UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA

Representações implícita e paramétrica de hipersuperfícies algébricas

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Maurício Lourenço Rodrigues da Silva

Orientador: Zaqueu Alves Ramos

São Cristóvão, 2019.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Silva, Maurício Lourenço Rodrigues
586r Representações implícita e paramétrica de hipersuperfícies algébricas / Maurício Lourenço Rodrigues Silva ; orientador Zaqueu Alves Ramos. - São Cristóvão, 2019.
40 f. : il.

Dissertação (mestrado profissional em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática. 2. Polinômios. 3. Hipersuperfícies 4. Álgebra. 5. Equações. 6. Funções (Matemática). Ramos, Zaqueu Alves orient. II. Título.

CDU 514.7

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Representações implícita e paramétrica de hipersuperfícies algébricas

por

Maurício Lourenço Rodrigues da Silva

Aprovada pela banca examinadora:

Prof. Zaqueu Alves Ramos - UFS
Orientador

Prof. André Vinicius Santos Dória - UFS
Primeiro Examinador

Prof. Fabio Lima Santos - UFRPE
Segundo Examinador

São Cristóvão, 28 de Maio de 2019

Agradecimentos

Primeiramente a Deus por está sempre presente na minha vida me dando força, sabedoria e saúde para superar as dificuldades e alcançar meus objetivos.

À todos os meus familiares que sempre acreditaram no meu potencial, em especial a minha mãe Elizabete, e as outras mães Dete e Ácacia por suas orações durante todo curso.

Agradeço a minha amada esposa, Danielly, que soube entender meus momentos de ausência, sempre contei com seu apoio para continuar.

Um agradecimento especial aos amigos/familiares, Aninha, Antônio Fernandes, Daniel, Ingrid, Jhon, Jorlan, José Hélio, José Thiago, Keu, Mauro, Michel e Nilton que me incentivaram a ingressar no PROFMAT, me deram embasamento, palavras de incentivo, me cercaram de boas vibrações e orientações. Este título não seria possível sem a colaboração de vocês!

Aos meus colegas de curso, hoje considerados amigos pelos momentos de estudos, aflições, alegrias, brincadeiras e o mais importante pela troca de experiências, em especial, agradeço ao companheirismo e a cumplicidade dos meus queridos amigos da "panela"por serem minha "família"e sempre dispostos a ajudar. Vocês tornaram essa vitória possível!

Aos professores doutores, Humberto, Evilson, Zaqueu, Giovana, André e Bruno pelos conhecimentos repassados e pelo incentivo.

Ao meu orientador Prof. Dr. Zaqueu e à banca examinadora pela contribuição por meio de sugestões para o aperfeiçoamento deste trabalho.

Enfim, a todos que contribuíram diretamente e indiretamente para a concretização deste sonho.

Resumo

O objeto central de estudo dessa dissertação são as hipersuperfícies algébricas. O principal aspecto que desejamos abordar é sobre como essas hipersuperfícies podem ser representadas. Mais especificamente, discutimos sobre as representações implícita e paramétrica. Mostraremos quais são as vantagens e desvantagens de cada uma delas e também discutimos o problema de obter uma representação a partir da outra.

Palavras Chave: Polinômio, hipersuperfície algébrica, equação implícita, função racional, equações paramétricas.

Abstract

The central object of this dissertation are the algebraic hypersurfaces. The main aspect we wish to address is how these hypersurfaces can be represented. More specifically, it is discussed implicit and parametric representations. We will show the advantages and disadvantages of each one of them and also discuss the problem of obtaining a representation from the other.

Keywords: Polynomial; algebraic hypersurfaces; implicit equation; rational function; parametric equations.

Conteúdo

Introdução

Nessa dissertação nos ocupamos em fazer um breve estudo sobre um dos mais fundamentais objetos da geometria algébrica, as chamadas *hipersuperfícies algébricas*. A grosso modo, estas hipersuperfícies são conjuntos soluções de uma equação polinomial. Esta noção abrange como exemplos particulares diversas figuras geométricas que nos são familiares desde o ensino básico, tais como retas, circunferências, elipses, hipérboles, parábolas, esferas, planos, cilindros, etc.

Fixada uma hipersuperfície algébrica, chamamos uma equação polinomial que a define de *representação implícita*. De forma geral, essas representações são úteis para decidir se um ponto pertence a hipersuperfície. Todavia, na maioria das situações, elas não são adequadas para produzir pontos que pertencem a hipersuperfície. Assim, surge a demanda de saber se existe uma forma alternativa de representar a hipersuperfície de modo a suprir essa deficiência da representação implícita. É nesse contexto que a *representação paramétrica racional* surge.

Nesse trabalho estaremos interessados em discurtir sobre estas duas formas de representar hipersuperfícies algébricas, a implícita e a paramétrica. Para isso, dividimos o trabalho em três capítulos os quais passamos a descrever brevemente.

No capítulo um fazemos um apanhado sobre os pré-requisitos algébricos que são necessários para entender os conceitos e resultados em torno da noção de hipersuperfície algébrica. Por exemplo, são tratadas nessa parte do texto as definições de anel, domínio, corpo, polinômios em várias variáveis e elementos irredutíveis. Um dos resultados mais importantes desse capítulo é o critério de Eisenstein, que nos fornece condições suficientes para identificar se um polinômio é ou não irredutível.

Iniciamos o capítulo dois introduzindo a definição precisa de uma hipersuperfície algébrica. Como veremos, os objetos que as definem são exatamente as equações implícitas. Um dos aspectos que tratamos neste capítulo é sobre a questão de quantas equações implícitas podem representar uma mesma hipersuperfície. Também lidamos com a noção de hipersuperfícies irredutíveis e verificamos como a propriedade de fatoração única em um anel de polinômios com coeficientes sobre um corpo se traduz em termos de decomposição de uma hipersuperfície em componentes irredutíveis.

No terceiro e último capítulo apresentamos a representação paramétrica racional. Com exem-

plos, discutimos em detalhes as representações paramétricas de hiperplanos e de esferas. Mostramos também que nem toda hipersuperfície admite uma tal representação. Finalizamos o capítulo apontando quais são as vantagens e desvantagens entre as representações implícitas e paramétricas.

Capítulo 1

Preliminares algébricos

O objetivo deste capítulo é apresentar alguns conceitos e resultados de caráter algébrico que serão úteis para a compreensão dos principais objetos desse trabalho. A principal referência utilizada nessa parte do texto é [4]. Ressaltamos que esse é um trabalho introdutório que busca dar uma visão panorâmica sobre o tema das representações implícita e paramétrica. Por essa razão, as demonstrações de alguns resultados mais longos ou mais técnicos serão omitidas.

1.1 Exemplos de estruturas algébricas

1.1.1 A estrutura de anel

Definição 1.1.1. Seja A um conjunto não vazio. Considere $+ : A \times A \to A$ e $\cdot : A \times A \to A$ duas operações em A chamadas, respectivamente, de *adição* e *multiplicação* de A. Diremos que a terna $(A, +, \cdot)$ é um *anel comutativo com identidade* se as seguintes propriedades forem verificadas:

(a) **Associatividade da adição**: quaisquer que sejam $a, b, c \in A$, $(a + b) + c = a + (b + c)$.

(b) **Comutatividade da adição:** quaisquer que sejam $a,\ b \in A$, $a + b = b + a$.

(c) **Existência do elemento neutro:** existe $0 \in A$ tal que para qualquer $a \in A$, $0 + a = a$.

(d) **Existência do elemento inverso:** para cada $a \in A$ existe $-a \in A$ tal que $a + (-a) = 0$.

(e) **Associatividade da multiplicação:** quaisquer que sejam $a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(f) **Comutatividade da multiplicação**: quaisquer que sejam $a, b \in A$, $a \cdot b = b \cdot a$.

(g) **Existência do elemento identidade**: existe $1 \in A$ tal que para cada $a \in A$ temos $1 \cdot a = a$.

(h) **Distributividade da multiplicação com relação à adição**: quaisquer que sejam $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Uma terna $(A, +, \cdot)$ satisfazendo as propriedades da Definição 1.1.1 exceto, possivelmente, as propriedades (f) e (g) é chamado simplesmente de *anel*. O acréscimo dos adjetivos *comutativo* e *com identidade* serve para enfatizar que a multiplicação satisfaz essas propriedades. Nesse texto estamos interessados apenas nos anéis comutativos com identidade. Assim, para efeito de simplicidade, cometeremos o abuso de chamá-los apenas de anéis.

Como percebemos da definição, a estrutura de anel é determinada pelo conjunto A e as operações de adição e multiplicação. É possível obter anéis distintos com o mesmo conjunto A, bastando para isso definir operações de adição ou multiplicação distintas. Desse modo, a rigor, toda vez que nos referíssemos a um anel comutativo com identidade deveríamos fazê-lo explicitando toda a terna $(A, +, \cdot)$. Contudo, quando as operações estão bem entendidas pelo contexto, é comum utilizarmos apenas o conjunto A para designar toda a estrutura.

Um instante de reflexão e rapidamente podemos nos dar conta que a noção de anel é uma formalização abstrata para o tipo de estrutura que encontramos em $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com suas respectivas operações de adição e multiplicação. Assim, em particular, esses são exemplos de anéis.

1.1.2 A estrutura de domínio de integridade

Definição 1.1.2. Seja A um anel. Um elemento $a \in A$ é chamado um *divisor de zero* de A se existe $b \in A \setminus \{0\}$ tal que $a \cdot b = 0$.

Utilizaremos a notação $Z(A)$ para representar o conjunto de todos os elementos de A que são divisores de zero em A. Claramente, $\{0\} \subset Z(A)$. A situação extremal em que $Z(A) = \{0\}$ é o conteúdo da seguinte definição:

Definição 1.1.3. Um anel A é dito *domínio de integridade* (ou simplesmente *domínio*) se $Z(A) = \{0\}$.

