Teorema de Zeros de Hilbert

Alunos: Daniela Moura Prata RA: 057735
Maribel Díaz Noguera RA: 049112
Welington Vieira Assunção RA: 030376

Professor: Fernando Torres

1 Introdução

O objetivo deste trabalho é estudar o Teorema de Zeros de Hilbert, também conhecido como Nullstellensatz. Este é um teorema de geometria algébrica que relaciona conjuntos algébricos e ideais em anéis de polinômios sobre corpos algebricamente fechados. Para isso, vamos fazer um breve estudo de anéis de valorização, necessário para o desenvolvimento do Nullstellensatz.

2 Anéis de valorização

Seja B um domínio de integridade e denotemos por k seu corpo de frações. Dizemos que B é um *anel de valorização* de k se, para cada $x \neq 0$, ou $x \in B$ ou $x^{-1} \in B$ (ou ambos).

Uma propriedade importante que será utilizada mais adiante é que se B é um anel de valorização de k, então B é integralmente fechado (em k). De fato, seja $x \in k$ integral sobre B. Então x satisfaz uma equação da forma

$$x^n + b_1 x^{n-1} + ... + b_n = 0,$$

com $b_i \in B$. Se $x \in B$, então não há nada o que demonstrar. Se não, então $x^{-1} \in B$ e portanto

$$x = -(b_1 + b_2 x^{-1} + ... + B_n x^{1-n}) \in B.$$

Sejam k um corpo e Ω um corpo algebricamante fechado. Seja Σ o conjunto de todos os pares (A, f) onde A é um subanel de k e f é um homomorfismo de A em Ω. Ordenamos parcialmente o conjunto Σ da seguinte maneira:

$$(A, f) \leq (A', f') \Leftrightarrow A \subseteq A' \text{ e } f'|_A = f.$$

As condições do Lema de Zorn são claramente satisfeitas, logo o conjunto Σ tem pelo menos um elemento maximal.

Seja (B, g) um elemento maximal de Σ. Estamos interessados em mostrar que B é um anel de valorização de k. Vamos começar com o seguinte lema:

Lema 2.1 *B é um anel local e $\mathcal{M} = Ker(g)$ é seu ideal maximal.*

Demonstração. Como $g(B)$ é um subanel de um corpo, temos que $g(B)$ é um domínio de integridade. Logo, o ideal $\mathcal{M} = ker(g)$ é primo. Podemos estender g à um homomorfismo $\overline{g} : B_{\mathcal{M}} \to \Omega$ definindo $\overline{g}(b/s) = g(b)/g(s)$, para todo $b \in B$ e $s \in S = B - \mathcal{M}$, pois $g(s) \neq 0$. Como o par (B, g) é maximal, segue que $B = B_{\mathcal{M}}$ e como $B_{\mathcal{M}}$ é local, segue então que B é um anel local e $\mathcal{M}$ é seu ideal maximal. $\square$

Lema 2.2 *Seja x um elemento não-nulo de k. Sejam $B[x]$ o subanel de k gerado por x sobre B, e $\mathcal{M}[x]$ a extensão de $\mathcal{M}$ em $B[x]$. Então ou $\mathcal{M}[x] \neq B[x]$ ou $\mathcal{M}[x^{-1}] \neq B[x^{-1}]$.*

Demonstração. Suponha que $\mathcal{M}[x] = B[x]$ e $\mathcal{M}[x^{-1}] = B[x^{-1}]$. Então temos

$$u_0 + u_1 x + ... + u_m x^m = 1, \quad u_i \in \mathcal{M} \tag{1}$$

e

$$v_0 + v_1 x^{-1} + ... + v_n x^{-n} = 1, \quad v_j \in \mathcal{M}, \tag{2}$$

onde podemos assumir que os graus m e n são os menores possíveis. Suponha $m \geq n$. Multiplicando (2) por x^n, temos

$$(1 - v_0)x^n = v_1 x^{n-1} + ... + v_n. \tag{3}$$

Como $v_0 \in \mathcal{M}$, segue do Lema 2.1 que $1 - v_0$ é inversível em B e portanto podemos reescrever (3) da seguinte forma:

$$x^n = w_1 x^{n-1} + ... + w_n, \quad w_i \in \mathcal{M}.$$

Logo podemos substituir x^m em (1) por $w_1 x^{m-1} + ... + w_n x^{m-n}$, obtendo

$$u_0 + u_1 x + ...u_m w_1 x^{m-1} + ... + u_m w_n x^{m-n} = 1,$$

e isto contradiz a minimalidade do expoente m. $\square$

Teorema 2.1 *Seja (B, g) um elemento maximal de Σ. Então B é um anel de valorização do corpo k.*

Demonstração. Temos que mostrar que se $x \neq 0$ é um elemento de k, então ou $x \in B$ ou $x^{-1} \in B$. Pelo Lema 2.2, podemos assumir que $\mathcal{M}[x]$ não é o ideal gerado pela unidade do anel $B' = B[x]$. Desse modo, $\mathcal{M}[x]$ está contido em um ideal maximal $\mathcal{M}'$ de B', e então temos $\mathcal{M}' \cap B = \mathcal{M}$, pois $\mathcal{M}' \cap B$ é um ideal próprio de B e contém $\mathcal{M}$. Logo o mergulho de B em B' induz um mergulho do corpo $k = B/\mathcal{M}$ no corpo $k' = B'/\mathcal{M}'$. Temos também $k' = k[\overline{x}]$ onde $\overline{x}$ é a imagem de x em k', logo $\overline{x}$ é algébrico sobre k, e portanto k' é uma extensão algébrica finita de k.

Agora o homomorfismo g induz um mergulho $\overline{g}$ de k em Ω, pois pelo Lema 2.1 $\mathcal{M}$ é o núcleo de g. Como Ω é algebricamente fechado, $\overline{g}$ pode ser estendido à um mergulho $\overline{g}'$ de k' em Ω. Fazendo a composição de $\overline{g}'$ com o homomorfismo natural $B' \to k'$, temos então um homomorfismo $g' : B' \to \Omega$ que estende g. Como o par (B, g) é maximal, segue que $B' = B$ e portanto $x \in B$. $\square$

Corolário 2.1 *Seja A um subanel de um corpo k. Então o fecho integral $\overline{A}$ de A em k é a interseção de todos os anéis de valorização de k que contém A.*

Demonstração. Seja B um anel de valorização de k tal que $A \subseteq B$. Sendo B integralmente fechado, segue que $\overline{A} \subseteq B$.
Reciprocamente, seja $x \notin \overline{A}$. Então x não está no anel $A' = A[x^{-1}]$. Logo x^{-1} é não inversível em A' e está portanto contido no ideal maximal $\mathcal{M}'$ de A'. Seja Ω um fecho algébrico do corpo $k' = A'/\mathcal{M}'$. Então a restrição à A do homomorfismo natural $A' \to k'$ define um homomorfismo de A em Ω. Pelo Teorema 2.1 este pode ser estendido a algum anel de valorização $B \supseteq A$. Como x^{-1} é levado no zero, segue que $x \notin B$. $\square$

Proposição 2.1 *Sejam $A \subseteq B$ domínios de integridade, B finitamente gerado sobre A, e v um elemento não-nulo de B. Então existe $u \neq 0$ em A com a seguinte propriedade: qualquer homomorfismo f de A em um corpo algebricamente fechado Ω tal que $f(u) \neq 0$ pode ser estendido a um homomorfismo g de B em Ω tal que $g(v) \neq 0$.*

Demonstração. Faremos a prova no caso em que B é gerado sobre A por um único elemento x. O caso geral seguirá por indução sobre o número de geradores.

