DIVISÃO DE POLINÔMIOS . . . EM MÚLTIPLAS VARIÁVEIS?

Caio H. S. de Souza

sob orientação do Prof. Dr. João Nivaldo Tomazella

Universidade Federal de São Carlos, SP, Brasil

caiohsouza36@gmail.com

Resumo

Trabalhando com anéis de polinômios em múltiplas variáveis $\mathbb{K}[x_1, ..., x_n]$ sobre corpos vamos discutir sobre como realizar nessa estrutura um algoritmo de divisão eficiente que nos ajude a responder a seguinte questão: dado um ideal de $\mathbb{K}[x_1, ..., x_n]$ como podemos decidir se um certo polinômio $g(x_1, ..., x_n)$ pertence ou não a esse ideal? Esse problema, conhecido como *Problema da Pertinência*, motiva a definição das chamadas bases de Gröebner que nos ajudam a descrever um bom algoritmo de divisão para qualquer ordem de monômios escolhida.

PALAVRAS-CHAVE: ALGEBRA COMUTATIVA; ALGORITMO; IDEAIS; NOETHERIANO.

O anel $\mathcal{A}[x_1, \ldots, x_n]$

Seja $\mathcal{A}$ um anel e $x_1, \ldots, x_n$ n indeterminadas. Um **polinômio em n indeterminadas** $p(x_1, \ldots, x_n)$ com coeficientes em $\mathcal{A}$ é uma soma formal

$$\sum_{i_1,\ldots,i_n \in \mathbb{N}} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

com os coeficientes em $\mathcal{A}$ e $a_{i_1,\ldots,i_n} \neq 0$ para um número finito de índices. Temos uma correspondência biunívoca (de fato isomorfismo) entre os conjuntos $\mathcal{A}[x_1, \ldots, x_n]$ e $\mathcal{A}[x_1][x_2] \ldots [x_n]$, donde podemos definir as operações em $\langle \mathcal{A}[x_1, \ldots, x_n], +, \cdot \rangle$ via pull-back.

Ordem de monômios

Chamaremos de termo de um polinômio algo da forma $a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$. Um monômio é um polinômio $x^\alpha = x_1^{i_1} \cdots x_n^{i_n}$ e seu grau é $deg(x^\alpha) = i_1 + \ldots + i_n$. Utilizaremos as n-uplas $\alpha = (i_1, \ldots, i_n) \in \mathbb{N}^n$ para estabelecer uma ordem entre os monômios. Algumas ordens possíveis são:

(Ordem Lexicográfica) *Sendo $\alpha = (i_1, \ldots, i_n)$ e $\beta = (i'_1, \ldots, i'_n)$ n-uplas que representam monômios, dizemos que $x^\alpha >_{lex} x^\beta$ se a primeira entrada não nula a partir da esquerda de $\alpha - \beta$ é positiva.*

(Ordem Lexicográfica Graduada) *Sendo $\alpha = (i_1, \ldots, i_n)$ e $\beta = (i'_1, \ldots, i'_n)$ n-uplas que representam monômios, dizemos que $x^\alpha >_{grlex} x^\beta$ se*

$$deg(x^\alpha) > deg(x^\beta) \text{ ou } deg(x^\alpha) = deg(x^\beta) \text{ e } x^\alpha >_{lex} x^\beta.$$

(Ordem Lexicográfica Graduada Reversa) *Sendo $\alpha = (i_1, \ldots, i_n)$ e $\beta = (i'_1, \ldots, i'_n)$ n-uplas que representam monômios, dizemos que $x^\alpha >_{grlexrv} x^\beta$ se*

$$deg(x^\alpha) > deg(x^\beta) \text{ ou } deg(x^\alpha) = deg(x^\beta) \text{ e a última entrada não nula } \alpha_j - \beta_j < 0.$$

Seja $p \in \mathbb{K}[x_1, \ldots, x_n]$. Dessa forma diremos que $deg(p)$ será então o máximo entre os graus de cada termo.

• **Monômio líder**: maior monômio x^α com coeficiente não nulo, denotado por $LM(p)$.

• **Termo líder**: monômio líder acompanhado de seu coeficiente, denotado $LT(p)$.

Exemplo: $p(x_1, x_2, x_3) = 4x_1^3x_2^5 + 4x_1^2x_3^6 + 3x_2 \in \mathbb{Z}[x_1, x_2, x_3]$ tem grau $deg(p(x_1, x_2, x_3)) = 8$ e está sob a Ordem Lexicográfica Graduada.

Problema da Pertinência

Sejam $g \in \mathbb{K}[x_1, \ldots, x_n]$ e $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal. Como decidir se um dado polinômio g pertence ou não a um determinado ideal $\mathcal{I}$? Esse é o chamado **Problema da Pertinência (Ideal Membership Problem)** . Para $n = 1$, $\mathbb{K}[x]$ é domínio de ideais principais, logo $\mathcal{I} = \langle f \rangle$ e basta fazer a divisão de g por f e olhar o resto. Agora, para $n \geq 2$, não temos que $\mathbb{K}[x_1, \ldots, x_n]$ é domínio de ideais principais. Vamos então implementar um algoritmo de divisão que nos permita responder a pergunta de modo parecido com o caso $n = 1$. Fixemos uma ordem de monômios $>$ em $\mathbb{K}[x_1, \ldots, x_n]$ e polinômios $f_1, \ldots, f_r$. Vamos "dividir" $g \in \mathbb{K}[x_1, \ldots, x_n]$ por $f_1, \ldots, f_r$.