Assim, dizer que um anel é um domínio é equivalente a dizer que o produto de dois elementos não nulos quaisquer é sempre um elemento não nulo. Obviamente, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de domínios. Apresentamos no exemplo a seguir um anel que não é domínio.

Exemplo 1.1.4. Denotemos o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$ por $\mathcal{F}(\mathbb{R}, \mathbb{R})$. Para cada $(f, g) \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \times \mathcal{F}(\mathbb{R}; \mathbb{R})$ definimos $f + g$ e $f \cdot g \in \mathcal{F}(X, \mathbb{R})$ por

$$(f + g)(x) := f(x) + g(x) \quad \text{e} \quad (f \cdot g)(x) := f(x) \cdot g(x)$$

para todo $x \in X$. É facilmente verificado que:

(a) A terna $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\cdot)$ é um anel.

(b) A função identicamente nula é o zero do anel $\mathcal{F}(\mathbb{R},\mathbb{R})$.

(c) A função identicamente igual a 1 é a identidade de $\mathcal{F}(\mathbb{R},\mathbb{R})$.

Agora, consideremos $f,\ g \in \mathcal{F}(\mathbb{R},\mathbb{R})$ definidas por:

$$f(x)=\begin{cases} 0, & \text{se } x \leqslant 0 \\ 1, & \text{se } x > 1 \end{cases} \qquad \text{e} \qquad g(x)=\begin{cases} 1, & \text{se } x \leqslant 0 \\ 0, & \text{se } x > 1 \end{cases}$$

Obviamente, f e g são elementos não nulos de $\mathcal{F}(\mathbb{R},\mathbb{R})$. No entanto, $f\cdot g = 0$. Assim, $Z(\mathcal{F}(\mathbb{R},\mathbb{R})) \neq \{0\}$, ou seja, $\mathcal{F}(\mathbb{R},\mathbb{R})$ não é domínio.

1.1.3 A estrutura de corpo

Definição 1.1.5. Seja A um anel. Um elemento $a \in A \setminus \{0\}$ é chamado invertível se existe $b \in A$ tal que $a \cdot b = 1$.

Convencionamos que o inverso multiplicativo de a é a^{-1}.

O conjunto de todos os elementos do anel A que são invertíveis em A será simbolizado por A^*.

Exemplo 1.1.6. $\mathbb{Z}^* = \{-1,1\}$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ e $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$.

Por definição, $A^* \subset A \setminus \{0\}$. Na situação extremal $A^* = A \setminus \{0\}$ temos a seguinte definição:

Definição 1.1.7. Um anel A é dito um corpo se $A^* = A \setminus \{0\}$.

Claramente, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos enquanto $\mathbb{Z}$ e $\mathcal{F}(\mathbb{R},\mathbb{R})$ não são corpos. As noções de domínio e corpos estão relacionadas pela seguinte proposição.

Proposição 1.1.8. *Se A é um corpo então A é um domínio.*

Prova. Sejam $a, b \in A$ tais que $ab = 0$. Digamos que $a \neq 0$. Devemos mostrar que $b = 0$. Como A é corpo e $a \neq 0$ então existe o inverso a^{-1} de a. Assim $a^{-1}ab = a^{-1}0$, ou seja, $b = 0$ como queríamos provar. □

Notadamente, a recíproca da Proposição 1.1.8 é falsa. Por exemplo, $\mathbb{Z}$ é um domínio que não é um corpo. Todavia, a recíproca torna-se verdadeira se supusermos que A é finito. O leitor interessado em maiores detalhes sobre essa afirmação pode consultar [4, Capítulo 1].

1.2 Domínios de fatoração única

Definição 1.2.1. Seja D um domínio e $a,\ b \in D$ com $b \neq 0$. Dizemos que b *divide* a em D, e denotamos $b|a$, se existe elemento $c \in D$ tal que:

$$a = bc. \tag{1.1}$$

Também dizemos nesse caso que b é um *divisor* de a em D.

Um elemento $a \in D$ não nulo e não invertível tem sempre como divisores em D os elementos de D^* e os elementos da forma ua, com $u \in D^*$. Chamamos esses divisores de a de *divisores triviais* de a.

Definição 1.2.2. Seja D um domínio. Um elemento não nulo e não invertível de D é dito *irredutível* se seus únicos divisores são os triviais.

Por exemplo, na terminologia acima, dizer que um número inteiro p é irredutível em $\mathbb{Z}$ significa que os únicos divisores de p são ± 1 e $\pm p$. O leitor atento notará que o que estamos chamando de número inteiro irredutível aqui é exatamente o que chamávamos no ensino básico de número inteiro *primo*.

Definição 1.2.3. Um domínio D é chamado *domínio de fatoração única* (DFU) se cada elemento $a \in D$ não nulo e não invertível pode ser fatorado como produto de fatores irredutíveis e tal fatoração é única no seguinte sentido: se $a = p_1 \cdots p_r = q_1 \cdots q_s$, onde p_i e q_i são elementos irredutíveis, então $r = s$ e, a menos de reordenação dos índices, $p_i = u_i q_i$, com $u_i \in D^*$, para cada $1 \leqslant i \leqslant r$.

Notação: Dado um elemento não nulo e não invertível a em um domínio de fatoração única escrevemos a fatoração em irredutíveis de a na forma $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ onde $p_i \neq up_j$, $\forall i \neq j$ e $u \in D^*$, com os p_i dois a dois distintos e os α_i sendo exatamente a quantidade de vezes que p_i ocorre como fator de a.

Exemplo 1.2.4. Todo corpo é um domínio de fatoração única. Essa afirmação segue por vacuidade pois o conjunto de elementos não nulo e não invertível de um corpo é vazio.

Exemplo 1.2.5. Do teorema fundamental da aritmética segue que $\mathbb{Z}$ é um domínio de fatoração única.

Uma propriedade importante dos elementos irredutíveis em domínios de fatoração única é dada pela seguinte proposição:

Proposição 1.2.6. *Seja* D *um domínio de fatoração única e* $p \in D$ *um elemento irredutível de* D. *Se* p *divide um produto* ab, *com* $a, b \in D$, *então* p *divide* a *ou* p *divide* b.

Prova. Se p divide a então não há o que demonstrar. Assim, suponhamos que p não divide a. Como p divide ab então p é um fator irredutível de ab. Mas os fatores irredutíveis de ab é a união dos fatores irredutíveis de a com os fatores irredutíveis de b. Pela unicidade dos fatores irredutíveis e pelo fato de que p não divide a segue que p divide b. □

Definição 1.2.7. Sejam D um domínio e a, b elementos de D (com a ou b não nulo). Um *máximo divisor comum* de a e b em D é um elemento $d \in D$ satisfazendo as seguintes propriedades:

(a) d divide a e d divide b.

(b) Se $d' \in D$ é tal que d' divide a e d' divide b então d' divide d.

Algumas observações que seguem imediatamente da definição de máximo divisor comum são:

(i) Para cada a não nulo, um máximo divisor comum entre a e 0 é a.

(ii) Se a é um elemento invertível de D então um máximo divisor comum de a e b é a.

(iii) Seja d um máximo divisor comum de a e b. Então e é o outro máximo divisor comum de a e b se, e somente se, $d = ue$ para algum $u \in D^*$.

Notação: Sejam D um domínio e a, b elementos de D (com a ou b não nulo). Usaremos a notação $\mathrm{mdc}(a, b)$ para denotar um máximo divisor comum de a, b. Note pela observação (iii) acima que $\mathrm{mdc}(a, b)$ é único a menos de multiplicação por elementos invertíveis de D.

Em geral, não é verdade que o máximo divisor comum entre dois elementos em um domínio D exista. Todavia, se D for um domínio de fatoração única então dois elementos sempre admitirão máximo divisor comum. Esse é o conteúdo da seguinte proposição:

Proposição 1.2.8. *Seja* D *um domínio de fatoração única. Suponha* a *e* b *dois elementos não nulos e não invertíveis de* D. *Digamos que* $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ *são as fatorações em irredutíveis de* a *e* b. *Então:*

$$\mathrm{mdc}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_n^{\min\{\alpha_n, \beta_n\}}.$$

Prova. Denotemos $d = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_n^{\min\{\alpha_n, \beta_n\}}$. Por construção, temos que d divide a e b. Agora, suponhamos d' um divisor comum de a e b. Em particular, $d' = p_1^{\gamma_1} \dots p_n^{\gamma_n}$. Note que $\gamma_i \leqslant \min\{\alpha_i, \beta_i\}$ para cada $1 \leqslant i \leqslant n$. Em particular, d' divide d e com isso provamos que $d = \mathrm{mdc}(a, b)$. □

1.3 Anéis de polinômios

Um polinômio em n *variáveis* $x_1, \ldots, x_n$ com *coeficientes* em um anel A é uma expressão formal do tipo

$$\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \tag{1.2}$$

onde os $a_{i_1,\ldots,i_n}$ são elementos em A diferentes de zero apenas para uma quantidade finita de índices $(i_1,\ldots,i_n) \in \mathbb{N}^n$. Cada $a_{i_1,\ldots,i_n}$ é chamado de *coeficiente* do polinômio. Denotamos a coleção de todos os polinômios em n variáveis $x_1, \ldots, x_n$ com coeficientes em A por $A[x_1, \ldots, x_n]$. É usual usarmos os símbolos

$$f(x_1, \ldots, x_n),\ g(x_1, \ldots, x_n),\ h(x_1, \ldots, x_n), \ldots$$

para representarmos polinômios de $A[x_1, \ldots, x_n]$ (para efeito de simplificar a notação também escrevemos $f,\ g,\ h, \ldots$). Dois polinômios

$$f(x_1, \ldots, x_n) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \quad \text{e} \quad g(x_1, \ldots, x_n) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} b_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

são iguais se seus coeficientes de mesmo índice forem iguais, ou seja, $a_{i_1,\ldots,i_n} = b_{i_1,\ldots,i_n}$ para cada $(i_1,\ldots,i_n) \in \mathbb{N}^n$.

