).

Proposição 3.5.3. *A topologia de Zariski em uma variedade é noetheriana.*

(i) *Toda cadeia decrescente* $X_1 \supset X_2 \supset \cdots$ *de variedades de* $\mathbb{A}^n$ *estabiliza.*

(ii) *Todo conjunto não vazio* Ω *de variedades de* $\mathbb{A}^n$ *possui um elemento minimal.*

Demonstração. Ambos os itens seguem do fato que o anel de polinômios é noetheriano. Para (i) perceba que uma *cadeia decrescente* de variedades $X_1 \supset X_2 \supset \cdots$ de $\mathbb{A}^n$ corresponde a uma *cadeia ascendente* de ideais de $\mathbb{K}[X_1, \ldots, X_n]$, que estabiliza, logo existe um inteiro positivo m tal que $k > m$ implica $X_k = X_m$. Para (ii) basta notar que, como $\mathbb{K}[X_1, \ldots, X_n]$ é um anel noetheriano, todo conjunto de ideais contém um ideal maximal J, logo para todo ideal não trivial $I \subsetneq J$ nesse conjunto temos $\mathcal{V}(I) \supset \mathcal{V}(J)$. ■

Definição 3.5.4. Seja $f \in \mathbb{K}[X_1, \ldots, X_n]$ e considere o subconjunto aberto de $\mathbb{A}^n$,

$$\mathbb{A}^n_f = \mathbb{A}^n \setminus f^{-1}(0) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n : f(a_1, \ldots, a_n) \neq 0\}.$$

O subconjunto $\mathbb{A}^n_f$ é chamado *aberto principal de* $\mathbb{A}^n$. Se X é uma variedade de $\mathbb{A}^n$, então os subconjuntos $X_f = X \setminus f^{-1}(0) = X \cap \mathbb{A}^n_f$, são chamados de *abertos principais de* X.

Os abertos principais $\mathbb{A}^n_f$ formam uma base para a topologia de Zariski em $\mathbb{A}^n$. Com efeito, basta mostrar que, dados um aberto $U \subset \mathbb{A}^n$ e um elemento $x \in U$, existe um aberto principal $\mathbb{A}^n_{f_x}$ tal que $x \in \mathbb{A}^n_{f_x} \subset U$ (veja [17], Lema 13.2). Como U é aberto, existe um ideal $I \in \mathbb{K}[X_1, \ldots, X_n]$ tal que $U = \mathbb{A}^n \setminus \mathcal{V}(I)$, assim para qualquer $0 \neq f_x \in I$ temos $f_x(x) \neq 0$, ou seja, $x \in \mathbb{A}^n_{f_x}$. Além disso $(f_x) \subset I$ implica $\mathcal{V}(I) \subset \mathcal{V}(f_x)$, portanto

$$\mathbb{A}^n_{f_x} = \mathbb{A}^n \setminus \mathcal{V}(f_x) \subset \mathbb{A}^n \setminus \mathcal{V}(I) = U.$$

3.6 Variedades irredutíveis

Como veremos nesta seção, toda variedade possui uma decomposição em *irredutíveis*. Além disso mostra-se que variedades irredutíveis são geradas por ideais primos de um anel de polinômios.

Definição 3.6.1. Uma variedade algébrica $X \subset \mathbb{A}^n$ é dita *irredutível* se é não vazia e não é união de duas subvariedades algébricas próprias, isto é,

$$X = X_1 \cup X_2 \;\Rightarrow\; X = X_1 \text{ ou } X = X_2.$$

O próximo resultado apresenta uma caracterização de uma variedade irredutível, envolvendo seu ideal do anel de polinômios associado.

Proposição 3.6.2. *Uma variedade $X \subset \mathbb{A}^n$ é irredutível se, e somente se, o ideal $\mathcal{I}(X)$ é primo.*

Demonstração. Vamos provar a contrapositiva deste resultado:

$$X \subset \mathbb{A}^n \text{ é redutível} \Leftrightarrow \mathcal{I}(X) \text{ não é primo.}$$

($\Rightarrow$) Seja $X = X_1 \cup X_2$, onde X_1 e X_2 são subvariedades próprias não vazias, com ideais $\mathcal{I}(X_1), \mathcal{I}(X_2)$. Como $\mathcal{I}(X) \subsetneq \mathcal{I}(X_j)$, $j = 1, 2$, existem $f_1 \in \mathcal{I}(X_1) \setminus \mathcal{I}(X)$ e $f_2 \in \mathcal{I}(X_2) \setminus \mathcal{I}(X)$. Afirmamos que $f_1 f_2 \in \mathcal{I}(X)$ e portanto $\mathcal{I}(X)$ não é primo. Com efeito, dado $x \in X$ temos $x \in X_1$ ou $x \in X_2$, então $f_1(x) = 0$ para todo $f_1 \in \mathcal{I}(X_1)$ ou $f_2(x) = 0$ para todo $f_2 \in \mathcal{I}(X_2)$. Em qualquer caso $(f_1 f_2)(x) = f_1(x) f_2(x) = 0$, logo $f_1 f_2 \in \mathcal{I}(X)$.

($\Leftarrow$) Se $I = \mathcal{I}(X)$ não é primo, existem $f_1, f_2 \in \mathbb{K}[X_1, \ldots, X_n] \setminus I$ tais que $f_1 f_2 \in I$. Defina novos ideais $J_i = (I, f_i)$, $i = 1, 2$. Perceba que

$$\mathcal{V}(J_i) = \mathcal{V}((I, f_i)) = \mathcal{V}(I) \cap \mathcal{V}(f_i)$$

e como $f_1 f_2 \in I$, mas $f_1, f_2 \notin I$, existem $x_i \in X$ tais que $f_i(x_i) = 0$, ou seja, $\mathcal{V}(I) \cap \mathcal{V}(f_i) \neq \varnothing$. Além disso existem $y_i \in X$ tais que $f_i(y_i) \neq 0$, logo $\mathcal{V}(J_i) \subsetneq X$. Agora note que é possível escrever X como a união de subvariedades próprias

$$X = \mathcal{V}(I) = \mathcal{V}(J_1 \cap J_2) = \mathcal{V}(J_1) \cup \mathcal{V}(J_2),$$

portanto X é uma variedade redutível. ■

Exemplos 3.6.3. (1) A variedade $V = \mathcal{V}(XY)$ é redutível, pois $V = V_1 \cup V_2$, onde $V_1 = \mathcal{V}(X)$ e $V_2 = \mathcal{V}(Y)$.

(2) Agora $V = \mathcal{V}(XY - 1)$ é uma variedade irredutível. Sabemos que um polinômio $f \in \mathbb{K}[X, Y]$ é irredutível se, e somente se, o ideal (f) é primo. É fácil ver que $XY - 1$ é um polinômio irredutível, logo $(XY - 1)$ é primo e como todo ideal primo é radical segue do Nullstellensatz que $\mathcal{I}(\mathcal{V}(XY - 1)) = \text{rad}(XY - 1) = (XY - 1)$, assim a Proposição 3.6.2 garante que V é irredutível.

(3) Mais geralmente, toda hipersuperfície $V = \mathcal{V}(f) \subset \mathbb{A}^n$, dada por um polinômio irredutível $f \in \mathbb{K}[X_1, \ldots, X_n]$, é uma variedade irredutível.

Reunindo a definição das aplicações $\mathcal{V}$ e $\mathcal{I}$, o Nulltellensatz de Hilbert, o Corolário 3.3.7 e a Proposição 3.6.2 acima, obtemos o seguinte "dicionário" entre a *geometria* do espaço afim $\mathbb{A}^n$ e a *álgebra* do anel de polinômios $\mathbb{K}[X_1, \ldots, X_n]$.

Corolário 3.6.4. *Seja $\mathbb{K}$ um corpo algebricamente fechado. Então as aplicações $\mathcal{V}$ e $\mathcal{I}$ induzem bijeções*

$$\begin{array}{ccc}
\left\{ \begin{array}{c} \textit{ideais radicais de} \\ \mathbb{K}[X_1,\ldots,X_n] \end{array} \right\} & \longleftrightarrow & \left\{ \textit{variedades algébricas } X \subset \mathbb{A}^n \right\}, \\
\cup & & \cup \\
\left\{ \begin{array}{c} \textit{ideais primos de} \\ \mathbb{K}[X_1,\ldots,X_n] \end{array} \right\} & \longleftrightarrow & \left\{ \textit{variedades irredutíveis } X \subset \mathbb{A}^n \right\}, \\
\cup & & \cup \\
\left\{ \begin{array}{c} \textit{ideais maximais de} \\ \mathbb{K}[X_1,\ldots,X_n] \end{array} \right\} & \longleftrightarrow & \left\{ \textit{pontos em } \mathbb{A}^n \right\}.
\end{array}$$

Teorema 3.6.5. *Seja $X \subset \mathbb{A}^n$ uma variedade. Então X possui uma decomposição*

$$X = X_1 \cup X_2 \cup \cdots \cup X_k, \tag{3.2}$$

com cada X_i uma variedade irredutível. Mais ainda, ordenando as variedades de forma que, se $i \neq j$ então $X_i \not\subset X_j$, a decomposição é única (a menos de reordenação dos índices) e as variedades X_i são chamadas componentes irredutíveis de X.

Demonstração. Seja Ω o conjunto das variedades que não possuem uma decomposição da forma (3.2). Vamos provar que $\Omega = \varnothing$. Suponha que Ω é não vazio, então pela Proposição 3.5.3 possui um elemento minimal X. Agora X não é irredutível, logo existem variedades $X_1, X_2 \subsetneq X$ tais que $X = X_1 \cup X_2$. Pela minimalidade de X segue que X_1 e X_2 possuem uma decomposição da forma (3.2), e juntando ambas obtemos uma decomposição em irredutíveis para X, contradição.

Para a unicidade suponha que

$$X = Y_1 \cup Y_2 \cup \cdots \cup Y_r$$

é outra decomposição em irredutíveis para X, onde não há redundância entre os Y_l, $l = 1, \ldots, r$. Deste modo, para cada $i = 1, \ldots, k$ temos

$$\begin{aligned}
X_i &= X_i \cap X \\
&= X_i \cap (Y_1 \cup Y_2 \cup \cdots \cup Y_r) \\
&= (X_i \cap Y_1) \cup (X_i \cap Y_2) \cup \cdots \cup (X_i \cap Y_r),
\end{aligned}$$

e como X_i é irredutível existe um índice l tal que $X_i = (X_i \cap Y_l)$, logo $X_i \subset Y_l$. De forma análoga, existe um índice j tal que $Y_l = (Y_l \cap X_j)$, ou seja, $Y_l \subset X_j$. Assim, como as decomposições são supostas irredundantes temos que $X_i \subset X_j$ implica $i = j$ e portanto $X_i = Y_l$. Em especial concluímos que $k = r$ e assim ambas as decomposições são iguais,

a menos de reordenação de índices. ■

3.7 Funções em variedades

Seja $V \subset \mathbb{A}^n$ uma variedade e $\mathcal{I}(V)$ seu ideal. Uma *função polinomial*, ou *regular*, em V é uma função $f : V \to \mathbb{K}$ da forma $v \mapsto F(v)$, para algum polinômio $F \in \mathbb{K}[X_1, \ldots, X_n]$, ou seja, f é a restrição de uma *avaliação polinomial* em V ($f = F|_V$). Definimos o *anel de funções regulares* de V por

$$\mathbb{K}[V] = \{f : V \to \mathbb{K} : f \text{ é uma função regular}\}.$$

Como veremos na proposição seguinte, o anel quociente $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$ é naturalmente o anel de funções em V.

Proposição 3.7.1. *Seja $V \subset \mathbb{A}^n$ uma variedade e $\mathcal{I}(V)$ seu ideal. Então temos um isomorfismo de anéis*

$$\mathbb{K}[V] \cong \frac{\mathbb{K}[X_1, \ldots, X_n]}{\mathcal{I}(V)}.$$

Demonstração. Considere o homomorfismo de anéis:

$$\pi : \mathbb{K}[X_1, \ldots, X_n] \longrightarrow \mathbb{K}[V],$$

dado por

$$f \longmapsto f|_V : V \to \mathbb{K}.$$

Note que $f \in \operatorname{Ker} \pi$ se, e somente se $f|_V$ é a função nula em V, isto é, $f|_V(v) = 0$ para todo $v \in V$, ou equivalentemente, $f \in \mathcal{I}(V)$. Desse modo $\operatorname{Ker} \pi = \mathcal{I}(V)$ e pelo primeiro teorema do isomorfismo para anéis temos

$$\mathbb{K}[V] \cong \frac{\mathbb{K}[X_1, \ldots, X_n]}{\mathcal{I}(V)}.$$

■

O anel de funções $\mathbb{K}[V]$ de uma variedade $V \subset \mathbb{A}^n$ possui uma estrutura natural de $\mathbb{K}$-álgebra. De fato, basta definir a multiplicação externa entre um escalar $\lambda \in \mathbb{K}$ e uma função $f \in \mathbb{K}[V]$ por

$$(\lambda f)(v) = f(\lambda v),$$

para todo $v \in V$. É fácil mostrar, usando a proposição anterior, que as $\mathbb{K}$-álgebras $\mathbb{K}[V]$ e $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$ são isomorfas.

3.7.1 Exemplos de variedades e anéis de funções

Exploramos alguns exemplos de variedades e seus respectivos anéis de funções regulares, que serão úteis ao longo do texto.

Exemplo 3.7.2. Como vimos na Seção 3.5, o espaço afim $\mathbb{A}^n$ é uma variedade com $\mathbb{A}^n = \mathcal{V}(0)$. O anel de funções de $\mathbb{A}^n$ pode ser escrito como,

$$\mathbb{K}[\mathbb{A}^n] \cong \frac{\mathbb{K}[X_1, \ldots, X_n]}{(0)} \cong \mathbb{K}[X_1, \ldots, X_n].$$

Exemplo 3.7.3. A cônica afim $C = \mathcal{V}(Y^2 - X) \subset \mathbb{A}^2$ possui anel de funções

$$\mathbb{K}[C] \cong \frac{\mathbb{K}[X, Y]}{(Y^2 - X)}.$$

Também pode-se mostrar que $\mathbb{K}[C] \cong \mathbb{K}[Y]$, para isso basta notar que a sobrejeção $\mathbb{K}[X, Y] \twoheadrightarrow \mathbb{K}[Y]$, dada por $X \mapsto Y^2, Y \mapsto Y$ possui o kernel $(Y^2 - X)$.

Os próximos dois exemplos são construções particulares de variedades, dados abertos principais do espaço afim (veja [19], Seção 4.13).

Exemplo 3.7.4. Seja $f = X \in \mathbb{K}[X]$ e considere o aberto principal

$$\mathbb{A}^1_f = \{a \in \mathbb{A}^1 : X(a) \neq 0\} = \mathbb{A}^1 \setminus 0.$$

A partir de $\mathbb{A}^1_f$ construímos uma variedade num espaço afim de dimensão maior, a dizer, $\mathbb{A}^2$: tome uma nova variável Y e considere o ideal $(XY - 1) \subset \mathbb{K}[X, Y]$. É fácil ver que a função

$$\varphi : \mathcal{V}(XY - 1) \to \mathbb{A}^1,$$

dada por

$$\varphi(x, 1/x) = x,$$

é uma bijeção entre $\mathcal{V}(XY - 1)$ e $\mathbb{A}^1_f$, deste modo identificamos o conjunto $\mathbb{A}^1_f$ com a variedade $\mathcal{V}(XY - 1)$. Nesse sentido o anel de funções de $\mathbb{A}^1_f$ é

$$\mathbb{K}[\mathbb{A}^1_f] \cong \frac{\mathbb{K}[X, Y]}{(XY - 1)}.$$

Ainda pode-se mostrar que $\mathbb{K}[\mathbb{A}^1_f]$ é isomorfo ao anel de polinômios de Laurent em uma variável, isto é, $\mathbb{K}[X, X^{-1}]$.

Exemplo 3.7.5. O conjunto das matrizes invertíveis de ordem n com entradas em $\mathbb{K}$

$$\mathrm{GL}_n(\mathbb{K}) = \{A \in \mathrm{M}_n(\mathbb{K}) : \det A \neq 0\},$$

também denotado simplesmente por GL_n quando não há confusão, é um aberto principal de $\mathbb{A}^{n^2}$, onde identificamos uma matriz $A = (a_{ij})$ com as coordenadas $(a_{11}, a_{12}, \ldots, a_{nn})$. De fato, basta notar que a função determinante é polinomial

$$\det(X_{11}, X_{12}, \ldots, X_{nn}) = \sum_{\sigma \in S_n} (-1)^{\sigma} X_{1\sigma(1)} X_{2\sigma(2)} \cdots X_{n\sigma(n)}.$$

Como no exemplo anterior, compreendemos o conjunto GL_n tal qual uma variedade, dentro do espaço afim $\mathbb{A}^{n^2+1}$: considere uma nova variável X_0 e tome o ideal $I = (X_0 \det -1) \subset \mathbb{K}[X_0, X_{11}, \ldots, X_{nn}]$. Perceba que a função

$$\varphi : \mathcal{V}(I) \to \mathbb{A}^{n^2},$$

dada por

$$\varphi(a_0, a_{11}, \ldots, a_{nn}) = (a_{11}, \ldots, a_{nn})$$

é uma bijeção entre $\mathcal{V}(I)$ e GL_n, logo identificamos GL_n com $\mathcal{V}(I) \subset \mathbb{A}^{n^2+1}$.

O anel de funções regulares de GL_n é descrito pelo isomorfismo

$$\mathbb{K}[\mathrm{GL}_n] \cong \frac{\mathbb{K}[X_0, X_{11}, \ldots, X_{nn}]}{(X_0 \det -1)}. \tag{3.3}$$

Esse isomorfismo também pode ser compreendido via o processo de localização em anéis comutativos, mais claramente $\mathbb{K}[\mathrm{GL}_n]$ pode ser visto como a localização de $\mathbb{K}[X_{11}, \ldots, X_{nn}]$ pelo ideal (det),

$$\mathbb{K}[\mathrm{GL}_n] \cong \mathbb{K}[X_{11}, \ldots, X_{nn}]_{\det}.$$

Por fim, via o isomorfismo (3.3) descrevemos os $n^2 + 1$ geradores de $\mathbb{K}[\mathrm{GL}_n]$. Para todo $M = (m_0, m_{11}, \ldots, m_{nn}) \in \mathrm{GL}_n$,

$$X_{ij} : \mathrm{GL}_n \to \mathbb{K}$$

é dado por

$$X_{ij}(M) = m_{ij},$$

e

$$X_0 : \mathrm{GL}_n \to \mathbb{K}$$

é dado por

$$X_0(M) = m_0 = \frac{1}{\det(M)}.$$

3.8 Morfismos de variedades

Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades afins. Escreva $X_1, \ldots, X_n$ e $Y_1, \ldots, Y_m$ para as coordenadas em $\mathbb{A}^n$ e $\mathbb{A}^m$, respectivamente.

Definição 3.8.1. Uma função $f : V \to W$ é um *morfismo* de variedades algébricas afins se existem m polinômios $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ tais que,

$$f(v) = (f_1(v), \ldots, f_m(v)),$$

para todo $v \in V$.

Um morfismo de variedades também é chamado de *função regular*, ou ainda, de *função polinomial*. Ao decorrer deste texto fazemos o uso dessas três nomenclaturas.

Observação 3.8.2. Vejamos que funções polinomiais são contínuas na topologia de Zariski. Sejam $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades e $f : V \to W$ uma função polinomial, dada por polinômios $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$. Dado um subconjunto fechado $Z \subset W$, digamos $Z = \mathcal{V}(g_1, \ldots, g_r)$, vamos mostrar que a sua pré-imagem $f^{-1}(Z) \subset V$ ainda é um conjunto fechado:

$$\begin{aligned} v \in f^{-1}(Z) &\Leftrightarrow f(v) \in Z \\ &\Leftrightarrow g_i(f(v)) = 0, \forall\, i = 1, \ldots, r \\ &\Leftrightarrow (g_i(f_1, \ldots, f_m))(v) = 0, \forall\, i = 1, \ldots, r \end{aligned}$$

e como a composição de polinômios ainda é um polinômio, segue que $h_i = g_i(f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n]$, para todo $i = 1, \ldots, r$. Assim, $f^{-1}(Z) = \mathcal{V}(h_1, \ldots, h_r)$.

Lema 3.8.3. *Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades afins. Uma função $f : V \to W$ é um morfismo de variedades se, e somente se, para todo $j = 1, \ldots, m$, a composta $Y_j \circ f \in \mathbb{K}[V]$, onde Y_j denota a j-ésima função coordenada em W.*

Demonstração. Se f é dada pelos polinômios $f_1, \ldots, f_m$ então a composta é dada por $Y_j \circ f(v) = f_j(v)$, portanto é regular. Reciprocamente, se $Y_j \circ f \in \mathbb{K}[V]$ para todo $j = 1, \ldots, m$, basta tomar polinômios $f_j \in \mathbb{K}[X_1, \ldots, X_n]$ tais que a imagem da função $Y_j \circ f$ pelo isomorfismo $\mathbb{K}[V] \cong \mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$ é a classe $f_j + \mathcal{I}(V)$. Desse modo f é dada por $f_1, \ldots, f_m$. ■

A composição de morfismos é definida da maneira usual. Se $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ e $U \subset \mathbb{A}^r$ são variedades e $f : V \to W$, $g : W \to U$ morfismos (com f dado por $f_1, \ldots, f_m \in \mathbb{K}[X_1, \ldots, X_n]$ e g por $g_1, \ldots, g_r \in \mathbb{K}[Y_1, \ldots, Y_m]$), então $g \circ f$ é dado por

$$g_1(f_1, \ldots, f_m), \ldots, g_r(f_1, \ldots, f_m) \in \mathbb{K}[X_1, \ldots, X_n].$$

Definição 3.8.4. Um morfismo $f : V \to W$ entre variedades é um *isomorfismo* se existe um morfismo $g : W \to V$, tal que $g \circ f = I_V$ e $f \circ g = I_W$, onde I_V, I_W denotam o morfismo identidade em V e W, respectivamente.