Suponha que x é transcendente sobre A, isto é, que nenhum polinômio não-nulo com coeficientes em A tem x como uma raiz. Seja $v = a_0x^n + a_1x^{n-1} ... + a_n$, e considere $u = a_0$. Então se $f : A \to \Omega$ é tal que $f(u) \neq 0$, existe $\xi \in \Omega$ tal que $f(a_0)\xi^n + f(a_1)\xi^{n-1} + ... + f(a_n) \neq 0$, pois Ω é infinito. Defina $g : B \to \Omega$ estendendo f como $g(x) = \xi$. Então $g(v) \neq 0$, como queríamos.

Suponha agora que x é algébrico sobre A, isto é, sobre o corpo de frações de A. Então v^{-1} também é algébrico sobre A, pois v é um polinômio em x. Logo temos equações da forma

$$a_0x^m + a_1x^{m-1} + ... + a_m = 0, \quad a_i \in A \tag{4}$$

e

$$b_0v^{-n} + b_1v^{1-n} + ... + b_n = 0, \quad b_j \in A. \tag{5}$$

Sejam $u = a_0b_0$, e $f : A \to \Omega$ tal que $f(u) \neq 0$. Então f pode ser estendido primeiro à um homomorfismo $f_1 : A[u^{-1}] \to \Omega$, definindo $f_1(u^{-1}) = f(u)^{-1}$, e depois, pelo Teorema 2.1, à um homomorfismo $h : C \to \Omega$, onde C é um anel de valorização contendo $A[u^{-1}]$. Por (4), x é integral sobre $A[u^{-1}]$, logo, pelo Corolário 2.1, $x \in C$, ou seja, C contém B e, em particular, $v \in C$. Por outro lado, por (5), v^{-1} é integral sobre $A[u^{-1}]$, e portanto pelo Corolário 2.1 novamente está em C. Logo v é inversível em C e portanto $h(v) \neq 0$. Agora basta tomar g como sendo a restrição de h em B. $\square$

Corolário 2.2 *Sejam k um corpo e B uma k-álgebra finitamente gerada. Se B é um corpo então ele é uma extensão algébrica finita de k.*

Demonstração. Basta tomar $A = k$, $v = 1$ e $\Omega =$ fecho algébrico de k na Proposição 2.1. $\square$

3 Teorema de Zeros de Hilbert ou Nullstellensatz

Nesta seção estudaremos o Nullstellensatz. Vamos começar com algumas definições. Sejam k um corpo algebricamente fechado e $A = k[X_1, ..., X_n]$ o anel de polinômios em n-variáveis com coeficientes em k. Se $J \subseteq A$, o conjunto

$$V(J) := \{P \in k^n;\ f(P) = 0, \forall f \in J\}$$

é chamado uma *variedade algébrica afim.*

Seja X um subconjunto de k^n. Definimos

$$I(X) := \{f \in A;\ f(P) = 0, \forall P \in X\}.$$

Este conjunto é um ideal no anel de polinômios A. Quando $X = V(J)$, ele é chamado o *ideal da variedade* $V(J)$.
Uma pergunta natural agora seria: qual a relação entre $I(V(J))$ e J? Vejamos o seguinte exemplo:

Exemplo 3.1 *Considere* $J = \langle X^2 + 1\rangle$ *ideal de* $\mathbb{R}[X]$. *Temos*

$$I(V(J)) = I(\emptyset) = \mathbb{R}[X] \neq J.$$

O exemplo acima diz que $I(V(J)) \neq J$, e em geral é isso que ocorre. O Nullstellensatz nos diz qual a relação entre $I(V(J))$ e J, sob certas condições.

Teorema 3.1 (Zeros de Hilbert ou Nullstellensatz) *Seja k um corpo algebricamente fechado.*

i) Todo ideal maximal no anel $A = k[X_1, ..., X_n]$ é da forma $\langle X_1 - a_1, ..., X_n - a_n\rangle$, onde $a_i \in k$.

ii) Seja J um ideal de A. Se $J \neq \langle 1\rangle$, então $V(J)$ é não-vazio.

iii) Para todo $J \subseteq A$, temos $I(V(J)) = \sqrt{J}$

Observação 3.1 *Os itens i) e ii) são conhecidos como a versão fraca do Nullstellensatz e o item iii) como a versão forte.*

