Solução de sistemas algébricos e aplicações em teoria de singularidades

Alain Jacquemard (Université de Bourgogne)

Ricardo Miranda Martins (Unicamp)

Neste artigo consideramos o problema de resolver sistemas de equações algébricas. Introduzimos uma ferramenta muito útil para este propósito, que é o cálculo das bases de Gröbner de um ideal de polinômios. Além disto, apresentamos a noção de escalier de um ideal e mostramos que tal objeto geométrico guarda muitas das propriedades do ideal. Veremos que tais informações podem ser utilizadas para calcular invariantes associados a singularidade de aplicações polinomiais.

Antes de iniciar propriamente o texto, convidamos o leitor a resolver o sistema abaixo, para $x, y, z \in \mathbb{R}$.

$$\begin{cases} -69xy - 81z^2 - 42xz - 48x^2 = 0 \\ -75x^3 + 78x^2y + 25y^2z + 30y^3 = 0 \\ 35x^4 - 64y^3z - 75x^2y^2 - 80z^4 + 91x^2z^2 = 0 \end{cases} \quad (1)$$

Como o sistema (1) é composto de polinômios homogêneos, é fácil deduzir que $x = 0, y = 0, z = 0$ é uma de suas soluções. Seria esta a única solução de (1)? Esta solução é isolada, ou existem outras soluções para (1) arbitrariamente próximas de $(0,0,0)$? O que acontece se ao invés de $x, y, z \in \mathbb{R}$, considerarmos $x, y, z \in \mathbb{F}$, em que $\mathbb{F}$ é $\mathbb{C}$ ou um corpo finito?

Se o sistema (1) fosse linear, todas estas perguntas seriam de fácil resposta. No fim da seção 3, responderemos a estas perguntas para nosso caso.

1 Introdução

Vamos denotar por $\mathbb{K}$ um dos corpos $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Z}_p$, p primo.

Sejam $p_1, \ldots, p_k$ polinômios nas variáveis $x_1, \ldots, x_n$ e coeficientes em $\mathbb{K}$ e considere o sistema

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ p_k(x_1, \ldots, x_n) = 0 \end{cases} \quad (2)$$

Dizemos que (2) é um *sistema de equações algébricas*, e denotamos por $\langle p_1, \ldots, p_k \rangle$ o ideal de $\mathbb{K}[x_1, \ldots, x_n]$ gerado por $p_1, \ldots, p_k$.

Dizemos que outro sistema

$$\begin{cases} q_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ q_l(x_1, \ldots, x_n) = 0 \end{cases}$$

$q_1, \ldots, q_l \in \mathbb{K}[x_1, \ldots, x_n]$, é *equivalente* a (2) se $\langle p_1, \ldots, p_k \rangle = \langle q_1, \ldots, q_l \rangle$.

Denote por

$$\mathcal{Z}(p_1, \ldots, p_k) = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n;\ p_j(x) = 0,\ j = 1, \ldots, k\}$$

o conjunto dos zeros de (2).

Note que se I é o ideal gerado por $p_1, \ldots, p_k$ e $q \in I$ então $q(x) = 0$ para todo $x \in \mathcal{Z}(p_1, \ldots, p_k)$. Assim, podemos definir $\mathcal{Z}(I) = \mathcal{Z}(p_1, \ldots, p_k)$ quando $I = \langle p_1, \ldots, p_k \rangle$. Note que dois sistemas equivalentes têm o mesmo conjunto de zeros. Se I é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$, definimos $Rad(I)$ como o conjunto dos polinômios $f \in \mathbb{K}[x_1, \ldots, x_n]$ para os quais existe $r \geq 1$ de modo que $f^r \in I$.

Dado um conjunto $A \subset \mathbb{K}^n$, denotamos por $\mathcal{I}(A)$ o ideal de $\mathbb{K}[x_1, \ldots, x_n]$ formado pelos polinômios que se anulam em A.

O problema básico que consideramos neste texto é:

Problema A. Dado um sistema de equações algébricas como (2), obter métodos eficientes para construir sistemas equivalentes a ele, de modo que, a partir de um novo sistema, seja fácil obter informações relativas ao conjunto de soluções $\mathcal{Z}(I)$ (existência, dimensão,...), assim como sobre a estrutura de I.

No caso de sistemas lineares, o método da eliminação de Gauss é uma ferramenta eficiente para calcular o posto do sistema, assim como para resolvê-lo. Desenvolveremos uma espécie de análogo ao método de Gauss no caso não linear.

Ora, se $I = \langle p_1, \ldots, p_k \rangle$, então $\mathcal{Z}(I) = \mathcal{Z}(p_1, \ldots, p_k)$. Portanto, para descrever $\mathcal{Z}(I)$ uma boa estratégia é encontrar um "bom" conjunto gerador para I e resolver o sistema determinado por esses geradores.

Devemos então determinar o que é um "bom" conjunto gerador para I.

Primeira definição de "bom conjunto gerador": um conjunto gerador com o menor número possível de geradores.

Não é difícil ver que esta definição não é muito boa, já que mesmo sistemas com poucos geradores ainda são muito difíceis de serem resolvidos.