Exemplos 3.8.5. Considere as variedades $V = \mathcal{V}(Y^2 - X^3), W = \mathcal{V}(Y^2 - X^3 - X^2) \subset \mathbb{A}^2$. V e W descrevem curvas em $\mathbb{A}^2$, que podem ser parametrizadas por funções polinomiais:

$$\varphi : \mathbb{A}^1 \to V,\ t \mapsto (t^2, t^3)$$

e

$$\psi : \mathbb{A}^1 \to W,\ t \mapsto (t^2 - 1, t^3 - t).$$

Perceba que ψ não é um isomorfismo de variedades, pois falha em ser uma função injetora: $\psi(-1) = \psi(1) = 0$. E como veremos no Exemplo 3.8.9, a função φ também não é um isomorfismo de variedades, mesmo sendo bijetora.

Morfismos entre duas variedades estão intimamente relacionados com homomorfismos entre as respectivas álgebras de funções, como indica o teorema a seguir.

Teorema 3.8.6. *Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades.*

(1) *Uma função polinomial $f : V \to W$ induz um homomorfismo de $\mathbb{K}$-álgebras $f^* : \mathbb{K}[W] \to \mathbb{K}[V]$ dado pela composição de funções, isto é, $f^*(g) = g \circ f$.*

(2) *Reciprocamente, todo homomorfismo de $\mathbb{K}$-álgebras $\Phi : \mathbb{K}[W] \to \mathbb{K}[V]$ é da forma $\Phi = f^*$ para uma função polinomial $f : V \to W$ unicamente determinada.*

(3) *Se $f : V \to W$ e $g : W \to U$ são funções polinomiais, então os dois homomorfismos de anéis*

$$(g \circ f)^*, f^* \circ g^* : \mathbb{K}[U] \to \mathbb{K}[V]$$

coincidem.

Demonstração. Veja [19], Teorema 4.4. ■

Notação 3.8.7. O homomorfismo de $\mathbb{K}$-álgebras f^* do teorema anterior também é chamado de *comorfismo*.

Fixado o corpo $\mathbb{K}$ podemos considerar duas categorias. A primeira é a categoria VA($\mathbb{K}$) das variedades algébricas e a segunda é a categoria AlgAf($\mathbb{K}$) das $\mathbb{K}$-álgebras afins (veja o Exemplo 2.3.2 (10)).

O último teorema mostra que temos um funtor contravariante $F : \mathrm{VA}(\mathbb{K}) \to \mathrm{Alg}(\mathbb{K})$ que leva uma variedade V em sua álgebra de funções $\mathbb{K}[V]$, e que leva uma função polinomial $f : V \to W$ no homomorfismo de álgebras $f^* : \mathbb{K}[W] \to \mathbb{K}[V]$.

Perceba que $\mathbb{K}[V]$ realmente é uma álgebra afim, uma vez que é isomorfa ao quociente $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}(V)$, para algum inteiro positivo n, e o Nullstellensatz garante que $\mathcal{I}(\mathcal{V}(I)) = \text{rad}(I)$, onde $V = \mathcal{V}(I)$.

Reciprocamente, dada uma álgebra afim A e fixado um conjunto de n geradores, existe um isomorfismo $A \cong \mathbb{K}[X_1, \ldots, X_n]/I$, onde I é um ideal radical. Definimos a variedade afim $V = \mathcal{V}(I) \subset \mathbb{A}^n$ e assim temos um isomorfismo de $\mathbb{K}$-álgebras $A \cong \mathbb{K}[V]$. Também, dado um homomorfismo de $\mathbb{K}$-álgebras afins $\alpha : B \to A$, obtemos um homorfismo entre as álgebras de funções $\widehat{\alpha} : \mathbb{K}[W] \to \mathbb{K}[V]$ e pelo teorema anterior $\widehat{\alpha} = f^*$, para um único morfismo de variedades $f : V \to W$.

Corolário 3.8.8. *Uma função polinomial $f : V \to W$ é um isomorfismo se, e somente se, $f^* : \mathbb{K}[W] \to \mathbb{K}[V]$ é um isomorfismo.*

Exemplo 3.8.9. Considere as variedades $\mathbb{A}^1$, $V = \mathcal{V}(Y^2 - X^3) \subset \mathbb{A}^2$ e a função polinomial

$$\varphi : \mathbb{A}^1 \longrightarrow V,$$

dada por

$$t \longmapsto (t^2, t^3).$$

Como função φ é claramente uma bijeção, pois $\mathbb{K}$ é algebricamente fechado, entretanto **não é** um isomorfismo de variedades. Com efeito, seja

$$\varphi^* : \frac{\mathbb{K}[X, Y]}{(Y^2 - X^3)} \longrightarrow \mathbb{K}[T]$$

o comorfismo associado. Nos geradores φ^* é dado por

$$\overline{X} \longmapsto T^2,$$
$$\overline{Y} \longmapsto T^3,$$

e tem por imagem a $\mathbb{K}$-álgebra gerada por T^2 e T^3, isto é, $\mathbb{K}[T^2, T^3]$. Agora como T^2 e T^3 não geram T, temos que $\mathbb{K}[T^2, T^3] \subsetneq \mathbb{K}[T]$ e portanto φ^* não é sobrejetor.

O exemplo anterior demonstra que, na categoria das variedades algébricas, uma função bijetora não é necessariamente um isomorfismo.

Por fim definimos um tipo especial de morfismo de variedades.

Definição 3.8.10. Sejam V e W variedades algébricas. Um morfismo $f : V \to W$ é uma *imersão fechada* se

(i) f é uma função injetora;

(ii) a imagem $f(V)$ é um subconjunto fechado de W;

(iii) restringindo o contradomínio temos um isomorfismo de variedades $f : V \to f(V)$.

Como vimos no Exemplo 3.8.9 o morfismo $\varphi : \mathbb{A}^1 \to \mathbb{A}^2$, dado por $t \mapsto (t^2, t^3)$, é injetor e tem por imagem a variedade $\mathcal{V}(Y^2 - X^3)$, entretanto falha em ser uma imersão fechada, pois $\varphi : \mathbb{A}^1 \to \mathcal{V}(Y^2 - X^3)$ não é um isomorfismo. O próximo exemplo explora morfismos que são imersões fechadas.

Exemplo 3.8.11. Considere $\mathbb{A}^1$ e $\mathbb{A}^3$ os espaços afins sobre $\mathbb{R}$. Definimos um morfismo de variedades

$$\varphi : \mathbb{A}^1 \to \mathbb{A}^3,$$

por

$$\varphi(a) = (a, a^2, a^3).$$

Vejamos que esse morfismo é uma imersão fechada: como função φ é claramente injetora. A imagem de φ é o conjunto

$$\varphi(\mathbb{A}^1) = \{(x, y, z) \in \mathbb{A}^3 : y = x^2, z = x^3\},$$

que pode ser compreendido como os zeros do ideal $(Y - X^2, Z - X^3) \subset \mathbb{R}[X, Y, Z]$, isto é,

$$C_r = \varphi(\mathbb{A}^1) = \mathcal{V}(Y - X^2, Z - X^3).$$

No espaço tridimensional C_r é uma curva, conhecida como *cúbica retorcida* ou *twisted cubic*, a qual representamos abaixo:

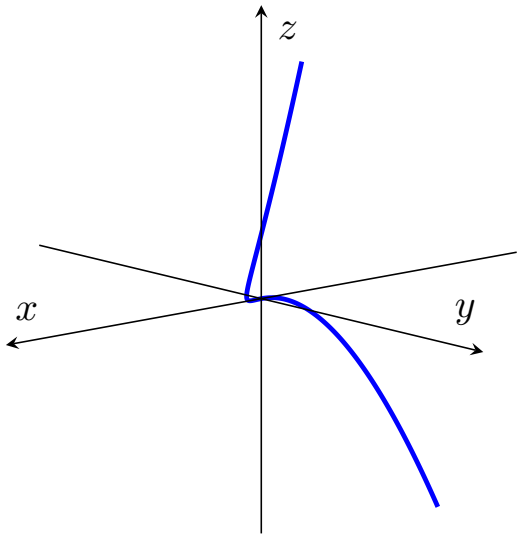


Figura 3.1: Cúbica retorcida.
Fonte: Autoria própria.

Por fim note que $\varphi : \mathbb{A}^1 \to C_r$ é um isomorfismo de variedades, pois admite um morfismo inverso $\psi : C_r \to \mathbb{A}^1$, dado por $\psi(x, y, z) = x$, logo φ é uma imersão fechada de $\mathbb{A}^1$ em $\mathbb{A}^3$.

Essa imersão pode ser generalizada para o espaço afim n-dimensional, sobre um corpo algebricamente fechado $\mathbb{K}$. Basta definir

$$\varphi : \mathbb{A}^1_{\mathbb{K}} \to \mathbb{A}^n_{\mathbb{K}}$$

por

$$\varphi(a) = (a, a^2, \ldots, a^n).$$

3.9 Produto de variedades

Nessa seção discutimos o produto de duas variedades algébricas, a partir da abordagem descrita em [10]. Para facilitar a escrita, convencionamos $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$, $\mathbb{K}[\mathbf{Y}] = \mathbb{K}[Y_1, \ldots, Y_m]$ e $\mathbb{K}[\mathbf{X}, \mathbf{Y}] = \mathbb{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.

Sejam $V = \mathcal{V}(I) \subset \mathbb{A}^n$ e $W = \mathcal{V}(J) \subset \mathbb{A}^m$ variedades algébricas afins não vazias, com ideais $I \subset \mathbb{K}[\mathbf{X}]$ e $J \subset \mathbb{K}[\mathbf{Y}]$. Identificamos o conjunto $\mathbb{A}^n \times \mathbb{A}^m$ com o espaço afim $\mathbb{A}^{n+m}$ e também os anéis de polinômios anteriores com subanéis de $\mathbb{K}[\mathbf{X}, \mathbf{Y}]$. Nestas condições o produto cartesiano das variedades V e W é naturalmente uma variedade afim: sabemos, pelo Corolário 3.2.5, que os anéis de polinômios são noetherianos, logo existem conjuntos finitos de geradores para I e J, a dizer $I = (f_1, \ldots, f_r)_{\mathbb{K}[\mathbf{X}]}$, $J = (h_1, \ldots, h_s)_{\mathbb{K}[\mathbf{Y}]}$. Assim, em termos destes geradores a variedade produto $V \times W \subset \mathbb{A}^{n+m}$ se escreve como

$$\begin{aligned} V \times W &= \mathcal{V}((f_1, \ldots, f_r, h_1, \ldots, h_s)_{\mathbb{K}[\mathbf{X},\mathbf{Y}]}) \\ &= \{(v, w) \in \mathbb{A}^{n+m} : v \in V, w \in W\}. \end{aligned}$$

Note que o ideal $(\mathcal{I}(V))_{\mathbb{K}[\mathbf{X},\mathbf{Y}]} + (\mathcal{I}(W))_{\mathbb{K}[\mathbf{X},\mathbf{Y}]}$, o qual denotamos apenas por $(\mathcal{I}(V)) + (\mathcal{I}(W))$, está contido em $\mathcal{I}(V \times W)$. A proposição a seguir mostra que essa inclusão é, na realidade, uma igualdade.

Proposição 3.9.1. *Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades algébricas afins não vazias.*

(1) *Se V e W são irredutíveis, então $V \times W$ também é.*

(2) *O ideal de $V \times W$ é $\mathcal{I}(V \times W) = (\mathcal{I}(V)) + (\mathcal{I}(W)) \subset \mathbb{K}[\mathbf{X}, \mathbf{Y}]$.*

(3) *Temos um isomorfismo de $\mathbb{K}$-álgebras $\mathbb{K}[V \times W] \cong \mathbb{K}[V] \otimes_{\mathbb{K}} \mathbb{K}[W]$.*

Demonstração. (1) Pela Proposição 3.6.2 basta mostrar que $\mathcal{I}(V \times W)$ é um ideal primo. Sejam $f_1, f_2 \in \mathbb{K}[\mathbf{X}, \mathbf{Y}]$ tais que $f_1 f_2 \in \mathcal{I}(V \times W)$. Fixado $w \in W$ arbitrário e $i = 1, 2$, definimos as subvariedades $V_i = \{v \in V : f_i(v, w) = 0\} \subset V$. Note que $V = V_1(w) \cup V_2(w)$, caso contrário existe $v \in V$ tal que $v \notin V_1(w)$, $v \notin V_2(w)$ e então $(f_1 f_2)(v, w) \neq 0$. Agora como V é irredutível devemos ter $V = V_1(w)$ ou $V = V_2(w)$. Deste modo segue que $W = W_1 \cup W_2$, onde $W_i = \{w \in W : V_i(w) = V\}$. Em especial

os conjuntos W_i são variedades, visto que $W_i = \{w \in W : f_i(v, w) = 0\}$, logo como W é suposto irredutível devemos ter $W = W_1$ ou $W = W_2$. No primeiro caso obtemos $f_1(v, w) = 0$ para todos $v \in V$, $w \in W$, portanto $f_1 \in \mathcal{I}(V \times W)$. Analogamente para o segundo caso deduzimos que $f_2 \in \mathcal{I}(V \times W)$, o que implica em $\mathcal{I}(V \times W)$ ser primo.

(2) Como $(\mathcal{I}(V)) + (\mathcal{I}(W)) \subset \mathcal{I}(V \times W)$, temos um homomorfismo sobrejetor de anéis

$$\varphi : \frac{\mathbb{K}[\mathbf{X}, \mathbf{Y}]}{(\mathcal{I}(V)) + (\mathcal{I}(W))} \longrightarrow\!\!\!\!\!\rightarrow \frac{\mathbb{K}[\mathbf{X}, \mathbf{Y}]}{\mathcal{I}(V \times W)},$$

logo pelo Lema 3.2.6 basta mostrar que φ é injetivo.

Sejam $\{\overline{f}_\lambda : \lambda \in \Lambda\}$ e $\{\overline{g}_\sigma : \sigma \in \Sigma\}$ bases dos $\mathbb{K}$-espaços vetoriais $\mathbb{K}[\mathbf{X}]/\mathcal{I}(V)$ e $\mathbb{K}[\mathbf{Y}]/\mathcal{I}(W)$, respectivamente, onde $f_\lambda \in \mathbb{K}[\mathbf{X}]$, $g_\sigma \in \mathbb{K}[\mathbf{Y}]$. Pode-se tomar, por exemplo, as bases descritas em [10], Teorema 1.2.8.

É sabido que todo polinômio em $\mathbb{K}[\mathbf{X}, \mathbf{Y}]$ pode ser escrito como uma soma de produtos da forma fg, onde $f \in \mathbb{K}[\mathbf{X}]$ e $g \in \mathbb{K}[\mathbf{Y}]$, portanto o conjunto dos produtos $f_\lambda g_\sigma$ módulo o ideal $(\mathcal{I}(V)) + (\mathcal{I}(W))$ gera $\mathbb{K}[\mathbf{X}, \mathbf{Y}]/(\mathcal{I}(V)) + (\mathcal{I}(W))$ sobre $\mathbb{K}$. Assim, mostrar que φ é injetiva é equivalente a mostrar que os produtos $f_\lambda g_\sigma$ são linearmente independentes módulo $\mathcal{I}(V \times W)$.

Sejam $x_{\lambda,\sigma} \in \mathbb{K}$ escalares, tais que

$$\sum_{\lambda \in \Lambda} \sum_{\sigma \in \Sigma} x_{\lambda,\sigma} f_\lambda g_\sigma \in \mathcal{I}(V \times W),$$

ou seja,

$$\sum_{\lambda \in \Lambda} \sum_{\sigma \in \Sigma} x_{\lambda,\sigma} f_\lambda(v) g_\sigma(w) = 0,$$

para todos $v \in V$, $w \in W$.

Basta mostrar que $x_{\lambda,\sigma} = 0$ para todos os índices λ, σ. Fixe um elemento $w \in W$ arbitrário e considere para todo $\lambda \in \Lambda$ os escalares

$$y_\lambda(w) = \sum_{\sigma \in \Sigma} x_{\lambda,\sigma} g_\sigma(w).$$

Note que $\sum_{\lambda \in \Lambda} y_\lambda(w) f_\lambda(v) = 0$, para todo $v \in V$. Agora como os polinômios f_λ são linearmente independentes módulo $\mathcal{I}(V)$, obtemos que $y_\lambda(w) = 0$ para todo λ. De maneira similar, como a relação acima é válida para todo $w \in W$ e os polinômios g_σ são linearmente independentes módulo $\mathcal{I}(W)$, concluímos que $x_{\lambda,\sigma} = 0$, para todos $\lambda \in \Lambda, \sigma \in \Sigma$.

(3) Considere a aplicação

$$\theta : \mathbb{K}[V] \times \mathbb{K}[W] \to \mathbb{K}[V \times W],$$

dada por

$$\theta(f, g)(v, w) = f(v)g(w).$$

Claramente θ é $\mathbb{K}$-bilinear, logo induz um homomorfismo de $\mathbb{K}$-álgebras $\overline{\theta} : \mathbb{K}[V] \otimes \mathbb{K}[W] \to \mathbb{K}[V \times W]$, dado por $\overline{\theta}(f \otimes g) = fg$. Vamos proceder mostrando que $\overline{\theta}$ é um isomorfismo.

Usando o fato que todo polinômio em $\mathbb{K}[\mathbf{X}, \mathbf{Y}]$ pode ser escrito como uma soma finita de elementos da forma fg, onde $f \in \mathbb{K}[\mathbf{X}]$ e $g \in \mathbb{K}[\mathbf{Y}]$, obtemos que toda função polinomial $f \in \mathbb{K}[V \times W]$ admite uma decomposição

$$f = \sum_{i=1}^{r} g_i h_i,$$

onde $g_i \in \mathbb{K}[V]$ e $h_i \in \mathbb{K}[W]$. Deste modo $\overline{\theta}$ é sobrejetor.

Para a injetividade seja $f = \sum_{i=1}^{r} g_i \otimes h_i$, com r minimal, tal que $\overline{\theta}(f) = 0$. Vamos mostrar que se $f \neq 0$, então $r = 1$. De fato, neste caso para algum $i = 1, \ldots, r$ temos $h_i \neq 0$, logo existe $w \in W$ tal que $h_i(w) \neq 0 \in \mathbb{K}$. Agora como $\sum_{i=1}^{r} g_i(v)h_i(w) = 0$, para todo $v \in V$, segue que $\sum_{i=1}^{r} h_i(w)g_i$ é a função nula em $\mathbb{K}[V]$, isto é, as funções g_i são linearmente dependentes sobre $\mathbb{K}$. Se r for maior que 1 podemos reduzir o número de $g_i's$, o que contradiz a minimalidade de r. Assim $r = 1$ e a relação $h_1(w)g_1 = 0$ implica $g_1 = 0$, logo f é o tensor nulo.

■

3.10 Conjuntos construtíveis

Esta seção é dedicada ao estudo de algumas propriedades dos conjuntos construtíveis, em especial enunciamos um teorema de Chevalley, que caracteriza imagens de morfismos de variedades.

Definição 3.10.1. Seja X um espaço topológico. Um *subconjunto localmente fechado* de X é a interseção de um subconjunto aberto e um subconjunto fechado. Um subconjunto *construtível* de X é uma união finita de subconjuntos localmente fechados.

O lema enunciado abaixo reune algumas propriedades conhecidas dos espaços topológicos e suas transformações, para mais detalhes veja, por exemplo, [17].

Lema 3.10.2. *Sejam X, Y espaços topológicos e $f : X \to Y$ uma função contínua.*

(1) *Se $X_1, \ldots, X_r$ são subconjuntos de X, então*

$$\bigcup_{i=1}^{r} \overline{X_i} = \overline{\bigcup_{i=1}^{r} X_i}.$$

(2) *Se $A \subset X$ é um subconjunto, então $f(\overline{A}) \subset \overline{f(A)}$. Em particular, se f é um homeomorfismo então $f(\overline{A}) = \overline{f(A)}$.*

(3) *Se X é irredutível, então $f(X)$ é irredutível.*

É conhecido que em um espaço noetheriano todo conjunto construtível contém um aberto denso de seu fecho (veja a Seção AG 1.3 em [5]). Entretanto este fato se mantém verdadeiro em espaços topológicos gerais, como mostra o teorema abaixo (veja [1], Lema 2.1).

Teorema 3.10.3. *Sejam X um espaço topológico e $Y \subset X$ um subconjunto construtível. Então Y contém um subconjunto aberto denso de $\overline{Y}$.*

Demonstração. Escreva $Y = \bigcup_{i=1}^{k} Y_i$, onde cada Y_i é localmente fechado. Denote $Z_i = \overline{Y_i} \setminus Y_i$ e $Z = \bigcup_{i=1}^{k} Z_i$. Vamos mostrar que o conjunto $W = \overline{Y} \setminus Z$ está contido em Y e é aberto denso em $\overline{Y}$.

Primeiramente, vejamos que $W \subset Y$. Note que, pelo Lema 3.10.2 (1)

$$Y \cup Z = \left(\bigcup_{i=1}^{k} Y_i\right) \cup \left(\bigcup_{i=1}^{k} Z_i\right) = \bigcup_{i=1}^{k} (Y_i \cup Z_i) = \bigcup_{i=1}^{k} \overline{Y_i} = \overline{\bigcup_{i=1}^{k} Y_i} = \overline{Y},$$

logo $W = \overline{Y} \setminus Z = (Y \cup Z) \setminus Z = Y \setminus Z \subset Y$.

Agora mostramos que W é aberto em $\overline{Y}$. Como cada Y_i é localmente fechado, digamos $Y_i = F_i \cap A_i$ com F_i fechado e A_i aberto, temos que Y_i é aberto em $\overline{Y_i}$. De fato,

$$\begin{aligned}
\overline{Y_i} &= \overline{F_i \cap A_i} \\
&= \overline{F_i} \cap \overline{A_i} \\
&= F_i \cap (A_i \cup \partial A_i) \\
&= (F_i \cap A_i) \cup (F_i \cap \partial A_i) \\
&= Y_i \cup (F_i \cap \partial A_i),
\end{aligned}$$

onde ∂A_i denota a fronteira $\overline{A_i} \setminus A_i$. Assim $F_i \cap \partial A_i$ é um conjunto fechado, logo Y_i é um subconjunto aberto de $\overline{Y_i}$. Deste modo Z_i é fechado em $\overline{Y_i}$ e portanto fechado em X, assim o seu complementar em $\overline{Y}$, $W = \overline{Y} \setminus Z$ é aberto. Resta mostrar que W é denso em $\overline{Y}$.

