Universidade de Aveiro Departamento de Matemática
2008

Filipa Nunes Nogueira

Bases de Gröbner e sistemas de equações às diferenças parciais

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações, realizada sob a orientação científica da Doutora Maria Paula Macedo Rocha Malonek, Professora Catedrática do Departamento de Matemática da Universidade de Aveiro

O júri

Presidente

Prof. Doutor Domingos Moreira Cardoso

Professor Catedrático do Departamento de Matemática da Universidade de Aveiro

Prof. Doutora Maria Paula Macedo Rocha Malonek

Professora Catedrática do Departamento de Matemática da Universidade de Aveiro (Orientadora)

Prof. Doutor Carlos Martins da Fonseca

Professor Auxiliar da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Agradecimentos

Neste espaço gostaria de deixar os meus sinceros agradecimentos a todos aqueles que de alguma forma contribuíram para que este trabalho se tornasse possível.

Em primeiro lugar expresso a minha gratidão à minha orientadora, Prof. Doutora Paula Rocha, pela forma como orientou o meu trabalho. As notas dominantes da sua orientação foram a permanente disponibilidade, dedicação, paciência e estímulo.

São também dignas de menção, e não vou esquecer, as palavras encorajadoras e reconfortantes da Prof. Doutora Gladys Jordan e do Prof. Doutor Leslie Bajuelos.

Finalmente, mas não menos importante, um agradecimento especial aos meus pais, irmão, cunhada, Pedro, Carla, Miriam e Sérgio que sempre me deram forças nas horas difíceis e apoiaram desde o primeiro momento.

Palavras-chave

Anéis de polinómios *nD*, bases de Gröbner, equações às diferenças parciais.

Resumo

Nesta dissertação estuda-se o conceito de bases de Göbner para ideais de polinómios em várias indeterminadas. Este conceito é aplicado à obtenção de formas alternativas para sistemas de equações às diferenças parciais que se adequam ao cálculo recursivo das soluções.

Keywords *nD* polynomial rings, Gröbner bases, partial difference equations.

Abstract In this thesis we study the concept of Gröbner bases for *nD* polynomial ideals. This concept is applied to the study of systems of partial difference equations, allowing alternative descriptions that are suitable for the recursive computation of solutions.

Índice

Introdução

O objectivo deste trabalho é o estudo de bases de Gröbner para ideais de anéis de polinómios em várias indeterminadas, bem como de uma aplicação destas bases ao estudo de sistemas de equações às diferenças parciais.

Um sistema de equações às diferenças parciais numa variável pode ser relacionado com um ideal no anel de polinómios em várias indeterminadas. A consideração de uma base de Gröbner reduzida para este ideal permite transformar este sistema num outro equivalente, que apresenta uma forma adequada para o cálculo das soluções equação a equação.

No Capítulo 1 desenvolve-se toda a teoria necessária à realização deste objectivo, estando coligidos na Secção 1.1 as definições, notações e resultados preliminares.

Na Secção 1.2 estuda-se os anéis de polinómios numa indeterminada (polinómios $1D$) passando-se, na Secção 1.3, a considerar anéis de polinómios em várias indeterminadas (polinómios nD). Enquanto os polinómios $1D$ constituem um domínio euclidiano (e portanto de ideais principais), o mesmo não sucede com os polinómios nD, que apenas constituem um anel noetheriano, sendo, por isso, de ideais finitamente gerados.

Na Secção 2.1 estuda-se o conceito de base de Gröbner, que corresponde a um conjunto de geradores de um ideal de polinómios nD com determinadas características. Como se verá na Secção 2.2, as propriedades das bases de Gröbner, em particular das bases

de Gröbner reduzidas, permitem a obtenção de representações de sistemas de equações às diferenças adequadas ao cálculo recursivo de soluções.

Nesta exposição utiliza-se numeração independente das fórmulas e figuras em cada secção.

Uma vez que a bibliografia não é muito extensa e permite identificar a proveniência das definições e resultados apresentados, optou-se por não se fazer referências ao longo do texto.

1

Anéis de polinómios

1.1 Preliminares

Ao longo do presente trabalho chamaremos **anel** a um anel comutativo $(A, +, \cdot)$, ou seja, a um conjunto não vazio A, munido por duas operações internas "+" e "·" tais que:

i. $(A, +)$ é um grupo abeliano (Elemento neutro 0_A, ou apenas 0 se não houver risco de ambiguidade);

ii. $(A, \cdot)$ é um semigrupo comutativo;

iii. A operação "·" é distributiva à direita e à esquerda em relação à operação "+", isto é, para todo $a, b, c \in A$:

   a. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

   b. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Caso não haja risco de ambiguidade relativamente às operações "+" e "·" consideradas, referir-nos-emos simplesmente ao anel A.

Se $(A, \cdot)$ for um monóide (semigrupo com elemento neutro 1_A, ou apenas 1, se não houver risco de ambiguidade) diz-se que A é um **anel com identidade**.

Um **corpo** $\mathbb{K}$ é um anel com identidade tal que $(\mathbb{K}\backslash\{0\},\cdot)$ é um grupo.

Um elemento $a \in A$ **divide** $b \in A\backslash\{0\}$ ou é **divisor** de b se existe $s \in A$ tal que $b = as$. Neste caso, escrevemos $a|b$ e também dizemos que b é **divisível** por a. Se $a|1_A$, então $a \in A$ é uma **unidade**.

Dizemos que $a \in A$ é um **divisor de zero,** se $a \neq 0$ e existe $s \neq 0$ tal que $as = 0$. Um anel com identidade tal que $1_A \neq 0_A$ e sem divisores de zeros é designado por **domínio de integridade** (ou apenas domínio).

Exemplos

1. $\mathbb{Z}$ é um domínio de integridade
2. $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, conjunto dos inteiros módulo 6, não é um domínio de integridade, porque, por exemplo, $\overline{2} \cdot \overline{3} = \overline{0}$ e $\overline{2}, \overline{3} \neq \overline{0}$.

Uma importante classe de domínios é a dos domínios euclidianos, que são definidos da forma que se segue.

Definição 1.1.1

Um **domínio euclidiano** é um domínio de integridade D onde se define uma função

$$\begin{aligned} \phi : D\backslash\{0_D\} &\longrightarrow \mathbb{Z}^+ \\ a &\mapsto \phi(a) \end{aligned}$$

tal que:

i. $ab \neq 0 \Rightarrow \phi(ab) \geq \phi(a)$;

ii. Sendo $a \in D,\ b \in D\backslash\{0_D\}$ existem $q,\ r \in D$ tais que $a = bq + r$, com $r = 0$ ou $\phi(r) < \phi(b)$.

Da definição resulta que se $a|b$ então $\phi(a) \leq \phi(b)$ para todo $a, b \in D\backslash\{0_D\}$. Uma vez que $1_D|a$, para todo $a \in D$, resulta também da definição que:

$$\phi(1_D) \leq \phi(a), \ \forall\, a \in D\backslash\{0_D\}.$$

Exemplo

$\mathbb{Z}$ é um domínio euclidiano. De facto, a função $\phi(x) = |x|$ satisfaz i. e ii.

Definição 1.1.2

O subanel $I \subseteq A$ é um **ideal** de A se para todo $a \in A$ e para todo $i \in I$ se tem $ai \in I$. Neste caso escreve-se $I \lhd A$.

Um ideal de um anel A é, portanto, um subanel fechado para a multiplicação por elementos de A.

Exemplos

1. A e $\{0\}$ são ideais triviais de A.
2. $\mathbb{Z}$ não é um ideal de $\mathbb{Q}$. De facto, dados $1 \in \mathbb{Z}$ e $\frac{1}{6} \in \mathbb{Q}$, temos que $1 \cdot \frac{1}{6} \notin \mathbb{Z}$.

Dizemos que um ideal I de um anel A, com $I \neq A$, é **maximal** se não existir nenhum ideal diferente de A que contenha I propriamente.

Isto significa que se $I \neq A$ e se J for um ideal de A tal que $I \subseteq J \subseteq A$, então $J = I$ ou $J = A$.

Seja M um subconjunto arbitrário de A. Designamos por **ideal gerado por** M e representamos por $I(M)$ a intersecção de todos os ideais de A que contêm M. Se existe um conjunto finito M tal que $I = I(M)$, dizemos que o ideal I é **finitamente gerado**.

Note-se que o ideal gerado por M é o menor ideal de A que contém M, de facto, se I é um ideal de A que contém M, então I contém o ideal gerado por M. Por convenção, $I(\emptyset) = \{0\}$.

Definição 1.1.3

A um ideal que pode ser gerado por um só elemento chama-se **ideal principal**.

O ideal principal (i.p.) gerado por um elemento ($x \in A$) representa-se por $I(x)$.

Um domínio de integridade em que todos os seus ideais são ideais principais diz-se **domínio de ideais principais** (d.i.p.).

Por exemplo, o anel $\mathbb{Z}$ é um domínio de ideais principais. Na secção que se segue consideraremos anéis de polinómios e mostraremos que o anel dos polinómios numa indeterminada é um d.i.p. enquanto que os anéis de polinómios em várias indeterminadas não o são.

Teorema 1.1.4

Seja D um domínio euclidiano. Então D é um d.i.p.

Demontração

Vamos provar que todo ideal de D é principal.

Seja I um ideal de D. Se $I = \{0\}$ ou $I = D$, isto é, se I for um ideal trivial de A, então I é principal.

Suponhamos que I é um ideal não trivial de D. Seja $a \in I\backslash\{0\}$ tal que $\phi(a)$ é mínimo. Dado $b \in I\backslash\{0\}$ existem $q, r \in D$ tais que $b = aq + r$ onde $r = 0$ ou $\phi(r) < \phi(a)$.

Uma vez que $r = b - aq \in I$ tem-se que $\phi(r) \geq \phi(a)$ e, consequentemente, deverá ter-se $r = 0$. Então $b = aq, q \in D$.

É agora fácil concluir que $I = I(a)$ e, portanto, I é ideal principal.

Assim, D é um d.i.p. ■

Observação 1.1.5

Não é difícil verificar que na demonstração anterior o elemento a é um $m.d.c$ de todos os elementos de $I = I(a)$, de acordo com a definição que se segue.

Definição 1.1.6

Seja D um domínio de integridade e $a_1, a_2, \cdots, a_n$ elementos de D. Diz-se que $d \in D$ é um **máximo divisor comum** de $a_1, a_2, \cdots, a_n$ e escreve-se $mdc\ (a_1, a_2, \cdots, a_n) = d$ se:

i. $d|a_i\,, \quad i = 1 \cdots n\,;$

ii. $d'|a_i\,, \quad i = 1 \cdots n \ \Rightarrow\ d'|d.$

Da definição resulta que se d é um máximo divisor comum de $a_1, a_2, \cdots, a_n$ e d' é também um máximo divisor comum de $a_1, a_2, \cdots, a_n$, então d e d' são associados, ou seja, existe uma unidade u tal que $d' = ud$ (e $d = u'd'$, onde $uu' = u'u = 1_A$). Portanto, o máximo divisor comum é único a menos do produto por uma unidade de D.

Uma classe de anéis com propriedades muito importantes é a classe dos anéis noetherianos[1], que engloba os d.i.p.

Definição 1.1.7

Um anel A, com identidade, diz-se **noetheriano** se para toda a cadeia ascendente $I_1 \subseteq I_2 \subseteq \cdots$ de ideais de A existe $n_0 \in \mathbb{N}$, tal que $I_n = I_{n_0}$, para $n \geq n_0$.

A condição da definição, que afirma que toda a cadeia ascendente de ideais se torna estacionária, é conhecida por condição das cadeias ascendentes (c.c.a.).

O teorema que se segue dá-nos uma outra caracterização para anéis noetherianos.

Teorema 1.1.8

As seguintes afirmações são equivalentes:

1) A é um anel noetheriano;
2) Qualquer subconjunto não vazio de ideais de A tem um elemento maximal (com respeito à inclusão);
3) Qualquer ideal de A é finitamente gerado, isto é dado um ideal $I \subset A$ existem $i_1, \cdots, i_n \in I$ tais que $I = I(i_1, \cdots, i_n)$.

[1] O termo noetheriano provém do nome da matemática alemã Emmy Noether

Demonstração

"1) ⇒ 2)"

Suponhamos, por redução ao absurdo, que existe um conjunto C, não vazio, de ideais de A que não tem nenhum elemento maximal. Neste caso, dado $I_1 \in C$ existe $I_2 \in C$ tal que $I_1 \subset I_2 \subset A$. Prosseguindo desta forma, construímos uma cadeia de ideais de A que não é estacionária, o que é um absurdo.

"2) ⇒ 3)"

Suponhamos, por redução ao absurdo, que I não é um ideal finitamente gerado. Neste caso, é fácil construir uma cadeia não estacionária de ideais $I(i_1) \subset I(i_1, i_2) \subset I(i_1, i_2, i_3) \subset \cdots$, onde $i_n \in I$ para todo $n \in \mathbb{N}$. É claro que o conjunto $C = \{I(i_1), I(i_1, i_2), I(i_1, i_2, i_3), \cdots\}$ não tem um elemento maximal, o que contraria a hipótese.

"3) ⇒ 1)"

Seja $I_1 \subseteq I_2 \subseteq \cdots$ uma cadeia de ideais de A. Então $I = \bigcup_{i=1}^{\infty} I_i$ é também um ideal. Por hipótese temos que $I = I(i_1, \cdots, i_n)$ para determinados $i_1, \cdots, i_n \in I$. Ora, é claro que existe $n_0 \in \mathbb{N}$ tal que $\{i_1, \cdots, i_n\} \subset I_{n_0}$ e portanto $I_n = I_{n_0}$ sempre que $n \geq n_0$, provando que A é noetheriano. ■

Exemplos

1. Um corpo $\mathbb{K}$ é um anel noetheriano, pois os seus únicos ideais são $I(0)$ e $I(1)$.
2. Tendo em conta a condição 3) do teorema anterior, todos os d.i.p. são, obviamente, anéis noetherianos, portanto, por exemplo, $\mathbb{Z}$ é um anel noetheriano.

1.2 Polinómios numa indeterminada

Chamamos polinómio p numa indeterminada x a uma expressão da forma:

$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

onde n é um número natural e os elementos $a_i,\ i = 0, 1, \cdots, n$ são os **coeficientes**. Se $a_n \neq 0$ dizemos que n é o **grau do polinómio** e denotamos $gr(p) = n$. Ao produto $a_i x^i$ chamamos **monómio**. Se $a_i \neq 0$ dizemos que o monómio $a_i x^i$ é um **termo** do polinómio p. Chamamos **termo independente** a a_0.

Ordenar um polinómio é escrevê-lo segundo as potências decrescentes (ou crescentes) da indeterminada x.

Denotamos o conjunto de todos os polinómios em x com coeficientes no corpo $\mathbb{K}$ por $\mathbb{K}[x]$ e representamos por $\mathcal{M}_x$ o conjunto de todos os monómios na indeterminada x.

As duas proposições que se seguem podem ser facilmente verificadas.

Proposição 1.2.1

$\mathbb{K}[x]$ munido com as operações usuais de adição e de multiplicação por um escalar é um domínio de integridade.

Proposição 1.2.2

Se f e g são dois elementos quaisquer de $\mathbb{K}[x]$, então:

i. $gr(f + g) \leq \max\{gr(f), gr(g)\}$;

ii. $gr(fg) = gr(f) + gr(g)$.

O resultado que a seguir demonstramos é crucial para concluir que o anel $\mathbb{K}[x]$ é um domínio euclidiano.

Teorema 1.2.3

Sejam p e d dois elementos de $\mathbb{K}[x]$, sendo $d \neq 0$,

$$p = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0, \qquad a_n \neq 0$$
$$d = b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0, \qquad b_m \neq 0.$$

Então existem polinómios q e r com $gr(r) < gr(d)$ ou $r = 0$, tais que:

$$p = dq + r \tag{1}$$

Demonstração

1º) $n < m$

O problema fica resolvido com $q = 0$ e $r = p$.

2º) $n \geq m$ (ou seja, $gr(p) \geq gr(d)$

Seja $q_1 \coloneqq a_n b_m^{-1} x^{n-m}$. Vem que

$$p = dq_1 + r_1. \tag{2}$$

Se $gr(r_1) < gr(d)$ ou $r_1 = 0$, então (2) prova o teorema.

Se $gr(r_1) \geq gr(d)$ procedemos para r_1 e d como fizemos para p e d. Neste caso, existem polinómios q_2 e r_2 tais que:

$$r_1 = dq_2 + r_2. \tag{3}$$

Substituindo (3) e (2) em (1) vem

$$p = d(q_1 + q_2) + r_2. \tag{4}$$

$$\text{Se } gr(r_2) < gr(d) \text{ ou } r_2 = 0 \tag{5}$$

então (4) é a resposta pretendida, com $r = r_2$ e $q = q_1 + q_2$.

Caso não se verifique (5), continuamos o procedimento anterior, agora com r_2 e d. Como os graus dos sucessivos restos r_i vão diminuindo, ao fim de um certo número (finito) de passos, por exemplo k, obteremos

$$p = d(q_1 + \cdots + q_k) + r_k \tag{6}$$

onde $r_k = 0$ ou $gr(r_k) < gr(d)$.

Os polinómios q e r procurados são então $r = r_k$ e $q = q_1 + \cdots + q_k$. ■

O algoritmo utilizado para demonstrar o teorema supracitado é conhecido como **algoritmo da divisão de Euclides**.

