Variedades algebraicas

1.3. Teorema de los ceros de Hilbert

Cualquiera de los tres enunciados siguientes se conoce como teorema de los ceros de Hilbert (o *nullstellensatz*).

(1.3.1) Teorema. (versión débil). *Sea k algebraicamente cerrado. Si I es un ideal propio de $k[x_1, \ldots, x_n]$, entonces*

$$V(I) \neq \emptyset.$$

(1.3.2) Teorema. (versión algebraica) *Si $k \hookrightarrow K$ es una extensión de cuerpos tal que $K = k[\alpha_1, \ldots, \alpha_n]$, y k es algebraicamente cerrado, entonces $K = k$.*

(1.3.3) Teorema. *Si k es algebraicamente cerrado e I es un ideal de $k[x_1, \ldots, x_n]$, entonces*

$$I(V(I)) = \mathrm{Rad}I.$$

(1.3.4) Veamos en primer lugar que los teoremas (1.3.1) y (1.3.2) son equivalentes.

(1.3.1) $\Rightarrow$ (1.3.2). Si $k \hookrightarrow K$ es una extensión de cuerpos y $K = k[\alpha_1, \ldots, \alpha_n]$, entonces, en virtud del primer teorema de isomorfía aplicado al epimorfismo de anillos

$$k[x_1, \ldots, x_n] \longrightarrow K;\ x_i \longmapsto \alpha_i, i \in \{1, \ldots, n\}$$

tenemos que

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

donde $\mathfrak{m}$ es el ideal maximal núcleo de dicho epimorfismo.
Por (1.3.1), existe $(a_1, \ldots, a_n) \in V(\mathfrak{m})$. Además, dado que

$$\mathfrak{m} \subseteq I(V(\mathfrak{m})) \subseteq I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n) \neq k[x_1, \ldots, x_n]$$

y $\mathfrak{m}$ es maximal, se tiene que $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, y por lo tanto $V(\mathfrak{m}) = \{(a_1, \ldots, a_n)\}$.
Luego $\mathfrak{m}$ es el núcleo del epimorfismo

$$k[x_1, \ldots, x_n] \longrightarrow k;\ f \longmapsto f(a_1, \ldots, a_n),$$

y de nuevo por el primer teorema de isomorfía,

$$k \cong k[x_1, \ldots x_n]/\mathfrak{m} \cong K.$$

(1.3.2) $\Rightarrow$ (1.3.1). Si $I \neq k[x_1, \ldots, x_n]$, entonces existe un ideal maximal $\mathfrak{m}$ tal que $I \subseteq \mathfrak{m}$. Luego $K = k[x_1, \ldots, x_n]/\mathfrak{m}$ es un cuerpo.
Denotemos ξ_i a la clase de x_i en el cociente para cada i. Entonces $K = k[\xi_1, \ldots, \xi_n]$, y $K = k$ por (1.3.2), o sea, para cada i existe $a_i \in k$ tal que $\xi_i = a_i$ en K. Luego $x_i - a_i \in \mathfrak{m}$ para cada i, de donde

$$(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$$

y por la maximalidad de $(x_1 - a_1, \ldots, x_n - a_n)$, este ideal coincide con $\mathfrak{m}$. Por tanto,

$$V(I) \supseteq V(\mathfrak{m}) = V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\} \neq \emptyset.$$

(1.3.5) Por otra parte, (1.3.1) es equivalente a (1.3.3).
En efecto, si k es algebraicamente cerrado e $I(V(I)) = \mathrm{Rad}I$ para cada ideal I de $k[x_1, \ldots, x_n]$, entonces las aplicaciones

$$\begin{array}{ccc} \{V \subseteq \mathbb{A}^n k; V \text{cjto. algebraico afin}\} & \xrightarrow{I} & \{I; I \text{ ideal radical de } k[x_1, \ldots, x_n]\} \\ V & \longmapsto & I(V) \end{array}$$