Suponha por contradição que W não é denso em $\overline{Y}$, assim existe um subconjunto aberto não vazio U de $\overline{Y}$ tal que $U \cap W = \varnothing$, isto é, Z contém U. Seja i_0 o menor índice

tal que $\bigcup_{i=1}^{i_0} Z_i$ contém um subconjunto aberto não vazio, digamos U, de $\overline{Y}$. Vejamos que $U \not\subset Z_i$, para $1 \leq i \leq i_0$. De fato, como Y_i é aberto temos que $Z_i = \overline{Y_i} \setminus Y_i = \partial Y_i$ é a fronteira de Y_i, logo se $U \subset Z_i$ e $x \in U$ temos $U \cap Y_i = \varnothing$, ou seja, U é uma vizinhança de x cuja interseção com Y_i é vazia, portanto $x \notin \partial Y_i = Z_i$, contradição. Disso concluímos que $U \not\subset Z_{i_0}$, em particular $i_0 > 1$. Deste modo $\varnothing \neq (U \setminus Z_{i_0}) \subset \bigcup_{i=1}^{i_0-1} Z_i$ e como Z_{i_0} é fechado, $U \setminus Z_{i_0}$ é aberto em $\overline{Y}$, o que contradiz a minimalidade e i_0. Portanto W é denso em $\overline{Y}$. ■

Segue diretamente do teorema anterior o seguinte resultado acerca do espaço topológico das variedades:

Corolário 3.10.4. *Seja X uma variedade. Então $Y \subset X$ é construtível se, e somente se, contém um subconjunto aberto denso de $\overline{Y}$.*

O corolário acima permite, por exemplo, mostrar que todo subgrupo abstrato de um grupo algébrico afim, que também é um conjunto construtível, é um subgrupo algébrico (veja o Teorema 4.1.20).

O próximo resultado, devido a *C. Chevalley*, garante que a imagem de um morfismo de variedades é um subconjunto construtível do contradomínio. Esse resultado é especialmente útil na teoria de grupos algébricos afins desenvolvida no Capítulo 4, onde mostra-se que a imagem de um morfismo de grupos algébricos afins é um subgrupo fechado (veja o Teorema 4.1.22).

Teorema 3.10.5 (Chevalley)**.** *Sejam X e Y variedades algébricas e $\varphi : X \to Y$ um morfismo. Então a imagem de φ é construtível em Y.*

Definição 3.10.6. Veja [**?**], Teorema 4.91.

Capítulo 4

Grupos algébricos

Nesse último capítulo desenvolvemos, baseados em [22], a teoria básica de grupos algébricos afins e ações de grupos algébricos em variedades, bem como apresentamos as noções gerais sobre álgebras de Hopf e as estruturas de comódulos. Como resultado principal demonstramos o Teorema 4.5.16, que garante que todo grupo algébrico afim é *linear*, ou seja, é isomorfo a um subgrupo fechado de algum *grupo linear geral*.

4.1 Grupos algébricos afins

Nesta seção desenvolvemos a teoria básica de grupos algébricos afins e apresentamos vários exemplos.

Definição 4.1.1. Sejam $\mathbb{K}$ um corpo algebricamente fechado e G uma variedade algébrica afim. Suponha que G é munido de uma estrutura de grupo abstrato, isto é, possui uma multiplicação associativa $m : G \times G \to G$, $(g, h) \mapsto gh$, uma aplicação de inversão $i : G \to G$, $g \mapsto g^{-1}$, e um elemento neutro 1_G satisfazendo os axiomas de um grupo:

$$(gh)k = g(hk),$$
$$1_G g = g 1_G = g,$$
$$gg^{-1} = g^{-1}g = 1_G,$$

para todos $g, h, k \in G$. Dizemos que (G, m, i), ou G abreviadamente, é um *grupo algébrico afim* se m e i são morfismos de variedades algébricas.

Observação 4.1.2. Fixado $x \in G$ as translações pela esquerda $l_x : G \to G$, $l_x(g) = xg$ e pela direita $r_x : G \to G$, $r_x(g) = gx$, são isomorfismos de variedades. De fato, a translação pela esquerda pode ser escrita como a composição

$$l_x = m \circ j_x \circ \theta_x,$$

onde o morfismo $\theta_x : G \to \{x\} \times G$ é dado por $\theta_x(g) = (x, g)$ e $j_x : \{x\} \times G \to G \times G$ é dado por $j(x, g) = (x, g)$. Assim l_x é uma função regular. Para ver que é um isomorfismo

basta notar que admite uma inversa regular $l_{x^{-1}}$. Um raciocínio análogo garante que r_x também é isomorfismo.

Compondo a translação pela esquerda l_x e a translação pela direita $r_{x^{-1}}$, obtemos um novo isomorfismo de variedades, a *conjugação por* x, $c_x = G \to G$, dada por $c_x(g) : xgx^{-1}$.

Definimos as subestruturas e morfismos entre grupos algébricos da maneira natural:

Definição 4.1.3. Seja G um grupo algébrico. Um subgrupo abstrato $H \subset G$ que também é um subconjunto fechado de G é chamado *subgrupo algébrico*, ou ainda *subgrupo fechado*, de G.

Definição 4.1.4. Sejam H e G grupos algébricos. Um *morfismo* de grupos algébricos é um morfismo de variedades $\varphi : H \to G$ que também é homomorfismo de grupos abstratos. Um *isomorfismo* de grupos algébricos é um isomorfismo de variedades que também é isomorfismo de grupos abstratos.

A seguir apresentamos alguns exemplos de grupos algébricos afins.

Exemplo 4.1.5. O *grupo algébrico aditivo* G_a é a variedade $\mathbb{A}^1$ com a estrutura de grupo dada pela soma do corpo $\mathbb{K}$, ou seja, $m : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ é dada por $m(x, y) = x + y$ e $i : \mathbb{A}^1 \to \mathbb{A}^1$ é dada por $i(x) = -x$.

Exemplo 4.1.6. O *grupo algébrico multiplicativo* G_m consiste no aberto $\mathbb{A}^1 \setminus \{0\}$, identificado com a variedade $\mathcal{V}(XY - 1) \subset \mathbb{A}^2$ como no Exemplo 3.7.4. A multiplicação $m : G_m \times G_m \to G_m$ é dada por $m((x, x^{-1}), (y, y^{-1})) = (xy, (xy)^{-1})$ e a inversão $i : G_m \to G_m$ por $i((x, x^{-1})) = (x^{-1}, x)$.

Note que os grupos aditivo e multiplicativo são abelianos, pois envolvem as operações do corpo $\mathbb{K}$.

Exemplo 4.1.7. O *grupo linear geral* GL_n é o aberto principal $\mathbb{A}^{n^2}_{\det}$, o qual identificamos com a variedade $\mathcal{V}(X_0 \det -1) \subset \mathbb{A}^{n^2+1}$, como no Exemplo 3.7.5. Perceba que por essa identificação, $\mathrm{GL}_n \subset \mathbb{A}^{n^2+1}$ ainda é um grupo abstrato, mais ainda, possui estrutra de grupo algébrico. Com efeito, a multiplicação é dada por

$$m(A, B) = N = (n_0, n_{11}, n_{12}, \ldots, n_{nn}),$$

onde

$$n_0 = (ab)_0 = a_0 b_0 \quad \text{e} \quad n_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj},$$

para todas $A = (a_0, a_{11}, a_{12}, \ldots, a_{nn}), B = (b_0, b_{11}, b_{12}, \ldots, b_{nn}) \in \mathrm{GL}_n$. Veja que a multiplicação definida acima herda a associatividade da operação de produto entre matrizes,

junto do fato que

$$(ab)_0 c_0 = \frac{1}{\det(AB)} \cdot \frac{1}{\det(C)} = \frac{1}{\det(A)\det(B)\det(C)} = \frac{1}{\det(A)} \cdot \frac{1}{\det(BC)} = a_0(bc)_0,$$

para quaisquer $A, B, C \in \mathrm{GL}_n$.

O elemento neutro de GL_n, o qual denotamos igualmente pela matriz identidade $\mathrm{Id}_n \in \mathrm{M}_n(\mathbb{K})$, é

$$\mathrm{Id}_n = (1, \delta_{11}, \delta_{12}, \ldots, \delta_{nn}),$$

onde δ_{ij} denota a função Delta de Kronecker.

A inversão de $A = (a_0, a_{11}, a_{12}, \ldots, a_{nn}) \in \mathrm{GL}_n$ é dada por

$$i(A) = (1/a_0, a_0 c_{11}, a_0 c_{21}, \ldots, a_0 c_{nn}),$$

onde $c_{ij} = (-1)^{i+j} \det(A(i|j))$ são os cofatores de A. Usando o fato que a multiplicação de uma matriz A por sua adjunta clássica é igual a $\det A \cdot \mathrm{Id}_n$, obtemos

$$i(A) \cdot A = A \cdot i(A) = \mathrm{Id}_n \,.$$

Os argumentos anteriores garantem que GL_n, visto como um subconjunto do espaço afim $\mathbb{A}^{n^2+1}$, ainda é um grupo. Por fim observamos que multiplicação e a inversão descritas acima são polinomiais entrada a entrada, logo pelo Lema 3.8.3 são morfismos de variedades.

Observação 4.1.8. É comum a identificação do grupo algébrico afim GL_n com matrizes $n \times n$, isto é, omite-se a "primeira coordenada" do espaço afim $\mathbb{A}^{n^2+1}$. Perceba que essa identificação não gera confusão, pois a coordenada da primeira posição é completamente determinada pelas demais n^2 coordenadas. Utilizaremos essa identificação com ênfase na Subseção 4.5.1.

Observação 4.1.9. Seja V um $\mathbb{K}$-espaço vetorial n-dimensional. Denotamos por $\mathrm{GL}(V)$ o grupo de autormorfismos de V, isto é, o grupo de todas as transformações lineares invertíveis de V para V. Fixada uma base de V os grupos $\mathrm{GL}(V)$ e GL_n são naturalmente isomorfos, via a correspondência entre a representação matricial de uma transformação linear em um sistema de coordenadas. Nesse sentido é possível compreender $\mathrm{GL}(V)$ como um grupo algébrico afim.

Exemplo 4.1.10. O *grupo afim* $\mathrm{Aff}_n(\mathbb{K})$, também denotado simplesmente por Aff_n, é definido como o produto cartesiano

$$\mathbb{A}^n \times \mathrm{GL}_n \subset \mathbb{A}^n \times \mathbb{A}^{n^2+1},$$

com multiplicação dada por

$$(u, A)(v, B) = (u + Av, AB), \tag{4.1}$$

onde identificamos $\mathbb{A}^n$ com matrizes coluna $n \times 1$. O termo Av é visto como o produto entre uma matriz $n \times n$ e uma matriz $n \times 1$, já AB é a multiplicação em GL_n, descrita no Exemplo 4.1.7, que inclui a coordenada X_0.

Note que a multiplicação definida por (4.1) é associativa:

$$\begin{aligned}((u, A)(v, B))(w, C) &= (u + Av, AB)(w, C)\\ &= (u + Av + (AB)w, (AB)C)\\ &= (u + A(v + Bw), A(BC))\\ &= (u, A)(v + Bw, BC)\\ &= (u, A)((v, B))(w, C)),\end{aligned}$$

para todos $(u, A), (v, B), (w, C) \in \mathrm{Aff}_n$.

É fácil ver que o elemento neutro dessa operação é $(0, \mathrm{Id}_n)$, onde $0 = (0, \ldots, 0) \in \mathbb{A}^n$.

Agora, a inversão de um elemento $(u, A) \in \mathrm{Aff}_n$ é dada por

$$(u, A)^{-1} = (-A^{-1}u, A^{-1}),$$

onde, novamente, $-A^{-1}u$ é visto como a multiplicação entre uma matriz $n \times n$ e um vetor coluna, e $A^{-1} = i(A)$ é a inversão em GL_n, dada no Exemplo 4.1.7.

O grupo afim admite a estrutura natural de variedade produto

$$\mathbb{A}^n \times \mathrm{GL}_n \hookrightarrow \mathbb{A}^{n^2+n+1},$$

mais especificamente, se $\mathbb{A}^n$ possui as coordenadas $X_1, \ldots, X_n$ e GL_n as coordenadas $X_0, X_{11}, X_{12}, \ldots, X_{nn}$, Aff_n é dado pelos zeros do ideal

$$(X_0 \det -1) \subset \mathbb{K}[X_1, \ldots, X_n, X_0, X_{11}, \ldots, X_{nn}].$$

Perceba que as operações de multiplicação e inversão do grupo afim envolvem apenas o produto, soma e inversão de matrizes em suas coordenadas, logo são funções regulares e então Aff_n é um grupo algébrico.

Por fim, se tomamos as coordenadas como acima, a álgebra de funções regulares de Aff_n é

$$\mathbb{K}[\mathrm{Aff}_n] \cong \frac{\mathbb{K}[X_1, \ldots, X_n, X_0, X_{11}, \ldots, X_{nn}]}{(X_0 \det -1)},$$

portanto, como funções, os geradores são dados por

$$X_k(u, A) = u_k,\ k = 1, \ldots, n,$$

$$X_0(u, A) = a_0,$$

e

$$X_{ij}(u, A) = a_{ij},\ i, j = 1, \ldots, n.$$

Exemplo 4.1.11. O centro de um grupo algébrico G,

$$\mathcal{Z}(G) = \{x \in G : xy = yx, \forall\ y \in G\},$$

é um subgrupo algébrico. De fato, $\mathcal{Z}(G)$ é subgrupo de G e as operações de multiplicação e inversão são restrições de morfismos, logo basta verificar que esse conjunto é fechado.

Para cada $y \in G$ considere a função

$$\psi_y : G \to G,$$

dada por

$$\psi_y = m \circ (l_y, l_{y^{-1}}) \circ (\mathrm{id}, i) \circ \delta,$$

onde $\delta : G \to G \times G$ é o morfismo diagonal, dado por $\delta(g) = (g, g)$. Como δ é uma função polinomial, segue que ψ_y é uma função regular para todo $y \in G$.

Agora note que

$$\mathcal{Z}(G) = \bigcap_{y \in G} \psi_y^{-1}(1_G),$$

isto é, $\mathcal{Z}(G)$ é interseção de pré-imagens de um fechado por uma função contínua, logo também é fechado.

Em particular se $G = \mathrm{GL}_n$ então $\mathcal{Z}(G) = \{\lambda\, \mathrm{Id}_n : \lambda \in \mathbb{K}^*\}$.

Exemplo 4.1.12. Se H e K são grupos algébricos afins, então $H \times K$ também é um grupo algébrico afim, com multiplicação e inversão dadas entrada a entrada. De fato, $m_{H\times K} = (m_H \times m_K) \circ (\mathrm{id} \times s \times \mathrm{id}) : H \times K \times H \times K \to H \times K$, onde m_H, m_K são as multiplicações de H e K, respectivamente, e $s : K \times H \to H \times K$ é função que inverte os fatores, evidentemente polinomial. Agora a inversão é dada por $i_{H\times K} = i_H \times i_K : H \times K \to H \times K$.

O grupo algébrico $H \times K$ é chamado de *produto direto* de H e K. Pode-se mostrar que $H \times K$ é um produto na categoria dos grupos algébricos.

Exemplos 4.1.13. Subgrupos de GL_n.

(1) O subgrupo das matrizes triangulares superiores invertíveis $B_n \subset \mathrm{GL}_n$ é um conjunto

fechado, pois $B_n = \mathcal{V}((X_{ij}, X_0 \det -1)_{1<j<i<n}) \subset \mathbb{A}^{n^2+1}$. Em particular B_n é isomorfo como variedade a $\mathbb{A}^{\frac{n(n-1)}{2}} \times \mathbb{K}^*$.

(2) O conjunto das matrizes diagonais invertíveis é um subgrupo fechado de GL_n, o qual denotamos por $D_n = \mathcal{V}((X_{ij}, X_0 \det -1)_{i\neq j}) \subset \mathbb{A}^{n^2+1}$.

(3) O subgrupo das matrizes unipotentes triangulares superiores U_n, composto por matrizes triangulares superiores cuja diagonal principal possui 1 em todas as posições, é um conjunto fechado de $\mathbb{A}^{n^2}$,

$$U_n = \mathcal{V}((X_{ij}, X_{kk} - 1)_{1<j<i<n:k=1,\ldots,n}).$$

Identificamos U_n com o subgrupo $\{1\}\times U_n$ de GL_n, visto que dada uma matriz $M \in U_n$ temos $\det M = 1$.

(4) O *grupo linear especial* das matrizes cujo determinante é igual a 1 é um grupo algébrico, denotado por $\mathrm{SL}_n = \mathrm{SL}_n(\mathbb{K}) = \{A \in \mathrm{M}_n(\mathbb{K}) : \det A = 1\}$. Como variedade,

$$\mathrm{SL}_n = \mathcal{V}(\det -1) \subset \mathbb{A}^{n^2}.$$

Identificamos SL_n como o subgrupo de GL_n: $\{A \in \mathrm{GL}_n : \det A = 1\} \subset \mathbb{A}^{n^2+1}$.

Proposição 4.1.14. *O grupo linear especial* SL_n *é uma variedade irrredutível, ou ainda,* SL_n *é um grupo algébrico conexo (veja a Definição 4.1.25).*

Demonstração. Seguimos os argumentos de [24], Exemplo 2.25. Basta mostrar que o ideal $(\det -1)$ é primo, visto que todo ideal primo é radical, assim o Nullstellensatz garante que $\mathcal{I}(\mathrm{SL}_n) = \mathrm{rad}(\det -1) = (\det -1)$ e da Proposição 3.6.2 segue a tese (compare com o Exemplo 3.6.3 (2)). Vamos proceder mostrando que o polinômio $\det -1 \in \mathbb{K}[X_{11}, \ldots, X_{nn}]$ é irredutível, e para isso verificaremos que o próprio det é irredutível.

Suponha que $\det -1 = fg$, onde $f = f_r + \cdots + f_1 + f_0$ e $g = g_s + \cdots + g_1 + g_0$ são polinômios em $\mathbb{K}[X_{11}, \ldots, X_{nn}]$ cujos termos f_i e g_j, $0 \leq i \leq r, 0 \leq j \leq s$ são homogêneos de grau i e j, respectivamente. Como det é um polinômio homogêneo, comparando o grau dos polinômios na igualdade

$$\det -1 = fg = f_r g_s + f_r g_{s-1} + \cdots + f_0 g_0$$

segue que $\det = f_r g_s$ e portanto é suficiente verificar que det não se fatora como o produto de outros dois polinômios.

Procedemos por indução no grau n de det. Para $n = 1$, $\det_1 = X_{11}$, que é irredutível. Suponha que $\det_{n-1}$ é irredutível e que existe uma fatoração $\det_n = fg$. Pela expressão do determinante sabemos que o grau da indeterminada X_{nn} em $\det_n$ é 1,

portanto X_{nn} aparece em apenas um dos fatores de $\det_n$, digamos f. Deste modo f é linear em X_{nn}, ou seja, existem polinômios $p, q \in \mathbb{K}[X_{11}, \ldots, X_{n(n-1)}]$ tais que

$$f = X_{nn} \cdot p + q.$$

Assim temos

$$\det_n = fg = X_{nn} \cdot pg + qg.$$

Pela expansão de Laplace nas indeterminadas $X_{n1}, \ldots, X_{nn}$ obtemos que o coeficente que acompanha X_{nn} é $\det_{n-1}$, ou seja, $\det_{n-1} = pg$. Pela hipótese de indução $\det_{n-1}$ é irredutível, logo $p = 1$ ou $g = 1$. Se $g = 1$ $\det_n$ é irredutível e acabou. Agora se $p = 1$ temos que $g = \det_{n-1}$ divide $\det_n$ e isso não pode ocorrer. De fato, para cada $n \in \mathbb{N}$ considere a matriz $L_n \in \mathrm{M}_n(\mathbb{K})$ cujas únicas entradas não nulas são $l_{n1} = l_{(n-1)2} = l_{(n-2)3} = \cdots = l_{1n} = 1$, isto é, a diagonal secundária é composta por 1 em todas as posições:

$$L_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Por um lado $\det_{n-1}(L_n) = 0$, visto que envolve apenas as entradas X_{ij} com $1 \leq i, j \leq n-1$ e a matriz $(n-1) \times (n-1)$ obtida eliminando a última linha e a última coluna de L_n possui uma coluna nula. Por outro lado, aplicando a expansão de Laplace em $\det_n(L_n)$ obtemos

$$\begin{aligned} \det_n(L_n) &= 1 \cdot (-1)^{1+n} \cdot \det(L_{n-1}) \\ &= 1 \cdot (-1)^{1+n} \cdot (-1)^{1+(n-1)} \cdot \det(L_{n-2}) \\ &= (-1)^{1+n} \cdot (-1)^n \cdot (-1)^{n-1} \cdot \ldots \cdot (-1)^3 \cdot (-1)^2 \\ &= (-1)^S, \end{aligned}$$

onde

$$\begin{aligned} S &= (n+1) + n + (n-1) + \cdots + 3 + 2 \\ &= 1 + 2 + 3 + \cdots + (n-1) + 2n \\ &= \frac{n(n-1)}{2} + 2n. \end{aligned}$$

Assim $\det_n(L_n) = (-1)^S = (-1)^{\frac{n(n-1)}{2}} \neq 0$ e portanto $\det_{n-1}$ não pode dividir $\det_n$. ■

Lema 4.1.15. *Seja $S \in \mathrm{GL}_n$. Então $G_S = \{X \in \mathrm{GL}_n : XSX^t = S\}$ é um subgrupo algébrico.*

Demonstração. G_S é claramente subgrupo de GL_n, logo as operações de multiplicação e inversão são regulares. Por outro lado as equações $XSX^t = S$ são polinomiais nas entradas de X, assim esse conjunto é fechado. ■

Exemplo 4.1.16. Se $\mathbb{K}$ é um corpo com característica diferente de 2 definimos o grupo ortogonal $O_n = O_n(\mathbb{K}) = G_{\mathrm{Id}} = \{X \in \mathrm{GL}_n : XX^t = \mathrm{Id}\}$. Como variedade

$$O_n = \mathcal{V}((f_{ij}, X_0 \det -1)) \subset \mathbb{A}^{n^2+1},$$

onde $f_{ij} = \sum_{k=1}^{n} X_{ik}X_{jk} - \delta_{ij},\ 1 \leq i, j \leq n$. Observe que, como $f_{ij} = f_{ji}$ podemos tomar $1 \leq i \leq j \leq n$.