Note-se que se tivermos um ideal $I = I(q)$, o algoritmo da divisão de dois polinómios permite-nos escrever qualquer elemento $p \in \mathbb{K}[x]$ como $p = dq + r$, onde $dq \in I(q)$, $r \notin I(q)$, grau(r) < grau(q) e grau(r) $\leq$ grau(i), $\forall i \in I$. Neste sentido, o resto r pode ser encarado como sendo equivalente a (congruente com) p a menos do ideal principal $I(q)$.

Vejamos, com um exemplo, como na prática se determina o quociente e o resto da divisão de dois polinómios.

Exemplo

Efectuar: $(3x^2 - 6x^3 + 2) : (2x^2 + 1)$.

Resolução:

$-6x^3 + 3x^2 + 0x + 2$	$2x^2 + 1$	Começa-se por escrever ordenadamente o dividendo e o divisor segundo as potências decrescentes de x, escrevendo também os termos nulos do dividendo.

$-6x^3+3x^2+0x+2 \quad \big\vert\, 2x^2+1$ $\qquad\qquad\qquad\quad -3x$	Dividem-se os termos de maior grau do dividendo e do divisor. $-6x^3 : 2x^2 = -3x$ O resultado é o termo de maior grau do quociente.
$-6x^3+3x^2+0x+2 \quad \big\vert\, 2x^2+1$ $6x^3 \quad\; +3x \qquad\quad -3x$ $3x^2+3x+2$	Multiplica-se o divisor pelo termo de maior grau do quociente, e subtrai-se o resultado ao dividendo, obtendo assim o resto parcial.
$-6x^3+3x^2+0x+2 \quad \big\vert\, 2x^2+1$ $6x^3 \quad\; +3x \qquad\quad -3x+3/2$ $3x^2+3x+2$ $-3x^2 \quad -3/2$ $3x+1/2$	Considera-se o resto parcial como novo dividendo e procede-se como anteriormente.

Este procedimento pára quando o grau do resto parcial for inferior ao grau do divisor. Neste caso, o resto parcial é o resto da divisão.

Corolário 1.2.4

O anel de polinómios $\mathbb{K}[x]$ é um domínio euclidiano.

Demonstração

Tendo em atenção o Teorema 1.2.3 e a Proposição 1.2.2 e se considerarmos em $\mathbb{K}[x]$ a função $\varphi(p) =$ grau de p se $p \neq 0$ e $\varphi(0) = -1$ observamos que as condições i. e ii. da Definição 1.1.1 são satisfeitas e, portanto, $\mathbb{K}[x]$ é um domínio euclidiano. ■

Pelo Teorema 1.1.4, podemos concluir que $\mathbb{K}[x]$ é um d.i.p.

Uma vez que $\mathbb{K}[x]$ é um domínio de integridade, podemos definir o máximo divisor comum entre polinómios $p_1, p_2, \cdots, p_n \in \mathbb{K}[x]$. Atendendo à Observação 1.1.5 obtemos a seguinte proposição.

Proposição 1.2.5

Se $d = mdc(p_1, p_2, \cdots, p_n)$, então $I(p_1, p_2, \cdots, p_n) = I(d)$, implicando que existem polinómios $\alpha_1, \alpha_2, \cdots, \alpha_n$ tais que $d = \alpha_1 p_1 + \alpha_2 p_2 + \cdots + \alpha_n p_n$.

Demonstração

Para demonstrarmos a proposição começamos por descrever o algoritmo que permite determinar um mdc, d, entre dois polinómios não nulos, $a, b \in \mathbb{K}[x]$ e $\alpha, \beta \in \mathbb{K}[x]$ tais que $\alpha a + \beta b = d$.

Sendo $\mathbb{K}[x]$ um domínio euclidiano, existem polinómios q e r com $gr(r_1) < gr(b)$ ou $r = 0$, tais que:

$$a = bq_1 + r_1. \tag{7}$$

Se $r_1 = 0$, é fácil concluir que $mdc(a, b) = b$.

Sejam $r_1, b \neq 0$. Então existem $r_2, q_2 \in \mathbb{K}[x]$ tais que:

$$b = r_1 q_2 + r_2\,, \quad gr(r_2) < gr(r_1). \tag{8}$$

Se $r_2 = 0$, $mdc(a, b) = r_1$.

Dados $r_1, r_2 \neq 0$, existem $r_3, q_3 \in \mathbb{K}[x]$ tais que:

$$r_1 = r_2 q_3 + r_3\,, \quad gr(r_3) < gr(r_2). \tag{9}$$

Suponhamos que podemos efectuar um certo número $k \in \mathbb{N}$ de passos obtendo:

$$r_{k-2} = r_{k-1} q_k + r_k\,, \quad gr(r_k) < gr(r_{k-1}). \tag{10}$$

Uma vez que

$$gr(b) > gr(r_1) > \cdots > gr(r_{k-1})$$

e $gr(p)$ é um número inteiro positivo, para qualquer polinómio p, este processo não pode prolongar-se indefinidamente, isto é, existe um passo do algoritmo onde se obtém um resto nulo. Suponhamos que $r_n = 0$. Temos, então,

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}\,, \quad gr(r_{n-1}) < gr(r_{n-2}) \tag{11}$$

$$r_{n-2} = r_{n-1}q_n. \tag{12}$$

Vamos ver que $mdc(a,b) = r_{n-1}$. De (12) concluímos que $r_{n-1}|r_{n-2}$, enquanto que de (12) e (11) concluímos que $r_{n-1}|r_{n-3}$. Conjugando (12) e (11) com (10) concluímos que $r_{n-1}|r_{n-4}$. Prosseguindo deste modo concluímos que $r_{n-1}|r_{n-i},\ i = 1, \cdots, n-2$. Como $r_{n-1}|r_2$ e $r_{n-1}|r_1$, (8) permite concluir que $r_{n-1}|b$. Por outro lado, os factos que $r_{n-1}|b,\ r_{n-1}|r_1$, conjuntamente com (7) permitem concluir que $r_{n-1}|a$. Temos então que

$$r_{n-1}|a \text{ e } r_{n-1}|b. \tag{i}$$

Seja agora $d \in \mathbb{K}[x]$ tal que $d|a$ e $d|b$. Vamos ver que então $d|r_{n-1}$. Uma vez que $d|a,\ d|b$ e (7) se verifica, conclui-se que $d|r_1$. Por outro lado, $d|r_1$, $d|b$ e (8) permitem concluir que $d|r_2$. Prosseguindo deste modo, concluímos que $d|r_{n-1}$. Assim,

$$d \in \mathbb{K}[x], d|a \text{ e } d|b \Rightarrow d|r_{n-1}. \tag{ii}$$

Decorre assim de (i) e de (ii) que $mdc(a,b) = r_{n-1}$, como pretendíamos.

Provemos agora que existem $\alpha, \beta \in \mathbb{K}[x]$ tais que $\alpha a + \beta b = r_{n-1}$.

A expressão (7) afirma que $a = bq_1 + r_1$. Logo, podemos escrever r_1 como combinação linear de a e b, mais concretamente, $r_1 = a - bq_1$. Substituindo r_1 em (8) temos $b = (a - bq_1)q_2 + r_2$, portanto, $r_2 = a(-q_2) + (1 + q_1q_2)b$, e mais uma vez o resto, r_2, pode ser escrito como combinação linear de a e b. Substituindo em (9) r_1 e de r_2 pelas expressões encontradas podemos escrever r_3 como combinação linear de a e b.

Repetindo o processo sucessivamente, obteremos uma expressão para r_{n-1} como combinação linear de a e b, $r_{n-1} = \alpha a + \beta b$, como pretendíamos.

Caso tenhamos três ou mais polinómios, determinamos o $mdc\ (p_1, p_2, \cdots, p_n)$ de forma recursiva tendo em conta que

$$mdc\ (p_1, p_2, \cdots, p_n) = mdc(mdc\ (p_1, \cdots, p_{n-1}), p_n), \qquad n = 3, \cdots$$

Este processo permite igualmente determinar os polinómios $\alpha_1, \alpha_2, \cdots, \alpha_n$ tais que $\alpha_1 p_1 + \alpha_2 p_2 + \cdots + \alpha_n p_n = mdc(p_1, p_2, \cdots, p_n)$.

Ainda falta provar que $I(p_1, p_2, \cdots, p_n) = I(d)$.

Uma vez que d divide $p_1, p_2, \cdots, p_n$, é óbvio que estes polinómios pertencem a $I(d)$ e, consequentemente, $I(p_1, p_2, \cdots, p_n) \subseteq I(d)$. Por outro lado, $d \in I(p_1, p_2, \cdots, p_n)$ já que existem polinómios $\alpha_1, \cdots, \alpha_n$ tais que $d = \alpha_1 p_1 + \cdots + \alpha_n p_n$. Portanto $I(d) \subseteq I(p_1, p_2, \cdots, p_n)$, concluindo-se deste modo que $I(p_1, p_2, \cdots, p_n) = I(d)$. ■

Ilustremos, com o seguinte exemplo, o cálculo do máximo divisor comum entre dois polinómios e a sua expressão como combinação linear destes polinómios.

Exemplo

Sejam $p, q \in \mathbb{R}[x]$,

$p = 2x^4 + 3x^3 + 4x^2 + 2x + 1$
$q = 3x^3 + 4x^2 + 4x + 1$

Dividindo p por q obtemos:

$$2x^4 + 3x^3 + 4x^2 + 2x + 1 = (3x^3 + 4x^2 + 4x + 1)\left(\frac{2}{3}x + \frac{1}{9}\right) + \frac{8}{9}x^2 + \frac{8}{9}x + \frac{8}{9}$$

Dividindo agora q pelo resto da divisão anterior obtemos um resto nulo. De facto:

$$3x^3 + 4x^2 + 4x + 1 = \left(\frac{8}{9}x^2 + \frac{8}{9}x + \frac{8}{9}\right)\left(\frac{27}{8}x + \frac{9}{8}\right)$$

Consequentemente, $\frac{8}{9}(x^2+x+1)$ é um $mdc\ (p,q)$.

Uma vez que o máximo divisor comum é determinado a menos de um factor invertível, tomaremos x^2+x+1 como $mdc\ (p,q)$ e vamos determinar $\alpha,\beta \in \mathbb{R}[x]$ tais que $\alpha p+\ \beta q = x^2+x+1$. Ora,

$$2x^4+3x^3+4x^2+2x+1 = (3x^3+4x^2+4x+1)\left(\frac{2}{3}x+\frac{1}{9}\right)+\frac{8}{9}x^2+\frac{8}{9}x+\frac{8}{9}.$$

Logo,

$$\begin{aligned}&(2x^4+3x^3+4x^2+2x+1)-(3x^3+4x^2+4x+1)\left(\frac{2}{3}x+\frac{1}{9}\right)\\&\quad=\frac{8}{9}(x^2+x+1)\\&\Leftrightarrow \frac{9}{8}(2x^4+3x^3+4x^2+2x+1)+\left(\frac{-6}{8}x+\frac{-1}{8}\right)(3x^3+4x^2+4x+1)\\&\quad=(x^2+x+1)\end{aligned}$$

Ou seja, $x^2+x+1=\alpha p+\ \beta q$, com $\alpha=\frac{9}{8}$ e $\beta=\left(\frac{-6}{8}x-\frac{1}{8}\right)$.

Definição 1.2.6

Os polinómios $p_1,p_2,\cdots,p_n \in \mathbb{K}[x]$ dizem-se **primos entre si** se $mdc\ (p_1,p_2,\cdots,p_n)=1$.

O seguinte corolário decorre da Proposição 1.2.5 e da definição anterior.

Corolário 1.2.7

Os polinómios $p_1,p_2,\cdots,p_n \in \mathbb{K}[x]$ são **primos entre si** se e só se existem $\alpha_1,\alpha_2,\cdots,\alpha_n \in \mathbb{R}[x]$ tais que:

$$\alpha_1p_1+\alpha_2p_2+\ \cdots\ +\alpha_np_n=1 \qquad \text{(Identidade de Bézout)}$$

1.3 Polinómios em várias indeterminadas

Um **monómio** em $x_1, \cdots, x_n$, com coeficiente num corpo $\mathbb{K}$, é o produto da forma $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, onde todos os expoentes $\alpha_1, \cdots, \alpha_n$ são inteiros não negativos. O grau total deste monómio é igual à soma $\alpha_1 + \cdots + \alpha_n$. Definindo $\underline{\alpha} := (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ e $\underline{x} := (x_1, \cdots, x_n)$, denotaremos o monómio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ por $\underline{x}^{\underline{\alpha}}$. Quando $\underline{\alpha} = (0, \cdots, 0)$, $\underline{x}^{\underline{\alpha}} = 1$. Chamaremos **multi-expoente** de um monómio $m = \underline{x}^{\underline{\alpha}}$ ao n-uplo $\underline{\alpha}$. O conjunto de todos os monómios em $\underline{x}$ será denotado por $\mathcal{M}_{\underline{x}}$, ou seja, $\mathcal{M}_{\underline{x}} = \{\underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{N}^n\}$.

Um **polinómio** p em $x_1, \cdots, x_n$ com coeficientes num corpo $\mathbb{K}$ é uma combinação linear finita de monómios que se escreve da seguinte forma:

$$p = \sum_{\underline{\alpha} \in \mathcal{A}} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}, \quad a_{\underline{\alpha}} \in \mathbb{K},$$

onde $\mathcal{A} \subset \mathbb{N}^n$ é um conjunto finito de índices.

Seja $p = \sum_{\underline{\alpha}} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$ um polinómio em $x_1, \cdots, x_n$:

i. Dizemos que $a_{\underline{\alpha}}$ é o **coeficiente** do monómio $\underline{x}^{\underline{\alpha}}$, que denotamos por $C(\underline{x}^{\underline{\alpha}}, p)$;

ii. Se $a_{\underline{\alpha}} \neq 0$, então $a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$ é um **termo** de p;

iii. O **grau** total de p é igual ao máximo dos graus dos monómios de cada um dos seus termos.

Denotamos o conjunto de todos os polinómios em $x_1, \cdots, x_n$ com coeficientes no corpo $\mathbb{K}$ por $\mathbb{K}[x_1, \cdots, x_n]$, ou simplesmente $\mathbb{K}[\underline{x}]$.

A proposição que se segue é fundamental para o estudo de ideais de polinómios em várias indeterminadas.

Proposição 1.3.1

$\mathbb{K}[\underline{x}]$ munido com as operações usuais da adição e da multiplicação por um escalar é um anel noetheriano.

Facilmente se prova que $\mathbb{K}[\underline{x}]$ munido com as operações usuais da adição e da multiplicação por um escalar é um anel. O facto de o anel $\mathbb{K}[\underline{x}]$ ser noetheriano decorre do seguinte resultado de índole mais geral.

Teorema 1.3.2

Se A é um anel noetheriano, então qualquer anel de polinómios com um número finito de indeterminadas sobre A é também noetheriano.

Demonstração

A demonstração deste teorema tem por base o lema que se segue.

Lema

Sejam A um anel noetheriano, I um ideal de $A[x_1]$, i um inteiro não negativo e denote-se por $L_i(I)$ o conjunto cujos elementos são o elemento 0 e os coeficientes de x^i nos polinómios pertencentes a I. Então $\{L_i(I)\}$ é uma sequência crescente de ideais em A. Além disso, se J for um ideal de $A[x_1]$ tal que $I \subseteq J$ e $L_i(I) = L_i(J)$, para $i \geq 0$, então $I = J$.

Demonstração do lema

Se $f, g \in I$ e $a \in A$, então $f + g, af, xf \in I$, portanto $L_i(I)$ é um ideal contido em $L_{i+1}(I)$, pelo que $\{L_i(I)\}$ é uma sequência crescente de ideais de A.

Seja $g \in J$ um polinómio de grau i. Como $L_i(I) = L_i(J)$, então existe $f_i \in I$, de grau i, tal que $g - f_i$ tem no máximo grau $i - 1$. Uma vez que I está contido em J, $g - f_i$ pertence a J. Como tal, podemos definir, por indução em j, uma sequência $\{f_{i+j}\}$ $(j = 0, 1, 2, \cdots)$ de elementos de I tal que f_{i+j} é zero ou tem grau $i + j$ e tal que o polinómio $h = g - (f_i + f_{i+1} + \cdots + f_{i+j})$ tem no máximo grau $i - j - 1$. Quando $j = i$, $h = 0$ e portanto $g \in I$. ■

Passando agora à demonstração do teorema, comecemos por considerar o caso de $A[x_1]$.

Seja $\{(I_s), s = 0, 1, \cdots\}$ uma sequência crescente de ideais de $A[x_1]$ e considere-se a sequência dupla $\{L_i(I_j)\}$ de ideais de A. Quando i ou j são fixos, a correspondente sequência simples $\{L_i(I_j)\}$ é crescente. Seja $L_p(I_q)$ o elemento maximal da sequência dupla em cima definida, cuja existência está garantida pelo Teorema 1.1.8. Temos $L_p(I_q) = L_i(I_j)$ se $i \geq p$ e $j \geq q$. Por outro lado, se i for fixo, a c.c.a. garante-nos que existe um inteiro $n(i)$ tal que $L_i(I_j) = L_i(I_{n(i)})$ para todo $j \geq n(i)$. Para $i \geq p$, podemos escolher $n(i) = q$. Portanto existe um inteiro $n_0 = máx\{n(1), \cdots, n(p-1), q\}$ tal que $L_i(I_j) = L_i(I_{n_0})$, para todo i e para todo $j \geq n_0$. Consequentemente, pelo Lema 1.3.2, $I_j = I_{n_0}$ para todo $j \geq n_0$.