y

$$\begin{array}{ccc} \{I; I \text{ ideal radical de } k[x_1, \ldots, x_n]\} & \xrightarrow{V} & \{V \subseteq \mathbb{A}^n k; V \text{ cjto. algebraico afin}\} \\ I & \longmapsto & V(I) \end{array}$$

son inversas una de la otra por (1.1.9) y porque $I(V(I)) = \mathrm{Rad}I = I$ para todo ideal radical I.
Luego V es una biyección, y dado que $V(k[x_1, \ldots, x_n]) = \emptyset$, si I es un ideal propio de $k[x_1, \ldots, x_n]$, entonces $V(I) \neq \emptyset$.
Recíprocamente, sea k algebraicamente cerrado y asumamos que $V(J) \neq \emptyset$ para todo ideal propio J de $k[x_1, \ldots, x_n]$. Si I es un ideal de $k[x_1, \ldots, x_n]$, por el teorema de la base de Hilbert existen $f_1, \ldots, f_n \in I$ tales que I es

el ideal $(f_1, \ldots, f_n)$. Por (1.1.7.8), para probar que $I(V(I)) = \mathrm{Rad}I$, basta comprobar que $I(V(I)) \subseteq \mathrm{Rad}I$.
Sea g un polinomio que se anula en todos los puntos $(a_1, \ldots, a_n) \in \mathbb{A}^n k$ donde se anulan $f_1, \ldots, f_n$ simultáneamente, y consideremos el ideal

$$J = (f_1, \ldots, f_n, x_{n+1}g - 1) \subseteq k[x_1, \ldots, x_n, x_{n+1}].$$

Entonces $V(J) = \emptyset$, porque si existe

$$(a_1, \ldots, a_n, a_{n+1}) \in V(J),$$

entonces $f_i(a_1, \ldots, a_n) = 0$ para $1 \leq i \leq n$, de donde $g(a_1, \ldots, a_n) = 0$, pero $a_{n+1}g(a_1, \ldots, a_n) = 1$.
Aplicando la hipótesis, el ideal J tiene que coincidir con $k[x_1, \ldots, x_n, x_{n+1}]$, y por lo tanto existen $h_1, \ldots, h_n, h \in k[x_1 \ldots, x_n, x_{n+1}]$ tales que

$$1 = \sum_{i=1}^{n} h_i f_i + h(x_{n+1}g - 1).$$

Sustituyendo formalmente x_{n+1} por $1/y$, se obtiene

$$\begin{aligned} 1 = &\sum_{i=1}^{n} h_i(x_1, \ldots, x_n, 1/y) f_i(x_1, \ldots, x_n) \\ &+ h(x_1, \ldots, x_n, 1/y)(g(x_1, \ldots, x_n)/y - 1) \ . \end{aligned}$$

Multiplicando formalmente por y^{p+1}, donde p es el mayor de los grados de $h, h_1, \ldots, h_n$ en x_{n+1}, y llamando h_i', resp. h', al polinomio $y^{p+1}h_i(x_1, \ldots, x_n, 1/y)$, resp. $y^p h(x_1, \ldots, x_n, 1/y)$, de $k[x_1, \ldots, x_n, y]$ tenemos

$$\begin{aligned} y^{p+1} = &\sum_{i=1}^{n} h_i'(x_1, \ldots, x_n, y) f_i(x_1, \ldots, x_n) \\ &+ h'(x_1, \ldots, x_n, y)(g(x_1, \ldots, x_n) - y). \end{aligned}$$

Sustituyendo y por g obtenemos

$$g^{p+1} = \sum_{i=1}^{n} h_i'' f_i \in I,$$

donde

$$h_i'' = h_i'(x_1, \ldots, x_n, g(x_1, \ldots, x_n)) \in k[x_1, \ldots, x_n].$$

Luego $g \in \mathrm{Rad}I$.

Antes de demostrar el teorema de los ceros (versión algebraica) introduciremos los conceptos de módulo y de integridad sobre un anillo.