Dado $X \in O_n$ então $\det X = \pm 1$, logo O_n não é irredutível.

Exemplo 4.1.17. Definimos o *grupo ortogonal especial* como o subgrupo $O_n \cap \mathrm{SL}_n$ de GL_n, e o denotamos por SO_n. Como variedade $\mathrm{SO}_n = \mathcal{V}((f_{ij}, \det -1)_{1 \leq i \leq j \leq n})$. Pode-se mostrar que SO_n é irredutível.

O próximo lema caracteriza os grupos algébricos afins em função de seus subconjuntos abertos.

Lema 4.1.18. *Sejam G um grupo algébrico afim, U e V subconjuntos abertos de G com V denso. Então $G = UV$, ou seja, todo elemento de G se escreve como produto de um elemento de U e um elemento de V.*

Demonstração. A inversão é um homeomorfismo, logo $i(U) = U^{-1}$ é aberto. A translação à direita por um elemento $x \in G$, r_x, também é um homeomorfismo, logo $r_x(U^{-1}) = U^{-1}x$ é aberto. Agora como V é denso $U^{-1}x \cap V \neq \varnothing$ para todo $x \in G$, logo existem $a \in U$ e $b \in V$ tais que $a^{-1}x = b$, então $x = ab$. ■

Lema 4.1.19. *Seja G um grupo algébrico afim e H um subgrupo abstrato, então $\overline{H}$ é um subgrupo algébrico de G.*

Demonstração. Como a inversão é um homeomorfismo, segue do Lema 3.10.2 (2) que $i(\overline{H}) = \overline{i(H)} = \overline{H}$, logo $\overline{H}$ é fechado para inversão. Agora as translações por elementos de G também são homeomorfismos, assim dado $x \in H$ temos $x\overline{H} = \overline{xH} = \overline{H}$, ou seja, $H\overline{H} \subset \overline{H}$. Portanto se $x \in \overline{H}$, então $Hx \subset \overline{H}$, assim $\overline{H}x = \overline{Hx} \subset \overline{H}$, o que implica $\overline{H}$ fechado para a multiplicação. ■

Para que um subgrupo abstrato de um grupo algébrico afim seja um subgrupo fechado, basta que, como conjunto, seja construtível:

Teorema 4.1.20. *Seja G um grupo algébrico afim e H um subgrupo abstrato que também é um subconjunto construtível de G. Então H é um subgrupo algébrico.*

Demonstração. Se H é construtível pelo Corolário 3.10.4 existe um aberto denso $U \subset \overline{H}$ com $U \subset H$. Pelo Lema 4.1.19 $\overline{H}$ é subgrupo algébrico de G. Como a inversão e as translações são homeomorfismos segue que U^{-1}, e portanto, hU^{-1} são abertos densos em $\overline{H}$, para todo $h \in \overline{H}$. Deste modo devemos ter $U \cap hU^{-1} \neq \varnothing$, ou seja, $h \in UU$ e então $\overline{H} = UU \subset HH = H$. ■

Definição 4.1.21. Seja G um grupo algébrico afim e $H \subset G$ um subgrupo fechado. Dizemos que H é um subgrupo *normal* se é normal como um subgrupo abstrato de G.

A partir do último teorema é possível verificar que o kernel e a imagem de um morfismo de grupos algébricos são subgrupos fechados.

Teorema 4.1.22. *Seja $\varphi : H \to G$ um morfismo de grupos algébricos afins. Então:*

(i) $\operatorname{Ker}\varphi \subset H$ *é um subgrupo normal fechado.*

(ii) $\operatorname{Im}\varphi \subset G$ *é um subgrupo fechado.*

Demonstração. (i) O kernel de um homomorfismo de grupos é um subgrupo normal. Agora como φ é uma função contínua e o kernel é a pré imagem do fechado $1_G \in G$, segue que $\operatorname{Ker}\varphi$ é fechado.

(ii) Pelo Teorema de Chevalley (3.10.5) $\operatorname{Im}\varphi$ é um subconjunto construtível e pelo Teorema 4.1.20 concluímos que é um subgrupo fechado.

■

Perceba que, em especial, a imagem de um morfismo de grupos algébricos afins é sempre uma variedade, o que não acontece em geral quando omite-se a estrutura algébrica de grupo.

Observação 4.1.23. Se $H, K \subset G$ são subgrupos fechados de G, com K normalizando H, isto é, $kHk^{-1} = H$ para todo $k \in K$, então HK é um subgrupo fechado de G. De fato, HK é a imagem do morfismo $m(\operatorname{id}|_H \times \operatorname{id}|_K) : H \times K \to G$, logo é construtível.

O próximo teorema apresenta algumas propriedades notáveis dos grupos algébricos afins.

Teorema 4.1.24. *Seja G um grupo algébrico afim.*

(1) *Para cada $x \in G$ existe uma única componente irredutível contendo x.*

(2) *A componente irredutível contendo a unidade (que denotamos G_1) é um subgrupo normal, fechado e de índice finito em G.*

(3) *Para cada $x \in G$ a componente irredutível que contém x é xG_1. Em particular esta componente é isomorfa como variedade a G_1.*

(4) *Se $H \subset G$ é um subgrupo fechado de G com índice finito então $H \supset G_1$. Em particular G_1 é o único subgrupo algébrico irredutível de G com índice finito.*

(5) *Se G e H são subgrupos algébricos afins e $\varphi : H \to G$ é um morfismo, então $\varphi(H_1) = \varphi(H)_1$.*

Demonstração. (1) Sejam $X_1, \ldots, X_r$ as componentes irredutíveis distintas de G que contém 1_G. A imagem da variedade irredutível $X_1 \times \cdots \times X_r$ pelo morfismo produto é uma variedade irredutível. Agora $X_1 \cdot \ldots \cdot X_r \subset X_i$ para algum $i = 1, \ldots, n$. Por outro lado $X_j \subset X_1 \cdot \ldots \cdot X_r$ para todo j, assim concluímos que $r = 1$.

(2) Pelo raciocínio do item anterior sabemos que $G_1G_1 = G_1$. Agora se i é a aplicação de inversão de G, então $i(G_1)$ é uma componente irredutível que contém 1_G, logo $i(G_1) = G_1$. Isso mostra que G_1 é um subgrupo algébrico de G. Para verificar que é normal em G notemos que fixado $g \in G$ o morfismo de conjugação $c_g : G \to G$, dado por $c_g(x) = gxg^{-1}$, é um isomorfismo de grupos algébricos afins. Assim, para todo $g \in G$ temos que gG_1g^{-1} é uma componente irredutível que contém a unidade de G, portanto $gG_1g^{-1} = G_1$.

Por fim, perceba que as classes laterais de G módulo G_1 são translações de G_1, logo também são componentes irredutíveis de G. Agora como G possui uma quantidade finita de componentes irredutíveis, segue que existem finitas classes laterais, isto é, G_1 tem índice finito em G.

(3) Se G' é uma componente irredutível contendo x, então $l_{x^{-1}}(G')$ é uma componente irredutível que contém 1_G e pelo item (1) segue que $l_{x^{-1}}(G') = G_1$. Mas $l_x l_{x^{-1}}(G') = l_x(G_1)$, portanto $G' = xG_1$.

(4) Por hipótese, existem finitas classes laterais de G módulo H. Sejam $g_1, \ldots, g_r \in G$, com $g_1 = 1_G$, tais que G é a união disjunta $G = \bigcup_{i=1}^{r} g_iH$. Perceba que cada classe lateral é um conjunto fechado, pois é a imagem de H por uma translação à esquerda. Deste modo escrevemos

$$G_1 = G_1 \cap G = G_1 \cap (\bigcup_{i=1}^{r} g_iH) = \bigcup_{i=1}^{r} (G_1 \cap g_iH).$$

Como G_1 é irredutível devemos ter $G_1 = G_1 \cap g_iH$, para algum $i = 1, \ldots, r$, ou seja, $G_1 \subset g_iH$ para algum índice i. Agora, do fato que $1_G \in g_1H$, concluímos que $i = 1$ e então $G_1 \subset H$.

(5) Primeiramente note que $\varphi(H_1)$ é fechado, pois é a imagem de um morfismo de grupos algébricos afins, também contém a unidade de G e é irredutível pelo Lema 3.10.2, assim pelo item (1) obtemos $\varphi(H_1) \subset \varphi(H)_1$. Para a inclusão contrária usamos o item (2), o qual garante que H_1 possui índice finito em H. Disso segue que $\varphi(H_1)$ possui índice finito em $\varphi(H)$, pois se $x_1H_1, \ldots, x_rH_1$ são as classes laterais de H módulo H_1, então $\varphi(H)$ se escreve como $\varphi(H) = \bigcup_{i=1}^{r} \varphi(x_i)\varphi(H_1)$. Agora pelo item anterior concluímos que $\varphi(H)_1 \subset \varphi(H_1)$, ou seja $\varphi(H_1) = \varphi(H)_1$.

■

Um espaço topológico X é dito *conexo* se não existem subconjuntos abertos não vazios $U, V \subset X$ tais que $X = U \cup V$. É sabido que se X é irredutível, então também é conexo, mas a recíproca nem sempre é verdadeira. O teorema anterior garante que no caso de um grupo algébrico afim G, as condições de irredutibilidade e conexidade são equivalentes. Com efeito, a componente irredutível que contém $x \in G$ é uma classe lateral de G_1, a dizer xG_1, assim quaisquer duas componentes irredutíveis de X são disjuntas e abertas em G (visto que o complemento de uma componente irredutível é uma união de fechados). Desse modo se G é uma variedade redutível, então não é conexa.

Esse fato motiva a definição a seguir.

Definição 4.1.25. Um grupo algébrico afim G é dito *conexo* se a variedade algébrica G é irredutível. Em outras palavras, G é conexo se $G = G_1$.

4.2 Ações de grupos algébricos afins em variedades

Definição 4.2.1. Sejam X uma variedade algébrica e G um grupo algébrico afim.

(i) Uma *ação regular à esquerda* de G em X é um morfismo de variedades algébricas $\varphi : G \times X \to X$, denotado por $\varphi(g, x) = g \cdot x$, que também é uma ação do grupo abstrato G em X, isto é

$$1_G \cdot x = x,$$
$$(gh) \cdot x = g \cdot (h \cdot x),$$

para todos $g, h \in G$ e $x \in X$. Neste caso dizemos que X é uma *G-variedade* à esquerda.

(ii) Uma *ação regular à direita* de G em X é um morfismo de variedades algébricas $\varphi : X \times G \to X$, denotado por $\varphi(x, g) = x \cdot g$, que também é uma ação do grupo

abstrato G em X, isto é

$$x \cdot 1_G = x,$$
$$x \cdot (gh) = (x \cdot g) \cdot h,$$

para todos $g, h \in G$ e $x \in X$. Neste caso dizemos que X é uma G-*variedade* à direita.

Ainda no contexto mais geral da teoria de ações, isto é, onde G é um grupo abstrato e X um conjunto, dizemos que um subconjunto $Y \subset X$ é G-*invariante* se é fechado para a ação de elementos de G.

Observação 4.2.2. Se X é uma G-variedade e fixando $g \in G$ a aplicação $\varphi_g : X \to X$ dada por $\varphi_g(x) = g \cdot x$ é um isomorfismo de variedades. De fato, primeiramente notamos que φ_g é a composição de morfismos $\varphi_g = \varphi \circ j_g \circ \theta_g$, onde $\theta_g : X \to \{g\} \times X$ é dado por $\theta_g(x) = (g, x)$ e $j_g : \{g\} \times X \to G \times X$ é dado por $j(g, x) = (g, x)$. Desta forma concluímos que φ_g é uma função regular. Agora basta notar que essa função também possui inversa regular, dada por $\varphi_{g^{-1}}$.

Fixando $x \in X$ a *aplicação de órbita* $\pi_x : G \to X$ é dada por $\pi_x(g) = g \cdot x$. Note que esta função também é um morfismo de variedades, pois $\pi_x = \varphi \circ j_x \circ \alpha_x$, onde $\alpha_x : G \to G \times \{x\}$, $g \mapsto (g, x)$ e $j_x : G \times \{x\} \to G \times X$ é dada por $j_x(g, x) = (g, x)$.

Também chamamos o morfismo $G \times X \to X \times X$ dado por $(g, x) \mapsto (g \cdot x, x)$, de *aplicação de órbita*.

Exemplos 4.2.3. (1) Seja G um grupo algébrico. O produto de G define uma ação regular à esquerda de G em si mesmo por $g \cdot h = gh$, para todos $g, h \in G$. De modo análogo definimos uma ação regular à direita de G em G, pondo $h \cdot g = hg$, para todos $g, h \in G$.

(2) O morfismo de conjugação $C : G \times G \to G$ dado por $C(g, h) = ghg^{-1}$ define uma ação regular à esquerda de G em G. De fato, $C = \psi \circ \gamma$, onde $\gamma : G \times G \to G \times G \times G$, $(g, h) \mapsto (g, h, g^{-1})$ e $\psi : G \times G \times G \to G$ denota o morfismo produto. Por outro lado é fácil ver que C satisfaz as condições de uma ação de grupos abstratos.

Definição 4.2.4. Seja G um grupo algébrico afim e X uma G-variedade. Se $x \in X$ a G-*órbita* de x é o conjunto $O(x) = \{g \cdot x : g \in G\}$. O *estabilizador* ou *subgrupo de isotropia* de $x \in X$ é $G_x = \{g \in G : g \cdot x = x\}$. Se $G_x = G$ dizemos que x é um *ponto fixo* para ação. Denotamos o conjunto de todos os pontos fixos por X^G, quando a ação estiver explícita.

Definição 4.2.5. Seja G um grupo algébrico afim. A órbita de um elemento $g \in G$ pela ação de conjugação é chamada de *classe de conjugação de* g, e o seu subgrupo de isotropia

é chamado *centralizador* do elemento $g \in G$. Notamos que para essa ação o conjunto dos pontos fixos coincide com o centro do grupo G.

Observação 4.2.6. Note que uma ação regular à *esquerda* de um grupo algébrico afim G em uma variedade X, induz uma ação à *direita* de G em $\mathbb{K}[X]$ dada por translações, isto é, dados $g, h \in G$ e $f \in \mathbb{K}[X]$ definimos $(f \cdot g)(x) = f(a \cdot x)$. De fato, $f \cdot 1 = f$ e

$$\begin{aligned}(f \cdot (gh))(x) &= f((gh) \cdot x) \\ &= f(g \cdot (h \cdot x)) \\ &= (f \cdot g)(h \cdot x) \\ &= ((f \cdot g) \cdot h)(x).\end{aligned}$$

De modo análogo, uma ação regular à *direita* de G em X induz uma ação à *esquerda* de G em $\mathbb{K}[X]$. Em especial, a ação regular à direita de G em G, dada pela multiplicação $x \cdot g = xg$, induz uma ação à esquerda de G em $\mathbb{K}[G]$ por $(g \cdot f)(x) = f(xg)$.

Definição 4.2.7. Sejam G um grupo algébrico afim e X uma G-variedade. Dados subconjuntos $Y, Z \subset X$ definimos o *transportador de Y para Z* como

$$\mathrm{Tran}_G(Y, Z) = \{g \in G : g \cdot Y \subset Z\}.$$

Definimos o *estabilizador* de Y como o conjunto $\mathrm{Tran}_G(Y, Y)$ e também o *centralizador* de Y como sendo $\mathcal{C}_G(Y) = \bigcap_{y \in Y} G_y$.

Definição 4.2.8. Seja $H \subset G$ um subgrupo fechado. Definimos o *normalizador* de H em G como $\mathcal{N}_G(H) = \{g \in G : gHg^{-1} = H\}$.

Observação 4.2.9. Seja H é um subgrupo fechado de G, considerado como uma G-variedade via a ação de conjugação. Temos que o estabilizador e o normalizador de H coincidem, isto é

$$\mathrm{Tran}_G(H, H) = \mathcal{N}_G(H).$$

De fato, a inclusão ($\supset$) é trivial, logo basta verificar ($\subset$). Suponha $H = \bigcup_{i=1}^{r} H_i$, onde cada H_i é uma componente irredutível. Aplicando o morfismo de conjungação c_g na igualdade anterior, temos

$$gHg^{-1} = \bigcup_{i=1}^{r} gH_ig^{-1}.$$

Agora como c_g é um isomorfismo de variedades temos que $c_g(H_i) = gH_ig^{-1}$ é uma subvariedade irredutível de H. Assim segue que a conjugação apenas permuta as componentes irredutíves de H e portanto $gHg^{-1} = H$, para todo $g \in G$.

Proposição 4.2.10. *O normalizador $\mathcal{N}_G(H)$ é um subgrupo abstrato de G. Mais ainda, $\mathcal{C}_G(H) \subset \mathcal{N}_G(H)$ é um subgrupo normal.*

Demonstração. A verificação que $\mathcal{N}_G(H)$ é um subgrupo de G é direta. Assim vamos mostrar que $\mathcal{C}_G(H) \subset \mathcal{N}_G(H)$ é um subgrupo normal. Primeiramente note que $\mathcal{C}_G(H) = \{g \in G : ghg^{-1} = h, \forall\ h \in H\}$. Agora dado $n \in \mathcal{N}_G(H)$ e $c \in \mathcal{C}_G(H)$, temos

$$(ncn^{-1})h(ncn^{-1})^{-1} = n(c(n^{-1}hn)c^{-1})n^{-1} = n(n^{-1}hn)n^{-1} = h,$$

para todo $h \in H$, portanto $ncn^{-1} \in \mathcal{C}_G(H)$. ■

O próximo resultado mostra que os elementos presentes na teoria de ações de grupos algébricos afins respeitam a estrutura de variedade, ou seja, são subconjuntos fechados.

Teorema 4.2.11. *Sejam G um grupo algébrico afim e X uma G-variedade. Então,*

(1) *Se $Y, Z \subset X$ são subconjuntos, com Z fechado, então* $\mathrm{Tran}_G(Y, Z)$ *é fechado.*

(2) *O subgrupo de isotropia de $x \in X$ é fechado. Em especial $\mathcal{C}_G(Y)$ é um subgrupo fechado.*

(3) *O conjunto X^G de pontos fixos é fechado.*

(4) *Se G é conexo, então G estabiliza todas as componentes irredutíveis de X.*

Demonstração. (1) Seja $\pi_x : G \to X$ a aplicação de órbita para um elemento $x \in X$. Afirmamos que $\mathrm{Tran}_G(Y, Z) = \bigcap_{y \in Y} \pi_y^{-1}(Z)$, e portanto como a aplicação de órbita é uma função contínua, o transportador de Y para Z é fechado. Com efeito,

$$\begin{aligned} g \in \mathrm{Tran}_G(Y, Z) &\Leftrightarrow \pi_y(g) \in Z, \forall\ y \in Y \\ &\Leftrightarrow g \in \pi_y^{-1}(Z), \forall\ y \in Y \\ &\Leftrightarrow g \in \bigcap_{y \in Y} \pi_y^{-1}(Z). \end{aligned}$$

(2) Basta notar que $G_x = \mathrm{Tran}_G(\{x\}, \{x\})$ e usar o item anterior.

(3) Dado $a \in G$, considere a aplicação $\varphi_g : X \to X$, dada por $\varphi_g(x) = g \cdot x$. Definimos o *gráfico* de φ_g, como o conjunto $\Gamma(\varphi_a) = \{(x, y) \in X \times X : x = g \cdot y\}$. Note que $\Gamma(\varphi_g)$ é um subconjunto fechado de $X \times X$, basta escrever a relação $x = g \cdot y$ em coordenadas. Agora o conjunto X^g dos pontos fixos por um elemento $g \in G$ é fechado, pois $X^g = \delta^{-1}(\Gamma(\varphi_g))$. Portanto, $X^G = \bigcap_{g \in G} X^g$ é fechado.

(4) Denote $\varphi : G \times X \to X$ a ação de G em X e X_1 uma componente irredutível de X. Se G é conexo então pela Proposição 3.9.1 (1), a variedade $G \times X_1$ é irredutível, portanto pelo Lema 3.10.2 (3) temos que $\varphi(G \times X_1) = G \cdot X_1$ também é irredutível. Agora $X_1 = 1 \cdot X_1 \subset G \cdot X_1$, assim pela maximalidade de X_1

$$G \cdot X_1 = X_1,$$

ou seja, G estabiliza X_1.

■

Corolário 4.2.12. *Sejam G um grupo algébrico conexo e $H \subset G$ um subgrupo normal e finito. Então $H \subset \mathcal{Z}(G)$.*

Demonstração. Como H é normal em G, para todo $h \in H$ e $g \in G$ temos $ghg^{-1} \in H$. Assim considere a ação $C : G \times H \in H$, dada por $C(g,h) = ghg^{-1}$.

Seja $H = H_1 \cup \cdots \cup H_r$ a decomposição de H em componentes irredutíveis. Note que, como H é finito, cada componente H_j é simplesmente um ponto, isto é, $H_j = \{h_j\}$ para todo $j = 1, \ldots, r$. Agora como G é conexo, pelo teorema anterior sabemos que estabiliza todo H_j, isto é,

$$G \cdot H_j = H_j \Rightarrow gh_jg^{-1} = h_j \Rightarrow gh_j = h_jg,$$

para todo $g \in G$ e $j = 1, \ldots, r$, deste modo temos $H \subset \mathcal{Z}(G)$. ■

Corolário 4.2.13. *Sejam G um grupo algébrico afim e $H \subset G$ um subgrupo fechado. Então $\mathcal{N}_G(H)$ e $\mathcal{C}_G(H)$ são subgrupos fechados de G. Em particular $\mathcal{Z}(G) = \mathcal{C}_G(G)$ é fechado.*

Demonstração. Segue diretamente do Teorema 4.2.11 e da Observação 4.2.9. ■

O próximo teorema explora um fato geométrico acerca das órbitas associadas a ação de um grupo algébrico afim.