Suponhamos agora que $A[x_1, \cdots, x_{n-1}]$ é um anel noetheriano. Uma vez que $A[x_1, \cdots, x_k] = A[x_1, \cdots, x_{k-1}][x_k]$, a nossa hipótese permite concluir que $A[x_1, \cdots, x_n]$ é um anel noetheriano.

Isto prova que $A[x_1, \cdots, x_n]$ é noetheriano ■

O anel $\mathbb{K}[x_1, \cdots, x_n]$ é um bom exemplo de como nem sempre domínios de integridade onde todos os ideais são finitamente gerados são d.i.p. De facto, consideremos, por exemplo, no anel $\mathbb{K}[x_1,\ x_2]$, o ideal gerado por $(x_1,\ x_2)$, $I = I(x_1,\ x_2)$. É claro que este ideal não pode ser gerado por um só elemento, logo $\mathbb{K}[x_1,\ x_2]$ não é um d.i.p.

Para prosseguirmos o estudo dos anéis de polinómios em várias indeterminadas e, nomeadamente, introduzirmos a noção de divisão, definimos em seguida o conceito de ordem admissível. Este conceito assume também particular importância no capítulo seguinte, onde se estudam as bases de Gröbner.

Definição 1.3.3

Chama-se **ordem admissível** a uma relação $\geq$ sobre o conjunto dos monómios $\mathcal{M}_{\underline{x}}$ que satisfaz as seguintes condições:

i. $\geq$ é uma relação de ordem total, ou seja, é uma relação reflexiva, transitiva e anti-simétrica, tal que $\forall m_1, m_2 \in \mathcal{M}_{\underline{x}}$, $m_1 \geq m_2$ ou $m_2 \geq m_1$.

ii. $m_1 \geq m_2 \Rightarrow rm_1 \geq rm_2$, para todos r, m_1, m_2 $\mathcal{M}_{\underline{x}}$, ou seja, $\geq$ é compatível com a multiplicação em $\mathbb{K}[\underline{x}]$;

iii. $r \geq 1$, para todo $r \in \mathcal{M}_{\underline{x}}$.

Nota

É também comum escrever-se $m_2 \leq m_1$ quando temos $m_1 \geq m_2$, $m_2 > m_1$, quando $m_2 \geq m_1$ e $m_2 \neq m_1$, $m_2 < m_1$, quando $m_2 \leq m_1$ e $m_2 \neq m_1$.

Definição 1.3.4

Uma relação de ordem total $\geq$ sobre um conjunto não vazio Σ é uma **boa ordem** se as seguintes condições são satisfeitas:

a) Qualquer subconjunto não vazio de Σ tem um elemento minimal em relação a $\geq$.

b) Qualquer cadeia descendente $s_1 \geq s_2 \geq \cdots$ em Σ é estacionária.

Lema 1.3.5

Uma ordem admissível $\geq$ sobre o conjunto dos monómios $\mathcal{M}_{\underline{x}}$ é uma boa ordem.

Demonstração

Pela alínea *iii.* da definição de ordem admissível, qualquer cadeia descendente $\underline{x}^{\underline{\alpha}_1} \geq \underline{x}^{\underline{\alpha}_2} \geq \underline{x}^{\underline{\alpha}_3} \geq \cdots$ em $\mathcal{M}_{\underline{x}}$ é estacionária.

Basta agora provar que qualquer subconjunto não vazio de $\mathcal{M}_{\underline{x}}$ tem um elemento minimal em relação a $\geq$. Suponhamos que qualquer sequência decrescente de elementos de $\mathcal{M}_{\underline{x}}$ estaciona, mas existe um subconjunto não vazio $S \subset \mathcal{M}_{\underline{x}}$ sem elemento minimal. Seja $\underline{x}^{\underline{\alpha}_1} \in S$, como $\underline{x}^{\underline{\alpha}_1}$ não é elemento minimal de S, então existe $\underline{x}^{\underline{\alpha}_2} \in S$ tal que $\underline{x}^{\underline{\alpha}_1} \geq \underline{x}^{\underline{\alpha}_2}$.

Ora, $\underline{x}^{\underline{\alpha_2}}$ também não é elemento minimal de S e, por isso, existe $\underline{x}^{\underline{\alpha_3}} \in S$ tal que $\underline{x}^{\underline{\alpha_2}} \geq \underline{x}^{\underline{\alpha_3}}$. Continuando desta forma, construímos uma sequência decrescente de elementos

$$\underline{x}^{\underline{\alpha_1}} \geq \underline{x}^{\underline{\alpha_2}} \geq \underline{x}^{\underline{\alpha_3}} \geq \cdots$$

que não é estacionária, o que contraria a hipótese. ■

Apresentamos, em seguida, algumas das ordens admissíveis mais usuais.

Ordem lexicográfica

Sejam $\underline{x}^{\underline{\alpha}}$ e $\underline{x}^{\underline{\beta}}$ dois monómios em $\mathbb{K}[\underline{x}]$. Dizemos que $\underline{x}^{\underline{\alpha}} \geq_{Lex} \underline{x}^{\underline{\beta}}$ se $\underline{x}^{\underline{\alpha}} = \underline{x}^{\underline{\beta}}$ ou a primeira componente não nula de $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$ é positiva, ou seja, se $\alpha_j - \beta_j > 0$ e $\alpha_i - \beta_i = 0,\ 1 \leq i < j$.

Utilizando a ordem lexicográfica as indeterminadas são ordenadas de forma decrescente, isto é $x_1 \geq_{Lex} x_2 \geq_{Lex} \cdots \geq_{Lex} x_n$.

Exemplos

1. $x_1 x_2^2 \geq_{Lex} x_2^3 x_3^4$, uma vez que $(1,2,0) - (0,3,4) = (1,-1,-4)$ tem a primeira componente positiva
2. $x_1^3 x_2^2 x_3^4 \geq_{Lex} x_1^3 x_2^2 x_3$, uma vez que a primeira componente não nula de $(3,2,4) - (3,2,1) = (0,0,3)$ é positiva.

Ordem de grau total-lexicográfica

Sejam $\underline{x}^{\underline{\alpha}}$ e $\underline{x}^{\underline{\beta}}$ dois monómios em $\mathbb{K}[\underline{x}]$. Dizemos que $\underline{x}^{\underline{\alpha}} \geq_{GrLex} \underline{x}^{\underline{\beta}}$ se $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, ou se $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ e $\underline{x}^{\underline{\alpha}} \geq_{Lex} \underline{x}^{\underline{\beta}}$.

Utilizando a ordem grau total-lexicográfica as indeterminadas continuam a ser ordenadas da seguinte forma: $x_1 \geq_{Lex} x_2 \geq_{Lex} \cdots \geq_{Lex} x_n$.

Exemplos

1. $x_1 x_2^2 x_3^3 \geq_{GrLex} x_1^2 x_2^2$ uma vez que $1 + 2 + 3 = 6 > 4 = 2 + 2$.
2. $x_1^2 x_2^2 x_3^2 \geq_{GrLex} x_1 x_2^2 x_3^3$, uma vez que $2 + 2 + 2 = 6 = 1 + 2 + 3$ e $(2,2,2) - (1,2,3) = (1,0,-1)$ tem a primeira componente positiva.

Uma outra ordem admissível (de certa forma menos intuitiva) é a ordem de grau total/lexicográfica reversa.

Ordem de grau total-lexicográfica reversa

Sejam $\underline{x}^{\underline{\alpha}}$ e $\underline{x}^{\underline{\beta}}$ dois monómios em $\mathbb{K}[\underline{x}]$. Dizemos que $\underline{x}^{\underline{\alpha}} \geq_{GrLexRev} \underline{x}^{\underline{\beta}}$ se $\underline{x}^{\underline{\alpha}} = \underline{x}^{\underline{\beta}}$ ou $\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$, ou se $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ a última componente não nula de $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$ é negativa, ou seja, se $\alpha_j - \beta_j < 0$ e $\alpha_i - \beta_i = 0,\ j < i \leq n$.

Utilizando a ordem de grau total-lexicográfica reversa as indeterminadas são igualmente ordenadas da seguinte forma: $x_1 \geq_{Lex} x_2 \geq_{Lex} \cdots \geq_{Lex} x_n$.

Exemplos

1. $x_1^4 x_2^7 x_3 \geq_{GrLexRev} x_1^4 x_2^2 x_3^3$, uma vez que $4 + 7 + 1 = 12 > 9 = 4 + 2 + 3$.
2. $x_1 x_2^5 x_3^2 \geq_{GrLexRev} x_1^4 x_2 x_3^3$, uma vez que $1 + 5 + 2 = 8 = 4 + 1 + 3$ e $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$ tem a última componente negativa.

No caso dos graus totais dos monómios serem diferentes, a ordem de grau total-lexicográfica ($GrLex$) e a ordem de grau total-lexicográfica reversa ($GrLexRev$) ordenam da mesma forma. A diferença entre estas duas ordens reside na ordenação aquando da igualdade dos graus totais. Nesta situação, a $LexGr$ utiliza a ordenação lexicográfica (Lex) e, portanto, dá importância às primeiras indeterminadas favorecendo a de maior expoente. Em contraste, a $GrLexRev$ dá importância às últimas indeterminadas favorecendo a de menor expoente.

Ilustremos através de dois exemplos a diferença entre a $LexGr$ e a $LexGRev$:

1. $x_1^5 x_2 x_3 \geq_{GrLex} x_1^4 x_2 x_3^2$, pois ambos os monómios possuem grau total 7 e $x_1^5 x_2 x_3 \geq_{Lex} x_1^4 x_2 x_3^2$ (a potência da primeira indeterminada em $x_1^5 x_2 x_3$ é maior do que em $x_1^4 x_2 x_3^2$). Neste caso também temos $x_1^5 x_2 x_3 \geq_{GrLexRev} x_1^4 x_2 x_3^2$, mas por outra razão: a menor indeterminada, x_3, aparece com uma potência inferior em $x_1^5 x_2 x_3$.
2. Em relação aos monómios $x_1^5 x_2^3 x_3$ e $x_1^6 x_2 x_3^2$, ambos de grau total 9, temos $x_1^5 x_2^3 x_3 \geq_{GrLexRev} x_1^6 x_2 x_3^2$ e $x_1^6 x_2 x_3^2 \geq_{GrLex} x_1^5 x_2^3 x_3$.

Definição 1.3.6

Fixando uma ordem admissível $\geq$ sobre $\mathbb{K}[\underline{x}]$ considere-se os termos do polinómio

$$p = \sum_{\underline{\alpha}} c_{\underline{\alpha}} \underline{x}^{\underline{\alpha}} \neq 0.$$

i. O **termo-líder** de p (com respeito a $\geq$) é o produto $c_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$, onde $\underline{x}^{\underline{\alpha}}$ é o maior monómio (com respeito a $\geq$) que ocorre em p com $c_{\underline{\alpha}} \neq 0$. Utiliza-se a notação $LT_{\geq}(p)$ ou, simplesmente, $LT(p)$, caso não haja confusão sobre a ordem admissível que está a ser utilizada.

ii. Ao coeficiente do termo-líder de p chama-se **coeficiente-líder** e ao monómio deste termo chama-se **monómio-líder**, denotam-se estes elementos, respectivamente, por $CLM(p)$ e $LM(p)$.

iii. O multi-expoente do monómio-líder é chamado de **multigrau de p** e é denotado por $multigrau(p)$.

Nota

Dados dois polinómios $p, q \in \mathbb{K}[\underline{x}]$, e fixada uma ordem admissível $\geq$ em $\mathcal{M}_{\underline{x}}$, dizemos que $p \geq q$ se $LM(p) \geq LM(q)$, $p \leq q$ se $q \geq p$, $p > q$ se $p \geq q$ e $p \neq q$ e $p < q$ se $p \leq q$ e $p \neq q$.

Exemplo

Consideremos $p = x_1^5 x_2^3 x_3 - x_1^6 x_2 x_3^2 + x_1^7$.

- Como a maior potência em x_1 aparece em x_1^7 temos que

$$LT_{\geq_{Lex}}(p) = x_1^7 \text{ e } multigrau_{\geq_{Lex}}(p) = (7,0,0).$$

- Os graus totais de $x_1^5 x_2^3 x_3$ e de $-x_1^6 x_2 x_3^2$ são iguais a 9 e superiores ao grau total de x_1^7, que é igual a 7. Nos termos com grau total 9, a maior potência em x_1 aparece em $-x_1^6 x_2 x_3^2$ e a menor potência em x_3 aparece em $x_1^5 x_2^3 x_3$, logo

$$LT_{\geq_{LexGr}}(p) = -x_1^6 x_2 x_3^2 \text{ e } LT_{\geq_{LexGRev}}(p) = x_1^5 x_2^3 x_3;$$

$$multigrau_{\geq_{LexGr}}(p) = (6,1,2) \text{ e } multigrau_{\geq_{LexGRev}}(p) = (5,3,1).$$

Algoritmo da divisão

Fixando uma certa ordem sobre os monómios, vamos poder generalizar o já conhecido algoritmo da divisão numa só indeterminada. Em vez de considerarmos a divisão por um só elemento, como acontece no caso dos polinómios numa indeterminada, vamos definir a divisão de um elemento $p \in \mathbb{K}[\underline{x}]$ por s polinómios $(p_1, \cdots, p_s)$. Este processo engloba, naturalmente, a divisão por um só polinómio e coincide com o algoritmo de Euclides, no caso dos polinómios com apenas uma indeterminada.

Proposição 1.3.7 (Algoritmo da divisão em $\mathbb{K}[\underline{x}]$)

Fixando uma ordem admissível $\geq$ qualquer em $\mathbb{K}[\underline{x}]$, seja $P = (p_1, \cdots, p_s)$ um s-uplo ordenado de polinómios em $\mathbb{K}[\underline{x}]$. Então qualquer polinómio $p \in \mathbb{K}[\underline{x}]$ pode ser escrito da seguinte forma:

$$p = a_1 p_1 + \cdots + a_s p_s + r,$$

onde $a_i, r \in \mathbb{K}[\underline{x}]$ são tais que:

i. $LT(a_i p_i) \leq LT(p)$, sempre que $a_i \neq 0$;

ii. $r = 0$ ou r é uma combinação linear de monómios, dos quais nenhum é divisível por $LT(p_i), i = 1 \cdots s$.

A r chama-se **resto da divisão** de p por P.

Demonstração

A existência dos $a_1, \cdots, a_s$ e r é provada pela apresentação do seguinte algoritmo que os determina:

Entrada: $p_1, \cdots, p_s, p$

Saída: $a_1, \cdots, a_s, r$

$a_1 := 0; \cdots ; a_s := 0; r := 0$

$d := p$

$i := 1$

Se $d = 0$ **escreva** mensagem de erro

Enquanto $d \neq 0$ **faça**

ocorreudivisão : = falso

Enquanto $i \leq s$ **e** ocorreudivisão = falso **faça**

se $LT(p_i)$ divide $LT(d)$ **então**

$$a_i := a_i + \frac{LT(d)}{LT(p_i)}$$

$$d := d - \left(\frac{LT(d)}{LT(p_i)}\right) p_i$$

ocorreudivisão : = verdadeiro

senão

$$i := i + 1$$

Fim (**Enquanto** $i \leq s$ **e** ocorreudivisão = falso)

Se ocorreudivisão = falso **então**

$$r := r + LT(d)$$

$$d := d - LT(d)$$

Fim (**Se** ocorreudivisão = falso)

Fim (**Enquanto** $d \neq 0$)

Neste algoritmo d representa o dividendo intermediário em cada passo e a variável booleana *ocorreudivisão* diz-nos quando algum $LT(p_i)$ divide o termo-líder do dividendo intermediário.

Notemos que em cada passo do ciclo "Enquanto … faça" principal, uma das seguintes situações ocorre:

- **Passo de divisão:** Se algum $LT(p_i)$ divide $LT(d)$, então o algoritmo adiciona o valor de $\frac{LT(d)}{LT(p_i)}$ a a_i.
- **Passo de resto:** Se nenhum $LT(p_i)$ divide $LT(d)$, então o algoritmo adiciona $LT(d)$ ao resto.

Para provarmos que o algoritmo funciona, mostraremos inicialmente que a condição

$$p = a_1 p_1 + \cdots + a_s p_s + d + r \qquad (1)$$

é verificada em todos os passos. Nos valores iniciais de $a_1, \cdots, a_s,\ d$ e r esta igualdade é claramente verdadeira. Supondo que em algum ponto do algoritmo esta igualdade é válida, se o passo seguinte for um "passo de divisão", então algum $LT(p_i)$ divide $LT(d)$ e teremos:

$$a_i p_i + d := \left[a_i + \frac{LT(d)}{LT(p_i)}\right] p_i + \left[d - \left(\frac{LT(d)}{LT(p_i)}\right) p_i\right].$$

Este facto mostra-nos que neste passo $a_i p_i + d$ fica inalterado. Como nenhuma outra variável do algoritmo é alterada, a igualdade (1) continua válida.

