Tema 5.- Teorema de los ceros de Hilbert[1]

5.1 Enunciado de los resultados

TEOREMA 5.1.1.– [Teorema de los ceros versión I] Sea K un cuerpo *algebraicamente cerrado* e I un ideal de $k[x_1, \cdots, x_n]$. Entonces:

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

La demostración es consecuencia del siguiente teorema, al cual se le conoce también como teorema de los ceros.

TEOREMA 5.1.2.– [Teorema de los ceros versión II] Sea K un cuerpo *algebraicamente cerrado.* Los ideales maximales de $k[x_1, \cdots, x_n]$ son de la forma:

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \text{ con } a_i \in k \quad i = 1, \cdots, n.$$

Pero, a su vez, éste es consecuencia directa del teorema que enunciamos a continuación, para cuya demostración necesitaremos usar ciertas propiedades de los elementos enteros sobre un anillo.

TEOREMA 5.1.3.– Sea k un cuerpo,y $S \supset k$ una k-álgebra finitamente generada por $x_1, \ldots, x_n$ (i.e. $S = k[x_1, \ldots, x_n]$). Si S es un cuerpo, entonces x_i es algebraico sobre k, $i = 1, \ldots, n$.

5.2 Demostración de los resultados

DEFINICIÓN 5.2.1.– Sea $A \subset B$ una extensión de anillos. Diremos que un elemento $b \in B$ es *entero sobre* A si $\exists g(x) \in A[x]$ mónico tal que $g(b) = 0$, es decir, si b verifica una ecuación de dependencia entera sobre A.

LEMA 5.2.2.– Dada una extensión de anillos $A \subset B$, tenemos que el conjunto formado por los elementos de B que son enteros sobre A es de nuevo un anillo.

PRUEBA: Sean x e y elementos de B enteros sobre A. Notamos $R = A[x, y]$, que es una A-álgebra finitamente generada por $x^i y^j$, con $i = 0, \cdots, n$ y $j = 0, \cdots, m$, siendo n y m los grados de dos polinomios que se anulen en x e y respectivamente. Renombramos el sistema $\{x^i y^j\}$ como $\{e_l\}$ y consideramos el homomorfismo de A-álgebras consistente en multiplicar por $x + y$:

$$v : R \longrightarrow R$$

$$v(f) = (x + y)f$$

Así, como $v(e_l) \in R$ para todo l, podemos expresar:

$$v(e_l) = \Sigma a_{ls} e_s$$

Expresando matricialmente las relaciones anteriores obtenemos lo siguiente:

$$[(a_{ls}) - vI] \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

[1]Estas notas han sido elaboradas con la colaboración de Belén Medrano y Beatriz Rodríguez, alumnas internas del Departamento de Álgebra.

Llamamos M a la matriz $[(a_{ls}) - vI]$ y mutiplicamos ambos miembros de la igualdad anterior por la matriz adjunta de M. Como se verifica que $adj(M)M = \det(M)$, tenemos:

$$\det(M) \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

De esto se deduce que $\det(M)e_l = 0$, para todo l. Entonces $\det(M)c = 0$ para todo $c \in R$. En particular $1 \in R$, con lo cual $\det(M) = 0$. Pero $\det(M)$ no es más que sumas de productos de $x + y$ y elmentos de A, que nos proporciona una ecuación con coeficientes en A que es verificada por $x + y$. Por tanto $x + y$ es entero sobre A.
Para probar que si x e y son elementos de B enteros sobre A entonces también lo es xy, se razona análogamente con el endomorfismo de R consistente en multiplicar por xy. □

LEMA 5.2.3.– Sea A un *dominio de factorización única* (DFU) y $Q(A)$ su cuerpo de fracciones. Entonces todo elemento de $Q(A)$ que sea entero sobre A pertenece a A (cuando esto ocurre se dice que A es *íntegramente cerrado*). Es decir, el anillo de los elementos de $Q(A)$ enteros sobre A es justamente A.

