O 'NULLSTELLENSATZ' DE HILBERT

FERNANDO FERREIRA

Neste capítulo, vamos demonstrar um célebre resultado de David Hilbert, muito importante em álgebra comutativa e, em especial, em geometria algébrica. A palavra alemã 'Nullstellensatz' pode traduzir-se por 'teorema do lugar dos zeros' e é, efectivamente, um teorema sobre a localização dos zeros de polinómios, a várias variáveis, sobre corpos. O que se segue pressupõe alguns conhecimentos básicos de álgebra sobre extensões de corpos, incluindo a existência e unicidade do fecho algébrico dum corpo. Também pressupomos familiaridade com a noção de ordinal e enumeração transfinita. Começamos por um lema:

Proposição 1. *Seja K um corpo e K_1 e K_2 extensões algebricamente fechadas de K. Suponhamos que $card(K_1) = card(K_2) > \max(\aleph_0, card(K))$. Então K_1 e K_2 são isomorfos sobre K.*

Demonstração. Seja κ a cardinalidade comum de K_1 e K_2. Vamos usar o método de "vai e vem". Considerem-se enumerações transfinitas $(a_\alpha)_{\alpha<\kappa}$ e $(b_\alpha)_{\alpha<\kappa}$ de K_1 e K_2, respetivamente. Vamos definir, por recursão transfinita em $\alpha < \kappa$, corpos K_1^α e K_2^α e isomorfismos (de corpos) $i_\alpha : K_1^\alpha \mapsto K_2^\alpha$, que são a identidade em K, tais que

i. para todo $\alpha < \kappa$, $K \subseteq K_1^\alpha \subseteq K_1$ e $K \subseteq K_2^\alpha \subseteq K_2$;
ii. $a_\alpha \in \mathrm{dom}(i_{2\alpha+1})$ e $b_\alpha \in \mathrm{im}(i_{2\alpha+2})$;
iii. se $\alpha < \beta$ então $K_1^\alpha \subseteq K_1^\beta$, $K_2^\alpha \subseteq K_2^\beta$ e i_β é extensão de i_α;
iv. para todo α, $card(K_1^\alpha) = card(K_2^\alpha) < \kappa$.

Definimos $K_1^0 = K_2^0 := K$ e i_0 a identidade. Para um ordinal da forma $2\alpha + 1$, há dois casos a considerar. No primeiro caso, a_α é algébrico sobre $K_1^{2\alpha}$. Neste caso, considere-se $p(X) \in K_1^{2\alpha}[X]$ um polinómio irredutível tal que $p(a_\alpha) = 0$. Seja $\overline{p}(X) \in K_2^{2\alpha}[X]$ o polinómio obtido a partir de $p(X)$ substituindo os seus coeficientes pelas correspondentes imagens através do isormorfismo $i_{2\alpha}$. É claro que $\overline{p}(X)$ é um polinómio irredutível sobre $K_2^{2\alpha}$. Visto que K_2 é algebricamente fechado, tome-se $b \in K_2$ tal que $\overline{p}(b) = 0$. Como sabemos de álgebra, os corpos $K_1^{2\alpha+1} := K_1^{2\alpha}(a_\alpha)$ e $K_2^{2\alpha+1} := K_2^{2\alpha}(b)$ são isomorfos (já que são isomorfos aos corpos de rutura $K_1^{2\alpha}[X]/\langle p(X)\rangle$ e $K_2^{2\alpha}[X]/\langle \overline{p}(X)\rangle$, respetivamente, e estes dois corpos de rutura são obviamente isomorfos) através dum isomorfismo $i_{2\alpha+1}$ que é extensão de $i_{2\alpha}$. No segundo caso, a_α é transcendente sobre $K_1^{2\alpha}$. Ora, a cardinalidade do fecho algébrico de $K_2^{2\alpha}$ é $\max(\aleph_0, card(K_2^{2\alpha}))$ e, portanto, é estritamente menor do que κ. Logo, podemos tomar b em K_2 que não esteja no fecho algébrico de $K_2^{2\alpha}$. Em suma, podemos tomar um elemento $b \in K_2$ transcendente sobre $K_2^{2\alpha}$. Novamente, por resultados de álgebra, sabemos que $K_1^{2\alpha+1} := K_1^{2\alpha}(a_\alpha)$ e $K_2^{2\alpha+1} := K_2^{2\alpha}(b)$ são isomorfos (já que são isomorfos aos corpos de fracções de $K_1^{2\alpha}[X]$ e $K_2^{2\alpha}[X]$, respetivamente, e estes corpos de frações são obviamente isomorfos) através dum isomorfismo $i_{2\alpha+1}$ que é extensão de $i_{2\alpha}$. Para um ordinal da forma $2\alpha + 2$ procedemos de modo análogo mas, desta vez, trocando os papéis de K_1 e K_2. No caso em que temos um ordinal limite $\lambda < \kappa$, definimos $K_1^\lambda := \bigcup_{\alpha<\lambda} K_1^\alpha$, $K_2^\lambda := \bigcup_{\alpha<\lambda} K_2^\alpha$ e $i_\lambda := \bigcup_{\alpha<\lambda} i_\alpha$.