Um polinômio de $A[x_1, \ldots, x_n]$ da forma $x_1^{i_1} \cdots x_n^{i_n}$ é chamado de *monômio*. Por outro lado, um polinômio da forma $a x_1^{i_1} \cdots x_n^{i_n}$, com $a \in A$, é chamado de *termo monomial*. Identificamos cada termo monomial da forma $a x_1^0 \cdots x_n^0$ com o elemento $a \in A$ Com isso, identificaremos A como um subconjunto de $A[x_1, \ldots, x_n]$. Estes polinômios serão chamados de *polinômios constantes*.

Para simplificar a notação, dada uma n-upla $\alpha = (i_1, \ldots, i_n)$, escreveremos $\mathbf{x}^\alpha$ para denotar o monômio $x_1^{i_1} \cdots x_n^{i_n}$. Com isso, um polinômio

$$f = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

ficará representado por

$$f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha \mathbf{x}^\alpha$$

Exemplo 1.3.1. $f = x_1^2 + x_2^2 + x_3^2 - 1$ e $h = ix_1 + x_2 + x_3 - 7$ são exemplos de polinômios de $\mathbb{C}[x_1, x_2, x_3]$.

Definição 1.3.2. Seja A um anel. Suponha $f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha \mathbf{x}^\alpha \quad \text{e} \quad g = \sum_{\alpha\in\mathbb{N}^n} b_\alpha \mathbf{x}^\alpha$ polinômios

de $A[x_1, \ldots, x_n]$. A *adição entre os polinômios* f e g é:

$$f + g := \sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha)\mathbf{x}^\alpha.$$

Exemplo 1.3.3. Sejam $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + 1$ e $g(x_1) = x_1^2 + x_1x_2 - 2x_1 + 1$. Segue da definição de adição que

$$f(x_1) + g(x_1) \;=\; 2x_1^2 + x_2^2 + x_1x_2 - 2x_1 + 2.$$

Observamos que todo polinômio de $A[x_1, \ldots, x_n]$ é escrito de forma única como uma soma de termos monomiais. Assim, para definir uma multiplicação em $A[x_1, \ldots, x_n]$ podemos iniciar definindo como multiplicar termos monomiais e, em seguida, estendemos esta multiplicação para todos os polinômios através da distributividade. A maneira que definimos a multiplicação entre dois termos monomiais $a\mathbf{x}^\alpha$ e $b\mathbf{x}^\beta$ é:

$$a\mathbf{x}^\alpha \cdot b\mathbf{x}^\beta := ab\mathbf{x}^{\alpha+\beta}.$$

Exemplo 1.3.4. Sejam $f(x_1, x_2) = x_1 - x_1x_2 + 1$ e $g(x_1, x_2) = x_1^2 + x_2^2$. Segue da definição de multiplicação que

$$\begin{aligned} f(x_1, x_2) \cdot g(x_1, x_2) &= (x_1 - x_1x_2 + 1) \cdot (x_1^2 + x_2^2) \\ &= x_1^3 + x_1x_2^2 - x_1^3x_2 - x_1x_2^3 + x_1^2 + x_2^2. \end{aligned}$$

Proposição 1.3.5. *Seja A um anel. O conjunto $A[x_1, \ldots, x_n]$ com as operações de adição e multiplicação acima definidas satisfaz as seguintes propriedades:*

(a) **A adição é associativa:** *para qualquer* $f, g, h \in A[x_1, \ldots, x_n]$, $(f + g) + h = f + (g + h)$.

(b) **A adição é comutativa:** *para qualquer* $f, g \in A[x_1, \ldots, x_n]$, $f + g = g + f$.

(c) **Existe elemento neutro para a adição:** *para qualquer* $f \in A[x_1, \ldots, x_n]$, $0 + f = f + 0 = f$.

(d) **Existência do elemento inverso para a adição:** *Para cada* $f \in A[x_1, \ldots, x_n]$, $f + (-1)f = 0$ (*usamos a notação* $-f$ *para denotar o polinômio* $(-1)f$).

(e) **A multiplicação é associativa:** *para qualquer* $f, g, h \in A[x_1, \ldots, x_n]$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

(f) **A multiplicação é comutativa:** *para qualquer* $f, g \in A[x_1, \ldots, x_n]$, $f \cdot g = g \cdot f$.

(g) **Existe elemento neutro para a multiplicação:** *para qualquer* $f \in A[x_1, \ldots, x_n]$, $f \cdot 1 = f$.

(h) **A multiplicação é distributiva com relação à adição:** *para qualquer* $f, g, h \in A[x_1, \ldots, x_n]$, $f \cdot (g + h) = f \cdot g + f \cdot h$

Em particular, $A[x_1, \ldots, x_n]$ *é um anel.*

Prova. Ver [4, Capítulo 3]. □

Doravante, chamaremos $A[x_1, \ldots, x_n]$ de *anel de polinômios em* n *variáveis com coeficientes sobre* A.

Na proposição abaixo listamos algumas propriedades que podem ser observadas no anel $A[x_1, \ldots, x_n]$.

Proposição 1.3.6. *Seja* A *um anel. Então:*

(a) $A[x_1, \ldots, x_n]$ *é domínio se, e somente se,* A *é domínio.*

(b) *Se* A *é domínio, então* $A[x_1, \ldots, x_n]^* = A^*$.

(c) $A[x_1, \ldots, x_n] = A'[x_n]$, *onde* $A' = A[x_1, \ldots, x_{n-1}]$.

Prova. Ver [2, Capítulo 3].

□

O item (c) da proposição acima é bastante útil pois permite que possamos reduzir muitos argumentos à anéis de polinômios em uma única variável.

Uma forma de "medir"um polinômio em uma variável é dada pelo conceito de grau.

Definição 1.3.7. Seja A um anel e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ um polinômio em uma variável não nulo. O grau de $f(x)$, denotado $\operatorname{gr} f(x)$, é o maior índice i tal que $a_i \neq 0$. O coeficiente a_d, com $d = \operatorname{gr} f(x)$, é chamado de *coeficiente líder* de f.

Resumimos algumas propriedades do grau na próxima proposição.

Proposição 1.3.8. *Sejam* A *um anel e* $f(x), g(x)$ *polinômios de* $A[x]$ *não nulos. Então:*

(a) *Se* $f(x) + g(x) \neq 0$, *então* $\operatorname{gr}(f(x) + g(x)) \leqslant \max\{\operatorname{gr} f(x), \operatorname{gr}(g(x)\}$.

(b) *Se* $f(x)g(x) \neq 0$, *então* $\operatorname{gr}(f(x)g(x)) \leqslant \operatorname{gr} f(x) + \operatorname{gr} g(x)$.

(c) *Se* A *é domínio, então* $f(x)g(x) \neq 0$ *e* $\operatorname{gr}(f(x)g(x)) = \operatorname{gr} f(x) + \operatorname{gr} g(x)$.

Prova. Ver [4, Capítulo 3]. □

Observação 1.3.9. Do item (c) da Proposição 1.3.8 segue que se A é um domínio então $A[x]$ é domínio. Em particular, usando a Proposição 1.3.6(c) e indução segue que $A[x_1, \ldots, x_n]$ é domínio se A é domínio.

Um importante resultado na teoria dos anéis de polinômios é:

Teorema 1.3.10. *Sejam* A *um anel* $f(x), g(x) \in A[x]$ *polinômios em uma única variável com coeficientes em* A. *Suponha que* $g(x)$ *é não nulo e tem coeficiente líder invertível em* A. *Então existem polinômios* $q(x), r(x) \in A[x]$, *com* $r(x) = 0$ *ou* $\operatorname{gr} r(x) < \operatorname{gr} g(x)$, *tais que*

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

Prova. Ver [4, Capítulo 3]. □

1.4 Irredutibilidade e fatoração única em anéis de polinômios

Teorema 1.4.1. *Se* D *é um domínio de fatoração única então o anel de polinômios* $D[x]$ *é um domínio de fatoração única.*

Prova. Ver [4, Capítulo 2]. □

Observação 1.4.2. (a) Se D é um domínio de fatoração então o anel de polinômios $D[x_1, \ldots, x_n]$ é também um domínio de fatoração única. Essa afirmação pode ser justificada por indução. Com efeito, para $n = 1$ a afirmação é exatamente o teorema anterior. Agora suponhamos que a afirmação é verdadeira para $n - 1$, isto é, $D' = D[x_1, \ldots, x_{n-1}]$ é domínio de fatoração única. Em particular, usando mais uma vez o teorema anterior segue que $D'[x_n]$ é domínio de fatoração única. Mas, pela Proposição 1.3.6 (c), $D[x_1, \ldots, x_n] = D'[x_n]$. Portanto, segue a afirmação desejada.
(b) Se k é um corpo então $k[x_1, \ldots, x_n]$ é um domínio de fatoração única. De fato, pelo Exemplo 1.2.4, k é um domínio de fatoração única. Assim, pelo item (a) desta observação segue o afirmado.

Toda vez que estamos diante de um domínio de fatoração única uma questão natural é entender como detectar se um elemento é ou não irredutível. Nesse trabalho estamos particularmente interessados nessa questão na situação em que o domínio de fatoração única é um anel de polinômios. Discutiremos logo a seguir duas classes de polinômios que são irredutíveis. Antes porém, fazemos uma pausa para a seguinte definição:

Definição 1.4.3. Seja D um domínio de fatoração única. Um polinômio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ de grau $n \geqslant 1$ é dito *primitivo* se não existe elemento irredutível de D que divida todos os coeficientes $a_n, \ldots, a_0$ simultaneamente.

Agora podemos ver a primeira classe de polinômios irredutíveis.

