Teorema da Base de Hilbert

Nelson Prata Pravato Serrano

Orientadora: Thais Maria Dalbelo

Bacharelado em Matemática

UFSCar, São Carlos, Departamento de Matemática

Rod. Washington Luiz, s/n, São Carlos - SP, 13565-905

nelsonppserrano@gmail.com, thaisdalbelo@dm.ufscar.br

Resumo

Neste trabalho apresentamos o Teorema da base de Hilbert bem como uma aplicação no estudo de variedades algébricas.

1. Preliminares

Nesta seção apresentamos alguns conceitos preliminares, que serão utilizados ao longo do trabalho. Para visão geral sobre tais conceitos indicamos ([1] e [2]).

Neste trabalho consideraremos *A* um anel comutativo com unidade $1 \neq 0$.

Definição 1 *Seja A um anel. Um subconjunto $I \subseteq A$ é dito ideal, se:*

(i) $\forall x, y \in I, x + y \in I;$

(ii) dados $x \in I,\ a \in A,\ ax \in I.$

Definição 2 *Um ideal $I \subseteq A$ é dito ideal gerado por $\{b_\lambda\}_{\lambda \in \Lambda}$, se para qualquer $x \in I$ temos que $x = a_1 b_{\lambda_1} + a_2 b_{\lambda_2} + ... + a_n b_{\lambda_n}$, onde $\forall i \in \mathbb{N},\ a_i \in A, b_{\lambda_i} \in \Lambda$.*

Exemplo 1 *O conjunto dos inteiros ($\mathbb{Z}$) munido da soma e produto usual é um anel, representado como $(\mathbb{Z}, +, \cdot)$. Um ideal do mesmo é $2\mathbb{Z} := \{2x;\ x \in \mathbb{Z}\}$. De fato, basta ver que a soma de números pares é par e o produto de um par por qualquer outro número inteiro também é par. E também o mesmo é finitamente gerado pelo 2, pois todo número par é múltiplo de 2.*

Definição 3 ([2]) *Seja A um anel. O conjunto de todos os polinômios em x com coeficientes em A é denotado por $A[x]$.*

Obeservemos que $A[x]$ também é um anel sendo a soma e produto usual de polinômios. Analogamente podemos definir um anel de "*n*"variáveis com coeficientes em *A*, denotados como $A[x_1, x_2, ..., x_n]$.

Exemplo 2 *Seja R o conjunto dos números Reais munido da soma e produto usual denotado por $(\mathbb{R}, +, \cdot)$. O anel de polinômios $\mathbb{R}[x]$ tem elementos da forma*

$$f(x) = a_0 + a_1 x + ... + a_d x^d$$

tal que $\forall i,\ a_i \in \mathbb{R},\ n \in \mathbb{N}$. Analogamente, $\mathbb{R}[x, y, z]$ é um anel de polinômio de três variáveis. Exemplos de elementos deste anel são $p_1(x, y, z) = x^2 + y^2 + z^2 - 1$ e $p_2(x, y, z) = y^2 - x^3 - x^2 z^2$.

Definição 4 ([1]) *Um anel A é dito **noetheriano** se uma das seguintes propriedades se verificam:*

(i) todo ideal $I \subseteq A$ é finitamente gerado;

(ii) toda cadeia ascendente de ideais estabiliza, isto é, se, dada uma cadeia de ideais

$$I_1 \subseteq I_2 \subseteq \cdots$$

então $I_i = I_{i+1}$ para $i >> 0$ suficientemente grande;

(iii) todo subconjunto $S \neq \emptyset$ de ideais de A tem um elemento maximal em S com relação a inclusão.

É possível mostrar ([1]) que as definições acima são equivalentes.

Definição 5 *Denotaremos o grau de um polinômio $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_d x^d$ tal que $a_d \neq 0$ por $\partial(f(x))$. Além disso a_d será chamado de coeficiente lider.*

2. Teorema da Base de Hibert

Teorema 1 ([1]) *Seja A um anel noetheriano. Então $A[x]$ é noetheriano.*

Demonstração:Mostraremos que qualquer ideal $I \subseteq A[x]$ é finitamente gerado. Para isto, para cada inteiro $d \geq 0$, defina o ideal em A

$$J_d := \{a \in A;\ a \text{ é coeficiente lider de algum} f(x) \in I \text{ de grau } d\} \cup \{0\}.$$

Iremos mostrar que J_d é um ideal. De fato, dados $r, s \in J_d$ e polinômios $f(x), g(x) \in I$ de grau d e com coeficientes lideres r e s respectivamente, temos que $f(x) + g(x) \in I$ é de grau $\leq d$, então, se $\partial(f(x) + g(x)) = d$ logo $r + s \in J_d$, agora, se $\partial(f(x) + g(x)) < d$, então, temos que $r = -s$, e como o 0 está em J_d, então a soma pertence a J_d.
Agora, tomemos $r \in A$ $s \in J_d$ e um polinômio $h(x) \in I$ de grau d e coeficiente lider igual a s. Note que se $r \neq 0$, então $r \cdot s \in J_d$ pela preservação do grau, se $r = 0$, temos que $0 \in J_d$, logo $r \cdot s \in J_d$
Além disso,

$$f(x) \in I \Rightarrow x f(x) \in I$$

e então concluímos que $J_d \subseteq J_{d+1}$ (basta ver que em J_d existe o 0). Como *A* é noetheriano, obtemos portanto uma cadeia ascendente estacionária (digamos a partir de um $D \geq d$).