Por construção, $i_\kappa := \bigcup_{\alpha<\kappa} i_\alpha$ é um isomorfismo de K_1 para K_2 que é a identidade em K. □

A linguagem da teoria dos corpos é a linguagem do cálculo de predicados com igualdade constituída por duas constante 0 e 1 e dois símbolos funcionais binários + e ·. A *teoria dos corpos* é dada pelos seguintes axiomas:

$\forall x \forall y \forall z\, ((x + y) + z = x + (y + z))$;
$\forall x\, (x + 0 = x)$;
$\forall x \exists y\, (x + y = 0)$;
$\forall x \forall y\, (x + y = y + x)$;
$\forall x \forall y \forall z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z))$;
$\forall x\, (x \cdot 1 = x)$;
$\forall x\, (x \neq 0 \to \exists y\, (x \cdot y = 1))$;
$\forall x \forall y\, (x \cdot y = y \cdot x)$;
$\forall x \forall y \forall z\, (x \cdot (y + z) = x \cdot y + x \cdot z)$;
$0 \neq 1$.

A *teoria dos corpos algebricamente fechados* CAF obtém-se da teoria dos corpos adicionando o seguinte conjunto infinito de axiomas:

$$\forall z_0 \forall z_1 \cdots \forall z_{n-1} \exists x\, (x^n + z_{n-1}x^{n-1} + \cdots + z_1 x + z_0 = 0),$$

um para cada natural positivo n.

Definição 1. *Uma teoria* T *diz-se* modelo-completa *se, sempre que* $\mathfrak{M}$ *e* $\mathfrak{N}$ *são modelos de* T *com* $\mathfrak{M} \subseteq \mathfrak{N}$*, então* $\mathfrak{M} \preccurlyeq \mathfrak{N}$.

Teorema 1 (Abraham Robinson)**.** *A teoria dos corpos algebricamente fechados é modelo-completa.*

Demonstração. Sejam K_1 e K_2 corpos algebricamente fechados (e, portanto, infinitos) com $K_1 \subseteq K_2$. Tome-se κ um cardinal (necessariamente infinito) maior do que $card(K_2)$. Pelo teorema de Löwenheim-Skolem ascendente, existem extensões elementares K_1' e K_2' de K_1 e K_2 (respetivamente) de cardinalidade κ. Pela Proposição anterior, K_1' e K_2' são corpos isomorfos sobre K_1. Podemos agora verificar que $K_1 \preccurlyeq K_2$. Com efeito, seja ϕ uma fórmula da linguagem da teoria dos corpos e s uma atribuição de valores das variáveis em K_1. Suponhamos que $K_1 \models \phi[s]$. Visto que $K_1 \preccurlyeq K_1'$, tem-se $K_1' \models \phi[s]$. Dado que K_1' e K_2' são corpos isomorfos sobre sobre K_1 (onde s toma valores) conclui-se que $K_2' \models \phi[s]$. Ora, visto que $K_2 \preccurlyeq K_2'$, vem finalmente $K_2 \models \phi[s]$. □

Note-se que a teoria dos corpos algebricamente fechados não é completa, pois há corpos algebricamente fechados de diferentes características. Dado p um número primo, considere-se o seguinte axioma car_p:

$1 + 1 + \ldots + 1 = 0$ onde estamos a somar p unidades.