Proposição 1.4.4. *Seja* D *um domínio de fatoração única. Então todo polinômio primitivo de grau* 1 *de* $D[x]$ *é irredutível.*

Prova. Seja $f(x) \in D[x]$ primitivo de grau 1, então $f(x)$ é da forma $f(x) = ax + b$ com $a \neq 0$. Digamos que $g(x), h(x) \in D[x]$ são tais que $f(x) = g(x)h(x)$. Para provar que $f(x)$ é irredutível devemos concluir que $g(x) \in D^*$ ou $h(x) \in D^*$. Obviamente, $g(x)$ e $h(x)$ são não nulos, pois $f(x)$ é não nulo. Por outro lado, pela Proposição 1.3.8(c), $\operatorname{gr} g(x) = 0$ ou $\operatorname{gr} h(x) = 0$, ou seja, $g(x) \in D \setminus \{0\}$ ou $h(x) \in D \setminus \{0\}$. Sem perda de generalidade, digamos que $g(x) \in D \setminus \{0\}$. Então, $g(x) = c$ para algum $c \in D \setminus \{0\}$. Note que c tem que ser um elemento invertível de D pois, caso contrário, $f(x)$ não seria primitivo. Portanto, $g(x) \in D^*$ e isso conclui a demonstração. □

Uma consequência imediata desta proposição é:

Corolário 1.4.5. *Seja* k *um corpo. Então todo polinômio de grau* 1 *de* $k[x]$ *é irredutível.*

Prova. Um corpo é um domínio de fatoração única que não contém elementos irredutíveis. Assim, em particular, todo polinômio de $k[x]$ é primitivo. Em particular, todo polinômio de grau 1 de $k[x]$ é primitivo. Com esta observação e a proposição anterior segue o desejado. □

Outros exemplos de polinômios irredutíveis podem ser obtidas através do seguinte teorema:

Teorema 1.4.6 (Critério de Eisenstein)**.** *Sejam* D *um domínio de fatoração única e* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *um polinômio em* $D[x]$ *de grau* $n \geqslant 1$ *primitivo. Se existe um elemento irredutível* $p \in D$ *tal que*

(i) p *não divide* a_n.

(ii) p *divide* $a_{n-1}, \ldots, a_0$.

(iii) p^2 *não divide* a_0

então $f(x)$ *é irredutível em* $D[x]$.

Prova. Suponhamos que $f(x)$ não é irredutível. Então existem $g(x), h(x) \in D[x] \setminus D^*$ tais que $f(x) = g(x)h(x)$. Observe que $g(x)$ e $h(x)$ não são polinômios constantes, pois do contrário $f(x)$ não seria primitivo. Assim, $r := \operatorname{gr} g(x) \geqslant 1$ e $s = \operatorname{gr} h(x) \geqslant 1$. Digamos que $g(x) = b_r x^r + \cdots + b_1 x + b_0$ e $h(x) = c_s x^s + \cdots + c_1 x + c_0$. Efetuando o produto $g(x)h(x)$ e comparando seus coeficientes com os de $f(x)$ obtemos:

$$\begin{aligned}
a_0 &= b_0 c_0 \\
a_1 &= b_0 c_1 + b_1 c_0 \\
a_2 &= b_0 c_2 + b_1 c_1 + b_2 c_0 \\
&\vdots \\
a_j &= b_0 c_j + b_1 c_{j-1} + \cdots + b_j c_0 \\
&\vdots \\
a_n &= b_0 c_n + b_1 c_{n-1} + \cdots + b_n c_0
\end{aligned}$$

Como p divide $a_0 = b_0c_0$ então, pela Proposição 1.2, p divide b_0 ou p divide c_0. Observe que p não pode dividir b_0 e c_0 simultaneamente pois por hipótese p^2 não divide a_0. Sem perda de generalidade, podemos supor que p divide b_0 e p não divide c_0. Temos que p divide $a_1 = b_0c_1 + b_1c_0$. Como p também divide b_0c_1 segue que p divide b_1c_0. Usando novamente a Proposição 1.2 e o fato de que p não divide c_0 obtemos que p divide b_1. Como p divide $a_2 = b_0c_2 + b_1c_1 + b_2c_0$ e p divide $b_0c_2 + b_1c_1$ obtemos que p divide b_2c_0. Novamente pela Proposição 1.2 e o fato de que p não divide c_0 concluímos que p divide b_2. Continuando dessa maneira concluímos que p divide todos os coeficientes de $g(x)$. Em particular, p divide $a_n = b_0c_j + b_1c_{j-1} + \cdots + b_jc_0$. Mas isso é um absurdo, pois por hipótese p não divide a_n. Sendo assim, $f(x)$ é irredutível como queríamos provar. □

Exemplo 1.4.7. Seja k um corpo. Afirmamos que $f(x, y) = x^2 + y^2 - 1$ é um polinômio irredutível de $k[x, y]$. Com efeito, pela Proposição 1.3.6(c), podemos olhar $k[x, y]$ como o anel de polinômios em uma variável $D[y]$, onde $D = k[x]$. Nessa perspectiva, $f(x, y)$ pode ser pensado como um polinômio de grau 2 na variável y da seguinte maneira

$$f(x, y) = a_2y^2 + a_1y + a_0,$$

onde $a_2 = 1$, $a_1 = 0$ e $a_0 = x^2 - 1 = (x + 1)(x - 1)$. Como $a_2 = 1$, não pode existir polinômio irredutível que divide todos os coeficientes de $f(x, y)$. Logo, $f(x, y)$ é polinômio primitivo de $D[y]$. Considere agora $p = x + 1$. Pelo Corolário 1.4.5, p é um polinômio irredutível de $D = k[x]$. Além disso, p não divide a_2, p divide a_1 e a_0 e p^2 não divide o termo independente a_0. Dessa forma, pelo critério de Eisenstein, segue que $f(x, y)$ é irredutível.

Capítulo 2

Hipersuperfícies algébricas

Nesse capítulo apresentamos o principal objeto de estudo desse trabalho, as hipersuperfícies algébricas. Veremos que elas são entes geométricos definidos por equações polinomiais. Estas equações polinomiais que definem as hipersuperfícies algébricas são exatamente o que chamamos de representação implícita.

2.1 Definições e resultados preliminares

Seja k um corpo e $f(x_1, \ldots, x_n)$ um polinômio não constante em n variáveis com coeficientes em k. A hipersuperfície algébrica H de k^n, definida pelo polinômio f, é o conjunto solução da equação

$$f(x_1, \ldots, x_n) = 0 \tag{2.1}$$

Chamamos (2.1) de *equação implícita* da hipersuperfície H.

As hipersuperfície algébricas de k^2 e k^3 são chamadas, respectivamente, de *curvas algébricas planas* e *superfícies algébricas espaciais*.

Observação 2.1.1. Hipersuperfícies algébricas são objetos muito manejáveis do ponto de vista computacional pois as equações que as definem envolvem somente um número finito de operações elementares de soma e multiplicação. Essa característica das hipersuperfícies algébricas é explorada em diversos contextos. Um destes diz respeito aos métodos existentes de aproximar hipersuperfícies “menos manejáveis"por hipersuperfícies algébricas (ver por exemplo o princípio por trás dos polinômios de Taylor em [6, Capítulo 3]).

Exemplo 2.1.2 (Hiperplanos)**.** Um *hiperplano* de k^n é uma hipersuperfície algébrica determinada por uma equação implícita da forma

$$a_1x_1 + \cdots + a_nx_n - b = 0, \tag{2.2}$$

onde ao menos um dos coeficientes $a_1, \ldots, a_n$ é não nulo. Observe que, para $n = 2$, os hiperplanos são exatamente as retas de k^2. Por outro lado, para $n = 3$ os hiperplanos correspondem aos planos de k^3.

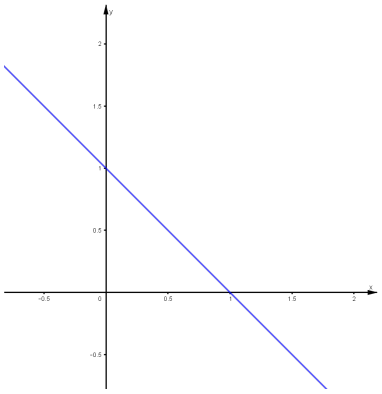

Figura 2.1: Hiperplano de $\mathbb{R}^2$

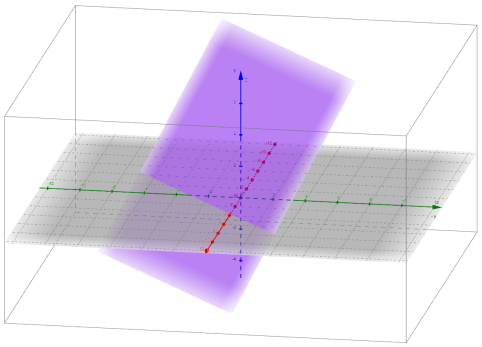

Figura 2.2: Hiperplano de $\mathbb{R}^3$

Exemplo 2.1.3 (Esfera $(n-1)$-dimensional)**.** A *esfera* $(n-1)$*-dimensional* é a hipersuperfície algébrica de k^n determinada pela seguinte equação implícita:

$$x_1^2 + \cdots + x_n^2 - 1 = 0. \tag{2.3}$$

A esfera 1-dimensional é o que costumamos chamar de circunferência. A esfera 2-dimensional é chamada simplesmente de esfera.