Demonstração. i) Sejam $\mathcal{M} \subset k[X_1, ..., X_n]$ um ideal maximal e $K := k[X_1, ..., X_n]/\mathcal{M}$. Considere φ a composição

$$\varphi : k \hookrightarrow k[X_1, ..., X_n] \to K.$$

Temos que K é corpo pois $\mathcal{M}$ é maximal, K é finitamente gerado como k-álgebra e φ é injetiva.
Pelo Corolário 2.2, K é algébrico sobre k e como k é algebricamente fechado, φ é um isomorfismo. Assim, para cada i, existe $X_i \in k[X_1, ..., X_n]$ tal que

$$X_i + \mathcal{M} = \varphi(a_i), \quad a_i \in k.$$

Mas $\varphi(a_i) = a_i + \mathcal{M}$, logo $X_i - a_i \in \mathcal{M}$, $i = 1, ..., n$. Então existem $a_1, ..., a_n \in k$ tais que $\langle X_1 - a_1, ..., X_n - a_n \rangle \subseteq \mathcal{M}$. Como $\langle X_1 - a_1, ..., X_n - a_n \rangle$ é um ideal maximal, segue que $\mathcal{M} = \langle X_1 - a_1, ..., X_n - a_n \rangle$.

ii) Seja J um ideal de A, com $J \neq \langle 1 \rangle$. Existe um ideal maximal $\mathcal{M}$ de A tal que $J \subseteq \mathcal{M}$ Por i), temos que $\mathcal{M} = \langle X_1 - a_1, ..., X_n - a_n \rangle$ e como $J \subseteq \mathcal{M}$, é claro que $V(\mathcal{M}) \subseteq V(J)$. Assim, $P = (a_1, ..., a_n) \in V(\mathcal{M})$ e portanto $P \in V(J)$.

iii) Seja $J \subseteq k[X_1, ..., X_n]$ e $f \in k[X_1, ..., X_n]$. Vamos introduzir a variável Y e considere o ideal

$$J_1 = \langle J, fY - 1 \rangle \subseteq k[X_1, ..., X_n, Y]$$

gerado por J e Y.
Temos que um ponto $Q \in V(J_1) \subseteq k^{n+1}$ é uma $n+1$-upla $Q = (a_1, ..., a_n, b)$ tal que

$$g(a_1, ..., a_n) = 0, \ \forall g \in J,$$

isto é,

$$P = (a_1, ..., a_n) \in V(J),$$

e

$$f(P)b = 1;$$

assim

$$f(P) \neq 0 \text{ e } b = f(P)^{-1}.$$

Vamos mostrar que $I(V(J)) \subseteq \sqrt{J}$, já que a inclusão contrária é clara.
Se $f \in I(V(J))$, então $f(P) = 0$ para todo $P \in V(J)$. Pelo que fizemos acima, $V(J_1) = \emptyset$ e pelo item ii), temos que $1 \in J_1$, assim

$$1 = \sum g_i f_i + g_0(fY - 1) \in k[X_1, ..., X_n] \tag{6}$$

com $f_i \in J$ e $g_0, g_i \in k[X_1, ..., X_n, Y]$.
Suponhamos que N seja a maior potência de Y que aparece em (6) em g_0, g_i. Multiplicando ambos os lados por f^N temos

$$f^N = \sum G_i(X_1, ..., X_n, fY)f_i + G_0(X_1, ..., X_n, fY)(fY - 1) \tag{7}$$

onde $G_i = f^N g_i$ é escrito como polinômio em $X_1, ..., X_n, (fY)$. Definindo $Y = f^{-1}$, temos

$$f^N = \sum G_i(X_1, ..., X_n, 1)f_i \in k[X_1, ..., X_n][f^{-1}].$$

Como G_i e f_i não dependem de f^{-1}, temos uma igualdade de polinômios em $k[X_1, ..., X_n]$, logo $f^N \in J$ e portanto $f \in \sqrt{J}$.
Portanto $\sqrt{J} = (I(V(J)))$. $\square$