Consideremos agora que o passo seguinte é um "passo de resto", então d e r serão alterados, contudo a soma $d + r$ manter-se-á inalterada, pois:

$$d + r := [d - LT(d)] + [r + LT(d)],$$

mantendo (1) inalterada. Observemos que o algoritmo pára quando $d = 0$ e, neste caso,

$$p = a_1 p_1 + \cdots + a_s p_s + r.$$

Como só serão adicionados a r termos que não forem divisíveis por $LT(p_i)$, segue que $a_1, \cdots, a_s$ e r possuem as propriedades desejadas quando o algoritmo pára.

Basta agora provar que o algoritmo pára em algum momento.

Notemos que o grau da variável d diminui sempre que d é redefinida ou então torna-se zero. De facto, se durante um "passo de divisão" d for redefinida como

$$d' := d - \left(\frac{LT(d)}{LT(p_i)}\right) p_i,$$

então

$$LT\left(\frac{LT(d)}{LT(p_i)} p_i\right) = \frac{LT(d)}{LT(p_i)} LT(p_i) = LT(d).$$

Logo d e $\left(\frac{LT(d)}{LT(p_i)}\right) p_i$ possuem o mesmo termo-líder e, consequentemente, a sua diferença d', se for não nula, possui grau total estritamente menor que o grau total de d.

Deste modo, nos dois casos, temos que o grau total de d diminui ou, então, torna-se zero.

Se o algoritmo nunca parar, dará origem a uma sequência infinita estritamente decrescente de monómios. A propriedade de boa ordem de $\geq$ referida no Lema 1.3.5 mostra-nos que isso nunca acontece. Assim, em algum momento terá de ser $d = 0$, ou seja, o algoritmo pára depois de algum número finito de passos.

Falta, ainda, estudar a relação entre o grau total de p e o grau total de $a_i p_i$, quando $a_i \neq 0$. Ora, qualquer termo de a_i é da forma $\frac{LT(d)}{LT(p_i)}$, para algum valor da variável d. O algoritmo começa com $d = p$ e, acabámos de ver que, o grau total de d vai diminuindo em cada passo. Logo, $LT(d) \leq LT(p)$, para qualquer valor não nulo da variável d.

Temos também que $LT(a_i) = \frac{LT(d)}{LT(p_i)}$, para algum valor de d, e, assim,

$$LT(a_i p_i) = LT(a_i)LT(p_i) = \frac{LT(d)}{LT(p_i)} LT(p_i) = LT(d) \leq LT(p),$$

concluindo a demonstração. ■

Exemplo

Para ilustrarmos o funcionamento do algoritmo, usaremos a ordem Lex em $\mathbb{R}[x_1, x_2, x_3]$ e dividiremos $p = x_1 x_2^3 x_3^2 + x_1 x_2 x_3^2$ por $p_1 = x_1 x_2 - 1$ e $p_2 = x_2 x_3^2 - 1$.

Inicialmente temos $a_1 = a_2 = r = 0$ e $d = p = x_1 x_2^3 x_3^2 + x_1 x_2 x_3^2$.

- Como $LT(p_1) = x_1 x_2$ divide $LT(d) = x_1 x_2^3 x_3^2$, temos um passo de divisão e

$$a_1 := a_1 + \frac{LT(d)}{LT(p_1)} = 0 + x_2^2 x_3^2 = x_2^2 x_3^2 ,$$

$$d := d - \left(\frac{LT(d)}{LT(p_1)}\right) p_1 = (x_1 x_2^3 x_3^2 + x_1 x_2 x_3^2) - (x_2^2 x_3^2)(x_1 x_2 - 1)$$
$$= x_1 x_2 x_3^2 + x_2^2 x_3^2.$$

- Neste passo, novamente, $LT(p_1)$ divide $LT(d) = x_1x_2x_3^2$, o que origina outro passo de divisão. Assim,

$$a_1 := x_2^2x_3^2 + x_3^2,$$

$$d := (x_1x_2x_3^2 + x_2^2x_3^2) - x_3^2(x_1x_2 - 1) = x_2^2x_3^2 + x_3^2.$$

- Agora, $LT(p_1)$ já não divide $LT(d) = x_2^2x_3^2$, no entanto $LT(p_2) = x_2x_3^2$ divide $LT(d)$, gerando-se, desta forma, mais um passo de divisão.

$$a_2 = x_2 \quad \text{e} \quad d = x_2 + x_3^2.$$

- Uma vez que nem $LT(p_1) = x_1x_2$ nem $LT(p_2) = x_2x_3^2$ dividem $LT(d) = x_2$, ocorre um passo de resto.

$$r := r + LT(d) = 0 + x_2 = x_2,$$

$$d := d - LT(d) = x_2 + x_3^2 - (x_2) = x_3^2.$$

- Para finalizar, ocorre um último passo de resto.

$$r := x_2 + x_3^2 \quad \text{e} \quad d := x_3^2 - x_3^2 = 0.$$

Neste ponto o algoritmo pára retornando os valores

$$a_1 = x_2^2x_3^2 + x_3^2, \ a_2 = x_2 \ \text{e} \ r = x_2 + x_3^2.$$

Deste modo, podemos escrever:

$$p = (x_2^2x_3^2 + x_3^2)(x_1x_2 - 1) + (x_2)(x_2x_3^2 - 1) + (x_2 + x_3^2).$$

Invertendo a ordem da divisão, ou seja, dividindo $p = x_1x_2^3x_3^2 + x_1x_2x_3^2$ primeiro por $p_2 = x_2x_3^2 - 1$ e depois por $p_1 = x_1x_2 - 1$, obtemos o seguinte resultado:

$$p = (x_1x_2^2 + x_1)\,(x_2x_3^2 - 1) + \,(x_2)\,(x_1x_2 - 1) + (x_1 + x_2),$$

o que mostra que os polinómios a_1 e a_2 e o resto encontrados pelo algoritmo da divisão não são unicamente determinados.

Note-se que o algoritmo de divisão apresentado permite escrever qualquer elemento p de $\mathbb{K}[\underline{x}]$ como

$$p = i + r, \quad \text{com } i \in I(p_1 \cdots p_s).$$

Assim, analogamente ao que foi referido no caso dos polinómios numa indeterminada, podemos encarar o resto r como sendo equivalente a p a menos do ideal $I(p_1 \cdots p_n)$ gerado por $p_1 \cdots p_n$.

Note-se que, uma vez que $\mathbb{K}[\underline{x}]$ é um anel noetheriano, todos os seus ideais são finitamente gerados. Isto permite aplicar o algoritmo de divisão para "reduzir" qualquer elemento relativamente a um ideal. Como ilustrado no exemplo anterior, o resultado desta operação não é único. Este problema será ultrapassado no capítulo que se segue com a introdução das bases de Gröbner.

2

Bases de Gröbner e equações às diferenças

2.1 Bases de Gröbner

Seja $\mathcal{R} := \mathbb{K}[\underline{x}]$ e consideremos um subconjunto finito $F \subseteq \mathcal{R}$. Dizemos que $r \in \mathcal{R}$ se **reduz** a $h \in \mathcal{R}$ **módulo** F e escrevemos $r \longrightarrow_F h$, se existem $f \in F, b \in \mathbb{K}$ e $m \in \mathcal{M}_{\underline{x}}$ tais que:

i. $b = \frac{C(LM(mf),r)}{CLM(f)}$;

ii. $C(LM(mf), r) \neq 0$;

iii. $h = r - bmf$.

Dizemos que h está na **forma normal módulo F** se não existe nenhum $h' \in \mathcal{R}$ tal que $h \longrightarrow_F h'$. Se h estiver na **forma normal módulo F** e existe uma cadeia finita $r \longrightarrow_F r_1 \longrightarrow_F \cdots \longrightarrow_F h$, então dizemos que h é uma **forma normal de r módulo F**.

A redução de um elemento $r \in \mathcal{R}$ módulo F pode explicar-se da seguinte forma: dado $r \in \mathcal{R}$, utilizamos monómios maximais dos elementos de $f \in F$, multiplicados por constantes (b) e monómios (m) adequados, para eliminar monómios de r. Em particular, o monómio-líder de f é usado para suprimir o monómio mf de r pelo que obtemos $C(LM(mf), h) = 0$.

Exemplo

Consideremos o anel $\mathbb{R}[x, y]$ e fixemos a ordem lexicográfica. Seja $F = \{x^2 - xy\}$. O polinómio $2x^3$ reduz-se a $2x^2y$ módulo F, $2x^3 \longrightarrow_F 2x^2y$. De facto, temos que:

i. $2 = \frac{C(LM(x^3 - x^2y), 2x^3)}{CLM(x^2 - xy)}$;

ii. $C\big(LM\big(x(x^2 - xy)\big), 2x^3\big) = C(LM(x^3 - x^2y), 2x^3) = 2 \neq 0$;

iii. $2x^2y = 2x^3 - 2x(x^2 - xy)$, com $2 \in \mathbb{R}$ e $x \in \mathcal{M}_{\underline{x}}$.

É de salientar que a obtenção da forma normal, h, de um elemento $q \in \mathcal{R}$ módulo $F = \{p\}$ corresponde ao processo de divisão de q por p, sendo h o resto da divisão de q por p. De facto, na divisão de q por p obtemos $q = ap + h$, com $LT(aq) \leq LT(p)$, se $a \neq 0$, sendo h nulo ou então igual a uma combinação linear de monómios, nenhum dos quais divisíveis por $LT(p)$.

Do primeiro passo da divisão resulta que $q = bmp + h$, onde m é um monómio e b é uma constante escolhida de modo a anular o LM de mp em q, supondo-se que $C(LM(mp), q) \neq 0$. Em h já não aparece $LM(mp)$. Este passo é coincidente com o primeiro passo de redução, $q \longrightarrow_F h$.

Se $LT(p)$ for menor ou igual a algum termo de h, efectuamos os mesmos passos que anteriormente, obtendo assim um segundo passo de redução, $h \longrightarrow_F h_1$. Deste modo,

$$h = b_1 m_1 p + h_1$$
$$q = bmp + b_1 m_1 p + h_1 = (bm + b_1 m_1)p + h_1$$

Este processo pára quando $LT(p)$ for estritamente maior do que qualquer termo de h. No final teremos que $C(LM(mp), h_k) = 0$, para todo o monómio m.

Por outro lado, na redução sucessiva de q módulo $F = \{p\}$, a ideia principal é usar o LT de p para suprimir monómios de q, de forma a obtermos as seguintes expressões:

$$q = bmp + h$$
$$h = b_1 m_1 p + h_1$$
$$q = bmp + b_1 m_1 p + h_1 = (bm + b_1 m_1)p + h_1$$
$$\dots$$

Procedemos desta forma sucessivamente e paramos quando já não pudermos reduzir h_k módulo $\{p\}$, isto é, quando $\forall m\ C(LM(mp), h_k) = 0$.

Podemos, portanto, concluir que a divisão de q por p coincide com a redução sucessiva de q módulo $F = \{p\}$.

Do mesmo modo é possível verificar que a obtenção da forma normal de um elemento $r \in \mathcal{R}$ módulo $F = \{p_1, \cdots, p_s\}$ corresponde ao processo de divisão de r por $\{p_1, \cdots, p_s\}$.

Exemplo

Consideremos o anel $\mathbb{R}[x, y]$ e fixemos a ordem lexicográfica. Seja $F = \{x^2 - xy\}$. Vamos comparar a divisão de x^3 por $x^2 - xy$ com a redução de x^3 à sua forma normal módulo F.

1) Divisão de $2x^3$ por $x^2 - xy$	2) Redução sucessiva de $2x^3$ módulo $F = \{x^2 - xy\}$
$\begin{array}{r\|l} 2x^3 & x^2 - xy \\ \hline -2x^3 + 2x^2y & 2x \\ \hline 2x^2y & \end{array}$	Como vimos no exemplo anterior, temos que: $$2x^3 \longrightarrow_F 2x^2y.$$
$\begin{array}{r\|l} 2x^2y & x^2 - xy \\ \hline -2x^2y + 2xy^2 & 2y \\ \hline 2xy^2 & \end{array}$	Continuando com a redução sucessiva vem: $$2x^2y \longrightarrow_F 2xy^2,$$ De facto, as seguintes condições são verificadas: i. $2 = \frac{C(LM(x^2y - xy^2), 2x^2y)}{CLM(x^2 - xy)}$; ii. $C(LM(x^2y - xy^2), 2x^2y) = 2 \neq 0$; iii. $2xy^2 = 2x^2y - 2y(x^2 - xy)$.
Pelo algoritmo da divisão de Euclides temos que: $$2x^3 = (2x + 2y)(x^2 - xy) + 2xy^2.$$ Resto da divisão: $2xy^2$	Como $LM(2xy^2) < LM(x^2 - xy)$, $2xy^2$ encontra-se na forma reduzida módulo $x^2 - xy$. Dado a que temos a seguinte cadeia: $$2x^3 \longrightarrow_F 2x^2y \longrightarrow_F 2xy^2$$ podemos concluir que $2xy^2$ é a forma

normal de $2x^3$ módulo $F = \{x^2 - xy\}$.

Como podemos verificar, a forma normal de $2x^3$ módulo $F = \{x^2 - xy\}$ corresponde ao resto da divisão de $2x^3$ por $x^2 - xy$.

Definição 2.1.1

Seja $\leq$ uma ordem total de $\mathcal{M}_{\underline{x}}$, $F \subseteq \mathcal{R}$ um conjunto finito e I um ideal de $\mathcal{R}$. Diz-se que F é uma **base de Gröbner** de I se as seguintes condições forem satisfeitas:

i. $I = I(F)$;

ii. Para todo $r \in \mathcal{R}$, a forma normal de r módulo F é única.

Uma base de Gröbner F é uma **base de Gröbner reduzida** se qualquer $f \in F$ estiver na forma normal módulo $F \backslash \{f\}$ e $CLM(f) = 1$.

Salientamos o facto de uma base de Gröbner não ser uma verdadeira base, uma vez que os seus elementos não são necessariamente independentes.

Dado um conjunto $F = \{f_1, \cdots, f_s\}$ de geradores do ideal $I = I(F)$ é sempre possível construi uma base de Gröbner de I .

O algoritmo para a construção de uma base de Gröbner de $I = I(F)$ utiliza o conceito de S-polinómio definido da forma que se segue.

Definição 2.1.2

Sejam f_1, f_2 dois polinómios mónicos, isto é, com $CLT(f_1) = CLT(f_2) = 1$. Chamamos S-polinómio de f_1 e f_2 a:

$$SP(f_1, f_2) \coloneqq \frac{mmc\big(LM(f_1), LM(f_2)\big)}{LM(f_1)} \cdot f_1 - \frac{mmc\big(LM(f_1), LM(f_2)\big)}{LM(f_2)} \cdot f_2,$$

onde $mmc\big(LM(f_1), LM(f_2)\big)$ é o mínimo múltiplo comum entre $LM(f_1)$ e $LM(f_2)$, ou seja, se $\text{multigrau}(f_1) = (\alpha_1, \cdots, \alpha_k)$, $\text{multigrau}(f_2) = (\beta_1, \cdots, \beta_k)$ e $\underline{\gamma} = (\gamma_1, \cdots, \gamma_k)$, com $\gamma_i = \max(\alpha_i, \beta_i)\,, i = 1 \cdots n$, $mmc\big(LM(f_1), LM(f_2)\big) = \underline{x}^{\underline{\gamma}}$.

O objectivo da utilização do conceito de S-polinómio, no algoritmo de construção de uma base de Gröbner, é que o $mmc\big(LM(f_1), LM(f_2)\big)$ é o primeiro monómio que pode ser reduzido tanto usando f_1 como usando f_2, podendo ser originada em cada um dos casos uma forma reduzida diferente. Esta situação tem que ser evitada na construção de uma base de Gröbner, onde qualquer elemento tem redução única módulo a base em questão.

O algoritmo para construir um base de Gröbner, que apresentamos em seguida, foi proposto por B. Buchberger em 1985.

Algoritmo para construir uma base de Gröbner

Dados de entrada: $F = \{f_1, \cdots, f_s\}$
Dados de saída: G, tal que $I(F) = I(G)$ e G é uma base de Gröbner

$G \coloneqq F$
$B \coloneqq \big\{\{f_1, f_2\} \mid f_1, f_2 \in G, f_1 \neq f_2\big\}$
Enquanto $B \neq \emptyset$ **fazer**
    $\{f_1, f_2\} \coloneqq$ par em B
    $B \coloneqq B - \big\{\{f_1, f_2\}\big\}$
    $h \coloneqq SP(f_1, f_2)$
    $h' \coloneqq$ forma normal de h módulo G
    Se $h' \neq 0$ então
        $B \coloneqq B \cup \big\{\{g, h'\} \mid g \in G\big\}$
        $G \coloneqq G \cup \{h'\}$

Exemplo

Seja $F = \{f_1, f_2\}$ um subconjunto de $\mathbb{R}[x_1, x_2]$ onde:

$$f_1 = x_1^2,$$
$$f_2 = x_1x_2 + x_2^2.$$

Vamos determinar uma base de Gröbner relativamente à ordem lexicográfica para o ideal $I = I(F)$ utilizando o algoritmo supracitado.

Comecemos com $B = \{(f_1, f_2)\}$ e calculemos o S-polinómio de f_1 e f_2. Verifica-se que

$$SP(f_1, f_2) = -x_1x_2^2.$$

Reduzindo este polinómio à sua forma normal módulo G obtemos o polinómio

$$x_2^3.$$

Como o polinómio obtido é diferente do polinómio nulo, de acordo com o algoritmo devemos acrescentar a G o polinómio

$$f_3 = x_2^3,$$

e obtemos $B = \{(f_1, f_3), (f_2, f_3)\}$.

