Uma breve introdução à teoria de Bases de Groebner

Rebecca Galves Gutierres Toledo [45]
Edney Augusto Jesus de Oliveira[46]

Resumo: Neste apresentamos uma introdução da teoria de Bases de Groebner e uma importante aplicação dela: como determinar a pertinência de um polinômio a um ideal polinomial. Usamos aqui polinômios em duas variáveis apenas por simplicidade notacional, pois tudo que estudamos pode ser facilmente generalizado para um número (finito) qualquer de variáveis. Vale destacar que o estudo de bases de Groebner é recente no meio matemático e foi desenvolvido inicialmente pelo matemático austríaco Bruno Buchberger em 1965, e foi assim denominada em homenagem ao seu orientador Wolfgang Groebner e ela possui diversas aplicações em álgebra comutativa além da que exibiremos. O primeiro passo para estudarmos as Bases de Groebner é estabelecer o anel de polinômios em duas variáveis. Assumindo que o conjunto dos polinômios em uma variável x com coeficientes em um corpo K é um anel comutativo com unidade denotado por $K[x]$ podemos definir de forma recursiva o anel de polinômios em duas variáveis com coeficientes em K do seguinte modo $K[x,y] := (K[x])[y]$.

No entanto, uma forma mais eficiente do ponto de vista operacional é construir o anel de polinômios em duas variáveis a partir dos seus representantes mais simples: os monômios. Um monômio em duas variáveis é uma expressão do tipo $x^\alpha y^\beta$, em que o vetor $(\alpha, \beta) \in \mathbb{Z}_+$ será chamado de multigrau de $x^\alpha y^\beta$. Definimos o grau de $x^\alpha y^\beta$, denotado por $\partial(x^\alpha y^\beta)$ como $|x^\alpha y^\beta| := \alpha + \beta$. Definimos e adotaremos neste trabalho a seguinte ordem entre os monômios de $K[x,y]$:

$$x^{\alpha_1} y^{\beta_1} < x^{\alpha_2} y^{\beta_2} \Leftrightarrow \text{ ou } \alpha_1 + \beta_1 < \alpha_2 + \beta_2 \text{ ou } \alpha_1 = \beta_1 = \alpha_2 + \beta_2 \text{ e } \beta_1 < \beta_2$$

A ordem monomial apontada acima é chamada de lexicográfica graduada reversa e não é a única ordem existente. Uma vez bem conhecido a definição de monômios, definimos um polinômio como uma combinação finita de monômios sobre o corpo K, isto é, dado $f \in k[x,y]$ temos

$$f = \sum_{\text{finito}} a_i x^{\alpha_i} y^{\beta_i} \tag{1}$$

e sobre essa ótica não é difícil demonstrar que o conjunto dos polinômios e um anel comutativo com unidade. Considerando o conjunto de todos os monômios escritos em (1) temos pela ordem monomial que existe um monômio maior do que os demais. Tal monômio é chamado de Monômio Líder de f, denotado por $ML(f)$. Se $ML(f) = x^{\alpha_s} y^{\beta_s}$, então dizemos que o Termo Líder de f é $TL(f) = a_s x^{\alpha_s} y^{\beta_s}$. Definimos o grau do polinômio f como o grau do seu monômio líder, ou seja, $\partial(f) := \partial(ML(f))$.

Construímos uma divisão polinomial em $K[x,y]$ de modo semelhante à divisão polinomial em uma variável, em que cada etapa analisamos os termos líderes do divisor e do dividendo. No

[45]Universidade Federal de Ouro Preto, rebecca.toledo@aluno.ufop.br
[46]Universidade Federal de Ouro Preto, edney@ufop.edu.br

entanto, constatamos que $K[x,y]$ não é um Domínio Euclidiano, ou seja, não existe um teorema nos moldes da divisão Euclidiana nesse conjunto em que o resto da divisão é sempre menor em certo sentido que o divisor, e para isso, basta notar que ao dividirmos x^2 por y, obtemos quociente nulo e resto x^2, cujo grau é maior que o do divisor.

Um problema importante no estudo de ideais é o problema da pertinência: Dados I um ideal de $K[x,y]$ e $f \in K[x,y]$, qual das duas afirmações é verdadeira $f \in I$ ou $f \notin I$?

