# Teorema de la base de Hilbert

23 de febrero de 2017

**Teorema 1.** *(Teorema de la base de Hilbert) Todo ideal de $k[x_1, \ldots, x_n]$ está finitamente generado.*

*Demostración.*

Observemos que $k[x_1, \ldots, x_n] = k[x_1][x_2] \cdots [x_n]$. Sabemos que $k$ es Noetheriano (todos sus ideales son finitamente generados), porque los únicos ideales de $k$ son $\{0\} =< 0 >$ y $k =< 1 >$.

**Nota 1.** *Si $K$ es cuerpo, $< 0 >$ y $< 1 >$ son sus únicos ideales.*

Vamos a demostrar que si $R$ es un anillo Noetheriano, entonces $R[x]$ es un anillo Noetheriano (y esto termina la demostración por inducción en $n$).

Sea $I$ un ideal de $R[x]$. Vamos a demostrar que está finitamente generado.

**Nota 2.** *Dado un polinomio: $p(x) = a_m x^m + \cdots + a_1 x + a_0$ el elemento $a_m \in R$ se llama* ***coeficiente lider****.*

Definimos el ideal $I_L = \{a \in R : a \text{ es coeficiente lider de algún } p(x) \in I\}$. $I_L$ es un ideal de $R$ por la proposición 3 tel tema 2. Por hipótesis, $I_L$ está finitamente generado, es decir, $I_L =< c_1, \ldots, c_m >\subset R$ para ciertos $c_i, i = 1, \ldots, m$.

Tomemos polinomios $g_1, \ldots, g_m$ que tengan como coeficientes líderes aquellos $c_i$. Sea $N$ el máximo grado de $g_1, \ldots, g_m$.

Fijado un grado $d$, definimos el ideal

$$I_d = \{a \in R : a \text{ es coeficiente lider de un } f(x) \in R \text{ de grado } d\} \cup \{0\}.$$

$I_d$ es un ideal de $R$, por lo tanto, $I_d =< c_{d,1}, \ldots, c_{d,m_d} >$. Tomamos $g_{d,1}, \ldots, g_{d,m_d}$ polinomios de $I$, de grado $d$ que los tengan como coeficientes líderes.

Veamos que

$$I =< g_1, \ldots, g_m, g_{N-1,1}, \ldots, g_{N-1,m_{N-1}}, \ldots, g_{1,1}, \ldots, g_{1,m_1}, \ldots, g_{0,1}, \ldots, g_{0,m_0} >$$

Para ello, tomemos un polinomio cualquiera $f \in I$, y vamos a escribirlo como suma de múltiplos de los $g_i, g_{d,j}$. Iremos bajando el grado de $f$, sumándole múltiplos de los $g_i, g_{d,j}$, hasta llegar al polinomio nulo.

Si $deg(f) \geq N \Rightarrow f = a_r x^r + \cdots + a_1 x + a_0 \Rightarrow a_r \in I_L =< c_1, \ldots, c_m >$.

Entonces, $\exists \alpha_1, \ldots, \alpha_n \in R$ tales que $a_r = \alpha_1 c_1 + \cdots + \alpha_m c_m$. Consideramos $f - \alpha_1 x^{r-deg(g_1)} g_1 - \cdots - \alpha_m x^{r-deg(g_m)} g_m$, así el término de grado $r$ tiene coeficiente 0. Y así hemos bajado el grado de $f$.

Se itera el razonamiento hasta que $deg(f) < N$. Ahora, se procede a cancelar el término lider restando múltiplos de $g_{d,1}, \ldots, g_{d,m_d}$, iterando hasta tener el grado 0, es decir, hasta que el polinomio sea constante, y sea una suma de múltiplos de$g_{0,1}, \ldots, g_{0,m}$.

Por lo tanto, el polinomio $f$ es suma de múltiplos de los $g_i$ y los $g_{d,j}$. $\square$

## Referencias

[1] Cox,D.,Little,J.,O'Shea,D. , *Ideals, Varieties, and Algorithms*, Springer-Verlag,2007.