# Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática


# Teorema dos Zeros de Hilbert


Alunos:

José Anderson Valença Cardoso RA: 069701

Luís Henrique de Miranda RA: 069703

Rafael Rodrigo Ottoboni RA: 040994

Prof: Fernando Torres



Campinas-SP

Junho de 2007


## Objetivo:

**-** Estabelecer o teorema clássico de zeros de Hilbert.

# Conteúdo

# 1 Definições e Resultados Preliminares

Dedicamos esta seção a apresentação de alguns resultados e definições que serão utilizados subsequentemente. Supomos conhecidas as noções básicas de aneis, ideais, módulos, etc. Iniciamos com alguns conceitos de extensões de corpos.

## 1.1 Extensões de Corpos

Se $F$ é um subcorpo de um corpo $E$, dizemos que $E$ é uma ***extensão*** do corpo $F$. Podemos considerar $E$ como um espaço vetorial sobre $F$, e dizemos que $E$ é uma ***extensão finita*** ou ***infinita***, quando o espaço vetorial tem dimensão finita ou infinita, respectivamente.

Seja $F$ um subcorpo de um corpo $E$. Um elemento $a \in E$ é dito ***algébrico*** sobre $F$ se existem $a_0, ..., a_n \in F$ tais que

$$a_n a^n + ... + a_1 a + a_0 = 0.$$

Uma extensão $E$ de $F$ é dita ***algébrica*** se qualquer elemento de $E$ é algébrico sobre $F$.

## 1.2 A-álgebras

Sejam $A, B$ anéis e $f : A \to B$ um homomorfismo de anéis. Se $a \in A$ e $b \in B$, definimos o produto

$$ab = f(a)b.$$

Esta definição de multiplicação escalar torna o anel $B$ um $A$-módulo. Dessa forma, $B$ tem estrutura de $A$-módulo assim como de anel. O anel $B$ com estrutura de $A$-módulo é chamado de ***$A$-álgebra***. Assim, uma $A$-álgebra é por definição um anel $B$ junto com um homomorfismo de anéis $f : A \to B$. Em particular, se $A$ é um corpo $K$ e $B \neq 0$ então $f$ é injetiva e portanto podemos identificar $K$ com sua imagem por $f$. Assim, uma $K$-álgebra é de fato um anel que contêm $K$ como subanel.

Sejam $f : A \to B$ e $g : A \to C$ dois homomorfimos de anéis. Dizemos que $h : B \to C$ ***é um homomorfismo de $A$-álgebras*** quando $h$ é homomorfismo de anéis e de $A$-Módulos.

Dizemos que uma $A$-álgebra $B$ é ***finita*** se $B$ é finitamente gerado como $A$-Módulo. Caso exista um conjunto finito $x_1, ..., x_n$ em $B$ tal que todo elemento de $B$ pode ser escrito como um polinômio em $x_1, ..., x_n$ com coeficientes em $f(A)$ então dizemos que B é uma $A$-álgebra ***finitamente gerada***; ou equivalentemente se existir um homomorfismo de $A$-álgebras entre o anel de polinômios $A[t_1, ..., t_n]$ sobre $B$.

## 1.3 Anéis e Módulos Noetherianos

Seja $M$ um $A$-módulo. Dizemos que $M$ satisfaz a ***condição de cadeia ascendente*** ($acc$) se cada cadeia ascendente de submódulos

$$N_1 \subseteq ... \subseteq N_n \subseteq ...$$

é estacionária, isto é existe $n$ tal que $N_n = N_{n+1} = ....$ Em particular, como o anel $A$ é um $A$-Módulo, dizemos que $A$ satisfaz ($acc$) se cada cadeia de ideais em $A$

$$I_1 \subseteq ... \subseteq I_n \subseteq ...$$

é estacionária. Dizemos que $M$ é ***Noetheriano*** se satisfaz ($acc$).

Enunciaremos agora alguns resultados que serão usados no decorrer do trabalho.