Escolhendo agora para eliminar de B, por exemplo, o par (f_1, f_3), ficamos com o novo conjunto $B = \{(f_2, f_3)\}$. Além disso, $h = SP(f_1, f_3) = 0 \longrightarrow_G 0 = h'$.

Repetindo o processo para o par (f_2, f_3) obtemos $B = \emptyset$ e $SP(f_2, f_3) = x_2^4$.

Reduzindo este polinómio à sua forma normal módulo G obtemos o polinómio nulo. Como $B = \emptyset$ o algoritmo pára e podemos concluir que o conjunto $G = \{f_1, f_2, f_3\}$ é uma base de Gröbner para o ideal gerado por f_1 e f_2.

As bases de Gröbner gozam de algumas propriedades importantes que passamos a enunciar.

Propriedades 2.1.3

Fixemos uma ordem total em $\mathcal{M}_{\underline{x}}$.

1. Seja $F \subseteq \mathcal{R}$ uma base de Gröbner e suponhamos que, para $h \in \mathcal{R}$, $LM(h) < LM(f)$ para todo $f \in F$. Então h está na forma normal módulo F.
2. Se F é uma base de Gröbner e $r \in \mathcal{R}$ é tal que $r = f + h$, com $f \in I(F)$ e $h \in \mathcal{R}$ está na forma normal módulo F, então h é uma forma normal de r módulo F.
3. Uma base de Gröbner reduzida de um ideal $I \subset \mathcal{R}$ é única.
4. $I(F) = \mathcal{R}$ se e só se a base de Gröbner reduzida de $I(F)$ for $\{1\}$.

Demonstração

1. Seja $F \subseteq \mathcal{R}$ uma base de Gröbner e $h \in \mathcal{R}$ tal que $LM(h) < LM(f)$ para todo $f \in F$.

   Suponhamos que h não está na forma normal módulo F, isto é, existe $h' \in \mathcal{R}\backslash\{h\}$ tal que h se reduz a h'. Então, existem $b \in \mathbb{K}, m \in \mathcal{M}_{\underline{x}}$ e $f_1 \in F$ tais que: $h' = h - bmf_1$ e $C(LM(mf_1), h) \neq 0$. Isto implica que $LM(mf_1) \leq LM(h)$ e portanto que $LM(f_1) \leq LM(h)$, o que contraria a hipótese.

2. Sejam F uma base de Gröbner e $r \in \mathcal{R}$ tais que $r = f + h$, onde $f \in I(F)$ e $h \in \mathcal{R}$ está na forma normal módulo F. Uma vez que $f \in I(F)$, $f \longrightarrow_F 0$. Então $r = f + h \longrightarrow_F h$. Como h está na forma normal módulo F, concluímos que h é uma forma normal de r módulo F.

3. Sejam F e $\tilde{F}$ duas bases de Gröbner reduzidas de um ideal $I \subseteq \mathcal{R}$. Então $\tilde{F} \subseteq I(F)$ e $F \subseteq I(\tilde{F})$. Assim, para todo $f \in F$

$$f \longrightarrow_{\tilde{F}} 0.$$

Deste modo existe $\tilde{f} \in \tilde{F}$ tal que $LT(\tilde{f}) \mid LT(f)$ (pois caso contrário $LT(f)$ estaria no resto da divisão de f por $\tilde{F}$).

Da mesma forma, para todo $\tilde{f} \in \tilde{F}$

$$\tilde{f} \longrightarrow_F 0$$

e portanto existe $f' \in F$ tal que $LT(f') \mid LT(\tilde{f})$, consequentemente $LT(f') \mid LT(f)$, onde f' e f pertencem a F. Como F é uma base de Gröbner reduzida, $f' = f$. Logo $LT(\tilde{f}) \mid LT(f)$ e $LT(f) \mid LT(\tilde{f})$.

Desta forma, para todo elemento $f \in F$ existe um elemento $\tilde{f} \in \tilde{F}$ tal que $LT(f) = LT(\tilde{f})$ e vice-versa, ou seja, F e $\tilde{F}$ têm o mesmo número de elementos e o conjunto dos termos-líder de F é igual ao conjunto dos termos-líder de $\tilde{F}$.

Consideremos $f - \tilde{f} \in I$, então

$$f - \tilde{f} \longrightarrow_F 0.$$

Vimos que $LT(f) = LT(\tilde{f})$, portanto estes termos cancelam-se. Os restantes termos de $f - \tilde{f}$ não são divisíveis por nenhum dos elementos de F. De facto, uma vez que f está na forma normal módulo $F\backslash\{f\}$, nenhum dos seus termos é divisível pelos termos-líder dos elementos de $F\backslash\{f\}$. Do mesmo modo, nenhum dos termos de $\tilde{f}$ é divisível pelos termos líder de $\tilde{F}\backslash\{\tilde{f}\}$. Uma vez que os termos-líder dos elementos de F e de $\tilde{F}$ coincidem, podemos concluir que nenhum dos termos de $f - \tilde{f}$ é divisível pelos termos-líder dos elementos de F. Portanto $f - \tilde{f}$ está na forma normal módulo F. Como por outro lado se tinha visto que $f - \tilde{f} \longrightarrow_F 0$, obtém-se que $f = \tilde{f}$, o que permite concluir que $F = \tilde{F}$.

4. Se $I(F) = \mathcal{R}$ então $1 \in I(F)$ e $\{1\}$ é uma base de Gröbner reduzida para $I(F)$. Uma vez que a base de Gröbner reduzida é única conclui-se que esta base é $\{1\}$. ■

No que se segue, a base de Gröbner reduzida de um ideal I será denotada por $BG(I)$.

Observação

Se $I = I(f)$ então $F = \{f\}$ é uma base de Gröbner para I e $\forall r \in I, \quad r \longrightarrow_F 0$. Caso f seja um polinómio mónico, então $F = \{f\}$ é uma base de Gröbner reduzida para I. Em particular, seja $\mathbb{K}[x]$ o anel de polinómios numa indeterminada x e com coeficientes em $\mathbb{K}$. Se $\leq_{\mathcal{M}_x}$ é uma ordem de $\mathcal{M}_x$ tal que $x^i \leq_{\mathcal{M}_x} x^j \Leftrightarrow i \leq j$ (onde agora $\leq$ é a ordem usual em $\mathbb{N}$), então, dado um conjunto $F = \{f_1, \cdots, f_k\} \subseteq \mathbb{K}[x]$, a base reduzida de Gröbner de $I(F)$ é apenas constituída pelo máximo divisor comum mónico d de $f_1, \cdots, f_k$, uma vez que $I(F) = I(d)$.

Exemplo

Consideremos o anel $\mathbb{R}[x]$ e os polinómios $f_1 = x^2 - 1$, $f_2 = x^2 - 2x + 1$, cujo máximo divisor comum é $x + 1$ ($mdc\ (f_1, f_2) = x + 1$). Verifica-se que:

i. $I(x + 1) = I(f_1, f_2)$;
ii. Para todo $r \in I(x + 1)$, $r = \gamma(x + 1)$, para algum $\gamma \in \mathbb{R}[x]$, sendo a forma normal de r módulo $(x + 1)$ única, já que coincide obviamente com o polinómio nulo.

Concluímos deste modo que são verificadas as condições da Definição 2.1.1, pelo que $F = \{x + 1\}$ é uma base de Gröbner para o ideal considerado.

Daqui em diante centraremos a nossa atenção no estudo de ideais de $\mathbb{K}[x_1, x_2]$. Além disso consideraremos apenas a ordem lexicográfica (que nos escusaremos de referir), uma vez que se trata da ordem relevante para a aplicação a considerar na Secção 2.2.

A proposição que se segue afirma que os multigraus dos elementos da base de Gröbner reduzida de I são minimais no conjunto dos multigraus dos elementos de I. Trata-

se de um resultado fundamental para o estudo dos sistemas de equações às diferenças parciais a levar a cabo na próxima secção.

Sejam $E \subseteq \mathbb{K}[x_1, x_2]$ e $S(E) \coloneqq \{LM(e) : e \in E\}$ um conjunto de polinómios e o conjunto dos correspondentes monómios-líder, respectivamente. Definamos $\mathcal{T}(E) \coloneqq \bigcup_{i,j \geq 0}\{x_1^i x_2^j S(E)\}$ e $\varepsilon(E) \coloneqq \{t \in \mathcal{T}(E) \mid t \notin x_1\mathcal{T}(E) \text{ e } t \notin x_2\mathcal{T}(E)\}$. Note-se que $\mathcal{T}(E)$ é o conjunto dos monómios-líder dos elementos do ideal gerado por E e $\varepsilon(E)$ é o conjunto dos elementos minimais de $\mathcal{T}(E)$.

Proposição 2.1.4

Seja $F \subseteq \mathbb{K}[x_1, x_2]$ uma base de Gröbner reduzida. Então as seguintes condições são satisfeitas.

i. Para qualquer monómio $m \in S(F)$ há um único elemento $f \in F$ tal que $LM(f) = m$;

ii. $S(F) = \varepsilon\big(I(E)\big)$.

Para provarmos a segunda parte desta proposição é conveniente demonstrar o lema que se segue.

Lema 2.1.5

Seja $F = \{f_1 \leq f_2 \leq \cdots \leq f_n\} \subseteq \mathbb{K}[x_1, x_2]$ uma base de Gröbner reduzida e, para todo $f \in \mathcal{R}$, denotemos, respectivamente, por $d_1(f)$ e por $d_2(f)$ os expoentes de x_1 e de x_2 do monómio-líder de f. Então:

1. $d_1(f_1) < d_1(f_2) < \cdots < d_1(f_n)$ e $d_2(f_1) > d_2(f_2) > \cdots > d_2(f_n)$.

2. $f_1 \leq f$, para todo $f \in I(F)\backslash\{0\}$.

3. Se $0 \neq f \in I(F)$ e $f_k \leq f < f_{k+1}$, então $d_1(f) < d_1(f_{k+1})$, $d_2(f) \geq d_2(f_k)$ e além disso $f \in I(f_1, \cdots, f_k), k = 1, \cdots, n-1$. Se $0 \neq f \in I(F)$ e $f_n \leq f$, então $d_2(f) \geq d_2(f_n)$.

Demonstração

1.

Suponhamos que $f_k, f_{k+1} \in F$ e $d_1(f_k) = d_1(f_{k+1}) =: d$. Então $f_k(x_1, x_2) = \varphi_d(x_2)x_1^d + \cdots + \varphi_1(x_2)x_1 + \varphi_0(x_2)$ e $f_{k+1}(x_1, x_2) = \psi_d(x_2)x_1^d + \cdots + \psi_1(x_2)x_1 + \psi_0(x_2)$, para determinados polinómios φ_i, ψ_i $(i = 1, \cdots, d)$, com $\varphi_d \neq 0 \neq \psi_d$. Além disso, o grau de $\psi_d(x_2)$ terá que ser maior ou igual do que o grau de $\varphi_d(x_2)$, pois $f_k \leq f_{k+1}$. Desta forma, é claro que f_{k+1} pode ser reduzido módulo $F\backslash\{f_{k+1}\}$ e, como tal, F não é uma base de Gröbner reduzida, o que contraria a hipótese. Logo, podemos concluir que $d_1(f_k) < d_1(f_{k+1})$.

Suponhamos agora que $d_2(f_{k+1}) \geq d_2(f_k)$. Então f_{k+1} pode ser reduzido usando f_k, contrariando o facto de que F é uma base de Gröbner reduzida. Portanto $d_2(f_{k+1}) < d_2(f_k)$.

2.

Seja $0 \neq f \in I(F)$ e suponhamos que $f < f_1$. Então $f < h$ para todo $h \in F$ e, pela Propriedade 2.1.3 (1.), f está na forma normal módulo F. Por outro lado, pela Propriedade 2.1.3 (2.), 0 é também uma forma normal de f módulo F, o que contraria o facto de F ser uma base de Gröbner. Logo, $f_1 \leq f$, para todo $0 \neq f \in I(F)$.

3.

Seja $0 \neq f \in I(F)$ e suponhamos que $f_k \leq f < f_{k+1}$ para algum $k \in \{1, \cdots, n-1\}$. Além disso, assumamos que $d_1(f) = d_1(f_{k+1})$ (pelo que $d_2(f) < d_2(f_{k+1})$). Então usando qualquer um dos f_i's, $i = 1, \cdots, n-1$, o monómio-líder de f não pode ser suprimido, o que implica que a forma normal de f é um polinómio não nulo. Por outro lado, como $f \in I(F)$ a Propriedade 2.1.3 (2.) diz-nos que 0 é a forma normal de f módulo F, o que é um absurdo. Então concluímos que $d_1(f) < d_1(f_{k+1})$. De forma análoga se prova que $d_2(f) \geq d_2(f_k)$.

Suponhamos que $f \notin I(f_1, \cdots, f_k)$ e seja f' a forma normal de f módulo $I(f_1, \cdots, f_k)$. Então $f' \neq 0$, $f' < f_{k+1}$ e $f' \in I(F)$, portanto f' pode ser reduzido a 0 módulo F. Além disso, como f' está na forma normal módulo $I(f_1, \cdots, f_k)$, f' não pode ser reduzido usando qualquer um dos f_i's, $i = 1, \cdots, k$. Então, f' reduz-se a 0 módulo $\{f_{k+1}, \cdots, f_n\}$, o que significa que $f_j \in \{f_{k+1}, \cdots, f_n\}$ pode ser usado para suprimir o monómio-líder de f', o que é um absurdo, uma vez que $f' < f_{k+1} \leq \cdots \leq f_n$. Assim, concluímos que $f \in I(f_1, \cdots, f_k)$.

Seja agora $0 \neq f \in I(F)$ tal que $f_n \leq f$. Se $d_2(f) < d_2(f_n)$, então facilmente se verifica por, 1., que não é possível suprimir o monómio-líder de f na redução módulo $\{f_1, \cdots, f_n\}$. Isto implica que a forma normal de f módulo F é um polinómio não nulo, o que é um absurdo uma vez que $f \in I(F)$. Logo, $d_2(f) \geq d_2(f_n)$. ■

Demonstração da Proposição 2.1.4

i.

Seja $F \subseteq \mathbb{K}[x_1, x_2]$ uma base de Gröbner reduzida. Por definição de $S(F)$, para todo $m \in S(F)$ existe $f \in F$ tal que $m = LM(f)$.

Suponhamos que existem $f_1, f_2 \in F$ tal que $m = LM(f_1) = LM(f_2)$ e $f_1 \neq f_2$. Então f_1 pode ser pode ser reduzido usando f_2 (e reciprocamente) e, portanto, f_1 não está na forma normal módulo $F \backslash \{f_1\}$, o que contradiz o facto de F ser uma base de Gröbner reduzida. Logo, $f_1 = f_2$, ou seja, para qualquer $m \in S(F)$ existe um único elemento $f \in F$ tal que $LM(f) = m$.

ii.

O facto de que $S(F) = \varepsilon\big(I(E)\big)$ decorre facilmente do Lema 2.5. ■

Dado um conjunto F de polinómios, denotemos por $\mathfrak{M}(F)$ o conjunto dos multigraus dos elementos de $I(F)$, isto é, $\mathfrak{M}(F) := \{multigrau(i) : i \in I(F)\}$. As Figuras 1 e 2 ilustram o tipo de forma que o conjunto $\mathfrak{M}(F)$ pode assumir.

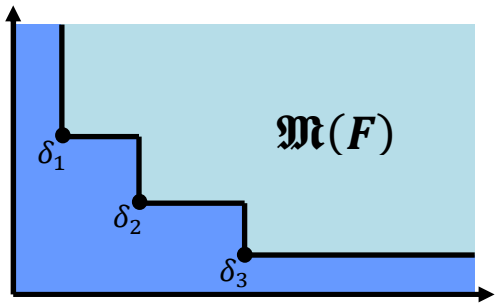


Figura 1
Legenda: $\{f_1, f_2, f_2\} = BG(I(F))$
$\delta_i = multigrau(f_i),\ \ i = 1,2,3$

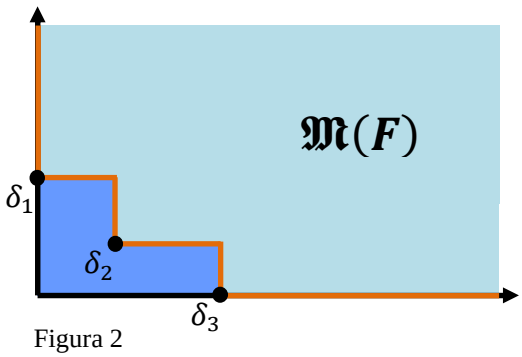


Figura 2
Legenda: $\{f_1, f_2, f_2\} = BG(I(F))$
$\delta_i = multigrau(f_i),\ \ i = 1,2,3$

As situações representadas nas Figuras 1 e 2 diferem pelo facto de numa delas $\mathbb{N}^2\backslash\mathfrak{M}(F)$ ser finito e noutra ser infinito. A Proposição a seguir mencionada dá-nos uma condição necessária e suficiente para que $\mathbb{N}^2\backslash\mathfrak{M}(F)$ seja finito.