Exemplo 1. *Sejam* $p_1(x,y,z) = x^2y + x^3z + y^2z$ *e* $p_2(x,y,z) = xy^2 + xz^2 + yz$. *Resolver o sistema*

$$\begin{cases} p_1(x,y,z) = 0, \\ p_2(x,y,z) = 0, \end{cases}$$

ainda é difícil, mesmo com somente dois polinômios (o conjunto-solução é união de variedades de dimensões diferentes).

Segunda definição de "bom conjunto gerador": um conjunto gerador que, mesmo sendo muito grande, nos dê mais informações sobre a estrutura do ideal.

Neste caso, buscamos uma base para o ideal I que, por exemplo, nos permita decidir se um dado polinômio f pertence ou não a I.

Neste ponto o leitor pode estar pensando "*Ora, isto é fácil: divida f pelos geradores e pronto. Se o resto for zero, então $f \in I$; caso contrário, $f \notin I$.*"

Esta estratégia é baseada em unicidade de restos, e tal coisa só vale em geral para polinômios em uma variável. Relembrando, seja $I = \langle p_1(x), \ldots, p_k(x) \rangle$ um ideal em $\mathbb{K}[x]$. O anel $\mathbb{K}[x]$ é um anel principal (e isto só vale para polinômios em uma variável!), ou seja, todo ideal pode ser gerado por somente um elemento: no caso, $p(x) = \text{mdc}(p_1(x), \ldots, p_k(x))$. Dado um polinômio $f(x) \in \mathbb{K}[x]$, dividimos $f(x)$ por $p(x)$ obtendo únicos $q(x), r(x) \in \mathbb{K}[x]$ de modo que $f(x) = q(x)p(x) + r(x)$, onde $grau(r(x)) < grau(p(x))$ ou $r(x) \equiv 0$. Temos que $f(x) \in I$ se, e só se, $r(x) \equiv 0$.

Vejamos o que acontece com polinômios em duas variáveis.

Exemplo 2. *Sejam* $p_1(x,y) = xy + 1$, $p_2(x,y) = y^2 - 1$ *e* $f(x,y) = xy^2 - x$. *Defina* $I = \langle p_1, p_2 \rangle$. *Queremos saber se* $f \in I$ *e tentaremos usar a estratégia do parágrafo anterior para isto. Note que* $f(x,y) = yp_1(x,y) + 0 \cdot p_2(x,y) + (y - x)$, *ou seja, o resto da divisão de* f *por* p_1, p_2 *não deu zero, o que aparentemente sugere que* $f \notin I$. *Veja o próximo exemplo.*

Exemplo 3. *Sejam* $p_1(x,y) = xy + 1$, $p_2(x,y) = y^2 - 1$ *e* $f(x,y) = xy^2 - x$. *Defina* $I = \langle p_1, p_2 \rangle$. *Queremos saber se* $f \in I$ *e tentaremos usar a estratégia do parágrafo anterior para isto. Note que* $f(x,y) = 0 \cdot p_1(x,y) + x \cdot p_2(x,y) + 0$, *ou seja, o resto da divisão de* f *por* p_1, p_2 *é zero, logo* $f \in I$.

O Exemplo 2 sugere que $f \notin I$, mas o Exemplo 3 nos diz que $f \in I$. O que está errado? Nada. O fato é que para saber se $f \in I$, não se pode escolher um conjunto arbitrário de geradores para I e efetuar a divisão. Na próxima seção veremos como escolher um bom conjunto de geradores que permite tal abordagem. Uma descrição muito boa e detalhada do método pode ser encontrada em [1].

O restante deste artigo está organizado da seguinte forma. Na seção 2 apresentamos alguns resultados clássicos sobre sistemas de equações polinomiais. Na seção 3 apresentamos os conceitos de ordem monomial e base de Gröbner. Na seção 4, apresentamos o *escalier* de um ideal, e na seção 5 discutimos algumas aplicações.

2 Teoremas de Hilbert

Nesta seção apresentaremos dois teoremas clássicos sobre sistemas de equações algébricas sobre corpos algebricamente fechados, o Teorema da Base e o Teorema dos Zeros, ambos devidos a David Hilbert. Vamos fixar $\mathbb{K} = \mathbb{C}$, mas os resultados a seguir valem para qualquer corpo algebricamente fechado.

Enquanto o Teorema da Base de Hilbert nos dirá que todo ideal em $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado, o Teorema dos Zeros de Hilbert irá assegurar que sistemas de equações algébricas em $\mathbb{K}$ sempre têm solução.

Teorema 1 (Versão "fraca" do Teorema dos Zeros de Hilbert)**.** *Se I é um ideal próprio de $\mathbb{K}[x_1, \ldots, x_n]$ então $\mathcal{Z}(\mathcal{I}) \neq \varnothing$.*

O Teorema 1 nos diz que sistemas como (2) sempre têm solução sobre $\mathbb{C}$, desde que o ideal gerado pelos polinômios $p_1, \ldots, p_k$ seja próprio. A versão "forte" do Teorema 1 é

Teorema 2 (Teorema dos Zeros de Hilbert)**.** *Seja I um ideal de $\mathbb{K}[x_1, \ldots, x_n]$ e $p \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $p(x) = 0$ para todo $x \in \mathcal{Z}(\mathcal{I})$. Então existe um número natural r tal que $p^r \in I$.*

Usando as notações introduzidas na seção 1, podemos enunciar o Teorema 2 como $\mathcal{I}(\mathcal{Z}(I)) = Rad(I)$.