**Proposição 1.1** *Seja $M$ um $A$-módulo. $M$ é Noetheriano se, e somente se, todo submódulo de $M$ é finitamente gerado.*

**Demonstração:** Veja Proposição 6.2 de [1].

□

**Proposição 1.2** *Sejam $A$ um anel Noetheriano e $M$ um $A$-módulo finitamente gerado. Então $M$ é Noetheriano.*

**Demonstração:** Veja Proposição 6.5 de [1].

□

**Proposição 1.3** *Sejam $A$ um anel Noetheriano e $I$ um ideal de $A$. Então $A/I$ é um anel Noetheriano.*

**Demonstração:** Veja Proposição 6.5 de [1].

□

# 2 Teorema dos Zeros de Hilbert

**Teorema 2.1** *(Teorema da base de Hilbert) Seja $A$ anel Noetheriano, então $A[X]$ é anel Noetheriano.*

**Demonstração:** Pela definição de anel Noetheriano, se todo ideal I de um anel R é finitamente gerado então R é Noetheriano. Assim para provamos que $A[X]$ é Noetheriano tomemos $J \lhd A$ e mostremos que $J$ é finitamente gerado.

Seja $J \lhd A$ e defina

$$I_m = \{a \in A \,\text{tq}\, \exists\, t = ax^m + \text{polinômio de ordem menor que m}, t \in J, a \neq 0\} \cup \{0\}.$$

Observe que $I_m \lhd A$. De fato:

$a_1, a_2 \in I_m \Rightarrow (\exists f_1 = a_1x^m +$ polinômio de grau menor que $m$ ou $a_1 = 0)$ e $(\exists f_2 = a_2x^m +$ polinômio de grau menor que $m$ ou $a_2 = 0)$.

Se $a_1 = 0 = a_2 \Rightarrow a_1 - a_2 = 0 \in I_m$.

Se $a_1 = 0$ e $a_2 \neq 0 \Rightarrow a_1 - a_2 = -a_2 \in I_m$, pois $-f_2 \in J$.

Se $a_1 \neq 0$ e $a_2 = 0 \Rightarrow a_1 - a_2 = a_1 \in I_m$, pois $f_1 \in J$.

Se $a_1 \neq 0$ e $a_2 \neq 0 \Rightarrow f_1, f_2 \in J \Rightarrow f_1 - f_2 \in J \Rightarrow a_1 - a_2 \in I_m$.

Se $a \in A$ e $a_1 = 0 \Rightarrow aa_1 = 0 \in I_m$

Se $a \in A$ e $a_1 \neq 0$ e $aa_1 \neq 0 \Rightarrow af_1 \in J \Rightarrow aa_1 \in I_m$.

Logo $I_m \lhd A$.

Note que $I_m \subset I_{m+1} \subset \ldots \forall m$. Seja $0 \neq a \in I_m$, então existe $f \in J$ tal que $f = ax^m +$ polinômio de grau menor que m. Portanto $xf = ax^{m+1} +$ polinômio de grau menor que $m$ está em $J$, visto que $J \lhd A[X]$. Logo $a \in I_{m+1}$.

Assim temos uma cadeia crescentes de ideais de $A$ e como $A$ é Noetheriano esta cadeia estabiliza, ou seja, existe $i_0$ tal que $\forall i \geq i_0$ obtemos $I_i = I_{i_0}$. Portanto, como cada submódulo de um módulo Noetheriano é finitamente gerado (1.1), cada ideal de um anel Noetheriano é finitamente gerado. Desta forma, para cada $i \leq i_0$ vamos fixar um conjunto de geradores$\{a_{i_1}, \ldots a_{ik_i}\}$ de $I_i$, ou seja $I_i = \displaystyle\sum_{i \leq j \leq k_i} Aa_{i_j}$.

Se $a_{i_j} \neq 0$, então $\exists f_{i_j} \in J$ tal que $f_{i_j} = a_{i_j} x^i +$ polinômio de grau menor que $i$.

Se $a_{i_j} = 0$ defina $f_{i_j} = 0 \in J$.

Agora o objetivo é mostrar que $\{f_{i_j}\}, 0 \leq i \leq i_0$ e $1 \leq j \leq k_i$ gera $J$ como ideal de $A[X]$.

Para mostrar o objetivo tome $f \in J - \{0\}$. Assim $f = ax^m +$ polinômio de grau menor que $m$ e $0 \neq a \in I_m$.

Temos que ou $m > i_0$ ou $m \leq i_0$.