Proposição 2.1.6

Seja F um subconjunto finito de $\mathbb{K}[x_1, x_2]$. Então $\mathbb{N}^2\backslash\mathfrak{M}(F)$ é finito se e só se os elementos de F são primos entre si.

Demonstração

(⇐): Seja $F = \{f_1, \cdots, f_k\} \subseteq \mathbb{K}[x_1, x_2]$ e suponhamos que $f_1, \cdots, f_k$ não são primos entre si. Então $d = mdc(f_1, \cdots, f_k) \neq 1$. Como $\mathfrak{M}(F) \subset \mathfrak{M}(d)$, $\mathbb{N}^2\backslash\mathfrak{M}(d) \subset \mathbb{N}^2\backslash\mathfrak{M}(F)$. Mas, sendo $d \neq 1$, $\mathbb{N}^2\backslash\mathfrak{M}(d)$ é infinito, e por isso também $\mathbb{N}^2\backslash\mathfrak{M}(F)$ será infinito. Podemos desta forma concluir que se $\mathbb{N}^2\backslash\mathfrak{M}(F)$ for finito então os elementos de F são primos entre si.

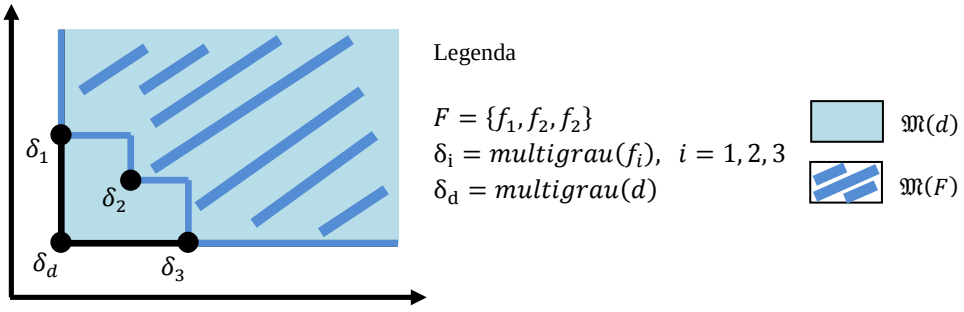


Figura 3

(⇒): Comecemos por provar um facto essencial à demonstração desta proposição.

Lema

Seja $F = \{f_1, \cdots, f_k\} \subseteq \mathbb{K}[x_1, x_2]$ um conjunto de polinómios primos entre si. Então existe em $I(F)$ um polinómio p_1 só em x_1 e um polinómio p_2 só em x_2.

Demonstração do Lema

Seja $F = \{f_1, \cdots, f_k\} \subseteq \mathbb{K}[x_1, x_2]$ tal que $mdc(f_1, \cdots, f_k) = 1$. Denotemos por $\mathbb{K}(x)$ o corpo das fracções associado ao anel $\mathbb{K}[x]$.

Encaremos $f_1, \cdots, f_k$ como elementos de $\mathbb{K}(x_1)[\,x_2]$, ou seja, com polinómios em x_2 com coeficientes racionais em x_1. Não é difícil verificar que se $mdc(f_1, f_2) = 1$ em $\mathbb{K}[x_1, x_2]$, então $mdc(f_1, f_2) = 1$ em $\mathbb{K}(x_1)[\,x_2]$.

Como $\mathbb{K}(x_1)[\,x_2]$ é um domínio euclidiano, existem $\alpha_1, \cdots, \alpha_k \in \mathbb{K}(x_1)[\,x_2]$ tais que:

$$\alpha_1 f_1 + \cdots + \alpha_r f_k = 1.$$

Escrevendo $\alpha_i = \frac{\eta_i}{\beta}$, $\eta_i \in \mathbb{K}[\,x_1, x_2]$, $\beta \in \mathbb{K}[x_1]$, $i = 1, \cdots, k$ temos que:

$$\eta_1 f_1 + \cdots + \eta_k f_k = \beta.$$

Portanto, $p_1 = \beta$ é um polinómio em x_1 pertencente a $I(f_1, \cdots, f_k)$.

Analogamente se prova que existe um polinómio p_2 em x_2 tal que $p_2 \in I(f_1, \cdots, f_k)$. ■

Seja $F = \{f_1, \cdots, f_k\} \subseteq \mathbb{K}[x_1, x_2]$ um conjunto formado por polinómios $f_1, \cdots, f_k$ primos entre si. Então, como vimos no lema supracitado, existem em $I(F)$ um polinómio p_1 só em x_1 e um polinómio p_2 só em x_2. Designando $\delta \coloneqq grau(p_1)$ e $\theta \coloneqq grau(p_2)$, conclui-se que $(0, \theta)$ e $(\delta, 0)$ são elementos de $\mathfrak{M}(F)$, pelo que $\mathbb{N}^2 \backslash \mathfrak{M}(F)$ é finito. ■

2.2 Sistemas de equações às diferenças parciais

Nesta secção vamos estudar o problema do cálculo recursivo das soluções de sistemas de equações às diferenças (parciais) lineares e de coeficientes constantes.

Estas equações são do tipo:

$$\sum_{\underline{l}\in L} \alpha_{\underline{l}} w(\underline{k}+\underline{l}) = 0, \qquad \forall \underline{k} \in T$$

onde $T = \mathbb{N}^n$ (convencionando-se que $0 \in \mathbb{N}$), n é um número natural positivo, $\underline{k} \coloneqq (k_1, \cdots, k_n) \in \mathbb{N}^n$, o multi-índice $\underline{l} \coloneqq (l_1, \cdots, l_n)$ percorre o conjunto finito $L \subset T$, $\alpha_{\underline{l}} \in \mathbb{R}$ e a sequência multidimensional (nD) $w \in \mathbb{R}^T = \mathbb{R}^{\mathbb{N}^n}$, onde $\mathbb{R}^{\mathbb{N}^n}$ designa o conjunto de todas as sequências reais nD, isto é, de todas as funções de $\mathbb{N}^n$ em $\mathbb{R}$.

No caso $n = 1$, obtemos uma equação às diferenças (totais).

$$\alpha_p w(k+p) + \alpha_{p-1} w(k+p-1) + \cdots + \alpha_1 w(k+1) + \alpha_0 w(k) = 0, k \in \mathbb{N} \quad (1)$$

Definindo o deslocamento

$$\begin{aligned} \sigma : \mathbb{R}^{\mathbb{N}} &\longrightarrow \mathbb{R}^{\mathbb{N}} \\ w &\longmapsto \sigma w \end{aligned}$$

tal que $\sigma w(k) = w(k+1)$ e $\sigma^l = \sigma^{l-1} \circ \sigma$, (1) pode ser escrito como

$$\left(\alpha_p \sigma^p + \alpha_{p-1}\sigma^{p-1} + \cdots + \alpha_0\right) w(k) = 0.$$

Introduzindo o operador linear às diferenças $p(\sigma) = \alpha_p \sigma^p + \alpha_{p-1}\sigma^{p-1} + \cdots + \alpha_0$ associado ao polinómio $p(x) = \alpha_p x^p + \alpha_{p-1} x^{p-1} + \cdots + x_0$, (1) pode ser reescrito como

$$p(\sigma) w = \underline{0},$$

onde $\underline{0}$ designa a sequência nula.

É de salientar que a composição dos operadores lineares às diferenças corresponde à multiplicação dos polinómios correspondentes, isto é, $p(\sigma) \circ q(\sigma) = t(\sigma)$, com $t(x) = p(x)q(x)$, como podemos constatar no exemplo que se segue.

Exemplo

Consideremos $p(x) = x + 1$ e $q(x) = x - 1$.

$$\begin{aligned}\big(p(\sigma) \circ q(\sigma)\big)w &= p(\sigma)(q(\sigma)w) \\ &= p(\sigma)(\sigma w - w) \\ &= \sigma(\sigma w - w) + (\sigma w - w) \\ &= \sigma^2 w - \sigma w + \sigma w - w \\ &= \sigma^2 w - w \\ &= (\sigma^2 - 1)w\end{aligned}$$

Por outro lado, definindo $t(x) = p(x)q(x)$, obtém-se

$$t(x) = (x + 1\,)(x - 1\,) = x^2 - 1,$$

pelo que $t(\sigma) = \sigma^2 - 1 = p(\sigma) \circ q(\sigma)$, como queríamos verificar.

Suponhamos, sem perda de generalidade, que $\alpha_p \neq 0$. Então, as soluções da equação (1) podem ser calculadas recursivamente do seguinte modo:

$$\begin{cases} w(0) = \alpha_0 \\ w(1) = \alpha_1 \\ \quad\vdots \\ w(p-1) = \alpha_{p-1} \end{cases} \tag{2}$$

$$\left\{ w(k+p) = -\frac{\alpha_{p-1}}{\alpha_p} w(k+p-1) - \cdots - \frac{\alpha_0}{\alpha_p} w(k)\,, \qquad k \in \mathbb{N} \right. \tag{3}$$

onde a equação (3) permite calcular os sucessivos valores de w a partir dos seus p valores anteriores, sendo os valores de $w(0), \cdots, w(p-1)$ dados pelas condições iniciais (2).

Exemplo

A sequência de Fibonacci é a solução da equação linear às diferenças

$$w(k+2) = w(k+1) + w(k), \qquad k \in \mathbb{N}, \tag{4}$$

correspondente às condições iniciais $w(0) = 1$ e $w(1) = 1$.

Utilizando o deslocamento σ, a equação (4) toma a forma:

$$\begin{aligned} &\sigma^2 w(k) = \sigma w(k) + w(k)\,, k \in \mathbb{N} \\ &\Leftrightarrow \sigma^2 w(k) - \sigma w(k) - w(k) = 0\,, k \in \mathbb{N} \\ &\Leftrightarrow (\sigma^2 - \sigma - 1)\, w = \underline{0}. \end{aligned}$$

Neste caso, o operador linear às diferenças correspondente é $p(\sigma)$, com $p(x) = x^2 - x - 1$.

À semelhança do que acontece com outros tipos de equações, podemos considerar sistemas de equações às diferenças numa variável w:

$$\begin{cases} p_1(\sigma)w = \underline{0} \\ p_2(\sigma)w = \underline{0} \\ \quad \vdots \\ p_s(\sigma)w = \underline{0} \end{cases} \tag{5}$$

ou, equivalentemente, na forma matricial:

$$\begin{bmatrix} p_1(\sigma) \\ p_2(\sigma) \\ \vdots \\ p_s(\sigma) \end{bmatrix} w = \begin{bmatrix} \underline{0} \\ \vdots \\ \underline{0} \end{bmatrix}.$$

O conjunto das soluções de (5) é representado por $\mathcal{S}(p_1, \cdots, p_s)$. Dizemos que dois sistemas são equivalentes se possuírem o mesmo conjunto de soluções.

Proposição 2.2.1

Se $I(p_1, \cdots, p_s) = I(\tilde{p}_1, \cdots, \tilde{p}_l)$, então os sistemas de equações

$$\begin{bmatrix} p_1(\sigma) \\ p_2(\sigma) \\ \vdots \\ p_s(\sigma) \end{bmatrix} w = \begin{bmatrix} \underline{0} \\ \vdots \\ \underline{0} \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} \tilde{p}_1(\sigma) \\ \tilde{p}_2(\sigma) \\ \vdots \\ \tilde{p}_l(\sigma) \end{bmatrix} w = \begin{bmatrix} \underline{0} \\ \vdots \\ \underline{0} \end{bmatrix}$$

são equivalentes.

Demonstração

Sejam $I = I(p_1, \cdots, p_s)$ e $\tilde{I} = I(\tilde{p}_1, \cdots, \tilde{p}_l) = I$ e suponhamos que $I = \tilde{I}$. Então existem $\alpha_{ij}(x)$, $\beta_{ij}(x) \in \mathbb{R}[x]$ tais que:

$$\begin{aligned} p_1(x) &= \alpha_{11}(x)\tilde{p}_1(x) + \cdots + \alpha_{1s}(x)\tilde{p}_l(x) & \tilde{p}_1(x) &= \beta_{11}(x)p_1(x) + \cdots + \beta_{1s}(x)p_s(x) \\ p_2(x) &= \alpha_{21}(x)\tilde{p}_1(x) + \cdots + \alpha_{2s}(x)\tilde{p}_l(x) & \tilde{p}_2(x) &= \beta_{21}(x)p_1(x) + \cdots + \beta_{2s}(x)p_s(x) \\ &\vdots & &\vdots \\ p_s(x) &= \alpha_{s1}(x)\tilde{p}_1(x) + \cdots + \alpha_{sl}(x)\tilde{p}_l(x) & \tilde{p}_l(x) &= \beta_{s1}(x)p_1(x) + \cdots + \beta_{ss}(x)p_s(x). \end{aligned}$$

Seja $w \in \mathcal{S}(p_1, \cdots, p_s)$. Então $p_j(\sigma)w = \underline{0}$, com $j = 1, \cdots, s$ e $\tilde{p}_i(\sigma)w = \big(\beta_{i1}(\sigma)p_1(\sigma) + \cdots + \beta_{is}(\sigma)p_s(\sigma)\big)w = \beta_{i1}(\sigma)p_1(\sigma)w + \cdots + \beta_{is}(\sigma)p_s(\sigma)w = \underline{0}$, $i = 1 \cdots l$, pelo que $w \in \mathcal{S}(\tilde{p}_1, \cdots, \tilde{p}_l)$. Assim, $\mathcal{S}(p_1, \cdots, p_s) \subset \mathcal{S}(\tilde{p}_1, \cdots, \tilde{p}_l)$.

Analogamente se prova que $\mathcal{S}(\tilde{p}_1, \cdots, \tilde{p}_l) \subset \mathcal{S}(p_1, \cdots, p_s)$. ■

A proposição que acabámos de demonstrar permite associar a cada ideal I de $\mathbb{R}[x]$ um conjunto de sequências reais w, que designaremos por $I^{\perp}$, dado por

$$I^{\perp} = \{w \in \mathbb{R}^{\mathbb{N}} : i(\sigma)w = \underline{0}, \ \forall i \in I\}.$$

Este conjunto coincide com o conjunto de soluções de qualquer sistema associado a polinómios $p_1(x), \cdots, p_s(x)$ tais que $I = I(p_1, \cdots, p_s)$.

Uma vez que $\mathbb{R}[x]$ é um d.i.p., cada seu ideal I é da forma $I(p)$, para dado $p \in \mathbb{R}[x]$, pelo que

$$I^{\perp} = \{w \in \mathbb{R}^{\mathbb{N}} : p(\sigma)w = \underline{0}\}.$$

Em particular, como vimos no capítulo anterior, $I(p_1, \cdots, p_s) = I\big(mdc\,(p_1, \cdots, p_s)\big)$. Portanto, tendo em conta a Proposição 2.2.1, $\mathcal{S}(p_1, \cdots, p_s) = \mathcal{S}\big(mdc\,(p_1, \cdots, p_s)\big)$, ou seja,

$$\begin{cases} p_1(\sigma)w = \underline{0} \\ p_2(\sigma)w = \underline{0}, \\ \quad \vdots \\ p_s(\sigma)w = \underline{0} \end{cases} \quad \Leftrightarrow \quad d(\sigma)w = \underline{0}$$

onde $d(\sigma) = mdc(p_1(\sigma), \cdots, p_s(\sigma))$.

Este resultado é muito útil para o cálculo recursivo das soluções, porque é claramente mais simples usar uma só equação, do que considerar um sistema de equações.

No caso das sequências multidimensionais nD, com $n > 1$, podemos efectuar um estudo semelhante ao que foi levado a cabo no caso unidimensional, $n = 1$. Neste caso é necessário definir deslocamentos parciais $\sigma_1, \cdots, \sigma_n$ e os operadores lineares às diferenças parciais. No presente estudo vamos focar apenas o caso bidimensional $(2D)$, isto é, $n = 2$.

Em duas dimensões, definimos os deslocamentos σ_1, σ_2 como:

$$\begin{aligned} \sigma_1 : \mathbb{R}^{\mathbb{N}^2} &\longrightarrow \mathbb{R}^{\mathbb{N}^2} \\ w &\longmapsto \sigma w \end{aligned}$$

tal que $\sigma_1 w(k_1, k_2) = w(k_1 + 1, k_2)$ e ${\sigma_1}^l = {\sigma_1}^{l-1} \circ \sigma_1$;

$$\begin{aligned} \sigma_2 : \mathbb{R}^{\mathbb{N}^2} &\longrightarrow \mathbb{R}^{\mathbb{N}^2} \\ w &\longmapsto \sigma w \end{aligned}$$

tal que $\sigma_2 w(k_1, k_2) = w(k_1, k_2 + 1)$ e $\sigma_2{}^l = \sigma_2{}^{l-1} \circ \sigma_2$.

Note-se que, também no caso $n = 2$, a composição dos operadores lineares às diferenças corresponde à multiplicação dos polinómios correspondentes. Ou seja, $p(\sigma_1, \sigma_2) \circ q(\sigma_1, \sigma_2) = t(\sigma_1, \sigma_2)$ onde $t(x_1, x_2) = p(x_1, x_2) \cdot q(x_1, x_2)$.

Usando os deslocamentos σ_1 e σ_2, um sistema de equações às diferenças em duas dimensões pode ser escrito como:

$$\begin{cases} p_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ p_2(\sigma_1, \sigma_2)\, w = \underline{0} \\ \vdots \\ p_s(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases} \tag{6}$$

sendo $p_1(x_1, x_2), \cdots, p_s(x_1, x_2)$ polinómios de $\mathbb{R}[x_1,\ x_2]$.