(1.3.6) Definición. Sea A un anillo conmutativo. Un *A–módulo* es un grupo abeliano M dotado de una ley de composición externa

$$\cdot : A \times M \longrightarrow M$$

que verifica

(1.3.6.1) $a(m+m') = am + am'$ para todo $a \in A$ y $m, m' \in M$;

(1.3.6.2) $(a+a')m = am + a'm$ para todo $a, a' \in A$ y $m \in M$;

(1.3.6.3) $(aa')m = a(a'm)$ para todo $a, a' \in A$ y $m \in M$;

(1.3.6.4) $1m = m$ para todo $m \in M$.

(1.3.7) Ejemplos. Si A es el anillo $\mathbb{Z}$ de los enteros, entonces todo grupo abeliano M es un A–módulo. Luego los $\mathbb{Z}$–módulos son exactamente los grupos abelianos.
Si A es el cuerpo k, entonces los A–módulos son exactamente los k–espacios vectoriales.
Si A es un anillo, entonces A es un A–módulo con la multiplicación de A.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Si M es un B–módulo, entonces M es también un A–módulo por *restricción de escalares*, es decir, con el producto dado por $am = f(a)m$ para todo $a \in A$ y todo $m \in M$.

(1.3.8) Un subconjunto N del A–módulo M se dice que es un *submódulo de M* si N es un A–módulo con las operaciones restringidas de las de M, o equivalentemente, si

(1.3.8.1) $N \neq \emptyset$, y

(1.3.8.2) $an + a'n' \in N$ para todo $a, a' \in A$ y todo $n, n' \in N$.

(1.3.9) Ejemplo. Tanto $\{0\}$ como M son submódulos del A–módulo M.
Los submódulos del A–módulo A son exactamente los ideales de A.
Si $\{N_i\}_{i \in I}$ es una familia de submódulos de M, entonces la intersección

$$\bigcap_{i \in I} N_i$$

y la suma

$$\sum_{i \in I} N_i = \{m \in M; \exists i_1, \ldots, i_r \in I, n_j \in N_{i_j}, m = \sum_{j=1}^{r} n_j\}$$

son submódulos de M.

(1.3.10) Sea M un A–módulo y N un submódulo de M. Dado que en particular N es un subgrupo normal de M (M es grupo abeliano), podemos construir el grupo (abeliano) cociente M/N. Dicho grupo cociente tiene estructura de A–módulo con el producto dado por $a\overline{m} = \overline{am}$, y se denomina *$A$–módulo cociente.*

(1.3.11) Definición. Sean M y N A–módulos. Un *homomorfismo de A–módulos* o *A–homomorfismo* es una aplicación $f : M \longrightarrow N$ tal que

$$f(m+m') = f(m) + f(m') \quad , \quad f(am) = af(m)$$

para todo $a \in A$ y todo $m, m' \in M$.
Si el homomorfismo f es inyectivo, resp. sobreyectivo, resp. biyectivo, se dice que f es un *monomorfismo*, resp. *epimorfismo*, resp. *isomorfismo* de A–módulos.

(1.3.12) Si $f : M \longrightarrow N$ es un A–homomorfismo, entonces

$$\mathrm{Ker} f = \{m \in M; f(m) = 0\}$$

es un submódulo de M e

$$\mathrm{Im} f = \{n \in N; \exists m \in M, f(m) = n\}$$

es un submódulo de N.

(1.3.13) Un conjunto de elementos $G \subseteq M$ se dice que es un *sistema generador del A–módulo M* si para todo $m \in M$ existen $a_1, \ldots, a_n \in A$ y $m_1, \ldots, m_n \in G$ tales que

$$m = \sum_{i=1}^{n} a_i m_i.$$

Se dice que M es *finitamente generado* si existe un sistema generador finito G de M.
Aunque M sea un A–módulo finitamente generado, sus submódulos no tienen por qué serlo. Por ejemplo, sea $A = k[x_i]_{i \in I}$ el anillo de los polinomios en las (infinitas) indeterminadas $\{x_i\}_{i \in \mathbb{N}}$ con coeficientes en k. Entonces A está finitamente generado como A–módulo pues, por ejemplo, $\{1\}$ es un sistema generador, y sin embargo el ideal $I = (\{x_i\})_{i \in \mathbb{N}}$ no es finitamente generado, porque en caso de serlo la cadena ascedente de ideales

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

se estacionaría.