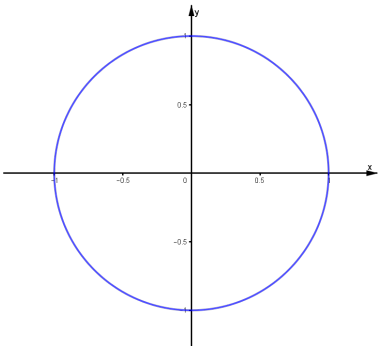

Figura 2.3: Esfera de $\mathbb{R}^2$

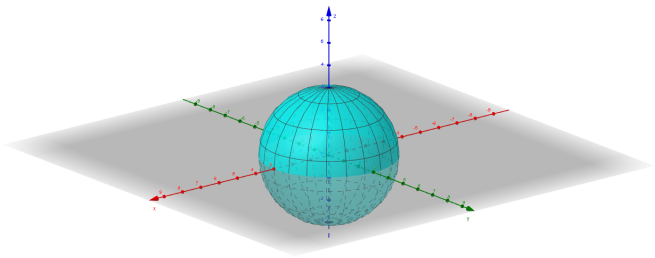

Figura 2.4: Esfera de $\mathbb{R}^3$

Exemplo 2.1.4 (Rosácea)**.** A *rosácea de quatro pétalas* é a curva cuja equação polar é $r = \operatorname{sen} 2\theta$ (ver Figura 2.5). Afirmamos que esta curva também pode ser notada como uma curva algébrica plana definida pela equação implícita

$$(x^2 + y^2)^3 - 4x^2y^2 = 0. \tag{2.4}$$

Com efeito, relembramos que a relação entre as coordenadas cartesianas e polares é dada por

$$\begin{cases} x &= r\cos\theta \\ y &= r\,\mathrm{sen}\,\theta \end{cases} \tag{2.5}$$

A afirmação segue das seguintes equivalências:

$$(x^2+y^2)^3 - 4x^2y^2 = 0 \Leftrightarrow (r^2\cos^2\theta + r^2\mathrm{sen}^2\theta)^3 - 4r^4\cos^2\theta\mathrm{sen}^2\theta = 0 \Leftrightarrow r^2 - 4\cos^2\theta\mathrm{sen}^2\theta$$

$$\Leftrightarrow r^2 = (2\cos\theta\mathrm{sen}\,\theta)^2 \Leftrightarrow r^2 = (\mathrm{sen}\,2\theta)^2 \Leftrightarrow r = \mathrm{sen}\,2\theta.$$

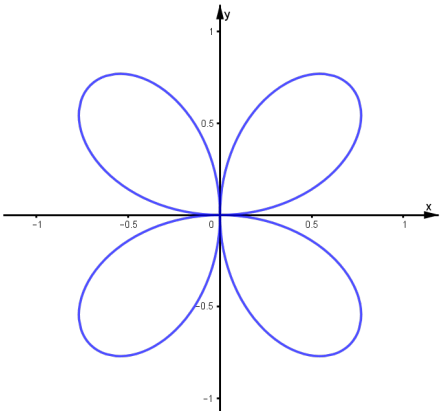

Figura 2.5: Rosácea $r = \mathrm{sen}\,2\theta$

2.2 Ambiguidade da representação implícita

Observamos que a definição de hipersuperfície algébrica de k^n associa cada polinômio não constante em n variáveis com coeficientes em um corpo k a um subconjunto de k^n. De fato, temos a seguinte função

$$\mathcal{V} : k[x_1,\ldots,x_n] \setminus k \to \{\text{hipersuperfícies algébricas de } k^n\} \tag{2.6}$$

onde, para cada $f \in k[x_1,\ldots,x_n]$, $\mathcal{V}(f)$ é a hipersuperfície algébrica com equação implícita

$$f(x_1,\ldots,x_n) = 0.$$

Em particular,

$$\mathcal{V}(f) = \{(a_1,\ldots,a_n) \mid f(a_1,\ldots,a_n) = 0\}.$$

Por construção, $\mathcal{V}$ é um sobrejeção. A questão natural é:

Questão 2.2.1. *Existe uma aplicação $\mathcal{V}$ que seja injetora? Ou seja, quando as hipersuperfícies algébricas de k^n são determinadas unicamente por sua equação implícita?*

Veremos que de modo geral a resposta para essa pergunta é negativa.

Proposição 2.2.2. *Sejam f e g polinômios não constantes de $k[x_1, \ldots, x_n]$ que tem os mesmos fatores irredutíveis. Então, $\mathcal{V}(f) = \mathcal{V}(g)$.*

Prova. Digamos que $f = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $g = p_1^{\beta_1} \cdots p_n^{\beta_n}$, com $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \geqslant 1$, sejam as fatorações em irredutíveis de f e g. Suponhamos que o ponto $(a_1, \ldots, a_n)$ pertence a $\mathcal{V}(f)$. Então,

$$p_1(a_1, \ldots, a_n)^{\alpha_1} \cdots p_n(a_1, \ldots, a_n)^{\alpha_n} = 0. \tag{2.7}$$

Como um corpo é um domínio de integridade (ver Proposição 1.1.8) segue da igualdade (2.7) que $p_i(a_1, \ldots, a_n) = 0$ para algum $1 \leqslant i \leqslant n$. Dessa forma,

$$\begin{aligned} g(a_1, \ldots, a_n) &= p_1(a_1, \ldots, a_n)^{\beta_1} \cdots p_i(a_1, \ldots, a_n)^{\beta_i} \cdots p_n(a_1, \ldots, a_n)^{\beta_n} \\ &= p_1(a_1, \ldots, a_n)^{\beta_1} \cdots 0^{\beta_i} \cdots p_n(a_1, \ldots, a_n)^{\beta_n} \\ &= 0. \end{aligned} \tag{2.8}$$

Daí, $(a_1, \ldots, a_n) \in \mathcal{V}(g)$. Logo, $\mathcal{V}(f) \subset \mathcal{V}(g)$. Por um argumento análogo concluímos a inclusão contrária $\mathcal{V}(g) \subset \mathcal{V}(f)$ e daí temos a igualdade desejada. □

Definição 2.2.3. Dizemos que um polinômio $f \in k[x_1, \ldots, x_n]$ é *reduzido* se para todo fator irredutível p de f, tivermos que p^2 não divide f, i.e., se $p_1, \ldots, p_n$ são os fatores irredutíveis de f, onde $p_i \neq u p_j$, $\forall i \neq j$ e $u \in k^*$, então $f = p_1 \cdots p_n$.

Seja f um polinômio não constante de $k[x_1, \ldots, x_n]$. Digamos que $f = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ é a fatoração em irredutíveis de f. Definimos o *reduzido* de f por

$$f_{\text{red}} = p_1 \cdots p_n.$$

Assim, um polinômio $f \in k[x_1, \ldots, x_n] \setminus k$ é *reduzido* se $f = f_{\text{red}}$. Segue da Proposição 2.2.2 que se restringirmos a aplicação $\mathcal{V}$ ao conjunto dos polinômios reduzidos de $k[x_1, \ldots, x_n] \setminus k$ teremos ainda uma sobrejeção no conjunto de todas as hipersuperfícies de k^n. Precisamente, a função

$$\mathcal{V} : \{f \in k[x_1, \ldots, x_n] \setminus k \mid f \text{ é reduzido}\} \to \{\text{hipersuperfície algébrica de } k^n\} \tag{2.9}$$

é sobrejetora. A questão agora é se esta restrição é injetora. Podemos ver que de modo geral não. De fato, consideremos $f, g \in k[x_1, \ldots, x_n]$ sendo polinômios reduzidos tais que $f = \lambda g$, onde $\lambda \in k^*$. É imediato notar que nesse caso $\mathcal{V}(f) = \mathcal{V}(g)$. Todavia, sob certas hipóteses sobre o corpo k esse é o único tipo de ambiguidade que pode ocorrer. Veremos que esse é o caso quando $k = \mathbb{C}$.

Teorema 2.2.4. *Sejam* $f, g \in \mathbb{C}[x_1, \ldots, x_n] \setminus \mathbb{C}$ *polinômios reduzidos. Então as seguintes afirmações são equivalentes:*

(a) $\mathcal{V}(f) = \mathcal{V}(g)$.

(b) $f = \lambda g$ *para algum* $\lambda \in \mathbb{C}^*$.

Prova. Ver [1, Capítulo 1]. □

2.3 Hipersuperfícies algébricas irredutíveis

Uma hipersuperfície algébrica H de k^n é *irredutível* se pode ser definida por uma equação implícita

$$f(x_1, \ldots, x_n) = 0,$$

com $f(x_1, \ldots, x_n)$ sendo um polinômio irredutível de $k[x_1, \ldots, x_n]$.

Exemplo 2.3.1. Consideremos o hiperplano H de k^n definido pela equação implícita

$$a_1x_1 + \cdots + a_nx_n - b = 0$$

com $a_1, \ldots, a_n, b \in k$ e ao menos um dos a_i diferente de zero. Sem perda de generalidade, suponhamos que $a_n \neq 0$. Consideremos $D = k[x_1, \ldots, x_{n-1}]$. Podemos olhar $f(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n - b$ como um polinômio de $D[x_n]$ da seguinte maneira:

$$f(x_1, \ldots, x_n) = a_nx_n + c$$

onde $c = a_1x_1 + \cdots + a_{n-1}x_{n-1} - b$. Observe que visto dessa maneira, $f(x_1, \ldots, x_n)$ é um polinômio de grau 1 com coeficientes em D e primitivo. Assim, pela Proposição 1.4.4, $f(x_1, \ldots, x_n)$ é irredutível em $D[x_n] = k[x_1, \ldots, x_n]$. Portanto, o hiperplano H é hipersuperfície algébrica irredutível.

Exemplo 2.3.2. Consideremos a esfera S de k^2 definida pela equação implícita

$$x^2 + y^2 - 1 = 0.$$

De acordo com o Exemplo 1.4.7, o polinômio $f(x, y) = x^2 + y^2 - 1$ é irredutível. Sendo assim, a esfera S de k^2 é uma hipersuperfície algébrica irredutível.

As hipersuperfícies algébricas irredutíveis são uma espécie de "blocos fundamentais" para o conjunto de todas as hipersuperfícies algébricas. Essa afirmação é melhor compreendida através da seguinte proposição:

Proposição 2.3.3. *Toda hipersuperfície algébrica de* k^n *pode ser escrita como união finita de hipersuperfícies algébricas irredutíveis de* k^n.