Teorema 4.2.14. *Seja G um grupo algébrico afim agindo regularmente em uma variedade algébrica X. Então para todo $x \in X$, $O(x)$ é aberta em $\overline{O(x)}$.*

Demonstração. Considere o morfismo de variedades $\varphi_x : G \to \overline{O(x)}$, dado por $\varphi_x(g) = g \cdot x$. Pelo Teorema de Chevalley (3.10.5) $O(x) = \varphi_x(G)$ é um subconjunto construtível e pelo Corolário 3.10.4 contém um aberto denso não vazio U de $\overline{O(x)}$.

Como U é não vazio, existem $u \in U$ e $h \in G$ tais que $u = h \cdot x$, logo $h^{-1} \cdot u = x$. Agora dado $z = g' \cdot x \in O(x)$, temos

$$z = g' \cdot (h^{-1} \cdot u) = (g'h^{-1}) \cdot u = g \cdot u,$$

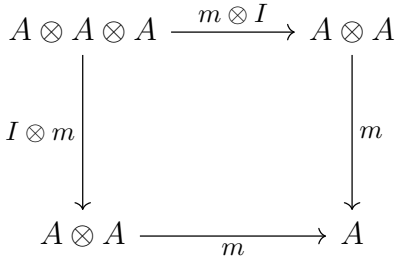
ou seja, $z \in g \cdot U$. Como tomamos z arbitrário na órbita de x, segue que

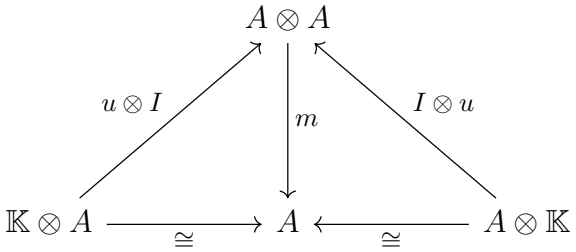
$$O(x) = \bigcup_{g \in G} g \cdot U,$$

e cada $g \cdot U$ é aberto, pois φ_x é um homeomorfismo. Assim, concluímos que $O(x)$ é aberto em $\overline{O(x)}$. ■

4.3 Álgebras de Hopf e grupos algébricos

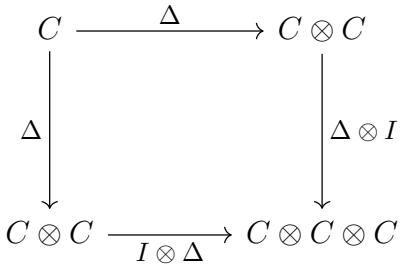
Seja $\mathbb{K}$ um corpo. Como vimos na Proposição 2.6.9 uma $\mathbb{K}$-álgebra pode ser definida por uma tripla (A, m, u), onde A é um $\mathbb{K}$-espaço vetorial e $m : A \otimes A \to A$, $u : \mathbb{K} \to A$ são transformações lineares, tais que os seguintes diagramas são comutativos:

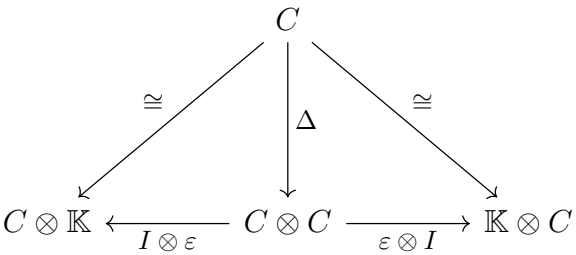




Revertendo as flechas dos diagramas anteriores obtemos uma estrutura dual à de álgebra, a estrutura de coálgebra.

Definição 4.3.1. Seja $\mathbb{K}$ um corpo. Uma $\mathbb{K}$-coálgebra é uma tripla (C, Δ, ε) consistindo em um $\mathbb{K}$-espaço vetorial C e duas transformações lineares $\Delta : C \to C \otimes C$, $\varepsilon : C \to \mathbb{K}$ tais que os diagramas abaixo são comutativos.





O primeiro diagrama é chamado de *coassociatividade* de C e o segundo de *counidade*.

Uma transformação linear $f : C \to D$ entre coálgebras é chamada de *morfismo de coálgebras* se $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$ e $\varepsilon_D f = \varepsilon_C$.

Notação 4.3.2 (Sweedler para coálgebras)**.** Denotamos $\Delta^2 = (\Delta \otimes I)\Delta = (I \otimes \Delta)\Delta : C \to C \otimes C \otimes C$. Também usamos, ao invés da notação comum em somatórios,

$$\Delta(c) = \sum_{i=1}^{n} (c_1)_i \otimes (c_2)_i,$$

a convenção

$$\Delta(c) = \sum c_1 \otimes c_2,$$

onde o índice i é omitido e os elementos c_1, c_2 percorrem C em uma soma finita. Para Δ^2 a convenção é análoga:

$$\Delta^2(c) = (\Delta \otimes I)\Delta(c) = \sum c_{1,1} \otimes c_{1,2} \otimes c_2,$$

ou ainda,

$$\Delta^2(c) = (I \otimes \Delta)\Delta(c) = \sum c_1 \otimes c_{2,1} \otimes c_{2,2}.$$

Exemplos 4.3.3. Alguns exemplos de coálgebras:

(1) Um corpo $\mathbb{K}$ arbitrário munido das transformações lineares: $\Delta : \mathbb{K} \to \mathbb{K} \otimes \mathbb{K}$ sendo o isomorfismo canônico $\Delta(\alpha) = \alpha \otimes 1$ e $\varepsilon : \mathbb{K} \to \mathbb{K}$ a identidade, é uma $\mathbb{K}$-coálgebra.

(2) Seja S um conjunto não vazio e considere $\mathbb{K}S$ o $\mathbb{K}$-módulo livre sobre S, isto é, o $\mathbb{K}$-espaço vetorial de base S. Então $\mathbb{K}S$ é uma coálgebra com coproduto e counidade definidos por $\Delta(s) = s \otimes s$, $\varepsilon(s) = 1$, para todo $s \in S$. De fato,

$$(\Delta \otimes I)\Delta(s) = (\Delta \otimes I)(s \otimes s) = (s \otimes s) \otimes s = (I \otimes \Delta)\Delta(s),$$

o que implica a coassoatividade. E as igualdades

$$(\varepsilon \otimes I)\Delta(s) = (\varepsilon \otimes I)(s \otimes s) = 1 \otimes s,$$
$$(I \otimes \varepsilon)\Delta(s) = (I \otimes \varepsilon)(s \otimes s) = s \otimes 1,$$

concluem a counidade.

Quando um $\mathbb{K}$-espaço vetorial possui ambas as estruturas de álgebra e coálgebra, de forma que as aplicações sejam "compatíveis", o chamamos de *biálgebra*. A definição precisa deste conceito é feita a seguir.

Definição 4.3.4. Seja $\mathbb{K}$ um corpo. Uma *biálgebra* sobre $\mathbb{K}$ é uma quíntupla $(B, m, u, \Delta, \varepsilon)$, onde (B, m, u) é uma álgebra associativa com unidade e (B, Δ, ε) é uma coálgebra, tal que $\varepsilon : B \to \mathbb{K}$ e $\Delta : B \to B \otimes B$ são homomorfismos de $\mathbb{K}$-álgebras.

Pode-se mostrar que a condição de compatibilidade entre as estruturas pode ser exigida nas aplicações m e u, isto é, a condição de Δ e ε serem homomorfismos de $\mathbb{K}$-álgebras, é equivalente a m e u serem homomorfismos de $\mathbb{K}$-coálgebras (veja a Proposição 4.4.4 em [9]).

Vejamos agora alguns exemplos de biálgebras.

Exemplos 4.3.5. (1) O corpo $\mathbb{K}$ possui estrutura de álgebra e de coálgebra, além disso são compatíveis, visto que as aplicações Δ e ε definidas no Exemplo 4.3.3 (1) são homomorfismos de $\mathbb{K}$-álgebras.

(2) Seja G um semigrupo. A *álgebra de semigrupo* $\mathbb{K}G$ consiste no $\mathbb{K}$-espaço vetorial livre sobre G, munido da multiplicação dada por $g \cdot h = gh$, para todos $g, h \in G$. Como vimos no Exemplo 4.3.3 (2) $\mathbb{K}G$ é uma coálgebra com $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$, para todo $g \in G$. Além disso, $\Delta(gh) = gh \otimes gh = (g \otimes g)(h \otimes h) = \Delta(g)\Delta(h)$ e $\varepsilon(gh) = 1 = \varepsilon(g)\varepsilon(h)$, logo esse espaço vetorial é uma biálgebra.

Sejam C e A dois $\mathbb{K}$-espaços vetoriais. É bem conhecido que o conjunto das transformações lineares de C para A, denotado por $\mathrm{Hom}_{\mathbb{K}}(C, A)$, é naturalmente munido da estrutura de $\mathbb{K}$-espaço vetorial. A definição abaixo indica que, quando os espaços vetoriais possuem uma estrutura adicional, a dizer, C a de coálgebra e A a de álgebra, é possível definir um produto entre transformações lineares, chamado de *produto de convolução*.

Definição 4.3.6. Sejam $\mathbb{K}$ um corpo, (A, m, u) uma $\mathbb{K}$-álgebra e (C, Δ, ε) uma $\mathbb{K}$-coálgebra. Dadas transformaçoes lineares $f, g \in \mathrm{Hom}_{\mathbb{K}}(C, A)$ o *produto de convolução* de f e g é definido como a aplicação $f \star g \in \mathrm{Hom}_{\mathbb{K}}(C, A)$, dada por $(f \star g)(c) = \sum f(c_1)g(c_2)$.

Pode-se mostrar que o $\mathbb{K}$-espaço $\mathrm{Hom}_{\mathbb{K}}(C, A)$ munido da operação de convolução é uma $\mathbb{K}$-álgebra, cuja unidade é $u\varepsilon$.

Observação 4.3.7. Perceba que a transformação linear $f \star g$ pode ser definida pela comutatividade do diagrama

$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ {\scriptstyle f \star g}\downarrow & & \downarrow{\scriptstyle f \otimes g} \\ A & \xleftarrow[m]{} & A \otimes A \end{array}$$

onde m denota a multiplicação de A.

Uma álgebra de Hopf nada mais é do que uma biálgebra junto de um operador linear especial, chamado antípoda. Mais especificamente:

Definição 4.3.8. Uma biálgebra C com a propriedade do operador linear indentidade $I \in \mathrm{End}_{\mathbb{K}}(C)$ ser invertível por convolução é chamada *álgebra de Hopf*, e a inversa por convolução de I, isto é, o operador $S_C : C \to C$, é chamado de antípoda.

A seguir descrevemos dois exemplos clássicos de álgebras de Hopf.

Exemplos 4.3.9. (1) *Álgebra de Grupo.* Seja G um grupo multiplicativo e $\mathbb{K}G$ a álgebra de grupo associada, isto é, a álgebra de semigrupo descrita no Exemplo 4.3.5. Como visto no exemplo citado, $\mathbb{K}G$ é uma biálgebra, com estrutura de coálgebra dada por $\Delta(g) = g \otimes g$ e $\varepsilon(g) = 1$ para todo $g \in G$. Vamos verificar que a estrutura adicional de inversão presentes nos grupos induz em $\mathbb{K}G$ uma estrutura de álgebra de Hopf, com antípoda $S : \mathbb{K}G \to \mathbb{K}G$, dada por $S(g) = g^{-1}$ e estendida por linearidade.

Com efeito,

$$\begin{aligned}(S \star I)(g) &= \sum S(g_1)I(g_2) \\ &= S(g)I(g) \\ &= g^{-1}g \\ &= 1 \\ &= u\varepsilon(g)\end{aligned}$$

e

$$\begin{aligned}(I \star S)(g) &= \sum I(g_1)S(g_2) \\ &= I(g)S(g) \\ &= gg^{-1} \\ &= 1 \\ &= u\varepsilon(g).\end{aligned}$$

(2) *Álgebra de polinômios* $\mathbb{K}[X]$. Introduzimos uma estrutura de coálgebra em $\mathbb{K}[X]$: pela propriedade universal da $\mathbb{K}$-álgebra $\mathbb{K}[X]$, existe um único homomorfismo de $\mathbb{K}$-álgebras $\Delta : \mathbb{K}[X] \to \mathbb{K}[X] \otimes \mathbb{K}[X]$ tal que $\Delta(a) = a \otimes 1$ para $a \in \mathbb{K}$ e $\Delta(X) = X \otimes 1 + 1 \otimes X$. Note que,

$$\begin{aligned}((\Delta \otimes I)\Delta)(X) &= (\Delta \otimes I)(X \otimes 1 + 1 \otimes X) \\ &= (\Delta \otimes I)(X \otimes 1) + (\Delta \otimes I)(1 \otimes X) \\ &= (X \otimes 1 + 1 \otimes X) \otimes 1 + (1 \otimes 1) \otimes X \\ &= X \otimes 1 \otimes 1 + 1 \otimes X \otimes 1 + 1 \otimes 1 \otimes X\end{aligned}$$

e

$$\begin{aligned}((I\otimes\Delta)\Delta)(X) &= (I\otimes\Delta)(X\otimes 1+1\otimes X)\\ &= (I\otimes\Delta)(X\otimes 1)+(I\otimes\Delta)(1\otimes X)\\ &= X\otimes(1\otimes 1)+1\otimes(X\otimes 1+1\otimes X)\\ &= X\otimes 1\otimes 1+1\otimes X\otimes 1+1\otimes 1\otimes X.\end{aligned}$$

Portanto, novamente pela propriedade universal de $\mathbb{K}[X]$ temos $(\Delta\otimes I)\Delta = (I\otimes\Delta)\Delta$, o que conclui Δ associativo.

Para a counidade definimos $\varepsilon : \mathbb{K}[X] \to \mathbb{K}$ por $\varepsilon(X) = 0$ e $\varepsilon(a) = a$, para todo $a \in \mathbb{K}$. É fácil ver que $(\varepsilon\otimes I)\Delta = (I\otimes\varepsilon)\Delta$, deste modo concluímos que $(\mathbb{K}[X], m, u, \Delta, \varepsilon)$ é uma biálgebra.

Resta mostrar que I é invertível por convolução. Utilizando a propriedade universal de $\mathbb{K}[X]$ obtemos um homomorfismo de $\mathbb{K}$-álgebras $S : \mathbb{K}[X] \to \mathbb{K}[X]$, dado por $S(X) = -X$ e $S(a) = a$, para todo $a \in \mathbb{K}$. Vejamos que S é antípoda.

$$\begin{aligned}(S\star I)(X) &= S(X)I(1)+S(1)I(X)\\ &= (-X)\cdot 1+1\cdot X\\ &= 0\\ &= u\varepsilon(X)\end{aligned}$$

e

$$\begin{aligned}(S\star I)(a) &= S(a)I(1)\\ &= a\cdot 1\\ &= a\\ &= u\varepsilon(a),\end{aligned}$$

logo $S\star I = u\varepsilon$. Analogamente verifica-se $I\star S = u\varepsilon$.

Agora discutimos a principal álgebra de Hopf deste trabalho: a álgebra de funções de um grupo algébrico afim.

Definição 4.3.10. Sejam $\mathbb{K}$ um corpo algebricamente fechado e (G, m, i) um grupo algébrico afim. Definimos as aplicações:

- $\Delta : \mathbb{K}[G] \to \mathbb{K}[G]\otimes\mathbb{K}[G]$ pela composição $\iota_G \circ m^*$, onde $\iota_G : \mathbb{K}[G\times G] \xrightarrow{\sim} \mathbb{K}[G]\otimes\mathbb{K}[G]$ é o isomorfismo descrito na Proposição 3.9.1 (3), e m^* é o comorfismo induzido pela multiplicação de G;

- $\varepsilon : \mathbb{K}[G] \to \mathbb{K}$ sendo o homomorfismo de álgebras dado pela avaliação na identidade de G, ou seja, $\varepsilon(f) = f(1_G)$;
- $S : \mathbb{K}[G] \to \mathbb{K}[G]$ como o comorfismo i^*, induzido pela inversão de G, isto é, $S(f)(g) = f(g^{-1})$, para todo $g \in G$ e $f \in \mathbb{K}[G]$.

Observação 4.3.11. Sempre que nos referirmos a estrutura de álgebra de Hopf associada a um grupo algébrico afim, as aplicações Δ, ε e S são as definidas acima.

O lema a seguir se trata de uma propriedade notável da aplicação Δ da álgebra de funções de um grupo algébrico afim, a qual usamos extensivamente ao decorrer do texto.

Lema 4.3.12. *$\Delta(f) = \sum f_1 \otimes f_2$ se, e somente se, $f(xy) = \sum f_1(x)f_2(y)$, para todo $x, y \in G$.*

Demonstração. Primeiramente dado $f \in \mathbb{K}[G \times G]$ note que

$$\begin{aligned} & \iota_G(f) = \sum f_1 \otimes f_2 \\ \Leftrightarrow\ & \iota_G^{-1}(\iota_G(f)) = \iota_G^{-1}(\sum f_1 \otimes f_2) \\ \Leftrightarrow\ & f = \sum f_1 f_2, \end{aligned}$$

ou seja,

$$\iota_G(f) = \sum f_1 \otimes f_2 \Leftrightarrow f(x, y) = \sum f_1(x)f_2(y),$$

para todo $(x, y) \in G \times G$. Logo

$$\begin{aligned} & \Delta(f) = \sum f_1 \otimes f_2 \\ \Leftrightarrow\ & \iota_G(m^*(f)) = \sum f_1 \otimes f_2 \\ \Leftrightarrow\ & m^*(f) = \iota_G^{-1}(\sum f_1 \otimes f_2) \\ \Leftrightarrow\ & f(xy) = \sum f_1(x)f_2(y), \end{aligned}$$

para todo $x, y \in G$. ■

Teorema 4.3.13. *Sejam $\mathbb{K}$ um corpo algebricamente fechado e G um grupo algébrico afim. A álgebra $\mathbb{K}[G]$ junto das aplicações Δ, ε e S é uma álgebra de Hopf.*

Demonstração. Coassociatividade. Pelo Lema 4.3.12 sabemos que

$$\Delta(f) = \sum f_1 \otimes f_2 \Leftrightarrow f(xy) = \sum f_1(x)f_2(y),$$

para todos $x, y \in G$. Portanto

$$(\Delta \otimes I)\Delta(f) = \sum f_{1,1} \otimes f_{1,2} \otimes f_2 \Leftrightarrow f((xy)z) = \sum f_{1,1}(x)f_{1,2}(y)f_2(z),$$

para todos $x, y, z \in G$. De modo análogo temos

$$(I \otimes \Delta)\Delta(f) = \sum f_1 \otimes f_{2,1} \otimes f_{2,2} \Leftrightarrow f(x(yz)) = \sum f_1(x) f_{2,1}(y) f_{2,2}(z),$$

para todos $x, y, z \in G$.

Agora como G é associativo, obtemos $f((xy)z) = f(x(yz))$, ou seja

$$\sum f_{1,1}(x) f_{1,2}(y) f_2(z) = \sum f_1(x) f_{2,1}(y) f_{2,2}(z)$$

para todos $x, y, z \in G$. Portanto

$$(\Delta \otimes I)\Delta = (I \otimes \Delta)\Delta.$$

Counidade. Basta mostrar que, para todo $f \in \mathbb{K}[G]$

$$f = \sum \varepsilon(f_1) f_2 \quad \text{e} \quad f = \sum f_1 \varepsilon(f_2).$$

Para isso tome $x = 1_G$ no Lema 4.3.12, deste modo temos

$$f(y) = \sum f_1(1_G) f_2(y) = \sum \varepsilon(f_1) f_2(y),$$

para todo $y \in G$, portanto $f = \sum \varepsilon(f_1) f_2$. Tomando $y = 1_G$ obtemos a outra igualdade.
Antípoda. É necessário mostrar que

$$(S \star I)(f) = u\varepsilon(f) \quad \text{e} \quad (I \star S)(f) = u\varepsilon(f),$$

para todo $f \in \mathbb{K}[G]$, ou seja,

$$(\sum S(f_1) f_2)(y) = \varepsilon(f) 1(y) \quad \text{e} \quad (\sum f_1 S(f_2))(y) = \varepsilon(f) 1(y),$$

para todo $y \in G$.

Agora para obter as igualdades acima, primeiramente tomamos $x = y^{-1}$ no Lema 4.3.12,

$$f(1_G) = \sum f_1(y^{-1}) f_2(y) = \sum S(f_1)(y) f_2(y) = (\sum S(f_1) f_2)(y),$$

e tomando $y = x^{-1}$ obtemos a segunda igualdade. ■

Nos exemplos abaixo descrevemos as expressões do coproduto, counidade e antípoda para a álgebra de funções dos grupos aditivo G_a, multiplicativo G_m e linear geral GL_n.

Exemplos 4.3.14. (1) G_a. Sabemos que a álgebra de funções do grupo aditivo é isomorfa a álgebra de polinômios em uma variável $\mathbb{K}[X]$. Como função polinomial X é dado

por $X(g) = g$, para todo $g \in G_a$. Agora note que

$$X(g+h) = g + h = 1(g)X(g) + X(h)1(h) = (1 \cdot X + X \cdot 1)(g+h),$$

para todos $g, h \in G_a$, portanto pelo Lema 4.3.12 temos $\Delta(X) = 1 \otimes X + X \otimes 1$, onde $1 \in \mathbb{K}[G_a]$ é a função constante igual a $1 \in \mathbb{K}$.

O elemento neutro de G_a é $0 \in \mathbb{K}$, logo $\varepsilon(X) = X(0) = 0$ e por fim $S(X) = -X$.