(1.3.14) Definición. Sea A un subanillo de B. Se dice que un elemento $b \in B$ es *entero sobre* A si existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$.

Todo elemento de un anillo A es entero sobre A.

(1.3.15) Lema. *Sea A un subanillo del dominio de integridad B. Las siguientes afirmaciones son equivalentes para $b \in B$:*

(1.3.15.1) *b es entero sobre A;*

(1.3.15.2) *$A[b]$ es un A–módulo finitamente generado;*

(1.3.15.3) *existe un subanillo C de B tal que $A[b] \subseteq C$ y C es finitamente generado como A–módulo.*

Demostración. (1) $\Rightarrow$ (2) Si b es entero sobre A, entonces existe un polinomio mónico

$$f = x^n + a_1 x^{n-1} + \cdots + a_n \in A[x]$$

tal que $f(b) = 0$. Luego

$$b^n = \sum_{i=1}^{n} -a_i b^{n-i},$$

por lo tanto para cada $m \geq n$ existen $d_1, \ldots, d_n \in A$ tales que

$$b^m = \sum_{i=1}^{n} d_i b^{n-i}.$$

En efecto, por inducción sobre $m \geq n$, si $b^m = \sum_{i=1}^{n} d_i b^{n-i}$, entonces

$$b^{m+1} = b \sum_{i=1}^{n} d_i b^{n-i} = d_1 b^n + b \sum_{i=2}^{n} d_i b^{n-i} = \sum_{i=2}^{n} d_i b^{n-i+1} - \sum_{i=1}^{n} d_1 a_i b^{n-i}.$$

Luego $\{1, b, \ldots, b^{n-1}\}$ es un sistema generador de $A[b]$ como A–módulo.

(2) $\Rightarrow$ (3) El propio $C = A[b]$ es un subanillo de B que tiene a $A[b]$ como subanillo y por hipótesis es un A–módulo finitamente generado.

(3) $\Rightarrow$ (1) Sea $\{c_1, \ldots, c_n\}$ un sistema generador de C como A–módulo. Dado que $bc_i \in C$, existen $a_{i1}, \ldots, a_{in} \in A$ tales que

$$bc_i = a_{i1}c_1 + \ldots + a_{in}c_n$$

para $1 \leq i \leq n$. Luego $(c_1, \ldots, c_n)$ es solución del sistema de n ecuaciones lineales con n incógnitas $Hx = 0$ donde H es la matriz

$$H = \begin{pmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & b - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & b - a_{nn} \end{pmatrix} \in M_n(A[b]).$$

Multiplicando por la matriz H^* de los adjuntos de la traspuesta de H, y teniendo en cuenta que $H^*H = \det H \; I_n$, donde I_n es la matriz identidad, se tiene que

$$\det H \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \det H \; I_n \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = H^* \; H \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

Luego $\det H c_i = 0$ para $1 \leq i \leq n$, y dado que el elemento 1 de C se puede expresar como $1 = \sum_{i=1}^{n} d_i c_i$, con $d_1, \ldots, d_n \in A$, tenemos $\det H = 0$. Pero el determinante de H tiene la forma

$$\det H = b^n + e_1 b^{n-1} + \cdots + e_n$$

con $e_1, \ldots, e_n \in A$, luego b es entero sobre A. □

(1.3.16) Corolario. *Si A es un subanillo de B y $\{b_1, \ldots, b_n\}$ son elementos de B enteros sobre A, entonces $A[b_1, \ldots, b_n]$ es un A–módulo finitamente generado.*

Demostración. Inducción sobre n.

El caso $n = 1$ es (1) $\Rightarrow$ (2) del lema.