Para cada $d = 0, 1, 2, ..., D$, escolha um conjunto finito $S_d \subseteq I$ de polinômios de grau d cujos coeficientes líderes geram J_d (é possivel pois A é noetheriano, então todo ideal é finitamente gerado) e seja

$$S = \cup_{d=0}^{D} S_d$$

ou seja, S é finito, pois os J_d são finitamente gerados, então $S = \{p_1(x), p_2(x), p_3(x), ..., p_n(x)\}$. Mostraremos que S gera I.

Seja $K \subseteq A[x]$ o ideal gerado por S. Claramente $K \subseteq I$. Reciprocramente, dado $f(x) \in I$, iremos usar indução no grau de $f(x)$ para mostrar que $f(x) \in K$. Então, se o grau de $f(x)$ é igual a zero, é óbvio que $f(x) \in K$, então suponha $d \geq 0$, se $d \leq D$ então existe uma combinação linear dos elementos de S que descrevem $f(x)$ pela construção dos $p_i(x)$.

Se $d > D$, em relação a J_i, como *A* é noetheriano $J_d = J_D$, logo existe uma combinação linear dos polinômios em $\{x^{d-D} \cdot p(x);\ p(x) \in S_D\}$ com mesmo coeficiente lider de $f(x)$. Assim, em ambos os casos, existem monômios $m_i(x) = c_i x^{e_i}$ ($c_i \in A$) e polinomios $p_1(x), p_2(x), p_3(x), ..., p_i(x) \in S$ tais que $\partial(f(x)) = d$ e $\partial(m_1(x)p_1(x) + m_2 p_2(x) + ... + m_i p_i(x)) = d$ e alé disso, $f(x)$ e $(m_1(x)p_1(x) + m_2 p_2(x) + ... + m_i p_i(x))$ têm o mesmo coeficiente lider, de modo que

$$\partial(f(x) - m_1(x)p_1(x) - m_2 p_2(x) - ... - m_i p_i(x)) < d.$$

Tome $p(x) = f(x) - m_1(x)p_1(x) - m_2 p_2(x) - ... - m_i p_i(x)$ e observe que $\partial(p(x)) < d$, então pela hipótese de indução nos graus, $p(x) \in K$, e como K é um ideal, e os $m_i p_i(x)$ estão em K então $f(x)$ está em K.

Corolário 1 *Se A é noetheriano, então $A[x_1, x_2, ..., x_n]$ é noetheriano.*

3. Aplicação

A seguir, faremos uma aplicação do Teorema da *base de Hilbert* no estudo de conjuntos especiais que chamamos de **conjuntos algébricos**. Para tanto nessa seção consideraremos $A = \mathbb{C}$.
Seja $\mathbb{C}[x_1, x_2, ..., x_n]$ o anel de polinômios em n variáveis sobre $\mathbb{C}$. Desta forma, faz sentido falar no conjunto de zeros de $f(x) \in \mathbb{C}[x_1, x_2, ..., x_n]$ que denotaremos como

$$Z(f) := \{p \in \mathbb{C}^n;\ f(p) = 0\}.$$

De forma mais geral, se T for um subconjunto de $\mathbb{C}[x_1, x_2, ..., x_n]$, podemos definir o conjunto de zeros de T como sendo

$$Z(T) := \{p \in \mathbb{C}^n; f(p) = 0,\ \forall f(x) \in T\}.$$

Podemos mostrar que se I for um ideal de $\mathbb{C}[x_1, x_2, ..., x_n]$ gerado por T então $Z(T) = Z(I)$. Mais ainda, como $\mathbb{C}$ é um anel noetheriano, então pelo Corolário 1 então $\mathbb{C}[x_1, x_2, ..., x_n]$ é noetheriano, logo, qualquer ideal I tem um número finito de geradores, $f_1, .., f_r$, por tanto, $Z(T)$ pode se expresar como o conjunto de zeros comuns de um número finito de polinômios. Além disso, muitas propriedades de $Z(T)$ podem ser obtidas utilizando informações ideal I.

No caso em que I é um ideal radical, i.e $I = \sqrt{I} := \{r \in A;\ r^n \in I,$ para algum $n \in \mathbb{N}\}$, chamamos o conjunto $Z(I)$ de variedade algébrica.

Variedades algébricas são objetos particularmente interessantes muito estudados em várias áreas da matemática e também de outras áreas do conhecimento.

Exemplo 3 *Considere a função polinomial $f : \mathbb{C}^2 \to \mathbb{C}$ dada por $f(x, y) = y^2 - x^3$. Neste caso, temos que $Z(f)$ é um subconjunto irredutivel de $\mathbb{C}^2$ e portanto uma variedade algébrica.*

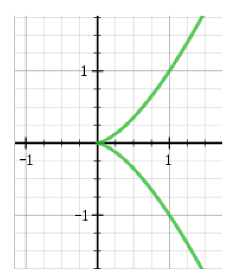

***Figura 1:** cúspide*

Observe que a curva acima não é regular na origem de $\mathbb{C}^2$. Dizemos que tal curva possui uma singularidade na origem de $\mathbb{C}^2$.
Objetos singulares fazem parte do nosso cotidiano e são frequentemente estudados em várias áreas. Por exemplo, em teoria de nós, ótica, robótica e visão computacional. As cúspides, por exemplo, aparecem na odontologia, uma vez que as coroas dentárias são constituídas pela união de cúspides.

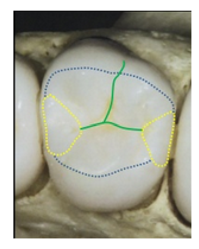

***Figura 2:** cúspide*

Referências

[1] H. Borges e E. Tengan álgebra comutativa em quatro movimentos *IMPA, Rio de Janeiro*, 2015.

[2] J. B. Fraleigh. A First Course in Abstract Algebra *Addison-Wesley Pub*, 1982.