A hipótese do corpo ser algebricamente fechado é realmente necessária nos teoremas acima. Considere, por exemplo, o polinômio $x^2 + 1$ em $\mathbb{R}[x]$. Claramente, $I = \langle x^2 + 1 \rangle$ é um ideal próprio de $\mathbb{R}[x]$, mas $\mathcal{Z}(I) = \varnothing$.

A prova dos Teoremas 2 e 1 pode ser encontrada em [2] e faz uso do Teorema da Base de Hilbert. Outra demonstração muito criativa pode ser encontrada em [7].

Lembramos que um anel A é dito *noetheriano* se toda cadeia de ideais tem um elemento maximal, isto é, dada uma cadeia $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$, existe um inteiro positivo s de modo que $I_s = I_{s+1} = \ldots$. No caso especial dos anéis comutativos com unidade, A é noetheriano se, e só se, todo ideal de A é finitamente gerado.

Teorema 3 (Teorema da base de Hilbert I)**.** *Se A é um anel noetheriano, então $A[x]$ também é noetheriano.*

Em nosso contexto, o teorema acima pode ser enunciado como

Teorema 4 (Teorema da base de Hilbert II)**.** *Todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado.*

Uma prova do Teorema 3 pode ser vista em [2]. A prova original, um resultado de existência nada construtivo, foi rejeitada inicialmente por Paul Gordan, por ser muito abstrata. Ao rejeitar o artigo, Gordan disse: "Isto não é matemática. Isto é teologia." Algum tempo depois, Hilbert melhorou sua demonstração, tornando-a um pouco mais acessível. Desta vez, o comentário de Gordan foi: "Eu estou convencido de que mesmo teologia tem seus méritos." Estes fatos, folcóricos ou não, estão descritos em [9].

A teoria que descrevemos abaixo dá um método computacional para encontrar um conjunto de geradores "especiais" de um ideal, chamado de base de Gröbner. Esse conjunto pode ser encontrado *via* computador, por exemplo, e o mesmo computador pode decidir se um outro elemento está ou não no ideal. Ou seja, existem conjuntos geradores especiais que nem sempre são minimais e que são mais úteis sob o ponto de vista computacional. Esses conjuntos são sempre finitos no caso de anéis de polinômios e isso pode ser usado para dar uma demonstração do Teorema da Base de Hilbert.

3 Ordens monomiais e bases de Gröbner

Avisamos logo que, quando não houver risco de mal-entendimento, iremos apresentar definições e exemplos no caso de duas ou três variáveis.

Quando queremos dividir dois polinômios em uma variável, sabemos bem por onde começar: pelos termos de grau maior. Quando temos duas variáveis, x e y, como decidir quem é maior entre x^3 e y^3?

Fazemos isto introduzindo uma ordem no anel $\mathbb{K}[x,y]$. Existem algumas ordens possíveis (isto é, que respeitem a multiplicação monomial e são bem-ordenadas), mas iremos nos restringir a falar de duas delas, as mais usadas para nossos propósitos.

Ordem lexicográfica: dados os monômios $a_\alpha x^{\alpha_1} y^{\alpha_2}$ e $b_\beta x^{\beta_1} y^{\beta_2}$, com $a_\alpha b_\beta \neq 0$, dizemos que

$$a_\alpha x^{\alpha_1} y^{\alpha_2} >_{lex(x,y)} b_\beta x^{\beta_1} y^{\beta_2}$$

se $\alpha_1 > \beta_1$ ou se $\alpha_1 = \beta_1$ e $\alpha_2 > \beta_2$.

O subescrito *lex* vem de lexicográfica, ou seja, a ordem dá mais peso para a variável que vem primeiro na ordem alfabética: $x > y$.

Ordem lexicográfica reversa: como o próprio nome diz, tal ordem é semelhante à lexicográfica, mas revertida. No caso de variáveis x e y, é a ordem lexicográfica trocando x com y: $rlex(x,y) = lex(y,x)$.

Grau total + ordem lexicográfica reversa: dados os monômios $a_\alpha x^{\alpha_1} y^{\alpha_2}$ e $b_\beta x^{\beta_1} y^{\beta_2}$, dizemos que

$$a_\alpha x^{\alpha_1} y^{\alpha_2} >_{tdeg(x,y)} b_\beta x^{\beta_1} y^{\beta_2}$$

se $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$ ou se ($\alpha_1 + \alpha_2 = \beta_1 + \beta_2$ e $\alpha_2 > \beta_2$) ou se ($\alpha_1 + \alpha_2 = \beta_1 + \beta_2$, $\beta_2 = \alpha_2$ e $\alpha_1 > \beta_1$). Esta ordem é menos injusta com uma das variáveis.

Em cada caso, se $p(x,y) \in \mathbb{K}[x,y]$ e o é uma ordem em $\mathbb{K}[x,y]$, denotamos por $tl_o(p)$ o termo líder de p, ou seja, o termo (com coeficiente não-nulo) de maior grau de p segundo a ordem o. Além disso, dados $p(x,y), q(x,y) \in \mathbb{K}[x,y]$, diremos que $p <_o q$ se $tl_o(p) <_o tl_o(q)$.

Exemplo 4. *Sejam* $p_1(x,y) = x^2y^3 + xy^5 + x^2y$, $p_2(x,y) = xy^2 + x^5y^3 + x^2y^4$.