(2) G_m. A álgebra de funções do grupo multiplicativo é isomorfa à álgebra de polinômios de Laurent em uma variável, isto é, $\mathbb{K}[X, X^{-1}]$ (veja o Exemplo 3.7.4). Como funções os geradores são dados por $X(g, g^{-1}) = g$ e $X^{-1}(g, g^{-1}) = g^{-1}$, para todo $(g, g^{-1}) \in G_m$. De modo similar ao exemplo anterior, avaliamos os geradores X e X^{-1} em produtos da forma $(g, g^{-1})(h, h^{-1})$, com $(g, g^{-1}), (h, h^{-1}) \in G_m$. Obtemos

$$\begin{aligned} X((g, g^{-1})(h, h^{-1})) &= X((gh, (gh)^{-1})) \\ &= gh \\ &= X((g, g^{-1}))X((h, h^{-1})) \end{aligned}$$

e

$$\begin{aligned} X^{-1}((g, g^{-1})(h, h^{-1})) &= X^{-1}((gh, (gh)^{-1})) \\ &= (gh)^{-1} \\ &= g^{-1}h^{-1} \\ &= X^{-1}((g, g^{-1}))X^{-1}((h, h^{-1})). \end{aligned}$$

Assim, pelo Lema 4.3.12 segue que

$$\Delta(X) = X \otimes X \text{ e } \Delta(X^{-1}) = X^{-1} \otimes X^{-1}.$$

Ao avaliar as funções X e X^{-1} na identidade de G_m, obtemos a mesma expressão para $\varepsilon(X)$ e $\varepsilon(X^{-1})$. De fato,

$$\varepsilon(X) = X((1,1)) = 1 = X^{-1}((1,1)) = \varepsilon(X^{-1}).$$

Por fim, a antípoda é dada por

$$S(X)(g, g^{-1}) = X((g^{-1}, g)) = g^{-1}$$

e

$$S(X^{-1})(g, g^{-1}) = X^{-1}((g^{-1}, g)) = g,$$

então,

$$S(X) = X^{-1} \text{ e } S(X^{-1}) = X.$$

(3) GL_n. A álgebra de funções de GL_n é isomorfa a $\mathbb{K}[X_0, X_{11}, \ldots, X_{nn}]$, onde $X_0 \det = 1$. Como função $X_0 : \mathrm{GL}_n \to \mathbb{K}$ é dado por $X_0(M) = m_0 = 1/\det(M)$.

Para o coproduto note que,

$$X_{ij}(MN) = (MN)_{ij} = \sum_k m_{ik} n_{kj} = \sum_k X_{ik}(M) X_{kj}(N),$$

para todo $M, N \in \mathrm{GL}_n$, logo pelo Lema 4.3.12 segue que $\Delta(X_{ij}) = \sum_k X_{ik} \otimes X_{kj}$.

De modo semelhante para X_0, temos

$$X_0(MN) = 1/\det(MN) = 1/\det(M) \cdot 1/\det(N) = X_0(M) X_0(N),$$

para todo $M \in \mathrm{GL}_n$, portanto $\Delta(X_0) = X_0 \otimes X_0$. O mesmo vale para a função det, isto é, $\Delta(\det) = \det \otimes \det$.

O elemento neutro de GL_n é a matriz identidade de ordem n, a dizer, Id_n. Assim

$$\varepsilon(X_{ij}) = X_{ij}(\mathrm{Id}_n) = \delta_{ij} \text{ e } \varepsilon(X_0) = X_0(\mathrm{Id}_n) = 1.$$

A antípoda na função X_0 é dada por

$$S(X_0)(M) = X_0 \circ i(M) = X_0(M^{-1}) = 1/\det(M^{-1}) = \det(M),$$

para todo $M \in \mathrm{GL}_n$. Assim, $S(X_0) = \det$. De modo análogo obtemos $S(\det) = X_0$.

Para concluir resta indicar a antípoda nas funções X_{ij}.

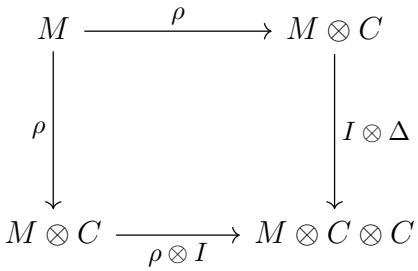
$$S(X_{ij})(M) = X_{ij} \circ i(M) = m_0 \tilde{c}_{ij} = X_0(M) c_{ji} = (-1)^{j+i} X_0(M) \det M(j|i),$$

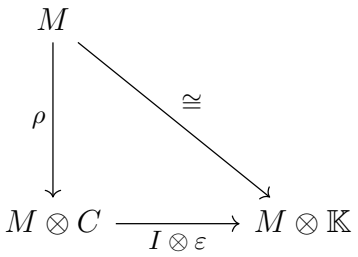
logo $S(X_{ij}) = (-1)^{j+i} X_0 \det_{(j|i)}$, onde a função $\det_{(j|i)}$ é dada por $\det_{(j|i)}(M) = \det M(j|i)$. Perceba que a função $\det_{(j|i)}$ nada mais é do que a composição de det com a função que elimina a linha j e coluna i de uma matriz, deste modo é regular.

4.4 Comódulos

Definição 4.4.1. Sejam $\mathbb{K}$ um corpo e (C, Δ, ε) uma coálgebra sobre $\mathbb{K}$. Um *C-comódulo* à direita é um par (M, ρ), onde M é um $\mathbb{K}$-espaço vetorial e $\rho : M \to M \otimes C$ uma

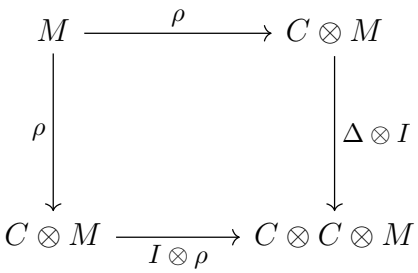
transformação linear tal que os diagramas abaixo são comutativos.

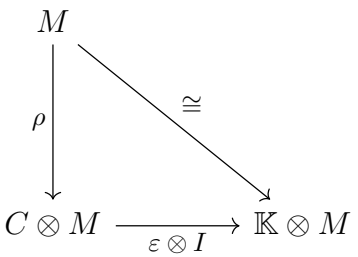




De forma análoga definimos comódulos à esquerda.

Definição 4.4.2. Sejam $\mathbb{K}$ um corpo e (C, Δ, ε) uma coálgebra sobre $\mathbb{K}$. Um *C-comódulo* à esquerda é um par (M, ρ), onde M é um $\mathbb{K}$-espaço vetorial e $\rho : M \to C \otimes M$ uma transformação linear tal que os diagramas abaixo são comutativos.





Quando apresentamos as coálgebras convencionamos a notação de somatório para a expressão do coproduto (veja a Notação 4.3.2). Faremos o mesmo para a aplicação de um comódulo.

Notação 4.4.3 (Sweedler para comódulos)**.** Seja M junto da aplicação $\rho : M \to M \otimes C$ um C-comódulo à direita. Para todo $m \in M$ escrevemos

$$\rho(m) = \sum m_0 \otimes m_1,$$

onde os elementos m_0 da primeira componente do tensor pertencem a M e os elementos m_1 da segunda componente pertencem a C.

No caso de M ser um C-comódulo à esquerda, denotamos

$$\rho(m) = \sum m_{-1} \otimes m_0.$$

Pela definição da estrutura de comódulo à direita podemos escrever $\rho^2 = (\rho \otimes I)\rho = (I \otimes \Delta)\rho : M \to M \otimes C \otimes C$ e na notação anterior temos

$$\rho^2(m) = \sum m_{0,0} \otimes m_{0,1} \otimes m_1 = \sum m_0 \otimes m_{1,1} \otimes m_{1,2}.$$

Para um comódulo à esquerda a convenção é similar,

$$\rho^2(m) = \sum m_{-1} \otimes m_{0,-1} \otimes m_{0,0} = \sum m_{-1,1} \otimes m_{-1,2} \otimes m_0.$$

Exemplos 4.4.4. (1) Uma coálgebra C possui estruturas de comódulo à esquerda e à direita sobre si mesmo, dadas pelo coproduto $\Delta : C \to C \otimes C$.

(2) Seja C uma coálgebra sobre $\mathbb{K}$ e M um $\mathbb{K}$-espaço vetorial. Então $M \otimes C$ admite uma estrutura de C-comódulo à direita $\rho : M \otimes C \to M \otimes C \otimes C$, induzida pelo coproduto Δ, isto é, $\rho = I \otimes \Delta$.

Por fim definimos o conceito de morfismo entre duas estruturas de comódulos à direita (para comódulos à esquerda a definição é análoga).

Definição 4.4.5. Sejam C uma coálgebra e $(M, \rho), (N, \psi)$ dois C-comódulos à direita. Uma transformação linear $f : M \to N$ é um *morfismo* de C-comódulos se o diagrama abaixo é comutativo.

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ \Big\downarrow{\scriptstyle \rho} & & \Big\downarrow{\scriptstyle \psi} \\ M \otimes C & \xrightarrow[f \otimes I]{} & N \otimes C \end{array}$$

4.5 Linearidade dos grupos algébricos afins

Definição 4.5.1. Sejam $\mathbb{K}$ um corpo arbitrário e G um grupo abstrato agindo em um $\mathbb{K}$-espaço vetorial V. Se para todo $g \in G$ a aplicação $\varphi_g : V \to V$, dada por $v \mapsto g \cdot v$, é uma transformação linear, dizemos que V é uma *representação* de G, ou que a ação é *linear*.

Perceba que se a ação $\varphi : G \times V \to V$ é linear, então as transformações lineares φ_g são automorfismos do espaço vetorial V, visto que para cada $g \in G$, φ_g e $\varphi_{g^{-1}}$ são inversas.

A definição de representação dada acima é equivalente à existência de um homomorfismo de grupos abstratos $\sigma : G \to \mathrm{GL}(V)$ (veja [21], Capítulo 8.3). Agora se G é grupo algébrico afim σ não é necessariamente um morfismo de variedades. Como veremos no Lema 4.5.11, uma condição necessária e suficiente para isso é que a ação associada seja *racional*.

Definição 4.5.2. Sejam G um grupo abstrato e M uma representação de G. Para cada funcional $\alpha \in M^*$ e $m \in M$ definimos a função $\alpha|m : G \to \mathbb{K}$ por $(\alpha|m)(x) = \alpha(x \cdot m)$, para todo $x \in G$. Uma função desta forma é chamada de *função M-representativa* ou apenas *função representativa*.

Observação 4.5.3. Sejam G um grupo abstrato que age por automorfismos em um $\mathbb{K}$-espaço vetorial M e $\mathbb{K}^G$ a $\mathbb{K}$-álgebra de todas as funções de G para $\mathbb{K}$. Definimos a aplicação $r_M : M \otimes M^* \to \mathbb{K}^G$ por $r_M(m \otimes \alpha) = \alpha|m$. Note que r_M é uma transformação linear bem definida, visto que a aplicação $R_M : M \times M^* \to \mathbb{K}^G$ dada por $R_M(m, \alpha) = \alpha|m$ é $\mathbb{K}$-bilinear.

Se M for um $\mathbb{K}$-espaço de dimensão finita então o subespaço das funções M-representativas também o é. Para observar esse fato consideremos uma base $\{e_1, \ldots, e_n\}$ de M e $\{e^1, \ldots, e^n\}$ sua base dual. Assim, os tensores $e_i \otimes e^j$ formam uma base de $M \otimes M^*$. Agora dados $\alpha \in M^*$ e $m \in M$ existem escalares $\lambda_{ij} \in \mathbb{K}$ tais que

$$m \otimes \alpha = \sum_{1 \leq i,j \leq n} \lambda_{ij} e_i \otimes e^j,$$

logo

$$\begin{aligned} \alpha|m &= r_M(m \otimes \alpha) \\ &= r_M\left(\sum_{1 \leq i,j \leq n} \lambda_{ij} e_i \otimes e^j\right) \\ &= \sum_{1 \leq i,j \leq n} \lambda_{ij} (e^j|e_i). \end{aligned}$$

Portanto as funções $\{e^j|e_i : 1 \leq i, j \leq n\}$ geram o espaço de todas as funções M-representativas.

Definição 4.5.4. Sejam G um grupo abstrato e M uma representação de G. Dizemos que a representação M é *localmente finita* se para cada $m \in M$ existir um subespaço $N \subset M$ de dimensão finita e G-invariante que contém m.

Note que, uma representação de dimensão finita é sempre localmente finita.

Notação 4.5.5. Seja G um grupo agindo em um $\mathbb{K}$-espaço vetorial M. Denotamos por $\langle G \cdot m \rangle$ o $\mathbb{K}$-subespaço gerado pela órbita de m, isto é, o subespaço $\langle g \cdot m : g \in G \rangle_{\mathbb{K}}$.

O lema a seguir apresenta um resultado análogo à existência de uma "base dual" de funcionais lineares, fixada uma base de um espaço vetorial de dimensão finita, agora no contexto do espaço de todas as funções de um conjunto S para $\mathbb{K}$.

Lema 4.5.6. *Sejam S um conjunto e V um subespaço vetorial não nulo e de dimensão finita de $\mathbb{K}^S$. Então existe uma base $\mathcal{B} = \{f_1, \ldots, f_n\}$ de V e um subconjunto $S' = \{s_1, \ldots, s_n\}$ de S tal que $f_i(s_j) = \delta_{ij}$ para todos os índices i e j.*

Demonstração. Vamos proceder por indução na dimensão de V. Para $n = 1$ seja $V = \langle f_1 \rangle$. Como $f_1 : S \to \mathbb{K}$ é uma função não nula, existe $s_1 \in S$ tal que $f_1(s_1) \neq 0$, logo basta tomar $S' = \{s_1\}$ e $\mathcal{B} = \{(f_1(s_1))^{-1} f_1\}$.

Suponha válido o resultado para $n = k$. Se $\{f_1, \ldots, f_{k+1}\}$ é uma base de V, então pela hipótese de indução podemos assumir que existem elementos $s_1, \ldots, s_k \in S$ tais que $f_i(s_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, k\}$.

A função f_{k+1}, restrita ao conjunto $\{s_1, \ldots, s_k\}$, pode ser descrita como uma combinação linear das funções $f_1, \ldots, f_k$. De fato, se $f_{k+1}(s_j) = \lambda_j$ para $j = 1, \ldots, k$, escrevemos

$$f_{k+1}(s_j) = \sum_{i=1}^{k} \lambda_i f_i(s_j)$$

e portanto

$$(f_{k+1} - \sum_{i=1}^{k} \lambda_i f_i)(s_j) = 0,$$

para todo $j = 1, \ldots, k$.

Como $f_1, \ldots, f_{k+1}$ são linearmente independentes, a função $f_{k+1} - \sum_{i=1}^{k} \lambda_i f_i$ é não nula, logo existe $s_{k+1} \in S$ tal que

$$(f_{k+1} - \sum_{i=1}^{k} \lambda_i f_i)(s_{k+1}) = \lambda \neq 0.$$

Assim definimos,

$$\widehat{f_{k+1}} = \lambda^{-1}(f_{k+1} - \sum_{i=1}^{k} \lambda_i f_i).$$

Por fim, para que as k primeiras funções se anulem em s_{k+1} basta tomar

$$\widehat{f_i} = f_i - f_i(s_{k+1})\widehat{f_{k+1}}$$

para todo $i = 1, \ldots, k$. Observamos que $\mathcal{B} = \{\widehat{f_1}, \ldots, \widehat{f_{k+1}}\}$ é uma base de V, visto que seus $k+1$ elementos geram uma base de V, e junto de $S' = \{s_1, \ldots, s_{k+1}\}$ satisfaz as condições procuradas. ∎

Proposição 4.5.7. *Seja M uma representação de um grupo abstrato G. As condições abaixo são equivalentes:*

(1) *M é uma representação localmente finita.*

(2) *Para todo $m \in M$ a G-órbita de m gera um espaço vetorial de dimensão finita.*

(3) *Para todo $m \in M$ a transformação linear $r_M(m \otimes -) : M^* \to \mathbb{K}^G$, dada por $r_M(m \otimes \alpha) = \alpha|m$, tem posto finito.*

(4) *O espaço M pode ser escrito como uma soma de subespaços G-invariantes de dimensão finita.*

Demonstração. Vamos proseguir demonstrando as implicações (2) $\Leftrightarrow$ (3), (1) $\Leftrightarrow$ (2) e (1) $\Leftrightarrow$ (4).

(2) $\Rightarrow$ (3). Seja $\{m_1, \ldots, m_n\}$ uma base para a G-órbita de $m \in M$ e considere um conjunto de funcionais $\{m^1, \ldots, m^n\} \subset M^*$, tais que $m^j(m_i) = \delta_{ij}$. Dado $x \in G$ escrevemos

$$x \cdot m = \sum_{i=1}^{n} \lambda_i m_i.$$

Aplicando os funcionais m^j na igualdade acima temos

$$(m^j|m)(x) = m^j(x \cdot m) = \sum_{i=1}^{n} \lambda_i m^j(m_i) = \lambda_j,$$

para todo $j = 1, \ldots, n$. Para concluir vamos demonstrar que o conjunto das funções representativas $\{m^1|m, \ldots, m^n|m\}$ gera o $\mathbb{K}$-espaço $\mathrm{Im}(r_M(m \otimes -))$. Dado $\alpha \in M^*$ temos que

$$\begin{aligned}(\alpha|m)(x) &= \alpha(x \cdot m) \\ &= \alpha(\sum_{i=1}^{n} \lambda_i m_i) \\ &= \alpha(\sum_{i=1}^{n} (m^i|m)(x) m_i) \\ &= \sum_{i=1}^{n} \alpha(m_i)(m^i|m)(x),\end{aligned}$$

para todo $x \in G$, logo $\alpha|m = \sum_{i=1}^{n} \alpha(m_i)(m^i|m)$ e com isso concluímos que todo elemento de $\mathrm{Im}(r_M(m \otimes -))$ se escreve como uma combinação linear dos elementos de $\{m^1|m, \ldots, m^n|m\}$.

(3) $\Rightarrow$ (2). Se $r_M(m\otimes -)$ possui posto finito então existem funções linearmente independentes $f_1,\ldots,f_n \in \mathrm{Im}(r_M(m\otimes -))$, tais que para todo $\alpha \in M^*$ existem escalares $\lambda_{i,\alpha}\in\mathbb{K}$ satisfazendo $\alpha|m = \sum_{i=1}^n \lambda_{i,\alpha} f_i$. Pelo Lema 4.5.6 existe uma base de $\mathrm{Im}(r_M(m\otimes -))$, que denotamos por $\{\widehat{f_1},\ldots,\widehat{f_n}\}$, e elementos $x_1,\ldots,x_n \in G$ tais que $\widehat{f_i}(x_j)=\delta_{ij}$. Escrevendo $\alpha|m = \sum_{i=1}^n \widehat{\lambda_{i,\alpha}}\widehat{f_i}$ obtemos $\widehat{\lambda_{j,\alpha}} = \alpha(x_j\cdot m)$ e portanto

$$\alpha(x\cdot m) = \sum_{i=1}^n \alpha(x_i\cdot m)\widehat{f_i}(x),$$

para todo $x\in G$, $\alpha\in M^*$.

Por outro lado,

$$\begin{aligned}
&\alpha(x\cdot m) = \alpha(\sum_{i=1}^n (x_i\cdot m)\widehat{f_i}(x)) \\
\Rightarrow\ &\alpha(x\cdot m) - \alpha(\sum_{i=1}^n (x_i\cdot m)\widehat{f_i}(x)) = 0 \\
\Rightarrow\ &\alpha(x\cdot m - \sum_{i=1}^n (x_i\cdot m)\widehat{f_i}(x)) = 0,
\end{aligned}$$

para todo $x\in G$, $\alpha\in M^*$. Logo temos que $x\cdot m - \sum_{i=1}^n (x_i\cdot m)\widehat{f_i}(x) = 0 \in M$, ou seja, $x\cdot m = \sum_{i=1}^n (x_i\cdot m)\widehat{f_i}(x)$. Portanto o conjunto $\{x_1\cdot m,\ldots,x_n\cdot m\}$ gera $\langle G\cdot m\rangle$.

(1) $\Rightarrow$ (2). Se M é uma representação localmente finita cada $m\in M$ pertence a um subespaço G-invariante $N_m \subset M$ de dimensão finita, portanto $x\cdot m \in N_m$ para todo $x\in G$. Assim concluímos que $\langle G\cdot m\rangle \subset N_m$, isto é, o espaço gerado pela órbita de m possui dimensão finita.

(2) $\Rightarrow$ (1). Para todo $m\in M$ o subespaço $\langle G\cdot m\rangle$ é G-invariante. De fato, $x\cdot(g\cdot m) = (xg)\cdot m \in \langle G\cdot m\rangle$, para todos $x,g\in G$. Agora como a órbita de m gera um subespaço de dimensão finita por hipótese, segue que M é uma representação localmente finita.

(1) $\Rightarrow$ (4). Denote N_m o subespaço G-invariante de dimensão finita associado a $m\in M$. Assim escrevemos

$$M = \sum_{m\in M} N_m.$$

(4) $\Rightarrow$ (1). Suponha que M pode ser escrito como $M = \sum_{\lambda\in\Lambda} N_\lambda$, onde cada N_λ é um subespaço G-invariante de dimensão finita. Desta forma todo $m\in M$ se escreve como $m = \sum_{\lambda\in\Lambda'} m_\lambda$, onde $\Lambda'\subset\Lambda$ é finito. Assim basta tomar $N_m = \sum_{\lambda\in\Lambda'} N_\lambda$. De fato, N_m possui dimensão finita e como é a soma de subespaços G-invariantes também é G-invariante. ■

Observação 4.5.8. Considere a ação regular à esquerda (respectivamente à direita) de G em $\mathbb{K}[G]$ dada por translações. Na nomenclatura da definição 4.5.1 $\mathbb{K}[G]$ é uma representação de G, a qual chamamos de *representação regular à esquerda* (respectivamente *à direita*).