**Caso** $m > i_0$.

$$Aa_{i_0 1} + \cdots + Aa_{i_0 k_0} = I_{i_0} = I_{i_0+1} = \cdots = I_m$$

e

$$\exists f_{i_0 j} x^{i_0} + \text{ polinômio de ordem menor que } .i_0$$

Como $a \in I_m$ temos $a = b_1 a_{i_0 1} + \cdots + a_{i_0 k_0}$, onde $b_i \in A$.

Seja $\overline{f} = b_1 f_{i_0 1} + \cdots + b_{k_0} f_{i_0 k_0}$, assim $\overline{f} = ax^{i_0}$ + polinômio de grau menor que $i_0$. Definindo $g = \overline{f} x^{m-i_0}$, temos $f - g = 0$ ou $f - g$ é um polinômio de grau menor que $m$.

Defina $\overline{J}$ ideal de $A[X]$ gerado por $\{f_{i_j}\}, i \leq i_0, j \leq k_i$, subconjunto de $J$.

Temos que $\overline{f} \in \overline{J}$ e $\overline{f} x^{m-i_0} \in \overline{J}$. Logo $f - g \in J$.

Prosseguindo desta forma, chegamos a um polinômio com grau menor que $i_0$, isto é cai no segundo caso:

**Caso** $m \leq i_0$

Seja $f \in J - \{0\}$, $f = ax^m$ + polinômio de grau menor que $m$,

$$a \in I_m = \sum_{1 \leq j \leq k_m} Aa_{m_j},$$

$$a = \sum_j b_j a_{m_j},$$

$$\overline{f} = \sum_j b_j f_{m_j}.$$

Logo, $f - \overline{f} \in J$ é nulo ou tem grau menor que m.

Esse processo é finito, então chegamos no zero. Logo $f - \overline{f_1} - \ldots \overline{f_z} = 0$ para alguns $\overline{f_i} \in \overline{J}$. Logo $f = \overline{f_1} + \ldots \overline{f_z} \in \overline{J}$.

Portanto $J \subset \overline{J}$ e como $\overline{J} \subset J$ então $J = \overline{J}$. Assim $J$ é finitamente gerado.

$\square$

**Corolário 2.2** *Seja $A$ Noetheriano, então $A[X_1, \ldots, X_n]$ é Noetheriano.*

**Demonstração:** Vamos fazer a prova por indução sobre $n$. Para $n = 1$ o resultado é válido pelo teorema anterior. Por hipótese de indução temos que $A[X_1, \ldots, X_{n-1}]$ é Noetheriano. Como $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, pela hipótese de indução e pelo teorema da base de Hilbert, concluímos que $A[X_1, \ldots, X_n]$ é Noetheriano.

$\square$

**Corolário 2.3** *Seja $A \subset B$ extensão de anéis tal que $B$ é uma $A-$álgebra finitamente gerada e $A$ um anel Noetheriano, então $B$ é Noetheriano.*

**Demonstração:** Pela definição de álgebra finitamente gerada temos que existe um homomorfismo sobrejetor $F : A[x_1, \ldots, x_n] \to B$. Assim, pelo corolário anterior segue o resultado.

$\square$

**Proposição 2.4** *Sejam $A \subset B \subset C$ extensão de anéis, $A$ anel Noetheriano, $C$ uma $A$-álgebra finitamente gerada e $C$ finitamente gerado como $B$-módulo. Então $B$ é uma $A$-álgebra finitamente gerada.*

**Demonstração:** $C$ é finitamente gerado como $B$-módulo, então existe $\{y_1, \ldots, y_s\} \subset C$ tal que $C = By_1 + \cdots + By_s$. $C$ também é uma $A$-álgebra finitamente gerada, isto é existe $\{c_1, \ldots, c_m\} \subset C$ tal que $C = A[c_1, \ldots, c_m]$. Assim existem $\{b_{ij}\}, \{b_{ijk}\} \subset B$ tais que

$$c_i = \sum_j b_{ij} y_j$$

e

$$y_i y_j = \sum_k b_{ijk} y_k.$$

Seja $B_0$ $A-$álgebra gerada pelos conjuntos $\{b_{ij}\}$ e $\{b_{ijk}\}$. Portanto $A \subset B_0 \subset B \subset C$.