(a) $tl_{lex(x,y)}(p_1) = x^2y^3$; $tl_{rlex(x,y)}(p_1) = xy^5$; $tl_{tdeg(x,y)}(p_1) = xy^5$.

(b) $p_1 <_{lex(x,y)} p_2$; $p_1 >_{rlex(x,y)} p_2$; $p_1 <_{tdeg(x,y)} p_2$.

Mais a frente responderemos à pergunta "Qual ordem devo usar?".

Por hora, fixemos uma ordem o em $\mathbb{K}[x_1,\ldots,x_n]$ e, dados $f, p_1, \ldots, p_k \in \mathbb{K}[x_1,\ldots,x_n]$, denotemos por $R(f,(p_1,\ldots,p_k))$ o resto da divisão de f por $(p_1,\ldots,p_k)$.

Sejam $f, p_1, p_2 \in \mathbb{K}[x,y]$. Queremos dividir f por (p_1,p_2) (nesta ordem). Se $tl_o(f) < tl_o(p_1)$ e $tl_o(f) < tl_o(p_2)$, então não há o que fazer. A única possibilidade é $f = 0 \cdot p_1 + 0 \cdot p_2 + f$, ou seja, a divisão retornará resto f.

Se $tl_o(f) > tl_o(p_1)$, então podemos dividir f por p_1. O resto desta divisão não será mais divisível por p_1, mas talvez o seja por p_2; neste caso, efetuamos a divisão. O novo resto não será mais divisível por p_2, mas talvez o seja por p_1; neste caso, efetuamos a divisão e continuamos. Fazemos o mesmo no caso $tl_o(f) > tl_o(p_2)$. No caso geral, temos um grafo, como na Figura 1.

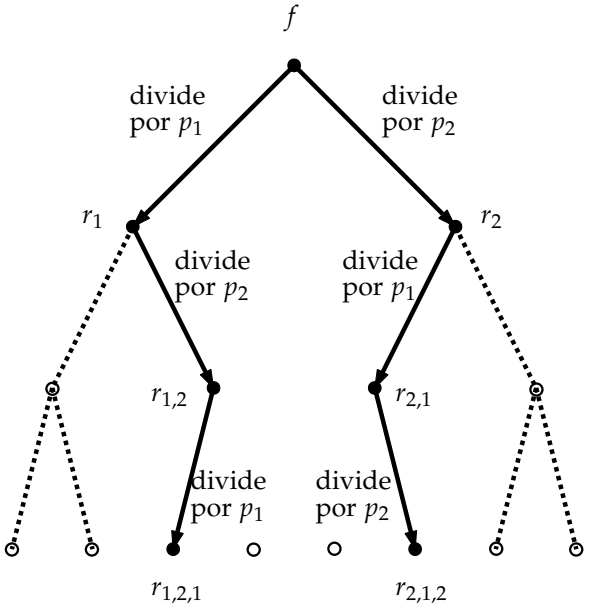

Figura 1: Divisões sucessivas

O problema com esta abordagem é que, como visto nos Exemplos 2 e 3, $r_{1,2,1}$ e $r_{2,1,2}$ podem ser diferentes.

Para contornar este problema, adicionaremos elementos $p_3, \ldots, p_\ell \in I$ de modo que, quando fizermos a divisão também por $p_3, \ldots, p_\ell$, o resto da divisão será único. Na Figura **??** isto é ilustrado no caso de adicionarmos somente um polinômio ao conjunto gerador.

Definição 1. *Sejam $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal. Se $p_1, \ldots, p_\ell \in I$ são tais que todo $p \in \mathbb{K}[x_1, \ldots, x_n]$ tem um único resto quando dividido por $(p_1, \ldots, p_\ell)$ e se $R(p, (p_1, \ldots, p_\ell)) = 0 \Leftrightarrow p \in I$, dizemos que $\{p_1, \ldots, p_\ell\}$ é um sistema de divisão completo para I, ou uma base de Gröbner para I.*

Note que no caso de uma base de Gröbner, os polinômios podem ser ordenados arbitrariamente.

Observação 1. *O termo "base" utilizado acima é um abuso de linguagem. Construiremos na verdade um conjunto gerador que possui a propriedade da Definição 1. Convencionou-se ao longo do tempo chamar tal conjunto gerador de base.*

Como construir uma base de Gröbner para um ideal I? Fixada a ordem o, o primeiro passo é escolher $p_1, \ldots, p_k \in I$ de modo que $I = \langle p_1, \ldots, p_k \rangle$.

Dados $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, seja $m = \text{mmc}(tl_o(f), tl_o(g))$. Defina

$$S(f,g) = \frac{m}{tl_o(f)} f - \frac{m}{tl_o(g)} g$$

o *S-polinômio* de f e g.

Agora vamos começar a construir a base de Gröbner a partir de $p_1, \ldots, p_k$.

Passo 1: Para cada par p_i, p_j, construa $S(p_i, p_j)$ e divida-o por $(p_1, \ldots, p_k)$. Seja $R(S(p_i, p_j), (p_1, \ldots, p_k))$ o resto desta divisão.