A teoria CAF_p dos corpos algebricamente fechados de característica p é a teoria axiomatizada por CAF e pelo axioma car_p. A teoria CAF_0 dos corpos algebricamente fechados de característica zero é a teoria axiomatizada por CAF e pelos axiomas $\neg car_p$, um para cada número primo p.

Corolário 1. *Dado* p *um número primo ou o número 0, a teoria* CAF_p *é completa.*

Demonstração. Suponhamos que p é um número primo. Sejam $\mathfrak{M}$ e $\mathfrak{N}$ modelos de CAF_p. Queremos ver que estes modelos são elementarmente equivalentes. É claro que $\overline{\mathbb{Z}/p\mathbb{Z}} \subseteq \mathfrak{M}$ e $\overline{\mathbb{Z}/p\mathbb{Z}} \subseteq \mathfrak{N}$, onde $\overline{\mathbb{Z}/p\mathbb{Z}}$ é o fecho algébrico do corpo finito $\mathbb{Z}/p\mathbb{Z}$. Dado que a teoria CAF_p é modelo-completa, $\overline{\mathbb{Z}/p\mathbb{Z}} \preccurlyeq \mathfrak{M}$ e $\overline{\mathbb{Z}/p\mathbb{Z}} \preccurlyeq \mathfrak{N}$. Logo, $\mathfrak{M} \equiv \mathfrak{N}$.

O caso de característica é 0 é semelhante, trabalhando-se com $\overline{\mathbb{Q}}$, o fecho algébrico de $\mathbb{Q}$. □

Antes de prosseguirmos com a discussão do Nullstellensatz, fazemos notar que o caso de característica zero dá origem ao denominado *princípio de transferência de Lefschetz.*

Corolário 2. *Os corpos* $\overline{\mathbb{Q}}$ *e* $\mathbb{C}$ *são elementarmente equivalentes.*

Corolário 3 (Hilbert)**.** *Seja* K *um corpo e* $\overline{K}$ *o seu fecho algébrico. Considere-se um sistema finito de equações e inequações*

$$\begin{cases} g_1(x_1, \ldots, x_k) = g_2(x_1, \ldots, x_k) = \cdots = g_n(x_1, \ldots, x_k) = 0 \\ f(x_1, \ldots, x_k) \neq 0 \end{cases}$$

onde $g_1, g_2, \ldots, g_n, f \in K[X_1, \ldots, X_k]$. Se este sistema tem solução numa extensão de K, então já tem solução em $\overline{K}$.

Demonstração. Considere-se a seguinte sentença σ com parâmetros em K:

$$\sigma := \exists x_1 \exists x_1 \cdots \exists x_k \left(\bigwedge_{i=1}^{n} g_i(x_1, \ldots, x_k) = 0 \wedge f(x_1, \ldots, x_k) \neq 0 \right)$$

Suponhamos que K' é uma extensão de K onde o sistema de equações e inequações tem solução, i.e., $K' \models \sigma$. Dado que σ é existencial, também se tem $\overline{K'} \models \sigma$, onde $\overline{K'}$ é o fecho algébrico de K'. Como $K \subseteq \overline{K} \subseteq \overline{K'}$ vem, pelo teorema anterior, $\overline{K} \preccurlyeq \overline{K'}$. Em particular, $\overline{K} \models \sigma$. Como se queria demonstrar. □

Teorema 2 (Nullstellensatz de Hilbert)**.** *Seja K um corpo algebricamente fechado e $f, g_1, \ldots, g_n \in K[X_1, \ldots, X_k]$ de tal sorte que todo o zero comum a $g_1, \ldots, g_n$ em K^k é necessariamente zero de f. Então existe um número natural r tal que*

$$f^r = \sum_{i=1}^{n} p_i g_i$$

para certos $p_1, \ldots, p_n \in K[X_1, \ldots, X_k]$.