Prova. Seja H uma hipersuperfície de k^n com equação implícita

$$f(x_1, \ldots, x_n) = 0.$$

Digamos que $f(x_1, \ldots, x_n) = p_1(x_1, \ldots, x_n) \cdots p_r(x_1, \ldots, x_n)$ é a fatoração em irredutíveis de $f(x_1, \ldots, x_n)$. Para cada $1 \leqslant i \leqslant r$, seja H_i a hipersuperfiície algébrica de k^n com equação implícita:

$$p_i(x_1, \ldots, x_n) = 0.$$

Afirmamos que

$$H = H_1 \cup \cdots \cup H_r.$$

Com efeito, considere $(a_1, \ldots, a_n) \in H$. Então,

$$p_1(a_1, \ldots, a_n) \cdots p_r(a_1, \ldots, a_n) = 0.$$

Recordemos que a conta nessa igualdade é realizada em um corpo k. Assim, como um corpo é um domínio segue que

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

para algum $1 \leqslant i \leqslant r$, ou seja, $(a_1, \ldots, a_n) \in H_i$ para algum $1 \leqslant i \leqslant r$. Logo,

$$H \subset H_1 \cup \cdots \cup H_r.$$

Agora suponhamos $(a_1, \ldots, a_n) \in H_1 \cup \cdots \cup H_r$. Então, existe $1 \leqslant i \leqslant r$ tal que $(a_1, \ldots, a_n) \in H_i$. Assim, $p_i(a_1, \ldots, a_n) = 0$. Logo,

$$f(a_1, \ldots, a_n) = p_1(a_1, \ldots, a_n) \cdots p_i(a_1, \ldots, a_n) \cdots p_r(a_1, \ldots, a_n) = 0.$$

Logo, $(a_1, \ldots, a_n) \in H$. Desse modo,

$$H_1 \cup \cdots \cup H_r \subset H$$

e com isso concluímos que

$$H = H_1 \cup \cdots \cup H_r.$$

□

Capítulo 3

Representação paramétrica racional de hipersuperfícies algébricas

Nesse capítulo introduzimos o conceito de representação paramétrica racional. Damos alguns exemplos de hipersuperfícies que são representadas parametricamente e de hipersuperfícies que não admitem tal representação. Também discutimos quais são as vantagens desse tipo de representação em comparação com a representação implícita.

3.1 Funções racionais

Sejam k um corpo e $p := p(t_1, \ldots, t_n)$, $q := q(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ com $q \neq 0$ dois polinômios em n variáveis com coeficientes em um corpo k. A fração $\frac{p}{q}$ é chamada de função racional de k^n. Duas funções racionais $\frac{p}{q}$ e $\frac{p'}{q'}$ de k^n são *iguais* se $pq' = p'q$.

Proposição 3.1.1. *Sejam* $p, q \in k[t_1, \ldots, t_n]$ *com* $q \neq 0$. *Então existem* $p', q' \in k[t_1, \ldots, t_n]$, *com* $q' \neq 0$, *tais que o máximo divisor de* p', q' *é igual a* 1 *e tais que* $\frac{p}{q} = \frac{p'}{q'}$.

Prova. Sejam $p = p_1^{a_1} \cdots p_n^{a_n}$ e $q = p_1^{b_1} \cdots p_n^{b_n}$ as fatorações em irredutíveis de p e q. Definamos $c_i = \min\{a_i, b_i\}$. Fazendo $p' = p_1^{a_1 - c_1} \cdots p_n^{a_n - c_n}$ e $q' = p_1^{b_1 - c_1} \cdots p_n^{b_n - c_n}$ segue a afirmação desejada. □

Segue da proposição acima que sempre podemos supor a representação $\frac{p}{q}$ de uma função racional em sua *forma reduzida*, ou seja, com o máximo divisor comum de p e q igual a 1.

Definição 3.1.2. Dizemos que a função racional $\frac{f}{g}$, escrita em sua forma reduzida, está definida em um ponto $(\alpha_1, \ldots, \alpha_n)$ de k^n se $g(\alpha_1, \ldots, \alpha_n) \neq 0$.

Exemplo 3.1.3. $f(t) = \dfrac{2t}{t^2+1}$ é uma função racional de $\mathbb{R}$. Como $t^2 + 1 \neq 0$ para cada $t \in \mathbb{R}$, então $f(t)$ está definida em todo $\mathbb{R}$.

Exemplo 3.1.4. $f(t_1, t_2) = \dfrac{1}{t_1^2 + t_2^2}$ é uma função racional de $\mathbb{R}^2$. Esta função não está definida em (0,0).

3.2 Parametrizações racionais

Uma parametrização racional de uma hipersuperfície algébrica H de k^n é determinada por uma coleção de funções racionais $f_1(t_1, \ldots, t_{n-1}), \ldots, f_n(t_1, \ldots, t_{n-1})$ tal que todo ponto com coordenadas

$$\begin{cases} x_1 &= f_1(t_1, \ldots, t_{n-1}) \\ \vdots & \vdots \\ x_n &= f_n(t_1, \ldots, t_{n-1}) \end{cases} \tag{3.1}$$

pertence a H e "quase todo ponto"de H é dessa forma.

A formulação matemática precisa para a expressão "quase todo ponto" é realizada por meio da topologia de Zariski. Todavia, como esse é apenas um trabalho introdutório, não nos aprofundaremos nesse aspecto. Apenas ressaltamos que:

(I) No caso específico em que a hipersuperfície é uma curva algébrica plana a expressão "quase todo ponto" é equivalente a dizer que, exceto uma quantidade finita de pontos, todos os demais tem a representação citada.

(II) No caso de hipersuperfícies algébricas arbitrárias, um caso particular para a expressão "quase todo ponto" é dizer que, exceto uma quantidade finita de pontos, todos os demais tem a representação citada.

Exemplo 3.2.1. Seja H um hiperplano de k^n com equação implícita

$$a_1x_1 + \cdots + a_nx_n - b = 0,$$

onde ao menos um dos coeficientes $a_1, \ldots, a_n$ é não nulo. Sem perda de generalidade, podemos supor que $a_1 \neq 0$. Assim, podemos escrever

$$x_1 = b/a_1 + (-a_2/a_1)x_2 + \cdots + (-a_n/a_1)x_n.$$

Com isso, uma representação paramétrica racional para H é:

$$\begin{cases} x_1 &= b/a_1 + (-a_2/a_1)t_1 + \cdots + (-a_n/a_1)t_{n-1} \\ x_2 &= t_1 \\ &\vdots \\ x_n &= t_{n-1} \end{cases} \tag{3.2}$$

Exemplo 3.2.2. Seja $\mathbf{v} = (v_1, \ldots, v_n)$ um vetor de k^n e $p = (a_1, \ldots, a_n)$ um ponto de k^n. A *reta* de k^n que passa pelo ponto p e tem $\mathbf{v}$ como vetor diretor é o conjunto dos pontos $(x_1, \ldots, x_n)$ de k^n da forma

$$\begin{cases} x_1 &= a_1 &+ v_1 t \\ x_2 &= a_2 &+ v_2 t \\ &\vdots \\ x_n &= a_n &+ v_n t \end{cases}$$

com $t \in k$.

Exemplo 3.2.3. Consideremos a esfera $(n-1)$-dimensional S com equação implícita

$$x_1^2 + \cdots + x_n^2 - 1 = 0.$$

Dada uma n-upla $(t_1, \ldots, t_{n-1}, 0) \in \mathbb{R}^n$, consideremos a reta r que passa pelo ponto $(0, \ldots, 0, 1) \in \mathbb{R}^n$ e tem $\mathbf{v} = (t_1, \ldots, t_{n-1}, -1)$ como vetor diretor. Pelo que vimos anteriormente, as coordenadas dos pontos da reta r são descritos pelas seguintes equações.

$$\begin{cases} x_1 &= &t_1 t \\ x_2 &= &t_2 t \\ &\vdots \\ x_{n-1} &= &t_{n-1} t \\ x_n &= 1 - &t \end{cases}$$

Queremos inicialmente encontrar os pontos de interseção entre a reta r e a esfera S. Para isso, basta encontrar os valores de t que satisfazem a equação:

$$(t_1 t)^2 + \cdots + (t_{n-1} t)^2 + (1-t)^2 - 1 = 0.$$

Fazendo as contas observamos que

$$t = 0 \quad \text{ou} \quad t = \frac{2}{1 + t_1^2 + \cdots + t_{n-1}^2}.$$

Assim, os pontos de interseção entre a reta r e a circunferência S são

$$(0, \ldots, 0, 1) \quad \text{e} \quad \left(\frac{2t_1}{1 + t_1^2 + \cdots + t_{n-1}^2}, \ldots, \frac{2t_{n-1}}{1 + t_1^2 + \cdots + t_{n-1}^2}, \frac{t_1^2 + \cdots + t_{n-1}^2 - 1}{1 + t_1^2 + \cdots + t_{n-1}^2} \right).$$

Com isso chegamos a conclusão que pontos $(x_1, \ldots, x_n) \in \mathbb{R}^n$ tais que

$$\begin{cases} x_1 &= \dfrac{2t_1}{1 + t_1^2 + \cdots + t_{n-1}^2} \\ &\vdots \\ x_{n-1} &= \dfrac{2t_{n-1}}{1 + t_1^2 + \cdots + t_{n-1}^2} \\ x_n &= \dfrac{t_1^2 + \cdots + t_{n-1}^2 - 1}{1 + t_1^2 + \cdots + t_{n-1}^2} \end{cases} \tag{3.3}$$

pertencem a S. Em particular, para mostrar que as equações em (3.3) definem uma parametrização racional de S é suficiente verificar que todo ponto de S, com exceção de p, tem coordenadas representadas pelas equações em (3.3). Para isso, consideremos $(\bar{x}_1, \ldots, \bar{x}_n)$ um ponto de S diferente de $(0, 0, \ldots, 0, 1)$. Consideremos a reta r que passa pelo ponto $(0, \ldots, 0, 1) \in \mathbb{R}^n$ e tem $\mathbf{v} = (\bar{x}_1, \ldots, \bar{x}_{n-1}, \bar{x}_n - 1)$ como vetor diretor. Por definição, as coordenadas dos pontos dessa reta são dados por

$$\begin{cases} x_1 &= \bar{x}_1 t \\ x_2 &= \bar{x}_2 t \\ &\vdots \\ x_{n-1} &= \bar{x}_{n-1} t \\ x_n &= 1 - (\bar{x}_n - 1)t \end{cases} \tag{3.4}$$