Passo 2: Se $R(S(p_i, p_j), (p_1, \ldots, p_k)) \neq 0$, defina $p_{k+1} = R(S(p_i, p_j), (p_1, \ldots, p_k))$ e reinicie o algoritmo com $(p_1, \ldots, p_k, p_{k+1})$ no lugar de $(p_1, \ldots, p_k)$. Se $R(S(p_i, p_j), (p_1, \ldots, p_k)) = 0$, volte para o **Passo 1** e escolha outro par.

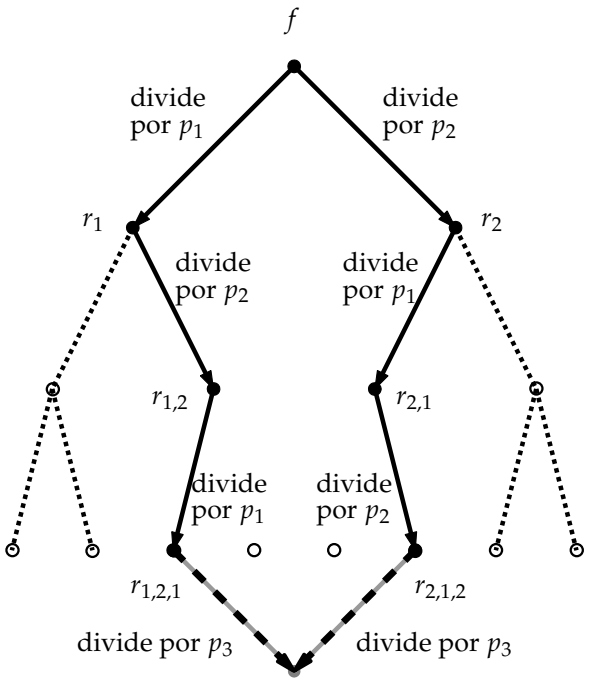

Figura 2: Divisões sucessivas, após o completamento.

Se todos os pares foram estudados e $\{p_1, \ldots, p_\ell\}$ é estacionário, então tal conjunto é uma base de Gröbner (em [1] há uma prova que este algoritmo realmente produz uma base de Gröbner).

Por fim, voltando ao problema (2), se $I = \langle p_1, \ldots, p_k \rangle$, calcular uma base de Gröbner $(p_1, \ldots, p_k, p_{k+1}, \ldots, p_\ell)$ para I **pode** ajudar a resolver (2). A escolha da ordem é fundamental neste ponto. Em particular, se a base de Gröbner for calculada usando a ordem lexicográfica, o sistema adquire uma forma triangular (se possível), o que geralmente torna sua solução mais simples.

Note que no caso de um sistema de equações lineares, a escolha da ordem lexicográfica induz a eliminação gaussiana no sistema. Porém, se o sistema inicial for homogêneo ou quase-homogêneo, é mais adequado utilizar a ordenação baseada no grau total.

Para terminar a seção, mataremos a curiosidade do leitor sobre os Exemplos 2 e 3. Se $I = \langle xy + 1, y^2 - 1 \rangle$, uma base de Gröbner para I é $(y^2 - 1, x + y)$, calculada usando $lex(x, y)$. Assim, se $f = xy^2 - x$, vemos que

$f = x(y^2 - 1)$; logo, $f \in I$.

Portanto, ganha o Exemplo 3.

Exemplo 5. *Neste exemplo retornamos à motivação inicial deste artigo, que é o sistema* (1). *Chamemos de p_1, p_2, p_3 os polinômios nas variáveis x, y, z que aparecem no sistema, nesta ordem. Calculando uma base de Gröbner para o ideal $I = \langle p_1, p_2, p_3 \rangle$ com a ordem lexicográfica $x < y < z$ e escrevendo tal base em forma de sistema, obtemos*

$$\begin{cases} z^7 = 0 \\ a_1 z^6 + a_2 y z^5 = 0 \\ a_3 z^6 + a_4 y^2 z^4 = 0 \\ a_5 z^5 + a_6 y z^4 + a_7 y^2 z^3 + a_8 y^3 z^2 = 0 \\ a_9 z^5 + a_{10} y z^4 + a_{11} y^2 z^3 + a_{12} y^4 z = 0 \\ a_{13} z^5 + a_{14} y z^4 + a_{15} y^2 z^3 + a_{16} y^5 = 0 \\ a_{17} z^4 + a_{18} y z^3 + a_{19} y^2 z^2 + a_{20} y^3 z + a_{21} y^4 + a_{22} x z^3 = 0 \\ a_{23} z^4 + a_{24} y z^3 + a_{25} y^2 z^2 + a_{26} y^3 z + a_{27} y^4 + a_{28} x y z^2 = 0 \\ a_{29} y^2 z + a_{30} y^3 + a_{31} x z^2 + a_{32} z^3 + a_{33} x y z + \\ \quad a_{34} y z^2 + a_{35} x y^2 + a_{36} x y + a_{37} z^2 + a_{38} x z + a_{39} x^2 = 0 \end{cases}$$

em que $a_1, \ldots, a_{39} \in \mathbb{R}$ são constantes não nulas.

Agora é fácil verificar nossa afirmação, já que da primeira equação obtemos que $z = 0$; fazendo esta substituição na sexta equação, obtemos $y = 0$; finalmente, da última equação, resulta $x = 0$. Note que esta solução é unica, independente do corpo $\mathbb{F}$ considerado.

Vamos utilizar a teoria das bases de Gröbner para provar o Teorema 3 (o Teorema da Base de Hilbert). Diremos que um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é *monomial* se I possui uma base (finita ou infinita) formada por monômios.