Pelo Lema 4.3.12 sabemos que $\Delta(f) = \sum f_1 \otimes f_2$ se, e somente se, $f(xy) = \sum f_1(x)f_2(y)$, para todos $x, y \in G$. Agora fixando $y \in G$ temos que,

$$(y \cdot f)(x) = f(xy) = \sum f_1(x)f_2(y),$$

para todo $x \in G$, logo $y \cdot f = \sum f_2(y)f_1$.

Analogamente para a ação à direita, $f \cdot x = \sum f_1(y)f_2$.

Lema 4.5.9. *Seja G um grupo algébrico afim. As representações regulares à esquerda e à direita são localmente finitas.*

Demonstração. Pela observação anterior dados $x \in G$ e $f \in \mathbb{K}[G]$ sabemos que, se $\Delta(f) = \sum_{i=1}^{r} g_i \otimes h_i$, então $x \cdot f = \sum_{i=1}^{r} h_i(x)g_i$ e $f \cdot x = \sum_{i=1}^{r} g_i(x)h_i$, ou seja, a órbita de f pela ação à esquerda é gerada pelos finitos elementos $g_1, \ldots, g_r \in \mathbb{K}[G]$ e a órbita de f pela ação à direita é gerada pelos finitos elementos $h_1, \ldots, h_r \in \mathbb{K}[G]$. Agora pela Proposição 4.5.7 segue que ambas as representações são localmente finitas. ■

Definição 4.5.10. Seja G um grupo algébrico afim e M um $\mathbb{K}$-espaço vetorial. Dizemos que uma ação linear $\varphi : G \times M \to M$ é *racional*, ou que M é uma *representação racional* de G, se as duas condições abaixo são satisfeitas:

(i) M é uma representação localmente finita.

(ii) Para todo $\alpha \in M^*$ e $m \in M$ a função representativa $\alpha|m$ é regular, isto é, $\alpha|m \in \mathbb{K}[G]$.

Lema 4.5.11. *Seja M uma representação de G de dimensão finita. A ação $\varphi : G \times M \to M$ é racional se, e somente se, o homomorfismo de grupos abstratos associado $\psi : G \to \mathrm{GL}(M)$, dado por $\psi(x)(m) = x \cdot m$, é um morfismo de grupos algébricos afins.*

Demonstração. Seja $\mathcal{B} = \{e_1, \ldots, e_n\}$ uma base de M e $\{e^1, \ldots, e^n\}$ sua base dual. Identificamos $\mathrm{GL}(M)$ com GL_n com respeito à $\mathcal{B}$. Agora, se a ação é dada por $g \cdot e_j = \sum_{i=1}^{n} c_{ij}(g)e_i$ para todo $g \in G$, então ψ é dado por

$$\psi(g) = (X_0(C), c_{11}(g), c_{12}(g), \ldots, c_{nn}(g)),$$

onde $C = (c_{ij}(g))_{i,j=1,\ldots,n} \in \mathrm{M}_n(\mathbb{K})$. Assim ψ é morfismo de grupos algébricos se, e somente se, $c_{ij} \in \mathbb{K}[G]$, para todos os índices i, j.

Note que,

$$(e^i|e_j)(g) = e^i(g \cdot e_j) = \sum_{k=1}^{n} c_{kj}(g)e^i(e_k) = c_{ij}(g),$$

para todo $g \in G$, ou seja, $e^i|e_j = c_{ij}$ para todo $i, j = 1, \ldots, n$.

Agora como M possui dimensão finita, já é uma representação localmente finita de G, logo do fato que o conjunto $\{e^j|e_i : 1 \leq i, j \leq n\}$ gera o $\mathbb{K}$-espaço de todas as funções representativas (veja a Observação 4.5.3), segue que para todo $\alpha \in M^*$ e $m \in M$ a função $\alpha|m$ pertence a $\mathbb{K}[G]$ se, e somente se, ψ é morfismo de grupos algébricos afins. ■

O lema a seguir é útil ao avaliar tensores contendo funções como alguma de suas componentes. No que segue $\mathcal{F}(X, M)$ denota o $\mathbb{K}$-espaço vetorial de todas as funções de X para M.

Lema 4.5.12. *Sejam M um $\mathbb{K}$-espaço vetorial e X uma variedade. Então a função $\theta : M \otimes \mathbb{K}[X] \to \mathcal{F}(X, M)$, definida por $\theta(m \otimes f)(x) = f(x)m$, é uma transformação linear injetiva. Em especial, dados $m_i, n_j \in M$ e $f_i, h_j \in \mathbb{K}[X]$, temos*

$$\sum_i m_i \otimes f_i = \sum_j n_j \otimes h_j \Leftrightarrow \sum_i f_i(x)m_i = \sum_j h_j(x)n_j,$$

para todo $x \in X$.

Demonstração. Primeiramente verificamos que θ está bem definida. Considere a aplicação

$$\eta : M \times \mathbb{K}[X] \to \mathcal{F}(X, M),$$

dada por

$$\eta(m, f)(x) = f(x)m.$$

Afirmamos que η é $\mathbb{K}$-bilinear. De fato,

$$\begin{aligned}\eta(\lambda_1 m_1 + \lambda_2 m_2, f)(x) &= f(x)(\lambda_1 m_1 + \lambda_2 m_2) \\ &= \lambda_1 f(x)m_1 + \lambda_2 f(x)m_2 \\ &= \lambda_1 \eta(m_1, f)(x) + \lambda_2 \eta(m_2, f)(x),\end{aligned}$$

logo

$$\eta(\lambda_1 m_1 + \lambda_2 m_2, f) = \lambda_1 \eta(m_1, f) + \lambda_2 \eta(m_2, f).$$

Para a segunda entrada,

$$\begin{aligned}\eta(m, \lambda_1 f_1 + \lambda_2 f_2)(x) &= (\lambda_1 f_1 + \lambda_2 f_2)(x)m \\ &= (\lambda_1 f_1(x) + \lambda_2 f_2(x))m \\ &= \lambda_1 f_1(x)m + \lambda_2 f_2(x)m \\ &= \lambda_1 \eta(m, f_1)(x) + \lambda_2 \eta(m, f_2)(x),\end{aligned}$$

portanto

$$\eta(m, \lambda_1 f_1 + \lambda_2 f_2) = \lambda_1 \eta(m, f_1) + \lambda_2 \eta(m, f_2).$$

Por fim,

$$\begin{aligned}\eta(\lambda m, f)(x) &= f(x)(\lambda m) \\ &= \lambda f(x)m \\ &= (\lambda f)(x)m \\ &= \eta(m, \lambda f)(x),\end{aligned}$$

deste modo

$$\eta(\lambda m, f) = \eta(m, \lambda f).$$

Pela propriedade universal do produto tensorial $M \otimes \mathbb{K}[X]$, θ é a única aplicação $\mathbb{K}$-linear que fatora η pela aplicação $t : M \times \mathbb{K}[X] \to M \otimes \mathbb{K}[X]$, portanto está bem definida.

Resta mostrar a injetividade de θ. Para isso tome $\sum_{i=1}^{n} m_i \otimes f_i \neq 0 \in \operatorname{Ker} \theta$. Note que podemos supor os m_i's linearmente independentes. Então temos

$$\begin{aligned}0 &= \theta(\sum_{i=1}^{n} m_i \otimes f_i)(x) \\ &= \sum_{i=1}^{n} \theta(m_i \otimes f_i)(x) \\ &= \sum_{i=1}^{n} f_i(x) m_i, \end{aligned} \tag{4.2}$$

para todo $x \in X$. Como $\sum_{i=1}^{n} m_i \otimes f_i \neq 0$, ao menos alguma função f_i é não nula, ou seja, existe $x \in X$ tal que $f_i(x) \neq 0$ e então (4.2) é uma contradição na independência linear entre os m_i's. Assim $\sum_{i=1}^{n} m_i \otimes f_i$ é o tensor nulo. ■

Toda representação racional de um grupo algébrico afim G pode ser munida de uma estrutura de $\mathbb{K}[G]$-comódulo à direita, e vice-versa. O próximo teorema detalha essa correspondência.

Teorema 4.5.13. *Sejam G um grupo algébrico afim e M um $\mathbb{K}$-espaço vetorial.*

(i) *Se $\varphi : G \times M \to M$ é uma ação racional, então a aplicação $\mathbb{K}$-linear $\rho_\varphi : M \to M \otimes \mathbb{K}[G]$ dada por $\rho_\varphi(m) = \sum m_0 \otimes m_1$ se, e somente se, $\varphi(x, m) = \sum m_1(x)m_0$ para todo $x \in G$, define uma estrutura de $\mathbb{K}[G]$-comódulo à direita em M.*

(ii) *Se M munido da aplicação $\mathbb{K}$-linear $\rho : M \to M \otimes \mathbb{K}[G]$, dada por $\rho(m) = \sum_i m_i \otimes f_i$, é um $\mathbb{K}[G]$-comódulo à direita, então a aplicação $\varphi_\rho : G \times M \to M$, $(x, m) \mapsto \sum_i f_i(x)m_i$ é uma ação racional.*

Demonstração. (i) Suponha a ação φ racional. Para todo $m \in M$ considere um conjunto linearmente independente $\Omega_m = \{m_1, \ldots, m_n\} \subset M$ que gere o $\mathbb{K}$-espaço $\langle G \cdot m \rangle_\mathbb{K}$ e um respectivo conjunto de funcionais lineares $\Omega_m^* = \{m^1, \ldots, m^n\} \subset M^*$, tais que $m^i(m_j) = \delta_{ij}$, para todos $1 \leq i, j \leq n$. Perceba que sempre existe um conjunto de vetores linearmente independentes nessas condições, uma vez que o subespaço $\langle G \cdot m \rangle_\mathbb{K}$ possui dimensão finita.

Dado $x \in G$ note que, se $x \cdot m = \sum_{i=1}^n \lambda_i m_i$, então $(m^i|m)(x) = \lambda_i$, para todo $i = 1, \ldots, n$. Agora, como a ação é racional, cada função representativa $f_i = m^i|m$ pertence a $\mathbb{K}[G]$, assim podemos definir uma aplicação $\rho_\varphi : M \to M \otimes \mathbb{K}[G]$ por $\rho_\varphi(m) = \sum_{i=1}^n m_i \otimes f_i$ se, e somente se, $x \cdot m = \sum_{i=1}^n f_i(x)m_i$, para todo $x \in G$.

Afirmamos que a imagem de um elemento $m \in M$ pela aplicação ρ_φ independe do conjunto Ω_m escolhido. Mais ainda, esta aplicação é $\mathbb{K}$-linear.

De fato, sejam $\Omega_m = \{m_1, \ldots, m_n\}$ e $\widehat{\Omega}_m = \{n_1, \ldots, n_r\}$ dois conjuntos de vetores linearmente independentes que geram o $\mathbb{K}$-espaço $\langle G \cdot m \rangle_\mathbb{K}$ e denote $f_i = m^i|m$, $h_j = n^j|m$, para $i = 1, \ldots, n$ e $j = 1, \ldots, r$. Pelo Lema 4.5.12,

$$\sum_{i=1}^n m_i \otimes f_i = \sum_{j=1}^r n_j \otimes h_j$$

se, e somente se,

$$\sum_{i=1}^n f_i(x)m_i = \sum_{j=1}^r h_j(x)n_j$$

para todo $x \in G$, o que é válido, pois ambos os lados da igualdade acima são expressões para o elemento $x \cdot m \in M$.

Agora provamos a linearidade de ρ_φ. Dados $m, m' \in M$ considere o subespaço $N = \langle G \cdot m \rangle_\mathbb{K} + \langle G \cdot m' \rangle_\mathbb{K}$. Evidentemente N contém m, m' e qualquer combinação linear $\alpha m + \beta m'$, com $\alpha, \beta \in \mathbb{K}$. Além disso N possui dimensão finita, pois é a soma de dois subespaços com esta propriedade. Deste modo considere uma base $\{n_1, \ldots, n_l\}$ de N e funções representativas $f_i = n^i|m, h_i = n^i|m' \in \mathbb{K}[G]$, para

$i = 1, \ldots, l$. Em relação a esta base escrevemos:

$$x \cdot m = \sum_{i=1}^{l} f_i(x) n_i$$

e

$$x \cdot m' = \sum_{i=1}^{l} h_i(x) n_i.$$

Portanto para todo $x \in G$ temos,

$$\begin{aligned} x \cdot (\alpha m + \beta m') &= \alpha(x \cdot m) + \beta(x \cdot m') \\ &= \alpha \sum_{i=1}^{l} f_i(x) n_i + \beta \sum_{i=1}^{l} h_i(x) n_i \\ &= \sum_{i=1}^{l} (\alpha f_i(x) + \beta h_i(x)) n_i, \end{aligned}$$

ou seja,

$$\begin{aligned} \rho_\varphi(\alpha m + \beta m') &= \sum_{i=1}^{l} n_i \otimes (\alpha f_i + \beta h_i) \\ &= \alpha \sum_{i=1}^{l} n_i \otimes f_i + \beta \sum_{i=1}^{l} n_i \otimes h_i \\ &= \alpha \rho_\varphi(m) + \beta \rho_\varphi(m'). \end{aligned}$$

Finalmente verificamos que M junto da aplicação ρ_φ é um $\mathbb{K}[G]$-comódulo à direita. Primeiramente, note que $\sum_{i=1}^{n} \varepsilon(f_i) m_i = \sum_{i=1}^{n} f_i(1_G) m_i = 1_G \cdot m = m$, portanto $(I \otimes \varepsilon) \circ \rho = \phi$, onde $\phi : M \xrightarrow{\sim} M \otimes \mathbb{K}$ é o isomorfismo canônico. Resta mostrar que ρ_φ satisfaz a relação

$$(\rho_\varphi \otimes I) \circ \rho_\varphi = (I \otimes \Delta) \circ \rho_\varphi,$$

isto é, que para todo $m \in M$,

$$\sum_{i=1}^{n} \rho_\varphi(m_i) \otimes f_i = \sum_{i=1}^{n} m_i \otimes \Delta(f_i). \tag{4.3}$$

Considere o isomorfismo $\theta : M \otimes \mathbb{K}[G] \otimes \mathbb{K}[G] \xrightarrow{\sim} M \otimes \mathbb{K}[G \times G]$. Sabemos que a

Equação 4.3 é válida se, e somente se,

$$\theta(\sum_{i=1}^{n} \rho_\varphi(m_i) \otimes f_i) = \theta(\sum_{i=1}^{n} m_i \otimes \Delta(f_i)). \tag{4.4}$$

Agora pelo Lema 4.5.12, a Equação 4.4 é válida se, e somente se,

$$\sum_{i=1}^{n} (x \cdot m_i) f_i(y) = \sum_{i=1}^{n} m_i f_i(xy)$$

para todos $x, y \in G$. O que se prova verdade, pois para quaisquer $x, y \in G$

$$\sum_{i=1}^{n} (x \cdot m_i) f_i(y) = x \cdot (y \cdot m) = (xy) \cdot m = \sum_{i=1}^{n} m_i f_i(xy),$$

concluindo este item.

(ii) Primeiramente provamos que $\varphi_\rho : G \times M \to M$ dada por $\varphi_\rho(x, m) = x \cdot m = \sum_i f_i(x) m_i$ é uma ação de G em M. A coassociatividade da estrutura de comódulo por ser escrita como

$$\sum_i m_{i,0} \otimes m_{i,1} \otimes f_i = \sum_i m_i \otimes f_{i,1} \otimes f_{i,2}.$$

Dado $y \in G$ arbitrário avaliamos a igualdade acima pela aplicação $\mathbb{K}$-linear $I \otimes \varepsilon_y \otimes I$, onde $\varepsilon_y : \mathbb{K}[G] \to \mathbb{K}$ é a avaliação em y, isto é, $\varepsilon_y(f) = f(y)$, obtendo

$$\sum_i m_{i,0} \otimes m_{i,1}(y) \otimes f_i = \sum_i m_i \otimes f_{i,1}(y) \otimes f_{i,2},$$

ou ainda,

$$\sum_i m_{i,1}(y) m_{i,0} \otimes 1 \otimes f_i = \sum_i m_i \otimes 1 \otimes f_{i,1}(y) f_{i,2}.$$

Pelo isomorfismo canônico $M \otimes \mathbb{K} \otimes \mathbb{K}[G] \cong M \otimes \mathbb{K}[G]$ temos,

$$\sum_i m_{i,1}(y) m_{i,0} \otimes f_i = \sum_i m_i \otimes f_{i,1}(y) f_{i,2}$$

e pelo Lema 4.5.12 a igualdade acima é válida se, e somente se,

$$\sum_i f_i(x) m_{i,1}(y) m_{i,0} = \sum_i f_{i,1}(y) f_{i,2}(x) m_i$$

para todo $x \in G$. Logo,

$$\begin{aligned} y \cdot (x \cdot m) &= y \cdot (\sum_i f_i(x) m_i) \\ &= \sum_i f_i(x)(y \cdot m_i) \\ &= \sum_i f_i(x) m_{i,1}(y) m_{i,0} \\ &= \sum_i f_{i,1}(y) f_{i,2}(x) m_i \\ &= \sum_i f_i(yx) m_i \\ &= (yx) \cdot m \end{aligned}$$

para todos $x, y \in G$.

Isto mostra que φ_ρ é compatível com o produto de G. Agora a counidade da estrutura de comódulo implica

$$\sum_i \varepsilon(f_i) m_i = m.$$

Assim, $1_G \cdot m = \sum_i f_i(1_G) m_i = m$.

Resta mostrar que a ação φ_ρ é racional. Para isso note que, fixado $m \in M$ arbitrário, o conjunto $\{m_i \in M : \rho(m) = \sum_i m_i \otimes f_i\}$ gera o subespaço $\langle G \cdot m \rangle$, logo pela Proposição 4.5.7 φ_ρ é localmente finita. Avaliando um funcional arbitrário $\alpha \in M^*$ na igualdade $x \cdot m = \sum_i f_i(x) m_i$ deduzimos que $\alpha | m = \sum_i \alpha(m_i) f_i$, ou seja, todas as funções M-representativas são regulares, o que conclui a demonstração.

■

Teorema 4.5.14. *Sejam G um grupo algébrico afim e V uma G-variedade via a ação regular à direita $\tau : V \times G \to V$. Então a ação à esquerda induzida de G em $\mathbb{K}[V]$ dada por translações é racional, ou ainda, $\mathbb{K}[V]$ é uma representação racional de G.*

Demonstração. Pelo Teorema 4.5.13 (ii) basta mostrar que existe uma aplicação $\mathbb{K}$-linear $\rho : \mathbb{K}[V] \to \mathbb{K}[V] \otimes \mathbb{K}[G]$ tal que o par $(\mathbb{K}[V], \rho)$ define um $\mathbb{K}[G]$-comódulo à direita e que a ação induzida φ_ρ coincide com a ação à esquerda de G em $\mathbb{K}[V]$ dada por translações.

Seja $\tau^* : \mathbb{K}[V] \to \mathbb{K}[V \times G]$ o comorfismo associado a ação, dado por $\tau^*(f)(v, g) = f(v \cdot g)$ e considere o isomorfismo de $\mathbb{K}$-álgebras $\theta : \mathbb{K}[V \times G] \xrightarrow{\sim} \mathbb{K}[V] \otimes \mathbb{K}[G]$, dado na notação de Sweedler por $\theta(h) = \sum h_0 \otimes h_1$, onde $h(v, g) = \sum h_0(v) h_1(g)$, para todo $(v, g) \in V \times G$.

Definimos $\rho : \mathbb{K}[V] \to \mathbb{K}[V] \otimes \mathbb{K}[G]$ pela composição $\rho = \theta \circ \tau^*$, assim

$$\rho(f) = \sum f_0 \otimes f_1$$

se, e somente se, $f(v \cdot g) = \sum f_0(v) f_1(g)$ para todo $v \in V$ e $g \in G$.

Primeiramente vamos verificar que $(\mathbb{K}[V], \rho)$ define um $\mathbb{K}[G]$-comódulo à direita. Para a coassociatividade, temos

$$((\rho \otimes I)\rho)(f) = (\rho \otimes I)(\sum f_0 \otimes f_1) = \sum \rho(f_0) \otimes f_1. \tag{4.5}$$

Por outro lado,

$$((I \otimes \Delta)\rho)(f) = (I \otimes \Delta)(\sum f_0 \otimes f_1) = \sum f_0 \otimes \Delta(f_1). \tag{4.6}$$

Usando o isomorfismo $\xi : \mathbb{K}[V] \otimes \mathbb{K}[G] \otimes \mathbb{K}[G] \xrightarrow{\sim} \mathbb{K}[V \times G \times G]$, temos que as Equações 4.5 e 4.6 são equivalentes se, e somente se, as funções $\xi(\sum \rho(f_0) \otimes f_1)$ e $\xi(\sum f_0 \otimes \Delta(f_1))$ coincidem para todo $(v, g, h) \in V \times G \times G$. Agora, isso ocorre de fato, pois

$$\begin{aligned}
\xi(\sum \rho(f_0) \otimes f_1)(v, g, h) &= \sum \rho(f_0)(v, g) f_1(h) \\
&= \sum f_0(v \cdot g) f_1(h) \\
&= f((v \cdot g) \cdot h) \\
&= f(v \cdot (gh)) \\
&= \sum f_0(v) f_1(gh) \\
&= \sum f_0(v) \Delta(f_1)(g, h) \\
&= \xi(\sum f_0 \otimes \Delta(f_1))(v, g, h).
\end{aligned}$$

Para a counidade, note que

$$\begin{aligned}
(\sum f_0 \varepsilon(f_1))(v) &= \sum f_0(v) \varepsilon(f_1) \\
&= \sum f_0(v) f_1(1_G) \\
&= f(v \cdot 1_G) \\
&= f(v),
\end{aligned}$$

para todo $v \in V$, ou seja, $(I \otimes \varepsilon)\rho = \phi$, onde $\phi : \mathbb{K}[V] \xrightarrow{\sim} \mathbb{K}[V] \otimes \mathbb{K}$ é o isomorfismo canônico.