A interseção da reta r com o hiperplano $x_n = 0$ é justamente o ponto em que t satisfaz a equação

$$1 - (\bar{x}_n - 1)t = 0,$$

ou seja,

$$t = \frac{1}{\bar{x}_n - 1}.$$

(lembre que $\bar{x}_n - 1 \neq 0$ pois $(\bar{x}_1, \ldots, \bar{x}_n)$ é diferente do ponto $(0, \ldots, 0, 1)$). Portanto, a interseção

da reta r com o hiperplano $x_n = 0$ é o ponto com coordenadas $(t_1, \ldots, t_{n-1}, 0)$ onde

$$\begin{cases} t_1 &= \dfrac{\bar{x}_1}{\bar{x}_n - 1} \\ &\vdots \\ t_{n-1} &= \dfrac{\bar{x}_{n-1}}{\bar{x}_n - 1} \end{cases} \tag{3.5}$$

Para esses valores de $t_1, \ldots, t_{n-1}$ temos

$$\begin{cases} \bar{x}_1 &= \dfrac{2t_1}{1 + t_1^2 + \cdots + t_{n-1}^2} \\ &\vdots \\ \bar{x}_{n-1} &= \dfrac{2t_{n-1}}{1 + t_1^2 + \cdots + t_{n-1}^2} \\ \bar{x}_n &= \dfrac{t_1^2 + \cdots + t_{n-1}^2 - 1}{1 + t_1^2 + \cdots + t_{n-1}^2} \end{cases} \tag{3.6}$$

Observação 3.2.4. Seja S a esfera de $\mathbb{R}^n$ com equação implícita

$$x_1^2 + \cdots + x_n^2 - 1 = 0.$$

No exemplo acima construimos uma correspondência que associa cada ponto de $(x_1, \ldots, x_n) \in S \setminus \{(0, \ldots, 1)\}$ a um único ponto $\left(\dfrac{\bar{x}_1}{\bar{x}_n - 1}, \ldots, \dfrac{\bar{x}_{n-1}}{\bar{x}_n - 1}, 0\right)$ pertencente ao hiperplano $x_n = 0$. Essa correspondência é muito importante e aparece em diversos contextos da matemática. Ela é usualmente denominada de *projeção estereográfica da esfera*.

Observação 3.2.5. No caso da esfera 1-dimensional os elementos geométricos que aparecem na dedução da parametrização da esfera são ilustrados através da seguinte figura:

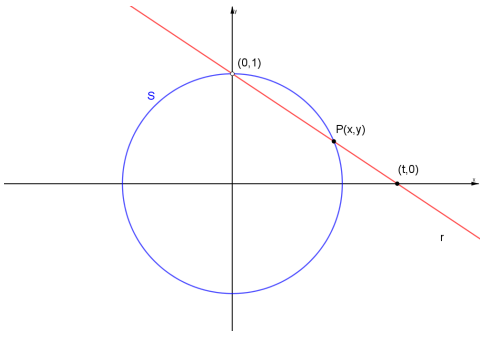

Figura 3.1

Observe que a medida que o ponto $(t, 0)$ se desloca para a direita o ponto P tende a se aproximar do ponto $(0, 1)$ e a reta r em vermelho tende a reta tangente à circunferência no ponto $(0, 1)$.

Observação 3.2.6. Uma particularidade da representação paramétrica racional da esfera $(n-1)$-dimensional obtida em (3.3) é que os coeficientes das funções polinomiais envolvidas são números inteiros. Isso permite encontrar uma infinidade de pontos da esfera $(n-1)$-dimensional cujas coordenadas são números racionais. Além disso, também é possível através dela encontrar soluções inteiras para a equação

$$x_1^2 + \cdots + x_n^2 = z^2. \tag{3.7}$$

De fato, para cada $(n-1)$-upla $(t_1, \ldots, t_{n-1})$ de números inteiros temos por (3.3) que a $(n+1)$ -upla $(x_1, \ldots, x_n, z)$ dada por

$$\begin{cases} x_1 &= 2t_1 \\ &\vdots \\ x_{n-1} &= 2t_{n-1} \\ x_n &= t_1^2 + \cdots + t_{n-1}^2 - 1 \\ z &= 1 + t_1^2 + \cdots + t_{n-1}^2 \end{cases} \tag{3.8}$$

é uma solução inteira para (3.7). Assim, como podemos perceber com esse exemplo, parametrizações racionais desse tipo onde os coeficientes dos polinômios envolvidos são números inteiros são bastante apropriadas para tratar problemas de teoria dos números.

Observação 3.2.7. Observe que no caso particular da esfera 1-dimensional a representação paramétricas obtida no Exemplo 3.2.3 tem o seguinte formato:

$$\begin{cases} x &= \dfrac{2t}{t^2+1} \\ y &= \dfrac{t^2-1}{t^2+1} \end{cases}$$

Todavia, sabemos que uma outra representação paramétrica para a esfera 1-dimensional é

$$\begin{cases} x &= \cos t \\ y &= \operatorname{sen} t \end{cases}$$

Obviamente, este segundo tipo de representação paramétrica não é racional. Comparando esses dois tipos de representações paramétricas vemos que o primeira é mais interessante do ponto de vista de cálculos, uma vez que as expressões que as definem envolvem apenas uma quantidade finita de operações aritméticas elementares.

3.3 Sobre a existência da representação paramétrica racional

Segue da própria definição de hipersuperfície algébrica a existência da representação implícita. O que não é óbvio é se uma hipersuperfície algébrica admite ou não uma representação paramétrica. De fato, nem sempre uma tal representação é possível. Para ilustrar esse fenômeno, apresentamos o seguinte exemplo.

Exemplo 3.3.1. Seja H a curva algébrica plana com equação implícita

$$x^m + y^m - 1 = 0,$$

com m sendo um inteiro $\geqslant 3$. Afirmamos que H não admite uma parametrização racional. Para provar essa afirmação, argumentaremos por redução ao absurdo. Assim, suponhamos que H admite uma representação paramétrica racional

$$\begin{cases} x = \dfrac{f(t)}{g(t)} \\ \\ y = \dfrac{p(t)}{q(t)} \end{cases}$$

Escrevendo

$$\frac{f(t)}{g(t)} = \frac{f(t)q(t)}{q(t)g(t)} \quad \text{e} \quad \frac{p(t)}{q(t)} = \frac{p(t)g(t)}{q(t)g(t)},$$

podemos supor a parametrização da seguinte forma:

$$\begin{cases} x = \dfrac{h_1(t)}{r(t)} \\ \\ y = \dfrac{h_2(t)}{r(t)} \end{cases} \tag{3.9}$$

onde $h_1(t), h_2(t), r(t)$ não possuem fator irredutível comum aos três. Temos:

$$\left(\frac{h_1(t)}{r(t)}\right)^m + \left(\frac{h_2(t)}{r(t)}\right)^m = 1. \tag{3.10}$$

Derivando os dois lados dessa igualdade com respeito a t vem:

$$\left(\frac{h_1(t)}{r(t)}\right)^{m-1} \left(\frac{h_1(t)}{r(t)}\right)' + \left(\frac{h_2(t)}{r(t)}\right)^{m-1} \left(\frac{h_2(t)}{r(t)}\right)' = 0. \tag{3.11}$$

Consideremos agora o seguinte sistema linear:

$$\begin{cases} \left(\dfrac{h_1(t)}{r(t)}\right)u + \left(\dfrac{h_2(t)}{r(t)}\right)v &= 1 \\ \left(\dfrac{h_1(t)}{r(t)}\right)'u + \left(\dfrac{h_2(t)}{r(t)}\right)'v &= 0 \end{cases} \tag{3.12}$$

Afirmação: $\delta(t) := \left(\dfrac{h_1(t)}{r(t)}\right)\left(\dfrac{h_2(t)}{r(t)}\right)' - \left(\dfrac{h_2(t)}{r(t)}\right)\left(\dfrac{h_1(t)}{r(t)}\right)' \neq 0.$

Para provarmos essa afirmação iniciamos observando que as funções racionais $\dfrac{h_1(t)}{r(t)}$ e $\dfrac{h_2(t)}{r(t)}$ não são ambas constantes, pois, do contrário, apenas um ponto de H seria representado pela parametrização racional (3.9), o que contradiz a definição de parametrização racional. Assim, podemos supor por exemplo que $\dfrac{h_2(t)}{r(t)}$ não é constante. De (3.10), temos

$$\left(\frac{h_1(t)/r(t)}{h_2(t)/r(t)}\right)^m + 1 = \frac{1}{(h_2(t)/r(t))^m}.$$

Como o lado direito dessa igualdade não é constante, segue que $\dfrac{h_1(t)/r(t)}{h_2(t)/r(t)}$ não é constante. Em particular,

$$\left(\frac{h_1(t)/r(t)}{h_2(t)/r(t)}\right)' \neq 0,$$

ou seja,

$$\frac{(h_1(t)/r(t))\,(h_2(t)/r(t))' - (h_2(t)/r(t))\,(h_1(t)/r(t))'}{(h_2(t)/r(t))^2} \neq 0.$$

Logo, $\delta(t) \neq 0$ e a afirmação segue.