Todo elemento de $C$ é um polinômio em $c_i$ como coeficientes em $A$. Usando a expressão de $c_i$ encontrada acima obtemos $C = B_0 y_1 + \cdots + B_0 y_s$, isto é $C$ é finitamente gerado como $B_0-$ módulo. Assim, do corolário anterior, temos que $B_0$ é Noetheriano e como $B$ é submódulo de $C$ segue dos resultados (1.2) que $B$ é finitamente gerado como $B_0-$ módulo. Logo, como $B_0$ é $A-$ álgebra finitamente gerada, segue que $B$ é uma $A-$ álgebra finitamente gerada.

$\square$

**Proposição 2.5** *Sejam $k$ um corpo e $k \subset E$ extensão de aneis tal que $E$ é uma $A-$álgebra finitamente gerada. Se $E$ é um corpo, então $k \subset E$ é uma extensão algébrica finita.*

**Demonstração:** Pela definição de álgebra finitamente gerada e usando o fato de $k$ ser corpo obtemos $E = k[y_1, \ldots, y_s]$. Como por hipótese $E$ é um corpo temos que $E = k(y_1, \ldots, y_s)$. Depois de uma renumeração dos geradores $y_1, \ldots, y_s$ podemos supor que $y_1, \ldots, y_r$ não são algebricos sobre $k$ e $yr + 1, \ldots, y_s$ são algébricos sobre $k$. Observe que $E_1 = k(y_1, \ldots, y_r) \subset k(y_1, \ldots, y_s) = E$ é uma extensão finita, pois $y_i, i > r$ é algébrico sobre $E_1$, logo $E = E_1(y_{r+1}, \ldots, y_s)$ e $dim_{E_1} E < \infty$. Assim, pela última próposição temos que $E_1$ é uma $k-$ álgebra finitamente gerada. Vamos mostrar que $r = 0$ e assim obteremos $E_1 = k$ concluindo que $k \subset E$ é uma extensão algébrica finita de corpos..

Suponha que $r \geq 1$. Daí $E_1 = k[\alpha_1, \ldots, \alpha_z]$, $\alpha_i \in E_1$. Portanto $\alpha_i = \frac{f_i}{g_i}$, onde $f_i, g_i \in k[y_1, \ldots, y_s]$, então

$$E_1 = k[\frac{f_1}{g_1}, \dots, \frac{f_z}{g_z}] \subset k[y_1, \dots, y_r, \frac{1}{g_{r+1}}, \dots \frac{1}{g_z}] = \bigcup_{a_i \geq 0} \frac{k[y_1, \dots, y_r]}{g_1^{a_1} \dots g_z^{a_z}}$$

Escolha $g = g_1 \dots g_z + 1$ o qual é irredutível e primo com cada $g_i$. Assim $\frac{1}{g}$ não está em $\frac{k[y_1,\dots,y_r]}{g_1^{a_1}\dots g_r^{a_r}}$, porém $E_1$ é corpo, isto é, $\frac{1}{g}$ está em $E_1 \subset \bigcup_{a_i \geq 0} \frac{k[y_1, \dots, y_r]}{g_1^{a_1} \dots g_z^{a_z}}$, uma contradição.

Logo $r = 0$ como queríamos.

□

**Teorema 2.6** *(Teorema de Zeros de Hilbert) Seja $k$ um corpo, $A$ uma $k-$álgebra fintamente gerada e $M$ um ideal maximal de $A$. Então o corpo $A/M$ é extensão algébrica de $k$.*

**Demonstração:** Tomamos $E = A/M$ e aplicamos a proposição anterior. Note que $A/M$ é uma $k-$álgebra finitamente gerado, pois $A$ o é e $A/M$ é corpo, já que $M$ é maximal.

□

# Referências


[1] Atiyah, M. F. and Macdonald, I. G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969.

[2] Kunz, E., *Introduction to Commutative Algebra and Algebric Geometry,* Birkhüser, Boston, 1985.

[3] Lang, S., *Algebra*, Addison-Wesley, New York, 1969.

[4] Larsen, M. D. and McCarthy, P. J., *Multiplicative Theory of Ideals*, Academic Press, London, 1971.