Tal como no caso $n = 1$, designando por $\mathcal{S}(p_1, \cdots, p_s)$ o conjunto das soluções de (6) e pondo $I = I(p_1, \cdots, p_s)$ e $I^{\perp} \coloneqq \{w \in \mathbb{R}^{\mathbb{N}} :\ i(\sigma)w = \underline{0}, \forall i \in I\}$, verifica-se que:

$$\mathcal{S}(p_1, \cdots, p_s) = I^{\perp}.$$

Ou seja, se $\tilde{p}_1, \cdots, \tilde{p}_l$ forem tais que $\tilde{I} = I(\tilde{p}_1, \cdots, \tilde{p}_l) = I$, então

$$\begin{cases} p_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ p_2(\sigma_1, \sigma_2)\, w = \underline{0} \\ \vdots \\ p_s(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases} \Leftrightarrow \begin{cases} \tilde{p}_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ \tilde{p}_2(\sigma_1, \sigma_2)\, w = \underline{0} \\ \vdots \\ \tilde{p}_l(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases}$$

Infelizmente, uma vez que $\mathbb{R}[x_1,\ x_2]$ não é um d.i.p., não é em geral possível obter $p \in \mathbb{R}[x_1,\ x_2]$ tal que $I(p_1, \cdots, p_s) = I(p)$. Isto significa que não é possível reduzir um sistema de equações às diferenças $2D$ a uma só equação equivalente, o que poderá levantar dificuldades à obtenção de esquemas recursivos para o cálculo das soluções.

Exemplo

Consideremos o seguinte sistema de equações às diferenças:

$$\begin{cases} w(k_1, k_2+3) - w(k_1, k_2+2) - w(k_1, k_2+1) + w(k_1, k_2) = 0 \\ w(k_1+1, k_2+1) + w(k_1+1, k_2) - w(k_1, k_2+1) - 2w(k_1, k_2) = 0 \end{cases} \tag{7}$$

Pretende-se calcular recursivamente as soluções de (7). O esquema de recursão a utilizar será obviamente bidimensional. Tendo em conta que as equações do sistema podem ser escritas como

$$\begin{cases} w(k_1, k_2+3) - w(k_1, k_2+2) - w(k_1, k_2+1) + w(k_1, k_2) = 0 \\ w(k_1+1, k_2+1) + w(k_1+1, k_2) = w(k_1, k_2+1) + 2w(k_1, k_2). \end{cases}$$

Uma possibilidade seria fazer uma recursão linha a linha, começando por exemplo por calcular os valores das soluções w na linha $k_1 = 0$, calculando depois, a partir desses valores, os valores de w na linha $k_1 = 1$ e assim sucessivamente, de acordo com a seguinte recursão.

Utilizando para isso as equações anteriores, o processo de cálculo seria o seguinte.

Cálculo das soluções na linha $k_1 = 0$:

Condições iniciais: $\begin{cases} w(0,0) = \alpha_{0,0} \\ w(0,1) = \alpha_{0,1} \\ w(0,2) = \alpha_{0,2} \end{cases}$

Recursão:

$$w(0, k_2+3) = w(0, k_2+2) + w(0, k_2+1) - w(0, k_2) \tag{8}$$

Cálculo das soluções nas linhas verticais seguintes, com $k_1, k_2 \in \mathbb{N}$:

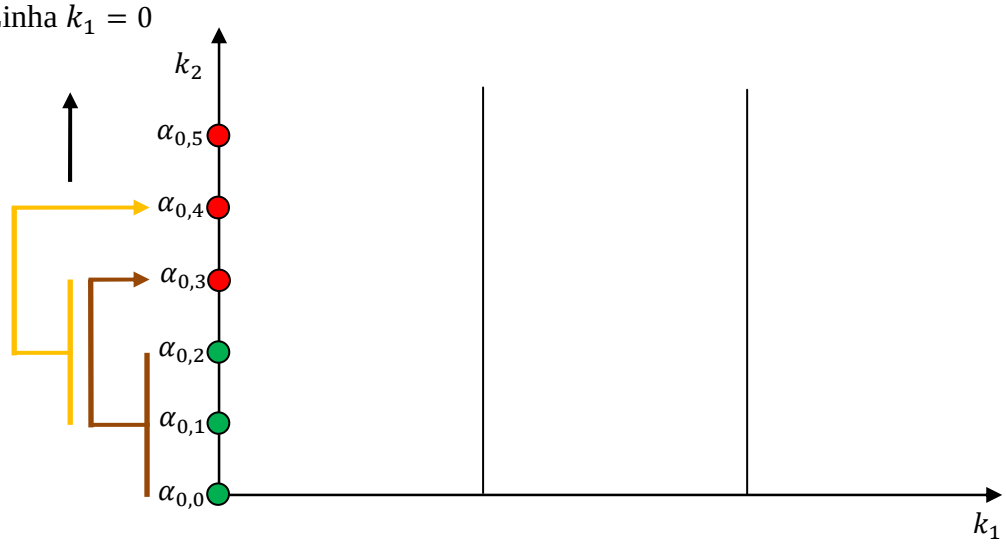
Condição inicial: $w(k_1+1, 0) = \alpha_{k_1+1,0}$

Recursão:

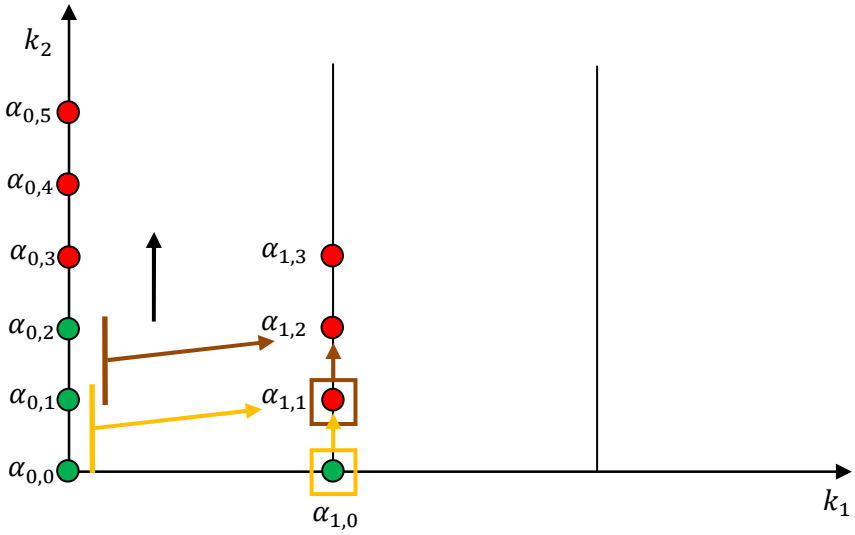
$$w(k_1+1,k_2+1) = -w(k_1+1,k_2) + w(k_1,k_2+1) + 2w(k_1,k_2) \quad (9)$$

Este processo está esquematizado nas figuras que se seguem.

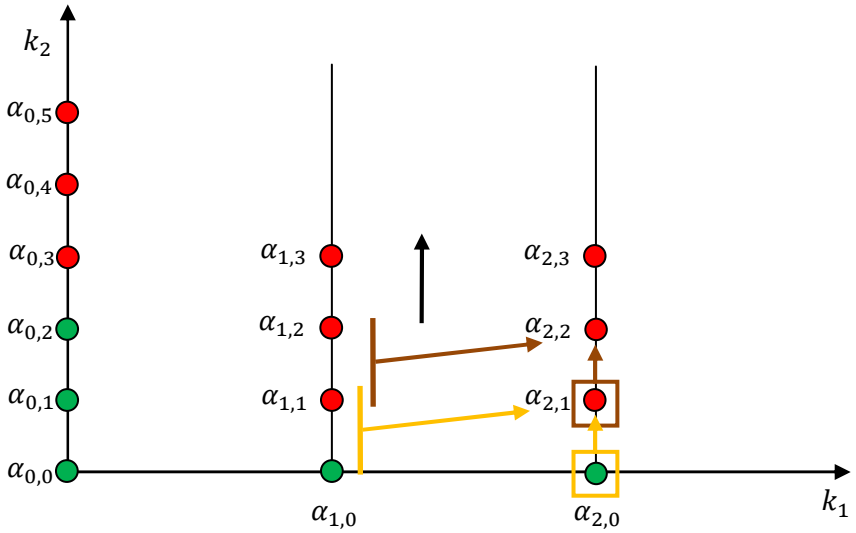
Linha $k_1 = 0$



Linha $k_1 = 1$



Linha $k_1 = 2$



No entanto, como veremos, este processo introduz soluções falsas. De facto, o sistema (7) pode escrever-se como

$$\begin{cases} \sigma_2^3 w(k_1,k_2) - \sigma_2^2 w(k_1,k_2) - \sigma_2 w(k_1,k_2) + w(k_1,k_2) = 0 \\ \sigma_2(\sigma_1 w)(k_1,k_2) + \sigma_1 w(k_1,k_2) - \sigma_2 w(k_1,k_2) - 2w(k_1,k_2) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} (\sigma_2^3 - \sigma_2^2 - \sigma_2 + 1)\, w = \underline{0} \\ (\sigma_2\sigma_1 + \sigma_1 - \sigma_2 - 2)\, w = \underline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} p_1(\sigma_1,\sigma_2)\, w = \underline{0} \\ p_2(\sigma_1,\sigma_2)\, w = \underline{0} \end{cases} \tag{10}$$

onde os operadores às diferenças lineares $p_1(\sigma_1,\sigma_2)$ e $p_2(\sigma_1,\sigma_2)$ estão associados, respectivamente, aos polinómios $p_1(x_1,x_2) = x_2^3 - x_2^2 - x_2 + 1$ e $p_2(x_1,x_2) = x_2x_1 + x_1 - x_2 - 2$.

Assim, o conjunto das soluções de (7) é dado por $I^{\perp}$ com $I = I\,(p_1,p_2)$. Note-se que

$$p(x_1,x_2) = (x_2-1)^2 p_2(x_1,x_2) - x_1 p_1(x_1,x_2) = -(x_2-1)^2(x_2+2) \in I.$$

Atendendo a que p_1 e p são polinómios numa só indeterminada, x_2, então o seu mdc, $d(x_1, x_2) = (x_2 - 1)^2$, é dado por uma combinação linear de p_1 e p (com coeficientes polinomiais) e, portanto, $I(p_1, p_2) = I(d, p_2)$. Por outro lado, $I(d, p_2) = I(d, \tilde{p}_2)$ com

$$\tilde{p}_2 = \frac{1}{4}(x_1 - 1)d + \frac{1}{4}(3 - x_2)p_2 = x_1 + \frac{1}{4}x_2 - \frac{7}{4}.$$

Isto permite concluir que as equações do sistema (10) são equivalentes a:

$$\begin{cases} d(\sigma_1, \sigma_2)w = \underline{0} \\ \tilde{p}_2(\sigma_1, \sigma_2)w = \underline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} (\sigma_2 - 1)^2 w = \underline{0} \\ \left(\sigma_1 + \frac{1}{4}\sigma_2 - \frac{7}{4}\right)w = \underline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} w(k_1, k_2 + 2) = 2w(k_1, k_2 + 1) - w(k_1, k_2) \\ w(k_1 + 1, k_2) = -\frac{1}{4}w(k_1, k_2 + 1) + \frac{7}{4}w(k_1, k_2). \end{cases} \quad (11)$$

Se agora aplicarmos o processo de cálculo recursivo com base na primeira equação, para a linha $k_1 = 0$, teremos:

Condições iniciais $\begin{cases} w(0,0) = \tilde{\alpha}_{0,0} \\ w(0,1) = \tilde{\alpha}_{0,1} \end{cases}$

Recursão:

$$w(0, k_2 + 2) = 2w(0, k_2 + 1) - w(0, k_2). \quad (12)$$

Além disso, para $k_1, k_2 \in \mathbb{N}$, a recursão para as restantes linhas verticais fica:

$$w(k_1 + 1, k_2) = -\frac{1}{4}w(k_1, k_2 + 1) + \frac{7}{4}w(k_1, k_2). \quad (13)$$

Em particular,

$$w(0,2) = 2\tilde{\alpha}_{0,1} - \tilde{\alpha}_{0,0} \text{ e}$$
$$w(k_1+1,0) = -\frac{1}{4}w(k_1,1) + \frac{7}{4}w(k_1,0),$$

o que mostra que não podemos arbitrar $w(0,2) = \alpha_{0,2} \in \mathbb{R}$ e $w(k_1+1,0) = \alpha_{k_1+1,0} \in \mathbb{R}$, como tínhamos antes.

Isto significa que a aplicação das recursões (8) e (9) introduz soluções falsas. O problema surge pelo facto do ideal I conter um polinómio, d, com grau inferior ao de p_1. Como consequência, o conjunto de valores $w(0,0), w(0,1), w(0,2)$ e $w(k_1+1,0)$ escolhidos como condições iniciais não é adequado, no sentido de a ele corresponder uma e uma só solução do sistema dado. De facto, uma vez que, na realidade, $w(0,2)$ depende de $w(0,0)$ e $w(0,1)$ e $w(k_1+1,0)$ depende de $w(k_1,1)$ e $w(k_1,0)$, se arbitrarmos todos estes valores podemos não obter uma solução do sistema.

Por outro lado, a recursão $(12)-(13)$ não introduz soluções estranhas, pois apesar de se usar a primeira equação de (11) apenas em (12) para o cálculo de $w(0,k_2)$, com $k_2 \in \mathbb{N}$, os valores de $w(1,k_2)$, $w(2,k_2)$, $w(3,k_2)$, etc. obtidos através de (13) com base na segunda equação do sistema também satisfazem a primeira equação do sistema.

De facto, supondo que para k_1 fixo, $k_2 \in \mathbb{Z}$, $w(k_1,k_2+2) = 2w(k_1,k_2+1) - w(k_1,k_2)$ e $w(k_1+1,k_2) = -\frac{1}{4}w(k_1,k_2+1) + \frac{7}{4}w(k_1,k_2)$, verifica-se que:

$$w(k_1+1,k_2+2) = -\frac{1}{4}w(k_1,k_2+3) + \frac{7}{4}w(k_1,k_2+2)$$
$$= -\frac{1}{4}[2w(k_1,k_2+2) - w(k_1,k_2+1)] + \frac{7}{4}[2w(k_1,k_2+1) - w(k_1,k_2)]$$
$$= -\frac{1}{4}[4w(k_1,k_2+1) - 2w(k_1,k_2) - w(k_1,k_2+1)] + \frac{7}{4}[2w(k_1,k_2+1) - w(k_1,k_2)]$$
$$= -\frac{1}{4}[3w(k_1,k_2+1) - 2w(k_1,k_2)] + \frac{14}{4}w(k_1,k_2+1) - \frac{7}{4}w(k_1,k_2)$$
$$= \frac{11}{4}w(k_1,k_2+1) - \frac{5}{4}w(k_1,k_2)$$
$$= 2\left(\frac{5}{4}w(k_1,k_2+1) + \frac{1}{4}w(k_1,k_2)\right) - \left(-\frac{1}{4}w(k_1,k_2+1) + \frac{7}{4}w(k_1,k_2)\right)$$

$$= 2\left(-\frac{1}{4}[2w(k_1, k_2+1) - w(k_1, k_2)] + \frac{7}{4}w(k_1, k_2+1)\right) - w(k_1+1, k_2)$$
$$= 2\left(-\frac{1}{4}w(k_1, k_2+2) + \frac{7}{4}w(k_1, k_2+1)\right) - w(k_1+1, k_2)$$
$$= 2w(k_1+1, k_2+1) - w(k_1+1, k_2).$$

Utilizando o algoritmo de B. Buchberger para construir uma base de Gröbner (descrito na secção 2.1), vamos verificar que $G = \{d, \tilde{p}_2\}$ é uma base de Gröbner reduzida para $I(p_1, p_2)$.

Seja $F = \{d, \tilde{p}_2\}$. Considerando a ordem lexicográfica,

$$SP(d, \tilde{p}_2) = -2x_1x_2 + x_1 - \frac{1}{4}x_2^3 + \frac{7}{4}x_2^2.$$

Como $SP(d, \tilde{p}_2) \longrightarrow_F 0$, $F = \{d, \tilde{p}_2\}$ é uma base de Gröbner para $I(d, \tilde{p}_2) = I(p_1, p_2)$.

Sejam $f_1 = d$ e $f_2 = \tilde{p}_2$. Então, cada polinómio f_i, com $i = 1, 2$, é mónico e está na forma normal módulo $F\backslash\{f_i\}$ e portanto F é uma base de Gröbner reduzida para $I(p_1, p_2)$.

Assim, podemos concluir que:

$$\begin{cases} p_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ p_2(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases} \quad (14) \quad \Leftrightarrow \quad \begin{cases} d(\sigma_1, \sigma_2) w = \underline{0} \\ \tilde{p}_2(\sigma_1, \sigma_2) w = \underline{0} \end{cases} \quad (15)$$

sendo a segunda descrição do problema adequada para o cálculo recursivo linha a linha proposto.

Nas Figuras 1 e 2 estão representados os conjuntos onde são dadas condições iniciais calculados com base nos sistemas de equações (14) e (15), respectivamente.