Dessa afirmação segue que o sistema (3.12) tem uma única solução que é dada por

$$u = \frac{(h_2(t)/r(t))'}{\delta(t)} \qquad \text{e} \qquad v = -\frac{(h_1(t)/r(t))'}{\delta(t)}$$

Mas, por (3.10) e (3.11),

$$u = (h_1(t)/r(t))^{m-1} \qquad \text{e} \qquad v = (h_2(t)/r(t))^{m-1}$$

também é solução de (3.12). Assim,

$$(h_1(t)/r(t))^{m-1} = \frac{(h_2(t)/r(t))'}{\delta(t)} \qquad \text{e} \qquad (h_2(t)/r(t))^{m-1} = -\frac{(h_1(t)/r(t))'}{\delta(t)},$$

ou seja,

$$(h_2(t)/r(t))' = \delta(t)(h_1(t)/r(t))^{m-1} \qquad \text{e} \qquad (h_1(t)/r(t))' = -\delta(t)(h_2(t)/r(t))^{m-1}.$$

Desenvolvendo os cálculos nessas duas igualdades obtemos

$$(h_2'(t)r(t) - h_2(t)r'(t))r(t)^{m-1} = (h_1(t)h_2'(t) - h_2(t)h_1'(t))h_1(t)^{m-1}$$

e

$$(h_1'(t)r(t) - h_1(t)r'(t))r(t)^{m-1} = -(h_1(t)h_2'(t) - h_2(t)h_1'(t))h_2(t)^{m-1}.$$

Dessas igualdades e do fato que $h_1(t), h_2(t), r(t)$ não possuem fator irredutível comum aos três segue que $r(t)^{m-1}$ divide $h_1(t)h_2'(t) - h_2(t)h_1'(t)$. Fazendo a divisão obtemos que $h_1(t)^{m-1}$ divide $h_2'(t)r(t) - h_2(t)r'(t)$ e que $h_2(t)^{m-1}$ divide $h_1'(t)r(t) - h_1(t)r'(t)$. Usando esses fatos e comparando graus segue que

$$(m-1)\text{grau}(h_1(t)) \leqslant \text{grau}(h_2(t)) + \text{grau}(r(t)) - 1,$$

$$(m-1)\text{grau}(h_2(t)) \leqslant \text{grau}(h_1(t)) + \text{grau}(r(t)) - 1$$

e

$$(m-1)\text{grau}(r(t)) \leqslant \text{grau}(h_1(t)) + \text{grau}(h_2(t)) - 1.$$

Somando essas três desigualdades membro a membro vem

$$(m-1)[\text{grau}(h_1(t)) + \text{grau}(h_2(t)) + \text{grau}(r(t))] \leqslant 2[\text{grau}(h_1(t)) + \text{grau}(h_2(t)) + \text{grau}(r(t))] - 3,$$

ou seja,

$$(m-3)[\text{grau}(h_1(t)) + \text{grau}(h_2(t)) + \text{grau}(r(t))] \leqslant -3.$$

Mas isso é um absurdo, pois, como $m \geqslant 3$, $(m-3)[\text{grau}(h_1(t)) + \text{grau}(h_2(t)) + \text{grau}(r(t))] \geqslant 0$.

3.4 Representação implícita versus representação paramétrica

Como vimos acima uma desvantagem da representação paramétrica racional é que nem toda hipersuperfície algébrica admite uma tal representação. Outro inconveniente é que em várias situações essas representações deixam de fora alguns pontos da hipersuperfície. Dito isso, o leitor pode então estar se perguntando sobre qual é a utilidade de introduzí-las. Em partes, a motivação para

investigar representações paramétricas é dada por questões da seguinte natureza

Questão 3.4.1. *Dada uma hipersuperfície algébrica* H *como produzir muitos pontos de* H? *Por exemplo, como podemos instruir um computador a desenhar uma curva algébrica plana?*

Por exemplo, considere a hipersuperfície algébrica H de $\mathbb{R}^3$ definida pela equação algébrica

$$-4x^3z + 3x^2y^2 - 4y^3 + 6xyz - z^2 = 0$$

Como produzir pontos pertencentes a H? Observe que, de posse apenas dessa representação um maneira de produzir pontos em H seria a seguinte: para cada para $(x_0, y_0) \in \mathbb{R}^2$ fixado, consideramos a equação na variável z

$$-z^2 + (-4x_0^3 + 6x_0y_0)z + 3x_0^2y_0^2 - 4y_0^3 = 0. \tag{3.13}$$

Para cada solução z_0 de (3.13) temos que a terna (x_0, y_0, z_0) é um ponto de H. Observe que essa forma de obter pontos de H tem como dificuldade o fato de necessitar resolver uma equação como (3.13) (de fato, essa dificuldade poderia ser mais drástica caso o grau da equação (3.13) fosse maior). Por outro lado, se considerássemos a representação paramétrica de H dada por

$$\begin{cases} x &= t_1 + t_2 \\ y &= t_1^2 + 2t_1t_2 \\ z &= t_1^3 + 3t_1^2t_2 \end{cases} \tag{3.14}$$

produzir pontos de H seria bastante simples, bastaria atribuirmos valores aos parâmetros t_1 e t_2 e efetuar operações aritméticas elementares de soma e multiplicação.

Vemos com essas discussões que a melhor forma de tratar problemas como na Questão 3.4.1 é através da representação paramétrica.

Por outro lado, de forma geral, a representação implícita é útil para decidir se pontos pertencem a hipersuperfície. Por exemplo, considere o ponto $(1, 0, 1)$. Para decidir se esse ponto pertence a hipersuperfície com equação ímplicita

$$-4x^3z + 3x^2y^2 - 4y^3 + 6xyz - z^2 = 0$$

basta fazer uma substituição. Em contrapartida, para resolver essa mesma questão usando a parametrização (3.14) necessitaríamos resolver o sistema:

$$\begin{cases} t_1 + t_2 &= 1 \\ t_1^2 + 2t_1t_2 &= 0 \\ t_1^3 + 3t_1^2t_2 &= 1 \end{cases} \tag{3.15}$$

3.5 Implicitação

Um problema que desperta muito interesse dos especialistas é:

Problema 3.5.1. *Dada uma coleção de funções racionais*

$$\begin{cases} x_1 &= f_1(t_1,\ldots,t_{n-1}) \\ \vdots & \vdots \\ x_n &= f_n(t_1,\ldots,t_{n-1}) \end{cases} \tag{3.16}$$

existe alguma hipersuperfície algébrica H *da qual essa coleção de funções racionais definam uma parametrização? Em caso afirmativo, como determinar a representação implícita de* H?

Este tipo de problema é chamado de *implicitação*. Existe muita teoria em geometria algébrica e álgebra comutativa dedicada a fornecer métodos para tratar esse tipo de problema. Algumas das ferramentas utilizadas para tratar esse tipo de problema são resultados como o Teorema 1.3.10, ou suas generalizações, realizadas através das chamadas *bases de Grobner* (ver por exemplo [1] para maiores detalhes sobre as bases de Grobner).

Para ilustrar como resultados tais como o Teorema 1.3.10 pode ser utilizado para tratar o problema de implicitação, consideremos

$$\begin{cases} x &= t^2 \\ y &= t^3 \end{cases} \tag{3.17}$$

Suponhamos a *priori* que de fato estas funções definem uma parametrização racional de uma hipersuperfície H. Digamos que a representação implícita de H é

$$f(x,y) = 0.$$

Desejamos explicitar $f(x,y)$. Considere o polinômio $g(x,y) = y^2 - x^3$. Denotemos por H' a curva algébrica plana com equação implícita $g(x,y) = 0$. Observe que

$$g(t^2,t^3) = 0,$$

para todo t. Temos com isso que, a menos de uma quantidade finita de pontos,

$$H \subset H'. \tag{3.18}$$

Agora, olhando $k[x,y] = A[y]$ com $A = k[x]$ e usando o Teorema 1.3.10 temos

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

onde $q, r \in k[x,y] = A[y]$ e $r = 0$ ou grau $r \leqslant 1$ (observe que o grau de r aqui é pensado no anel $A[y]$). Em particular, existem $a(x), b(x) \in A$ tais que

$$r = a(x)y + b(x).$$

Logo,

$$f(x,y) = (y^2 - x^3)q + a(x)y + b(x).$$

Dessa forma,

$$0 = f(t^2, t^3) = a(t^2)t^3 + b(t^2),$$

ou seja,

$$a(t^2)t^3 = -b(t^2).$$

Note que $a(x) = 0$ pois caso contrário do lado direito dessa última igualdade teríamos um polinômio de grau ímpar e do lado esquerdo um polinômio de grau par, o que é um absurdo. Assim, $b(t^2) = 0$ o que implica $b = 0$. Dessa forma, $r = 0$, ou seja,

$$f(x,y) = (y^2 - x^3)q.$$

Com essa igualdade concluímos que

$$H' \subset H. \tag{3.19}$$

De (3.18) e (3.19) segue que H e H' são iguais a menos de um conjunto finito de pontos. Todavia, é possível mostrar que duas hipersuperfícies que coincidem a menos de uma quantidade finita de pontos são iguais (ver [1, Capítulo 1]). Sendo assim, $H = H'$. Portanto, a equação implícita de H é

$$y^2 - x^3 = 0.$$

Bibliografia

[1] COX, D.; LITTLE, J.; O'SHEA, D. Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, New York: Springer-Verlag, 1992.

[2] CLARK, A.; Elements of Abstract Algebra. New York: Dover, 1971.

[3] DOMINGUES, H.; IEZZI, G.; Álgebra Moderna. São Paulo: Atual, 1982. 3a edição. 263p.

[4] GARCIA, A.; LEQUAIN, Y.; Elementos de Álgebra. Rio de Janeiro: Associação IMPA, 2003.326 p.

[5] GONÇALVES, A. Introdução à Álgebra. IMPA, Rio de Janeiro, 2012.

[6] LIMA, E. L.; Análise Real Vol. 2. Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2004.

[7] VAISENCHER, I.; Introdução às curvas algébricas planas. Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2017.

[8] STEWART, J.; Cálculo. 8. ed. São Paulo: Cengage Learning, 2017. v. 2. 672p.