Por fim, denotando a ação à esquerda de G em $\mathbb{K}[V]$ por $g \cdot f$, onde $g \in G$ e

$f \in \mathbb{K}[V]$, temos que

$$\begin{aligned}\varphi_\rho(g,f)(v) &= (\sum f_0(g)f_1)(v)\\ &= \sum f_0(g)f_1(v)\\ &= f(v\cdot g)\\ &= (g\cdot f)(v),\end{aligned}$$

o que conclui a demonstração. ■

Observação 4.5.15. Um caso particular do teorema anterior é quando V é o próprio grupo G e a ação regular induzida em $\mathbb{K}[G]$ é dada por $(x\cdot f)(y) = f(yx)$, para todo $x, y \in G$ e $f \in \mathbb{K}[G]$.

Agora apresentamos com detalhes o resultado principal deste capítulo, o qual garante que todo grupo algébrico afim é isomorfo a um subgrupo fechado de algum *grupo linear geral*.

Teorema 4.5.16 (Linearidade dos Grupos Algébricos Afins)**.** *Seja G um grupo algébrico afim. Então existe $n \in \mathbb{N}$ e uma imersão fechada $\psi : G \to \mathrm{GL}_n$ que também é um homomorfismo de grupos.*

Demonstração. Considere a ação regular à direita de G em G, dada por translações. Como vimos na Observação 4.2.6, essa ação induz uma ação à esquerda de G em $\mathbb{K}[G]$, que é racional pela Observação 4.5.15, ou seja, $\mathbb{K}[G]$ é uma representação racional de G. Deste modo, dado um conjunto finito de geradores de $\mathbb{K}[G]$ como álgebra, a Proposição 4.5.7 garante a existência de um $\mathbb{K}$-subespaço vetorial G-invariante e de dimensão finita $V \subset \mathbb{K}[G]$, contendo esses geradores.

Agora, pelo Lema 4.5.11 a ação racional $G \times V \to V$ induz um morfismo de grupos algébricos afins $\psi : G \to \mathrm{GL}(V)$, dado por $\psi(g)(v) = g\cdot v$. Afirmamos que ψ é um homomorfismo injetivo de grupos. De fato, se um elemento $g \in G$ satisfaz $\psi(g)(v) = v$, para todo $v \in V$, então como V é um gerador da álgebra $\mathbb{K}[V]$ devemos ter $g\cdot f = f$, para todo $f \in \mathbb{K}[G]$. Em particular, $f(g) = (g\cdot f)(1_G) = f(1_G)$, para todo $f \in \mathbb{K}[G]$ e portanto $g = 1_G$.

Para concluir que ψ é uma imersão fechada, primeiramente usamos o Teorema 4.1.22 (ii), o qual garante que a imagem de um morfismo de grupos algébricos afins é um subgrupo fechado. Resta mostrar que a função regular

$$\psi : G \to \mathrm{Im}(\psi)$$

é um isomorfismo de variedades. Pelo Corolário 3.8.8, é suficiente que o comorfismo

$$\psi^* : \mathbb{K}[\mathrm{Im}(\psi)] \to \mathbb{K}[G]$$

seja um isomorfismo de $\mathbb{K}$-álgebras.
ψ^* *injetor.*

$$\begin{aligned} & \psi^*(v)(g) = 0, \forall\ g \in G \\ \Leftrightarrow\ & v(\psi(g)) = 0, \forall\ g \in G \\ \Leftrightarrow\ & v(h) = 0, \forall\ h \in \mathrm{Im}(\psi) \\ \Leftrightarrow\ & v = 0. \end{aligned}$$

ψ^* *sobrejetor.* É suficiente mostrar que $V \subset \mathrm{Im}(\psi^*)$, pois V gera $\mathbb{K}[G]$ como uma $\mathbb{K}$-álgebra.

Seja $\{v_1, \ldots, v_n\}$ uma base de V e $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{K}[G]$ sua base dual, isto é, $\alpha_i = v_i^*$. Então, para todo $v \in V$ escrevemos

$$\Delta(v) = \sum_{i=1}^{n} v_i \otimes w_i.$$

Pela Observação 4.5.8, a ação de G em V nos dá

$$x \cdot v = \sum_{i=1}^{n} w_i(x) v_i,$$

para todo $x \in G$.

Note que, como $\alpha_i(v_j) = \delta_{ij}$ para todos os índices i, j, temos

$$\alpha_i(x \cdot v) = w_i(x),$$

para todo $x \in G$.

Considere a função representativa

$$\alpha_i | v : \mathrm{GL}(V) \to \mathbb{K},$$

dada pela ação de $\mathrm{GL}(V)$ em V, isto é

$$\begin{aligned} (\alpha_i | v)(T) &= \alpha_i(T \cdot v) \\ &= \alpha_i(T(v)) \\ &= \alpha_i(\sum_{j=1}^{n} \lambda_j v_j) \\ &= \lambda_i. \end{aligned}$$

Como a ação de $\mathrm{GL}(V)$ em V é regular, segue que $\alpha_i | v \in \mathbb{K}[\mathrm{GL}(V)]$, para todo

$i = 1, \ldots, n$ e então

$$\psi^*(\alpha_i|v)(x) = \alpha_i(x \cdot v) = w_i(x),$$

ou seja, $w_i \in \mathrm{Im}(\psi^*)$.

Por fim, como $\Delta(v) = \sum_{i=1}^n v_i \otimes w_i$, pelo Lema 4.3.12 temos $v = \sum_{i=1}^n v_i(1_G)w_i$ e portanto $v \in \mathrm{Im}(\psi^*)$. ■

4.5.1 Exemplos de linearização

Exemplo 4.5.17 (Grupo aditivo G_a)**.** A álgebra de funções $\mathbb{K}[G_a]$ é isomorfa ao anel de polinômios em uma indeterminada $\mathbb{K}[X]$ (veja o Exemplo 3.7.2). Seguindo os argumentos do Teorema 4.5.16 a ação à direita de G_a em G_a dada por $a \cdot b = a + b$, para todos $a, b \in G_a$, induz uma ação à esquerda de G_a em $\mathbb{K}[G_a]$, dada por $(a \cdot f)(x) = f(x + a)$.

Perceba que o subespaço de dimensão finita $V = \langle 1, X\rangle_{\mathbb{K}}$ gera $\mathbb{K}[G_a]$ como uma $\mathbb{K}$-álgebra e é G_a-invariante, pois

$$(a \cdot 1)(b) = 1(b \cdot a) = 1(b + a) = 1_{\mathbb{K}} = 1(b),$$

para todo $b \in G_a$ e

$$(a \cdot X)(b) = X(b \cdot a) = X(b + a) = b + a = a1(b) + X(b),$$

assim,

$$a \cdot X = a1 + X.$$

Logo pelo Teorema da linearidade dos grupos algébricos afins temos um homomorfismo de grupos que também é uma imersão fechada,

$$\psi : G_a \to \mathrm{GL}(V).$$

Em relação à base $\{1, X\}$ de V, escrevemos o morfismo acima como

$$\psi : G_a \to \mathrm{GL}_2,$$

dado por

$$\psi(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Exemplo 4.5.18 (Grupo multiplicativo G_m)**.** Como descrito no Exemplo 3.7.4 a álgebra de funções de G_m é isomorfa a álgebra de polinômios de Laurent em uma indeterminada, $\mathbb{K}[X, X^{-1}]$. Começamos com a ação à direita de G_m em G_m, dada por

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

Assim, a ação à esquerda induzida em $\mathbb{K}[G_m]$ é dada por

$$((a, a^{-1}) \cdot f)(b, b^{-1}) = f(ba, (ba)^{-1}).$$

Considere o subespaço vetorial $V = \langle X, X^{-1} \rangle_{\mathbb{K}}$ de $\mathbb{K}[G_m]$. Note que V possui dimensão finita, gera $\mathbb{K}[G_m]$ como uma álgebra e é G_m-invariante, pois

$$((a, a^{-1}) \cdot X)(b, b^{-1}) = X(ba, (ba)^{-1}) = ba = ab = aX(b, b^{-1}),$$

logo

$$(a, a^{-1}) \cdot X = aX,$$

e analogamente,

$$(a, a^{-1}) \cdot X^{-1} = a^{-1}X^{-1}.$$

Portanto o Teorema da linearidade garante a existência de um homomorfismo de grupos $\psi : G_m \to \mathrm{GL}(V)$, que também é uma imersão fechada. Em relação à base $\mathcal{B} = \{X, X^{-1}\}$ de V, temos que

$$\psi : G_m \to \mathrm{GL}_2,$$

é dado por

$$\psi((a, a^{-1})) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Perceba que o grupo $\psi(G_m)$ é, em particular, subgrupo algébrico de $\mathrm{SL}_2(\mathbb{K})$.

Exemplo 4.5.19 (Grupo afim Aff_n)**.** Nesse exemplo veremos duas formas de linearização para o grupo afim Aff_n:

(i) Pela ação à direita de Aff_n em Aff_n, dada por translações.

(ii) Via a ação à esquerda de Aff_n em $\mathbb{A}^n$.

(i) Procedemos como nos exemplos anteriores, seguindo os passos do Teorema 4.5.16.

A ação à direita de Aff_n em Aff_n dada por

$$(v, B) \cdot (u, A) = (v, B)(u, A) = (v + Bu, BA),$$

induz uma ação à esquerda de Aff_n em $\mathbb{K}[\mathrm{Aff}_n]$ por

$$((u, A) \cdot f)(v, B) = f((v + Bu, BA)).$$

Considere o seguinte espaço $\mathbb{K}$-vetorial, que gera $\mathbb{K}[\mathrm{Aff}_n]$ como uma álgebra:

$$V = \langle X_1, \ldots, X_n, X_0, X_{11}, \ldots, X_{nn} \rangle_{\mathbb{K}}.$$

Afirmamos que V é invariante pela ação do grupo afim. De fato, nas funções X_i, $i = 1, \ldots, n$:

$$\begin{aligned}((u, A) \cdot X_i)(v, B) &= X_i(v + Bu, BA) \\ &= (v + Bu)_i \\ &= (v)_i + (Bu)_i \\ &= v_i + \sum_{k=1}^{n} b_{ik}u_k \\ &= X_i(v, B) + \sum_{k=1}^{n} u_k X_{ik}(v, B),\end{aligned}$$

logo,

$$(u, A) \cdot X_i = X_i + \sum_{k=1}^{n} u_k X_{ik}.$$

Na função X_0:

$$((u, A) \cdot X_0)(v, B) = X_0(v + Bu, BA) = (ba)_0 = b_0 a_0 = a_0 X_0(v, B),$$

assim,

$$(u, A) \cdot X_0 = a_0 X_0.$$

Por fim, nas funções X_{ij}, $i, j = 1, \ldots, n$:

$$\begin{aligned}((u, A) \cdot X_{ij})(v, B) &= X_{ij}(v + Bu, BA) \\ &= (BA)_{ij} \\ &= \sum_{k=1}^{n} b_{ik}a_{kj} \\ &= \sum_{k=1}^{n} a_{kj} X_{ik}(v, B),\end{aligned}$$

portanto

$$(u, A) \cdot X_{ij} = \sum_{k=1}^{n} a_{kj} X_{ik}.$$

Deste modo, pelo Teorema da linearidade existe uma imersão fechada $\psi : \mathrm{Aff}_n \to \mathrm{GL}(V)$, dada por $\psi((u, A))(f) = (u, A) \cdot f$, que também é um homomorfismo de grupos. Fixada a base $\mathcal{B} = \{X_1, \ldots, X_n, X_0, X_{11}, \ldots, X_{nn}\}$ de V, o morfismo ψ é visto como

$$\psi : \mathrm{Aff}_n \to \mathrm{GL}_{n^2+n+1},$$

onde a imagem de um elemento $(u, A) \in \mathrm{Aff}_n$ é uma matriz quadrada de dimensão

n^2+n+1, representada por $(n+1)^2$ blocos $n\times n$, $n+1$ blocos $n\times 1$, $n+1$ blocos $1\times n$ e 1 bloco 1×1:

$$\left(\begin{array}{cccc|c|ccc|ccc}
1 & 0 & \cdots & 0 & 0 & & & & & & \\
0 & 1 & \cdots & 0 & 0 & & & & & & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & 0 & & & \cdots & & 0 & \\
0 & 0 & \cdots & 1 & 0 & & & & & & \\
\hline
0 & 0 & \cdots & 0 & a_0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\hline
u_1 & 0 & \cdots & 0 & 0 & & & & & & \\
u_2 & 0 & \cdots & 0 & 0 & & & & & & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & A & & & \cdots & & 0 & \\
u_n & 0 & \cdots & 0 & 0 & & & & & & \\
\hline
 & & \vdots & & \vdots & & \vdots & & & \ddots & & \vdots & \\
\hline
0 & 0 & \cdots & u_1 & 0 & & & & & & \\
0 & 0 & \cdots & u_2 & 0 & & & & & & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & 0 & & & \cdots & & A & \\
0 & 0 & \cdots & u_n & 0 & & & & & & \\
\end{array}\right)$$

Perceba que a matriz acima é triangular por blocos e, em certo sentido, ocupa "muito espaço" para as informações do grupo afim. Veremos que o próximo método de linearização é "mais econômico".

(ii) O grupo afim possui uma ação natural em $\mathbb{A}^n$, dada por

$$(u, A)\cdot v = Av + u,$$

para todo $v \in \mathbb{A}^n$.

Essa ação à esquerda induz uma ação à direita de Aff_n em $\mathbb{K}[\mathbb{A}^n]$ (veja a Observação 4.2.6):

$$(f\cdot(u,A))(v) = f(Av+u),$$

onde $f \in \mathbb{K}[\mathbb{A}^n]$ e $v \in \mathbb{A}^n$.

Considere o $\mathbb{K}$-subespaço $V = \langle 1, X_1, \ldots, X_n\rangle_{\mathbb{K}} \subset \mathbb{K}[\mathbb{A}^n]$. Vamos mostrar que existe um homomorfismo de grupos $\psi : \mathrm{Aff}_n \to \mathrm{GL}_{n+1}$, que também é uma imersão fechada.

Seja $\theta : \mathrm{Aff}_n \to \mathrm{GL}(V)$ a função dada por

$$\theta((u, A))(f) = f \cdot (u, A),$$

onde $f \in V$ é uma função regular de Aff_n. Em relação a base $\mathcal{B} = \{1, X_1, \ldots, X_n\}$ de V a função θ é dada por

$$(1 \cdot (u, A))(v) = 1(Av + u) = 1_{\mathbb{K}} = 1(v),$$

e

$$\begin{aligned}(X_i \cdot (u, A))(v) &= X_i(Av + u) \\ &= (Av)_i + u_i \\ &= \sum_{k=1}^{n} a_{ik} v_k + u_i \\ &= \sum_{k=1}^{n} a_{ik} X_k(v) + u_i 1(v),\end{aligned}$$

assim,

$$X_i \cdot (u, A) = \sum_{k=1}^{n} a_{ik} X_k + u_i 1.$$

Logo, matricialmente temos $\theta : \mathrm{Aff}_n \to \mathrm{GL}_{n+1}$, dada por

$$(u, A) \mapsto \begin{pmatrix} 1 & u_1 & u_2 & \cdots & u_n \\ 0 & a_{11} & a_{21} & \cdots & a_{n1} \\ 0 & a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix} = \left(\begin{array}{c|c} 1 & u \\ \hline 0 & A^t \end{array}\right).$$

Perceba que θ é bem definida, pois $\theta((u, A))$ é invertível se, e somente se, A é invertível. Mais ainda, é uma função regular, pois envolve somente uma "permutação" de coordenadas entre Aff_n e GL_{n+1}. Entretanto **não** é um homomorfismo de grupos, visto que $\theta((u, A)(v, B)) \neq \theta((u, A))\theta((v, B))$. Para corrigir esse problema definimos uma nova função regular:

$$\varphi : \mathrm{GL}_{n+1} \to \mathrm{GL}_{n+1},$$

dada pela transposição, isto é

$$\varphi(M) = M^t.$$

Agora considere o seguinte morfismo de variedades

$$\psi = \varphi \circ \theta : \mathrm{Aff}_n \to \mathrm{GL}_{n+1},$$

dado por

$$\psi((u, A)) = \left(\begin{array}{c|c} 1 & 0 \\ \hline u & A \end{array}\right).$$

Afirmamos que ψ é um homomorfismo injetor de grupos. Com efeito,

$$\begin{aligned} \psi((u, A)(v, B)) &= \psi((u + Av, AB)) \\ &= \left(\begin{array}{c|c} 1 & 0 \\ \hline u + Av & AB \end{array}\right) \\ &= \left(\begin{array}{c|c} 1 & 0 \\ \hline u & A \end{array}\right) \left(\begin{array}{c|c} 1 & 0 \\ \hline v & B \end{array}\right) \\ &= \psi((u, A))\psi((v, B)). \end{aligned}$$

Também vemos que ψ é claramente injetor, pois

$$u \neq v \ \text{ ou } \ A \neq B \Rightarrow \left(\begin{array}{c|c} 1 & 0 \\ \hline u & A \end{array}\right) \neq \left(\begin{array}{c|c} 1 & 0 \\ \hline v & B \end{array}\right).$$

Com isso concluímos que ψ é um morfismo injetor de grupos algébricos afins. Para que ψ seja uma imersão fechada basta mostrar que $\psi : \mathrm{Aff}_n \to \mathrm{Im}(\psi)$ é um isomorfismo de variedades. Assim considere o morfismo $\phi : \mathrm{Im}(\psi) \to \mathrm{Aff}_n$, dado por

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline u & A \end{array}\right) \mapsto (u, A).$$

Facilmente verificamos que $\phi \circ \psi = I_{\mathrm{Aff}_n}$ e $\psi \circ \phi = I_{\mathrm{Im}(\psi)}$, como queríamos.

Referências Bibliográficas

[1] AN, Jinpeng. Rigid geometric structures, isometric actions, and algebraic quotients. **arXiv**, 2011. Disponível em: https://arxiv.org/abs/1005.1423v2. Acesso em: 7 mai. 2021.

[2] ASSEM, Ibrahim. **Algèbre et Modules**: Cours et exercices. Ottawa: Presses de l'Université d'Ottawa, 1997. 330 p.

[3] BONIFANT, Araceli; MILNOR, John. On Real and Complex Cubic Curves. **arXiv**, 2017. Disponível em: http://arxiv.org/abs/1603.09018v2. Acesso em: 20 ago. 2020.

[4] BOREL, Armand. **Essays in the History of Lie Groups and Algebraic Groups**. Providence: American Mathematical Society, 2001. 184 p.

[5] BOREL, Armand. **Linear Algebraic Groups**. 2. ed. aum. Nova York: Springer-Verlag, 1991. 288 p.

[6] BRANNAN, David A. *et al.* **Geometry**. 2. ed. Nova York: Cambridge University Press, 2012. 602 p.

[7] CASSE, Ray. **Projective Geometry**: An Introduction. 1. ed. Nova York: Oxford University Press, 2006. 216 p.

[8] CASSELMAN, Bill. **Introduction to quadratic forms**. 2018. 15 p. Disponível em: https://www.math.ubc.ca/~cass/research/pdf/QForms.pdf. Acesso em: 13 fev. 2021.

[9] DĂSCĂLESCU, Sorin; NĂSTĂSESCU, Constantin; RAIANU, Şerban. **Hopf algebras**: an introduction. 1. ed. Nova York: Marcel Dekker, 2001. 420 p.

[10] GECK, Meinolf. **An Introduction to Algebraic Geometry and Algebraic Groups**. 1. ed. atual. Oxford: Oxford University Press, 2013. 307 p.

[11] HOCHSCHILD , Gerhard P. **Basic Theory of Algebraic Groups and Lie Algebras**. 1. ed. Nova York: Springer-Verlag, 1981. 267 p.

[12] HOFFMAN, Kenneth M.; KUNZE, Ray. **Linear Algebra**. 2. ed. Nova Jersey: Prentice Hall, 1971. 407 p.

[13] HUMPHREYS, James E. **Linear Algebraic Groups**. 1. ed. rev. Nova York: Springer-Verlag, 1995. 253 p.

[14] LAM, T.Y. **Introduction to Quadratic Forms over Fields**. 1. ed. Providence: American Mathematical Society, 2005. 550 p.

[15] MACEDO, Tiago. **Grupos algébricos e Hiperálgebras**. Dissertação (Mestrado em Matemática) - Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, p. 110, 2009. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/306921/1/Macedo_TiagoRodrigues_M.pdf. Acesso em: 11 mai. 2021.

[16] MARTIN, Maria Eugenia. **Álgebra Comutativa**. 23 de nov de 2014. 134 p. Notas de Aula. Disponível em: https://www.ime.usp.br/~eugenia/algebra-comutativa/algebra_comutativa.pdf. Acesso em: 5 fev. 2020.

[17] MUNKRES, James. **Topology**. 2. ed. Londres: Pearson Education Limited, 2013. 504 p.

[18] Polynomials vanishing on an infinite set. 2012. Pergunta de fórum. Disponível em: https://math.stackexchange.com/questions/102182. Acesso em: 19 fev. 2021.

[19] REID, Miles. **Undergraduate Algebraic Geometry**. Cambridge: Cambridge University Press, 2013; updated Tex version by the author: 2013. 136 p.

[20] REID, Miles. **Undergraduate Commutative Algebra**. Cambridge: Cambridge University Press, 1995. 168 p.

[21] ROTMAN, Joseph J. **Advanced Modern Algebra**. 1. ed. Nova Jersey: Prentice Hall, 2002. 1012 p.

[22] SANTOS, Walter Ferrer; RITTATORE, Alvaro. **Actions and Invariants of Algebraic Groups**. 1. ed. Nova York: CRC Press, 2005. 443 p.

[23] SILVERMAN, Joseph H. **The Arithmetic of Elliptic Curves**. 1. ed. Nova York: Springer-Verlag, 1986. 400 p.

[24] SOTTILE, Frank. Capítulo 2: **Affine Algebraic Geometry**. Notas de Aula. Disponível em: https://www.shsu.edu/~ldg005/data/689/Old.pdf. Acesso em: 10 jul. 2021.

[25] FULTON, William. **Algebraic Curves**: An Introduction to Algebraic Geometry. 3. ed. atual. 2008. Disponível em: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf. Acesso em: 5 ago. 2020.