Um importante resultado que nos auxiliará na tentativa de responder a pergunta acima é o Teorema da Base de Hilbert que nos garante a existência de um conjunto gerador finito para todo I de $K[x,y]$, ou seja, dado I ideal de $K[x,y]$ existe sempre $\{g_1, g_2, \ldots, g_r\} \subset K[x,y]$ tal que $I = \langle g_1, g_2, \ldots, g_r \rangle$.

Deste modo, a pergunta acima se resume em saber se existem $q_1, \ldots, q_r \in K[x,y]$ tais que $f = g_1q_1 + g_2q_2 + \ldots + g_rq_r$. A expressão acima nos motiva a generalizar a divisão polinomial para uma divisão com vários divisores, de modo que dados $f \in K[x,y]$ e os divisores (nesta ordem) $g_1, \ldots, g_r$ garantimos a existência de polinômios $q_1, \ldots, q_r$ e r em $K[x,y]$ tais que

$$f = g_1q_1 + g_2q_2 + \ldots + g_rq_r + r, \tag{2}$$

em que nenhum monômio de r é divisível por $TL(g_1), TL(g_2), \ldots, TL(g_r)$. Se escrevermos $G = \{g_1, \ldots, g_r\}$ denotamos $r = \bar{f}^G$. Além disso, se I é um ideal de $K[x,y]$ tal que $I = \langle g1, ..., gr \rangle$, escrevemos também $r = \bar{f}^I$.

Neste ponto, gostaríamos de afirmar que $f \in I$ se, e somente se, $\bar{f}^I = 0$. Obviamente se $\bar{f}^I = 0$ temos que $f \in I$, mas se alterarmos a ordem dos elementos em G não temos garantia da unicidade de r na expressão (2), então $\bar{f}^I \neq 0$ não implica em $f \notin I$ (a menos que se resolva (2) para todas as ordenações possíveis dos elementos de G). Isso motiva a próxima definição:

Definição 1. Seja $I \subset K[x,y]$ um ideal. Dizemos que $G = \{g_1, \ldots, g_r\} \subset I$ é uma base de Groebner para I, se: $\langle (TL(g1)), ..., (TL(gr)) \rangle = \langle TL(I) \rangle$. Note que a igualdade acima nem sempre ocorre, por exemplo, em $I = \langle x^2+y, x^2-1 \rangle$ temos que $y+1 = (x^2+y)-(x^2-1) \in I \Rightarrow y = TL(y+1) \in \langle TL(I) \rangle$, mas por outro lado $\langle (TL(x^2+y)), (TL(x^2-1)) \rangle = \langle x^2, x^2 \rangle = \langle (x^2) \rangle \not\ni y$.

Agora, mesmo que o conjunto gerador $G = \{g_1, \ldots, g_s\}$ de um ideal I não seja uma Base de Groebner, o Algoritmo de Buchberger gera a partir de G uma Base de Groebner:

Teorema 1 (Algoritmo de Buchberger). Sejam I um ideal do anel $K[x,y]$ e $G = \{g_1, g_2, \ldots, g_r\}$ um conjunto gerador de I. Para formar uma base de Groebner a partir de G usaremos o algoritmo a seguir.

1. Defina $G_0 = G$;
2. Para cada $a_j \neq a_i \in G_k$ calcule $\alpha_{ij} := \overline{\left(\frac{TL(a_i) \cdot a_j}{MDC(a_i, a_j)} - \frac{TL(a_j) \cdot a_i}{MDC(a_i, a_j)} \right)}^{G_k}$.

   Se $\alpha_{ij} \neq 0$, defina $G_{k+1} \cup \{\alpha_{ij}\}$, $k = k+1$ e reinicie o passo 2.

   Se $\alpha_{ij} = 0$, encontre outro par $a'_j \neq a'_i \in G_k$ e repita o processo dado no passo 2;

   Se $\alpha_{ij} = 0$ para todos os a_j, $a_i \in G_k$ passe para o passo 3.
3. G_k é uma base Grobner para I.

Teorema 2. Se G é uma base de Groebner para o ideal I. Se $f \in k[x,y]$ é tal que $\bar{f}^G = 0$ para alguma ordenação dos elementos de G, então $\bar{f}^G = 0$ para toda ordenação dos elementos de G.