A prova do próximo lema é deixada como exercício ao leitor (sugestão: indução no número de variáveis).

Lema 1 (Lema de Dickson)**.** *Todo ideal monomial em $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado.*

Vamos agora à prova de que $\mathbb{K}[x_1, \ldots, x_n]$ é noetheriano. Seja I um ideal não trivial em $\mathbb{K}[x_1, \ldots, x_n]$. Considere o conjunto $tl(I) = \{tl(f);\ f \in I\}$. Como $tl(I)$ é um ideal monomial, pelo Lema de Dickson existem $g_1, \ldots, g_s \in I$, de modo que $tl(I) = \langle tl(g_1), \ldots, tl(g_s) \rangle$. Suponha, sem perda de generalidade, que $tl(g_1), \ldots, tl(g_s)$ é uma base de Gröbner para $tl(I)$ (caso contrário, calcule uma e passe a trabalhar com a outra base).

É claro que $\langle g_1, \ldots, g_s \rangle \subseteq I$. Seja então $f \in I$ e escreva $f = h_1 g_1 + \ldots + h_s g_s + r$, onde nenhum termo de r é divisível por $tl(g_i)$, $i = 1, \ldots, s$. Isto implica que $tl(r) \notin \langle tl(g_1), \ldots, tl(g_s) \rangle$. Porém, note que $r \in I$.

Se $r \neq 0$, $tl(r) \in \langle tl(g_1), \ldots, tl(g_s) \rangle$, o que é um absurdo. Logo, $r = 0$. Isto conclui a prova de que $g_1, \ldots, g_s$ é uma base (finita) para I.

4 Escalier

Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal e fixe uma ordem monomial. Considere a aplicação $p \mapsto tl(p) = a_\alpha x^\alpha$, onde $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, e denote $exp(p) = \alpha$. O conjunto $Exp(I) = \{exp(p);\ p \in I\} \subset \mathbb{N}^n$ é chamado *conjunto de expoentes* de I.

Note que $Exp(I)$ é invariante por translação. Com efeito, observe que se $\alpha = (\alpha_1, \ldots, \alpha_n) \in Exp(I)$ e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, então

$$\alpha + \beta = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) \in Exp(I)\,,$$

pois se $\alpha = exp(p)$ então

$$\alpha + \beta = exp\left(\left(x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}\right) p\right)$$

e $\left(x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}\right) p \in I$, pois I é um ideal.

Pode ser provado (de forma análoga ao Lema de Dickson) que sempre existe uma *fronteira* finita para $Exp(I)$, isto é, um conjunto finito F de modo que $Exp(I) = F + \mathbb{N}^n$. O *escalier* $Esc(I)$ é a *única* fronteira de cardinalidade mínima para $Exp(I)$.

Na Figura 3, uma fronteira é o conjunto dos pontos de coordenadas inteiras sobre a curva em azul, incluindo as interseções com os eixos.

Exemplo 6. *Sejam $p_1 = x^2 y + x^7 y$ e $p_2 = x^3 y^2 + xy$, $I = \langle p_1, p_2 \rangle$ com a ordem lexicográfica. Assim, $exp(p_1) = (7, 1)$, $exp(p_2) = (3, 2)$. Sabemos, portanto, que os pontos $(7, 1)$ e $(3, 2)$ estão em $Exp(I)$. No entanto, a priori, é impossível descrever $Esc(I)$.*

Diz-se que uma base de Gröbner $\{p_1, \ldots, p_\ell\}$ é *minimal* para $I \subset \mathbb{K}[x_1, \ldots, x_n]$ se nenhum p_i, $i = 1, \ldots, \ell$, é tal que $exp(p_i) = exp(p_j) + \beta$, com $i \neq j$ e $\beta \in \mathbb{N}^\ell$.

O seguinte resultado nos diz como calcular $Esc(I)$.

Teorema 5. *Se $\{p_1, \ldots, p_\ell\}$ é uma base minimal de Gröbner para I, então $Esc(I) = \{exp(p_1), \ldots, exp(p_\ell)\}$.*

Exemplo 7. *Retomando o exemplo anterior, $p_1 = x^2y + x^7y$, $p_2 = x^3y^2 + xy$ e $I = \langle p_1, p_2 \rangle$. Uma base de Gröbner para I na ordem lexicográfica é dada por $\{xy + xy^6, x^2y + xy^3\}$. Portanto, $Esc(I)$ é como na Figura 4.*

5 Aplicações

Seja $f : \mathbb{C}^2 \to \mathbb{C}$ uma função polinomial com $f(0,0) = (0,0)$. Um ponto $z_0 = (z_1, z_2) \in \mathbb{C}^2$ é uma *singularidade isolada* para f se $f(z_0) = 0$ e existe $\varepsilon > 0$ tal que $f(z) \neq 0$ para todo $z \in B_*(z_0, \varepsilon)$, onde

$$B_*(z_0, \varepsilon) = \{z \in \mathbb{C}^2;\ |z - z_0| < \varepsilon,\ z \neq z_0\}.$$

O ideal jacobiano de f é definido como o conjunto

$$\partial(f) = \left\{ \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right\}.$$

Teorema 6. *A origem é uma singularidade isolada para f se, e só se,*

$$\mu(f) = \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x,y]}{\partial(f)} \right) < \infty.$$

A prova do Teorema 6 segue do Teorema dos Zeros de Hilbert, o *Nullstellensatz*. O quociente $\left(\frac{\mathbb{C}[x,y]}{\partial(f)} \right)$ é um espaço vetorial e o número $\mu(f)$ é conhecido como *número de Milnor*.