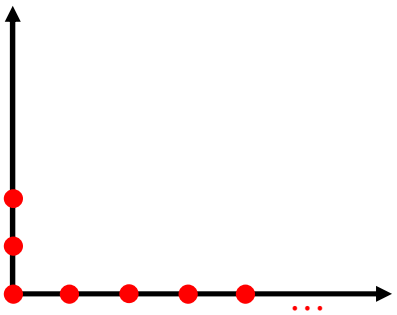


Figura 1

"Falsas" condições iniciais

Figura 2

"Verdadeiras" condições iniciais

A Figura 3 evidencia o facto de os pontos onde podem ser dadas condições iniciais (pontos de condição inicial) coincidirem com $\mathbb{N}^2 \setminus \mathfrak{M}(F)$.

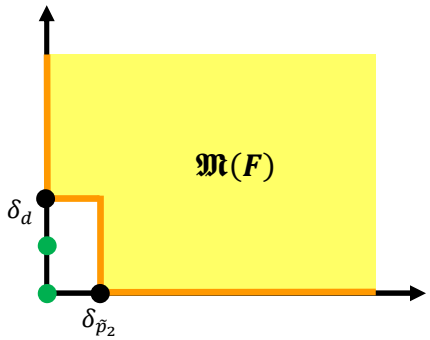


Figura 3

Legenda:

δ_d, $\delta_{\tilde{p}_2}$= Mutligraus de d e de $\tilde{p}_2$, respectivamente

● = Pontos de condição inicial

Este exemplo mostra que a aplicação do processo recursivo linha a linha proposto não pode ser feita com base numa versão arbitrária das equações do sistema, ou seja, num conjunto arbitrário de geradores do ideal I, uma vez que se corre o risco de tomar um conjunto de "condições iniciais " maior do que o real.

Se, dado um sistema de equações às diferenças parciais

$$\begin{cases} p_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ p_2(\sigma_1, \sigma_2)\, w = \underline{0} \\ \vdots \\ p_s(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases},$$

tomarmos uma descrição equivalente, correspondente à base de Gröbner reduzida de $I(p_1, \cdots, p_s)$, o processo recursivo linha a linha proposto permite obter todas as soluções do sistema sem introduzir falsas soluções. Isto decorre da Proposição 2.3, de acordo com a qual os multigraus dos elementos de uma base de Gröbner reduzida F de um ideal I são minimais no conjunto de multigraus dos elementos de I. Deste modo, designando, como na secção anterior, por $\mathfrak{M}(F)$ o conjunto dos multigraus dos elementos de $I(F)$, conclui-se que as equações do sistema (e as delas derivadas) não impõem qualquer restrição aos valores de $w(k_1, k_2)$ nos pontos de $\mathbb{N}^2 \setminus \mathfrak{M}(F)$ pelo que estes valores são "verdadeiras" condições iniciais, a designar livremente, originando uma única solução do sistema (ver Figura 4).

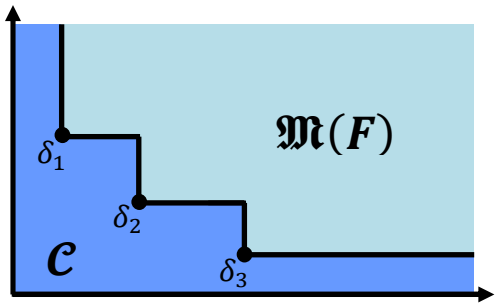


Figura 4
Legenda: $\mathcal{C}$ = Conjunto onde podem ser arbitradas condições iniciais
$F = \{f_1, f_2, f_2\}$
$\delta_i = multigrau(f_i),\ \ i = 1, 2, 3$

Por outro lado, o facto de os multigraus dos elementos de uma base de Gröbner reduzida serem minimais também garante que as correspondentes equações são compatíveis no seguinte sentido.

Suponhamos que os polinómios $f_1 < f_2 < \cdots < \mathrm{f_g}$ constituem uma base de Gröbner reduzida, relativamente à ordem lexicográfica, para $I(p_1, \cdots, p_s)$, sendo

$$f_i = f_{im_i}(y)x^{m_i} + \cdots + f_{i1}(y)x + f_{i0}(y), \qquad i = 1, \cdots, g.$$

Calculando w na vertical $K_1 = m_i$, a partir dos seus valores nas linhas verticais anteriores e das condições iniciais na linha $K_1 = m_i$, através da equação

$$f_i(\sigma_1, \sigma_2)w = \underline{0},$$

verifica-se que os valores obtidos também satisfazem as equações

$$\begin{cases} f_1(\sigma_1, \sigma_2)w = \underline{0} \\ \vdots \\ f_{i-1}(\sigma_1, \sigma_2)w = \underline{0} \end{cases}.$$

De facto, se tal não acontecesse, teria de existir uma restrição a w, do tipo $g(\sigma_1, \sigma_2)w = \underline{0}$, com $g(x,y) = g_m(y)x^m + \cdots + g_{1m}(y)x + g_0(y)$ e $m < m_i$, que não seria implicada pelas restrições $f_i(\sigma_1, \sigma_2)w = \underline{0}$, $i = 1, \cdots, m_i - 1$. Em termos de ideais, isto significa que $g(x,y) \notin I(f_1, \cdots, f_{i-1})$. Uma vez que $\{f_1, \cdots, f_{i-1}, f_i, \cdots, f_g\}$ é uma base de Gröbner reduzida para $I(p_1, \cdots, p_s)$, teríamos que $g(x,y) \notin I(p_1, \cdots, p_s)$. Mas isto é um absurdo, uma vez que as equações às diferenças a que w tem de satisfazer correspondem a polinómios do ideal $I(p_1, \cdots, p_s)$.

O próximo exemplo ilustra uma situação diferente da ocorrida no exemplo anterior, já que, como verificaremos, o conjunto de condições iniciais é infinito.

Exemplo

Consideremos o seguinte sistema de equações às diferenças:

$$\begin{cases} w(k_1+2,k_2+4) - 2w(k_1+2,k_2+3) + w(k_1+2,k_2+2) = 0 \\ w(k_1+3,k_2+2) + \frac{1}{4}w(k_1+2,k_2+3) - \frac{7}{4}w(k_1+2,k_2+2) = 0 \end{cases} \tag{16}$$

O sistema (16) pode escrever-se como

$$\begin{cases} \sigma_2^4(\sigma_1^2 w)(k_1,k_2) - 2\sigma_2^3(\sigma_1^2 w)(k_1,k_2) + \sigma_2^2(\sigma_1^2 w)(k_1,k_2) = 0 \\ \sigma_2^2(\sigma_1^3 w)(k_1,k_2) + \frac{1}{4}\sigma_2^3(\sigma_1^2 w)(k_1,k_2) - \frac{7}{4}\sigma_2^2(\sigma_1^2 w)(k_1,k_2) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} (\sigma_2^4\sigma_1^2 - 2\sigma_2^3\sigma_1^2 + \sigma_2^2\sigma_1^2)\, w = \underline{0} \\ \left(\sigma_2^2\sigma_1^3 + \frac{1}{4}\sigma_2^3\sigma_1^2 - \frac{7}{4}\sigma_2^2\sigma_1^2\right) w = \underline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} p_1(\sigma_1,\sigma_2)\, w = \underline{0} \\ p_2(\sigma_1,\sigma_2)\, w = \underline{0} \end{cases} \tag{17}$$

onde os operadores às diferenças lineares $p_1(\sigma_1,\sigma_2)$ e $p_2(\sigma_1,\sigma_2)$ estão associados, respectivamente, aos polinómios $p_1(x_1,x_2) = x_1^2x_2^4 - 2x_1^2x_2^3 + x_1^2x_2^2$ e $p_2(x_1,x_2) = x_1^3x_2^2 + \frac{1}{4}x_1^2x_2^3 - \frac{7}{4}x_1^2x_2^2$.

Assim, o conjunto das soluções de (16) é dado por $I^{\perp}$ com $I = I\,(p_1,p_2)$.

Antes de calcularmos as soluções, aplicando o processo recursivo linha a linha, vamos primeiro verificar se $F = \{p_1,p_2\}$ é uma base de Gröbner reduzida para $I(p_1,p_2)$, utilizando o algoritmo de B. Buchberger para construir uma base de Gröbner (descrito na secção 2.1).

De facto, considerando a ordem lexicográfica,

$$SP(p_1,p_2) = -2x_1^3x_2^3 + x_1^3x_2^2 - \frac{1}{4}x_1^2x_2^5 + \frac{7}{4}x_1^2x_2^4$$

e como $SP(d, \tilde{p}_2) \longrightarrow_F 0$, $F = \{p_1, p_2\}$ é uma base de Gröbner para $I(p_1, p_2)$.

Cada polinómio p_i, com $i = 1, 2$, é mónico e está na forma normal módulo $F\backslash\{p_i\}$, portanto F é uma base de Gröbner reduzida para $I(p_1, p_2)$. Desta forma, podemos aplicar o seguinte processo recursivo linha a linha para o cálculo das soluções com base nas equações (16).

Soluções nas linhas $k_1 = 0$ e $k_1 = 1$:

$$\text{Condições iniciais: } \begin{cases} w(0, k_2) = \alpha_{0,k_2} \\ w(1, k_2) = \alpha_{1,k_2} \end{cases}$$

Cálculo das soluções na linha $k_1 = 2$:

$$\text{Condições iniciais: } \begin{cases} w(2, 0) = \alpha_{2,0} \\ w(2, 1) = \alpha_{2,1} \\ w(2, 2) = \alpha_{2,2} \\ w(2, 3) = \alpha_{2,3} \end{cases}$$

Recursão:

$$w(2, k_2 + 4) = 2w(2, k_2 + 3) - w(2, k_2 + 2) \tag{18}$$

Cálculo das soluções nas linhas verticais seguintes, com $k_1, k_2 \in \mathbb{N}$:

$$\text{Condições iniciais: } \begin{cases} w(k_1 + 3, 0) = \alpha_{k_1+3,0} \\ w(k_1 + 3, 1) = \alpha_{k_1+3,1} \end{cases}$$

Recursão:

$$w(k_1 + 3, k_2 + 2) = -\frac{1}{4} w(k_1 + 2, k_2 + 3) + \frac{7}{4} w(k_1 + 2, k_2 + 2) \tag{19}$$

A Figura 5 representa os pontos onde podem ser dadas condições iniciais (pontos de condição inicial).

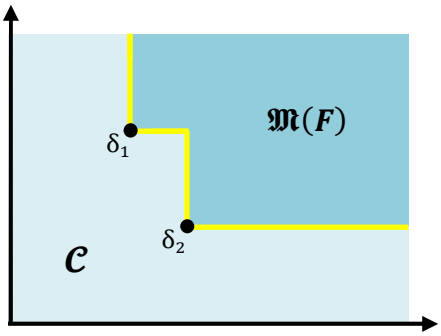


Figura 5
Legenda:
$\mathcal{C}$ = Conjunto onde podem ser arbitradas condições iniciais
$F = \{p_1, p_2\}$
$\delta_i = multigrau(p_i), \ \ i = 1, 2$

Como podemos observar, neste último exemplo o conjunto onde podem ser arbitradas condições iniciais é infinito (ver Figura 5), enquanto que no exemplo anterior o conjunto onde podem ser arbitradas condições iniciais é finito (ver Figura 3). Este facto ocorre, porque no segundo caso d e $\tilde{p}_2$ são primos entre si ($mdc(d, \tilde{p}_2) = 1$) e no primeiro caso p_1 e p_2 não são primos entre si ($mdc(p_1, p_2) = x_1^2 x_2^2 \neq 1$), o que está de acordo com a Proposição 2.1.6.

Terminamos esta secção enunciando uma proposição que resume as considerações anteriores.

Proposição 2.2.2

Dado um sistema de equações às diferenças parciais

$$\begin{cases} p_1(\sigma_1, \sigma_2)\, w = \underline{0} \\ \vdots \\ p_s(\sigma_1, \sigma_2)\, w = \underline{0} \end{cases}$$

com $p_i(x,y) \in \mathbb{R}[x,y], i = 1, \cdots, s,$ e $w \in \mathbb{R}^{\mathbb{N}^2}$, seja $F = \{f_1 < f_2 < \cdots < f_{g-1} < f_g\}$ a base de Gröbner reduzida para $I = (p_1, \cdots, p_s)$, relativamente à ordem lexicográfica. Suponha-se que

$$f_i = \sum_{k=0}^{m_i} f_{i,k}(y)x^k$$

com $f_{i,k}(y) \in \mathbb{R}[y],\ k = 0, \cdots, m_i,$ sendo $f_{i,m_i}(y) = y^{n_i} + h_{in_i-1}y^{n_i-1} \cdots + h_{i1}y + h_{i0},\ i = 1, \cdots, g.$ Então $w \in \mathcal{S}(I)$ se e só se existem números reais $\alpha_{k_1,k_2}, k_1 = 0, \cdots, m_1 - 1,\ k_2 \in \mathbb{N}, \alpha_{k_1,0}, \cdots, \alpha_{k_1,n_i-1},\ i = 1, \cdots, g-1, k_1 = m_i, \cdots, m_{i+1} - 1,\ \alpha_{k_1,0}, \cdots, \alpha_{k_1,n_g-1},\ k_1 = m_g, m_g + 1, m_g + 2, \cdots,$ tais que:

Para $k_1 = 0, \cdots, m_1 - 1$

$$w(k_1, k_2) = \alpha_{k_1,k_2}$$

Para $i = 1, \cdots, g - 1$

Para $k_1 = m_i, \cdots, m_{i+1} - 1$ e $k_2 \in \mathbb{N}$

$$w(k_1, 0) = \alpha_{k_1,0}$$
$$\vdots$$
$$w(k_1, n_i - 1) = \alpha_{k_1,n_i-1}$$
$$w(k_1, k_2 + n_i) = -\left(f_{i,m_i}(\sigma_2) - \sigma_2^{n_i}\right) w(k_1, k_2) - f_{i,m_i-1}(\sigma_2)\, w(k_1 - 1, k_2) - \cdots - f_{i,0}(\sigma_2)\, w(k_1 - m_i, k_2)$$

Para $k_1 \geq m_g$ e $k_2 \in \mathbb{N}$

$$w(k_1, 0) = \alpha_{k_1,0}$$
$$\vdots$$
$$w(k_1, n_g - 1) = \alpha_{k_1,n_g-1}$$
$$w(k_1, k_2 + n_g) = -\left(f_{g,m_g}(\sigma_2) - \sigma_2^{n_g}\right) w(k_1, k_2) - f_{g,m_g-1}(\sigma_2)\, w(k_1 - 1, k_2) - \cdots - f_{g,0}(\sigma_2)\, w(k_1 - m_g, k_2).$$

Considerações finais

Nesta dissertação apenas foram consideradas equações numa variável, estando cada equação associada a um polinómio. No caso dos sistemas de equações às diferenças parciais em q variáveis:

$$\begin{cases} p_{11}(\sigma_1,\sigma_2)w_1 + \cdots + p_{1q}(\sigma_1,\sigma_2)w_q = \underline{0} \\ \vdots \\ p_{s1}(\sigma_1,\sigma_2)w_1 + \cdots + p_{sq}(\sigma_1,\sigma_2)w_q = \underline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} \begin{bmatrix} p_{i1}(\sigma_1,\sigma_2) & \cdots & p_{iq}(\sigma_1,\sigma_2) \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_q \end{bmatrix} = \underline{0} \\ i = 1 \cdots s \end{cases},$$

com $p_{ij}(x,y) \in \mathbb{R}[x,y]$, cada equação estará associada a uma linha polinomial $\begin{bmatrix} p_{i1}(x,y) & \cdots & p_{iq}(x,y) \end{bmatrix}$ e o sistema a um módulo de $\mathbb{R}^{1\times q}\ [x,y]$. Assim, o instrumento relevante para o estudo deste tipo de sistemas seria as bases de Gröbner reduzidas para módulos, em vez de para ideais.

Uma outra questão interessante seria analisar o papel das bases de Gröbner reduzidas para módulos de anéis de polinómios, em mais do que duas indeterminadas, no

cálculo recursivo das soluções de sistemas gerais de equações às diferenças nD, com $n > 2$.

A determinação de bases de Gröbner e de formas normais de polinómios em casos mais complexos que os aqui apresentados pode ser feita com recurso a programas de Álgebra Computacional, como por exemplo o CoCoA[2]. Teríamos gostado de apresentar a resolução de alguns problemas com recurso a esta aplicação computacional, mas o tempo limitado de que dispúnhamos não o permitiu.

[2] CoCoA significa "**Co**mputations in **Co**mmutative **A**lgebra"

Bibliografia

B. Buchberger. *Gröbner Bases:* An Algorithmic Method in Polynomial Ideal Theory. Em N.K. Bose (ed.), *Multidimensional Systems Theory*, págs. 184-232, D. Reidel Publishing Company, 1985

B. Buchberger e F winkler. *Gröbner Bases and Applications.* Cambridge University Press, United Kingdom, 1998

L. Robbiano e M. Kreuzer. *Computational Commutative Algebra 1*. Spinger-Verlag, 2000

O. Zariski e P. Samuel. *Commutative Algebra 1*. Spinger-Verlag, 1958

P. Rocha, J. C. Willems. Canonical Computacional Forms for AR 2-D Systems. *Multidimensional Systems and Signal Processing*, 1, págs. 251-278, 1990