PRUEBA: Sea $a/b \in Q(A)$ (con m.c.d.$(a, b) = 1$) un elemento entero sobre A. Entonces, a/b verifica una ecuación de dependencia entera de la forma:

$$0 = \left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{a}{b}\right) + a_n, \quad a_i \in A,\ i = 1, \ldots, n.$$

Multiplicando la ecuación anterior por b^n, obtenemos lo siguiente:

$$0 = a^n + a_1 b a^{n-1} + \ldots + a_{n-1} b^{n-1} a + a_n b^n.$$

Luego: $-a^n = b(a_1 a^{n-1} + \ldots + a_{n-1} b^{n-2} a + a_n b^{n-1})$. Podemos considerar esta igualdad en A, con lo que $b \mid a^n$. Como m.c.d.$(a, b) = 1$, se verifica que $b \mid a$, lo cual prueba que $a/b \in A$. □

LEMA 5.2.4.– Sean A un dominio, $K = Q(A)$ su cuerpo de fracciones, y $L \supset K$ extensión de cuerpos. Si $\alpha_1, \ldots, \alpha_n \in L$ son algebraicos sobre K, entonces $\exists b \in A$ tal que $b\alpha_1, \ldots, b\alpha_n$ son enteros sobre A.

PRUEBA: Como α_1 es algebraico sobre K, entonces verifica una ecuación mónica con coeficientes en $Q(A)$, que podemos suponer en la forma:

$$0 = {\alpha_1}^m + \frac{a_1}{b}{\alpha_1}^{m-1} + \ldots + \frac{a_{m-1}}{b}\alpha_1 + \frac{a_m}{b},$$

donde $a_i, b \in A$ y $b \neq 0$, $i = 1, \ldots, n$. Multiplicando esta expresión por b^m, obtenemos:

$$0 = (b\alpha_1)^m + a_1 b(b\alpha_1)^{m-1} + \ldots + b^{m-1} a_{m-1}(b\alpha_1) + b^m a_m.$$

Luego, hemos obtenido una ecuación de dependencia entera para $b\alpha_1$. Llamando $b = b_1$, y repitiendo el mismo razonamiento para cada α_i, obtenemos $\forall i = 1 \cdots n$ un elemento $b_i \in A - \{0\}$ tal que $b_i a_i$ es entero sobre A. Así, $b = \prod_{i=1}^n bi$ verifica lo que queríamos. □

Ya estamos en condiciones de demostrar los teoremas que encunciamos al principio de esta sección.

Demostración del teorema 5.1.3:

Demostremos el resultado por inducción en n.

El caso n=1 sería trivial, ya que si x_1 fuese transcendente sobre k, $k[x_1]$ sería un anillo de polinomios en una variable con lo cual no podría ser un cuerpo.

Supongamos, pues, el resultado cierto para n-1,y veámoslo para el caso n. Como S es cuerpo, debe verificarse $k(x_1) \subset S$, por tanto $S = k(x_1)[x_2, \ldots, x_n]$ es un cuerpo. Por hipótesis de inducción, tenemos que x_i es algebraico sobre $k(x_1)$, para todo $i = 2, \ldots, n$.

Así, la extensión $k(x_1) \subset k(x_1)[x_2, \ldots, x_n]$ es algebraica. Luego basta probar que x_1 es algebraico sobre k. Razonando por (RA), supongamos que x_1 es trascendente sobre k.
Como $Q(k[x_1]) = k(x_1)$ y $x_2, \ldots, x_n$ son algebraicos sobre $k(x_1)$,aplicando el lema anterior, sabemos que $\exists b \in k[x_1]$ tal que bx_i es entero sobre $k[x_1]$, para todo $i = 2, \ldots, n$. Usando esto junto con el lema 5.2.2 se deduce que:

$$\forall f(x_1, \ldots, x_n) \in S, \exists e(f) \text{ tal que } b^{e(f)} f(x_1, \ldots, x_n) \text{ es entero sobre } k[x_1].$$

Como $k(x_1) \subset S$, la propiedad anterior se verificaría en particular para los elementos de $k(x_1)$. Así, si $w \in k(x_1)$ entonces $b^{e(w)} w \in k(x_1)$ es entero sobre $k[x_1]$ y, como éste es íntegramente cerrado por el lema 1.3, debe ser $b^{e(w)} w = a \in k(x_1)$, luego $w = a/b^{e(w)}$.