O número de Milnor é um invariante topológico para as fibras regulares $f^{-1}(c)$ para $c \in \mathbb{C}$ com $|c| = \varepsilon > 0$ pequeno. Mais que isto, qualquer destas fibras tem a topologia de um buquê composto de μ círculos.

Quando f é um polinômio, o cálculo de $\mu(f)$ pode ser feito a partir do escalier de $\partial(f)$.

Teorema 7. *Se f é um polinômio, então $\mu(f)$ é o número de pontos em $\mathbb{N}_*^2 \setminus Exp(\partial(f))$, onde $\mathbb{N}_*^2 = \mathbb{N}^2 \setminus \{(0,0)\}$.*

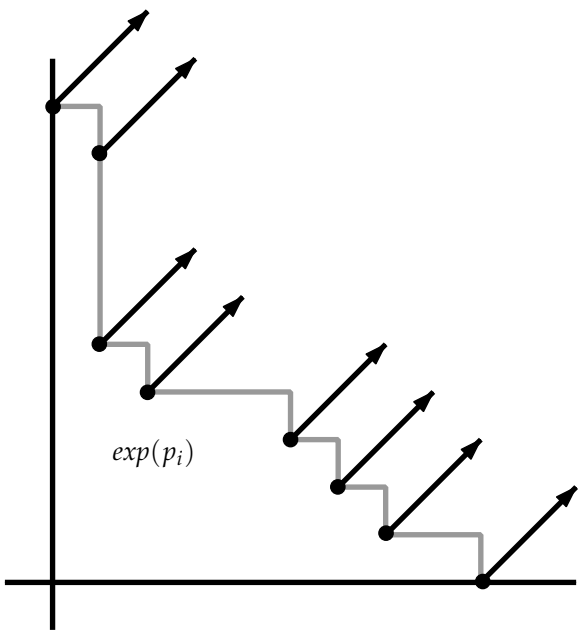

Figura 3: Exemplo de $Exp(I)$ para $I \subset \mathbb{K}[x,y]$. As setas representam a invariância por translação. Assim, $Exp(I)$ é toda a região acima da curva.

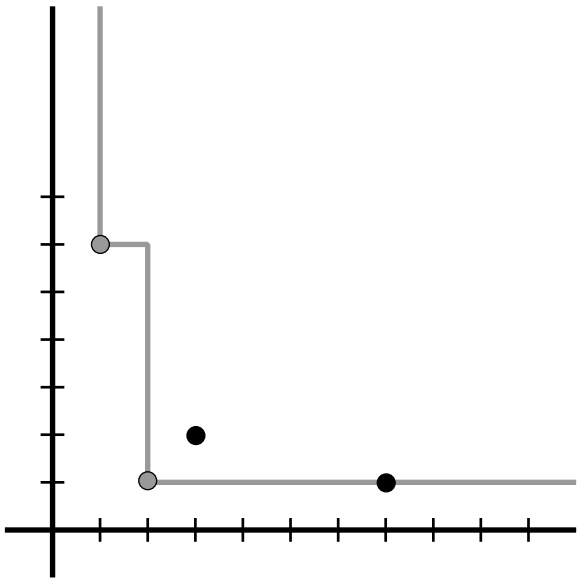

Figura 4: Na figura, $Esc(I)$ consiste dos dois pontos da cor cinza por onde passa a linha cinza. Os pontos pretos representam os polinômios iniciais e os de cor cinza os polinômios na base de Gröbner.

Exemplo 8. *Se* $f(x,y) = x^2y^2$, *então* $\partial(f) = \{2xy^2, 2x^2y\}$. *Uma base de Gröbner de* $\partial(f)$ *é* $\{xy^2, x^2y\}$. *Neste caso é fácil desenhar o escalier de* $\partial(f)$ *e ver que existem infinitos pontos no seu complementar. Logo, a origem não é uma singularidade isolada para* f. *(Claro que, neste exemplo, esta conclusão pode ser obtida de modo muito mais simples.)*

Exemplo 9. *Se* $f(x,y) = x^2y^2 + y^4 + x^3$, *então*

$$\partial(f) = \{2xy^2 + 3x^2, 2x^2y + 4y^3\}.$$

Uma base de Gröbner de $\partial(f)$ *é* $\{9y^3 + 2y^5, -3y^3 + xy^3, 2xy^2 + 3x^2\}$. *Neste caso, abaixo do escalier só existem 7 pontos. Logo, a origem é uma singularidade isolada.*

Apesar de termos considerado somente aplicações polinomiais neste texto, todos os resultados são válidos também para aplicações analíticas. A mesma abordagem é dada, por exemplo, em [8].

Os teoremas acima não valem para aplicações reais. Para estes casos, recomendamos ver [3, 10].

Para o leitor que gostou desta última seção, recomendamos [11]. Outras aplicações das bases de Gröbner em sistemas dinâmicos podem ser encontradas em [4].