Notação. *O recíproco deste resultado é obviamente verdadeiro.*

Demonstração. Sejam f e $g_1, \ldots, g_n$ como na hipótese do enunciado. Seja

$$I := \left\{ h \in K[X_1, \ldots, X_k] : \text{existem um número natural } r \text{ e} \right.$$

$$\left. p_1, \ldots, p_n \in K[X_1, \ldots, X_k] \text{ tais que } h^r = \sum_{i=1}^{n} p_i g_i \right\}$$

e admitamos, com vista a um absurdo, que $f \notin I$. Não é difícil de ver que I é um ideal (próprio) de $K[X_1, \ldots, X_k]$. A única cláusula não trivial a verificar é a de que I é fechado para a soma. Suponhamos que $h_1^r = \sum_{i=1}^{n} p_i g_i$ e $h_2^l = \sum_{i=1}^{n} q_i g_i$. Ora,

$$(h_1 + h_2)^{r+l} = \sum_{i+j=r+l} \binom{k+l}{i} h_1^i h_2^j$$

Sempre que $i + j = r + l$, vem $i \geq r$ ou $j \geq l$. Logo, cada parcela da soma acima tem como factor h_1^r ou h_2^l. Daqui conclui-se facilmente que $h_1 + h_2 \in I$.

Tem-se, pois, que I é um ideal próprio de $K[X_1, \ldots, X_k]$ que não contém nenhuma potência de f (e que contém $g_1, \ldots, g_n$). Pelo lema de Zorn, tome-se $J \supseteq I$ um ideal que não contém nenhuma potência de f e que seja maximal a respeito desta propriedade. Vamos argumentar que J é um ideal primo, i.e., que se $h_1 \notin J$ e $h_2 \notin J$ então $h_1 h_2 \notin J$. Dado que $h_1 \notin J$, por maximalidade de J, existem um número natural r, um polinómio q_1 de $K[X_1, \ldots, X_k]$ e um polinómio p_1 em J tais que $f^r = q_1 h_1 + p_1$. Semelhantemente, existem um número natural l, um polinómio q_2 de $K[X_1, \ldots, X_k]$ e um polinómio p_2 em J tais que $f^l = q_2 h_1 + p_2$. Logo,

$$f^{r+l} = (q_1 h_1 + p_1)(q_2 h_2 + p_2) = q_1 q_2 h_1 h_2 + q_1 h_1 p_2 + q_2 h_2 p_1 + p_1 p_2.$$

Ora, as três últimas parcelas acima estão em J. Daqui conclui-se que $h_1 h_2 \notin J$ pois, caso contrário, existiria uma potência de f em J.

Mostrámos que J é um ideal primo próprio. Logo, $K[X_1, \ldots, X_k]/J$ é um domínio de integridade. Seja K' o seu corpo de fracções. Como sabemos, podemos considerar K' uma extensão de K (através da imersão $a \rightsquigarrow (a + J)/(1 + J)$). Sejam $b_1, \ldots, b_k$ os seguintes elementos de K': $(X_1 + J)/(1 + J), \ldots, (X_k + J)/(1 + J)$, respetivamente. Por construção,

$$g_1(b_1,\ldots,b_k) = \cdots = g_n(b_1,\ldots,b_k) = 0 \text{ e } f(b_1,\ldots,b_k) \neq 0$$

e, portanto, o sistema de equações e inequações

$$\begin{cases} g_1(x_1,\ldots,x_k) = g_2(x_1,\ldots,x_k) = \cdots = g_n(x_1,\ldots,x_k) = 0 \\ f(x_1,\ldots,x_k) \neq 0 \end{cases}$$

tem solução em K'. Pelo corolário anterior, este sistema também tem solução em K, o que contradiz a hipótese do enunciado. □

Corolário 4. *Seja K um corpo algebricamente fechado e $g_1,\ldots,g_n \in K[X_1,\ldots,X_k]$ polinómios sem nenhum zero comum em K^k. Então existem polinómios $p_1,\ldots,p_n \in K[X_1,\ldots,X_k]$ tais que*

$$1 = \sum_{i=1}^{n} p_i g_i$$