Algoritmo de divisão para polinômios em múltiplas variáveis

Passo 0 : Colocando $g_0 = g$, olhamos para o monômio líder $LM(g_0)$: se não houver f_{j_0} tal que $LM(f_{j_0})|LM(g_0)$, então o processo é encerrado. Caso contrário, vamos cancelar o termo líder de g_0 fazendo $g_1 = g_0 - f_{j_0}q_{j_0}$, onde q_{j_0} é tal que $LT(g_0) = q_{j_0}LT(f_{j_0})$.

Passo i : Dado g_i, se não houver f_{j_i} tal que $LM(f_{j_i})|LM(g_i)$, então o processo é encerrado. Caso contrário, vamos cancelar o termo líder de g_i fazendo $g_{i+1} = g_i - f_{j_i}q_{j_i}$, onde q_{j_i} é tal que $LT(g_i) = q_{j_i}LT(f_{j_i})$.

A cada passo cancelamos os termos líderes e assim o grau dos polinômios g_i diminui:

$$LM(g_0) > LM(g_1) > \ldots > LM(g_i) > \ldots$$

Pela propriedade da boa ordem da ordem de monômios, essa cadeia eventualmente estabiliza ou termina de fato. Na primeira opção, que ocorre caso o processo não pare, precisamos ter $g_n = 0$ identicamente nulo a partir de algum n. Com isso, $0 = g_{n-1} - f_{j_{n-1}}q_{j_{n-1}}$, $g_{n-1} = g_{n-2} - f_{j_{n-2}}q_{j_{n-2}}, \ldots$
e substituindo regressivamente

$$g = \sum_{i=0}^{n-1} f_{j_i}q_{j_i} = \sum_{j=1}^{r} \left(\sum_{j_i=j} q_{j_i} \right) f_j = \sum_{j=1}^{r} h_j f_j.$$

e com isso vemos que $g \in \langle f_1, \ldots, f_r \rangle$.
Já no caso onde o processo de divisão se encerra, o último g_i é equivalente ao resto e temos

$$g = \sum_{j=1}^{r} h_j f_j + g_i.$$

▼

Porém, esse algoritmo sozinho ainda não é suficiente, pois nos deparamos com o seguinte contratempo:

Exemplo: *Tomemos $f_1 = x_1 + 2x_2 + 1$ e $f_2 = x_1 - x_2 - 5$ com a ordem $>_{grlex}$. O polinômio $g = x_2 + 2$ é tal que ambos $LM(f_1) = x_1 = LM(f_2)$ não dividem $LM(g) = x_2$, logo o processo de divisão para no passo inicial. Mas,*

$$f_1 - f_2 = 3x_2 + 6 = 3g,$$

ou seja, $g \in \mathcal{I} = (f_1, f_2)$.

Podemos observar que tal fato vai contra o que esperamos do algoritmo se quisermos utilizá-lo para resolver nosso problema.

Exemplo: Se tomarmos no exemplo acima $\overline{f_2} = -3x_2 - 6$, como $f_2 = \overline{f_2} + f_1$, temos que os ideais $\langle f_1, f_2 \rangle$ e $\langle f_1, \overline{f_2} \rangle$ são o mesmo. Aplicando o algoritmo, $LM(\overline{f_2})|LM(g_0)$, fazendo o processo seguir e chegamos a conclusão esperada ($g_1 = 0$).

Dessa forma, qual seria o conjunto de geradores (base) de $\mathcal{I} = \langle f_1, \ldots, f_r \rangle$ mais eficiente para aplicarmos o algoritmo da divisão?

• **Ideal dos termos líderes**: Seja $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ ideal. Fixada uma ordem de monômios, o ideal dos termos líderes de $\mathcal{I}$ é $LT(\mathcal{I}) := \langle LT(g) \,|\, g \in \mathcal{I} \rangle$.

Teorema: *Sejam $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ ideal gerado por $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $LT(\mathcal{I}) = \langle LT(f_1), \ldots, LT(f_r) \rangle$. Então $g \in \langle f_1, \ldots, f_r \rangle$ se, e somente se, o resto da divisão de g por $f_1, \ldots, f_r$ é zero.*

Exemplo: Sejam $f_1 = x_3 - x_1^5$ e $f_2 = x_2 - x_1^3$ com a Ordem Lexicográfica Graduada Reversa. Temos que $-x_1^2x_2 + x_3 \in \mathcal{I} = \langle f_1, f_2 \rangle$ mas ambos $LT(f_1)$ e $LT(f_2)$ não dividem $LT(-x_1^2x_2 + x_3)$.

Teorema: *Fixada uma ordem de monômios, seja $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal. Existe uma base $\{f_1, \ldots, f_r\}$ para $\mathcal{I}$ tal que $LT(\mathcal{I}) = \langle LT(f_1), \ldots, LT(f_r) \rangle$.* Uma base com tal propriedade é chamada **Base de Gröbner** para $\mathcal{I}$.

Exemplo: Para os polinômios $f_1 = -x_1^5 + x_3$ e $f_2 = -x_1^3 + x_2$, uma base de Gröbner para $\mathcal{I} = \langle f_1, f_2 \rangle$ é o conjunto

$$\{-x_1^5 + x_3,\ -x_1^3 + x_2,\ -x_2x_1^2 + x_3,\ x_2^2 - x_1x_3\}$$

Referências bibliográficas

HASSETT, BRENDAN. Introduction to Algebraic Geometry, Cambridge University Press, Cambridge, (2007).

TENGAN, EDUARDO; BORGES, HERIVELTO. Álgebra Comutativa em Quatro Movimentos, IMPA, Rio de Janeiro, (2015).