6 Usando o computador

O leitor deve ter percebido o quão tedioso pode ser calcular uma base de Gröbner manualmente. No entanto, rotinas para cálculo de bases de Gröbner estão implementadas na maioria dos softwares de computação algébrica. Vamos mostrar como usar dois destes softwares, o Maple e o GAP (Groups, Algorithms, Programming), para calcular tais bases. A grande vantagem do GAP é o fato de poder ser baixado gratuitamente. Já o Maple ganha por popularidade entre os não algebristas.

6.1 No Maple

A versão atual do Maple é a 14, mas muitas universidades brasileiras possuem licenças para versões antigas, como a 9. O pacote `Groebner` possui todos os comandos referentes a bases de Gröbner. O comando básico para calcular a base é

`Basis([`f_1`,...,`f_s`], plex(`x_1`,...,`x_n`))`.

Por exemplo, o comando

`Groebner[Basis]([`$x^2 + xy - y^2$`, `$xy^4 - yx^4$`], plex(x, y))`

calcula uma base de Gröbner para o ideal gerado pelos polinômios $f_1 = x^2 + xy - y^2$ e $f_2 = xy^4 - yx^4$ usando a ordem lexicográfica. Tal base é $g_1 = y^6$, $g_2 = -y^5 + 2xy^4$ e $g_3 = x^2 + xy - y^2$.

Para mais informações, veja o site do Maple: *www.maplesoft.com/products/maple/*.

6.2 No GAP

No GAP é preciso construir os elementos com os quais trabalharemos antes de efetuar o cálculo. Este é um procedimento usual.

```
F := Rationals;
R := PolynomialRing( F, [ "x", "y"]);
x := IndeterminatesOfPolynomialRing(R)[1];
y := IndeterminatesOfPolynomialRing(R)[2];
I := Ideal (R, [x*y+y^2,x^5]);
ordem := MonomialLexOrdering(x,y);
```

Feita a preparação, os comandos para calcular a base de Gröbner seguem abaixo. O segundo deles calcula uma base simplificada.

```
GroebnerBasis( I, ordem );
ReducedGroebnerBasis(I, ordem);
```

O resultado, neste exemplo, é `[`y^6`, `$x*y+y^2$`, `x^5`]` em ambos os casos.

Mais informações, veja o site do GAP: *www.gap-system.org/*.

7 Extensões

Enquanto as bases de Gröbner são calculadas para ideais, existe seu análogo para subálgebras: as *bases de*

Sagbi (sigla de *Subalgebra Analogue to Gröbner Basis for Ideals*). Tais bases podem ser infinitas, mesmo no caso de subálgebras finitamente geradas. Mais detalhes em [5].

Existe ainda uma teoria de bases de Gröbner para álgebras não comutativas, e os primeiros capítulos de [6] são uma boa introdução ao assunto. No entanto, no caso não comutativo, o problema é muito mais delicado; em particular, a base encontrada pode ser finita ou infinita, dependendo da ordem escolhida. Os cálculos das bases, neste contexto, são bem mais lentos do que no caso comutativo.

Referências

[1] COUTINHO, S. C. Demonstração automática de teoremas. In: *I Bienal da SBM*, Belo Horizonte: UFMG, 2002. Disponível em *www.mat.ufmg.br/eventos/bienal/textos.html*.

[2] COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. 3. ed. New York: Springer, 2006. (Undergraduate Texts in Mathematics)

[3] JACQUEMARD, A. Fibrations de Milnor pour des applications réelles. *Unione Matematica Italiana. Bollettino. Sezione B. Serie VII*, v. 3, p. 591–600, 1989.

[4] JACQUEMARD, A.; TEIXEIRA, M. A. Effective algebraic geometry and normal forms of reversible mappings. *Revista Matemática Complutense*, v. 15, n. 1, p. 31–55, 2002.

[5] KREUZER, M.; ROBBIANO, L. *Computational commutative algebra. 2.* Berlin: Springer, 2005.

[6] LI, H. *Noncommutative Gröbner bases and filtered-graded transfer.* Berlin: Springer, 2002. (Lecture Notes in Mathematics, 1795)

[7] MAY, J. P. Munshi's proof of the Nullstellensatz. *The American Mathematical Monthly*, v. 110, n. 2, p. 133–140, 2003.

[8] MILNOR, J.. *Singular points of complex hypersurfaces.* Princeton University Press, 1968. (Ann. of Maths. Studies, 61)

[9] REID, C. *Hilbert.* New York: Copernicus, 1996.

[10] RUAS, M. A. S.; DOS SANTOS, R. N. A. Real Milnor fibrations and (c)-regularity, *Manuscripta Mathematica*, v. 117, n. 2, p. 207–218, 2005.

[11] SEADE, J. On Milnor's fibration theorem for real and complex singularities. In: BRASSELET, J.-P.; DAMON, J.; TRANG, L. D.; OKA, M. (EDS). *Singularities in geometry and topology.* Hacksensack: World Scientific Publishing, 2007. p. 127-158.

Alain Jacquemard
Institut de Mathématiques de Bourgogne. UMR CNRS 5584, Université de Bourgogne, Dijon, France.
Alain.Jacquemard@u-bourgogne.fr

Ricardo Miranda Martins
Departamento de Matemática. Instituto de Matemática, Estatística e Computação Científica. UNICAMP, Campinas/SP.
rmiranda@ime.unicamp.br