En conclusión, todas las fracciones en $k(x_1)$,anillo de polinomios, tendrían un denominador que es una potencia de un elemento fijo, lo cual es contradicción. □

Demostración del teorema 5.1.2 (versión II):

Es inmediato ver que todos los ideales de la forma

$$\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$$

son maximales. Sea $f \in k[x_1, \cdots, x_n] \backslash \mathfrak{m}$. Dividiendo sucesivamente por $x_1 - a_1, \ldots, x_n - a_n$ obtenemos una expresión

$$f = c + \sum_{i=1}^{n} f_i(x_1, \ldots, x_n)(x_i - a_i) \text{ con } c \in k$$

Como $f \notin \mathfrak{m}$, debe ser $c \neq 0$, luego $(f) + \mathfrak{m} = (1)$ y así $\mathfrak{m}$ es maximal.
Queda probar que todos los ideales maximales son de esa forma. Sea $\mathfrak{m}$ un ideal maximal, por tanto, sabemos que

$$k[x_1, \ldots, x_n]/\mathfrak{m} = k[X_1, \ldots, X_n]$$

con $X_i = x_i + \mathfrak{m}$, $i = 1, \ldots, n$, es un cuerpo. En estas circunstancias, el lema 1.4 nos dice que X_i es algebraico sobre k, luego X_i puede ser considerado un elemento de k por ser k algebraicamente cerrado. Notamos $X_i = a_i$. Así, $x_i - a_i \in \mathfrak{m}$, para todo $i = 1, \ldots, n$, luego $(x_1 - a_1, \cdots, x_n - a_n) \subset \mathfrak{m}$. Como el ideal de la izquierda es ya maximal, se tiene la igualdad. □

Demostración del teorema 5.1.1 (versión I):

Claramente, se tiene la contención

$$\mathcal{I}(\mathcal{V}(I)) \supset \sqrt{I}$$

ya que sabemos que $\mathcal{I}(\mathcal{V}(I))$ es siempre un ideal radical y que se verifica $\mathcal{I} \subset \mathcal{I}(\mathcal{V}(I))$, entonces

$$\sqrt{I} \subset \sqrt{\mathcal{I}(\mathcal{V}(I))} = \mathcal{I}(\mathcal{V}(I))$$

Veamos la contención contraria. La prueba que damos se conoce con el nombre de truco de Rabinowitsch.

Sea $g \in \mathcal{I}(\mathcal{V}(I))$, x_{n+1} una nueva variable y consideremos el siguiente ideal

$$\mathfrak{b} = I^e + (1 - gx_{n+1})$$

Si $\mathfrak{b} \neq (1)$, habría un ideal maximal que lo contiene. Por el teorema 5.1.2 dicho ideal maximal sería de la forma

$$(x_1 - b_1, \cdots, x_n - b_n, x_{n+1} - b_{n+1})$$

Entonces, todos los polinomios de $\mathfrak{b}$ se tendrían que anular en el punto $b = (b_1, \cdots, b_n, b_{n+1})$. Como

$$f(b_1, \cdots, b_n) = 0, \, \forall f \in I^e$$

debe verificarse $g(b_1, \cdots, b_n) = 0$, luego $1 - gx_{n+1}$ no puede anularse en $\mathfrak{b}$, lo que supone una contradicción. Así pues, $\mathfrak{b} = (1)$. Entonces, se puede escribir:

$$1 = \sum_{i=1}^{n} h_i(x_1, \ldots, x_n, x_{n+1}) f_i + h_{n+1}(x_1, \cdots, x_n, x_{n+1})(1 - gx_{n+1})$$

Donde $f_i \in I^e \; \forall i = 1, \cdots, n$ .Haciendo $x_{n+1} = 1/g$ en la relación anterior, y quitando los denominadores que aparecen en las h_i, tendremos una expresión del tipo

$$g^p = \sum_{i=1}^{n} H_i(x_1, \ldots, x_n) f_i$$

lo que prueba que $g \in \sqrt{I}$. $\square$