Supongamos que $A[b_1, \ldots, b_{n-1}]$ es A–módulo finitamente generado. Entonces, dado que b_n es entero sobre A y por lo tanto sobre $A[b_1, \ldots, b_{n-1}]$, por el lema anterior tenemos que $A[b_1, \ldots, b_{n-1}, b_n]$ es un $A[b_1, \ldots, b_{n-1}]$–módulo finitamente generado. Luego $A[b_1, \ldots, b_{n-1}, b_n]$ es un A–módulo finitamente generado (ver (1.8.9)). □

(1.3.17) Corolario. *Sea A un subanillo de B. El conjunto*

$$C = \{b \in B; b \text{ es entero sobre } A\}$$

es un subanillo de B que contiene a A.

Demostración. Dado que todo elemento a de A es cero del polinomio mónico $x - a \in A[x]$, tenemos $A \subseteq C$.
Si $c, c' \in C$, por el corolario anterior $A[c, c']$ es un A–módulo finitamente generado, y como $c + c'$ y cc' son elementos de $A[c, c']$ se tiene que $A[c, c']$ es un subanillo de B que contiene tanto a $A[c + c']$ como a $A[cc']$. En virtud del lema, $c + c'$ y cc' son elementos de C. □

Demostración. **(del teorema de los ceros, versión algebraica).** Veamos que si $k \hookrightarrow K$ es una extensión de cuerpos y $K = k[\alpha_1, \ldots, \alpha_n]$, entonces $k \hookrightarrow K$ es algebraica por inducción sobre n.
Para $n = 1$, si $k \hookrightarrow k[\alpha_1]$ es una extensión de cuerpos entonces, por el primer teorema de isomorfía aplicado al epimorfismo

$$k[x] \longrightarrow k[\alpha_1];\ f \longmapsto f(\alpha_1),$$

el cuerpo $k[\alpha_1]$ es isomorfo al cociente $k[x]/(f)$, donde (f) es el ideal (principal) de $k[x]$ núcleo de dicho epimorfismo. Además, dado que $k[\alpha_1]$ es un cuerpo, tenemos que f es no nulo, y $f(\alpha_1) = 0$ en $k[\alpha_1]$. Luego $k \hookrightarrow k[\alpha_1]$ es algebraica.
Supongamos que toda extensión de cuerpos $k \hookrightarrow k[\alpha_1, \ldots, \alpha_n]$ es algebraica, y sea

$$k \hookrightarrow K = k[\alpha_1, \alpha_2, \ldots, \alpha_{n+1}]$$

una extensión de cuerpos.
Si denotamos por K_1 a $k(\alpha_1)$, entonces $K = K_1[\alpha_2, \ldots, \alpha_{n+1}]$, y por la hipótesis de inducción, $K_1 \hookrightarrow K$ es algebraica. Luego para todo $i \in \{2, \ldots, n+1\}$ existen $a_{i1}, \ldots, a_{in_i} \in K_1$ no todos nulos tales que

$$\alpha_i^{n_i} + a_{i1}\alpha_i^{n_i-1} + \cdots + a_{i,n_i} = 0.$$

Sea $a \in k[\alpha_1]$ un múltiplo común a los denominadores de todos los a_{ij}. Entonces, multiplicando por a^{n_i} para cada i,

$$(a\alpha_i)^{n_i} + aa_{i1}(a\alpha_i)^{n_i-1} + \cdots + a_i^n a_{in_i} = 0,$$

esto es, $a\alpha_i$ pertenece al anillo de los elementos enteros sobre $k[\alpha_1]$ para cada i.
Como cada $z \in K = k[\alpha_1, \ldots, a_{n+1}]$ es de la forma $z = f(\alpha_1, \ldots, \alpha_{n+1})$, con $f \in k[x_1, \ldots, x_{n+1}]$, llamando p al grado de f en las variables $x_2, \ldots, x_{n+1}$ tenemos que $a^p z$ también está en el anillo de los elementos enteros sobre $k[\alpha_1]$. En particular, esto es cierto para todo $z \in K_1$.
Si α_1 no fuese algebraico sobre k, entonces K_1 es isomorfo al cuerpo de fracciones de $k[x]$, y el párrafo anterior contradice la afirmación de (1.8.10). Luego $k \hookrightarrow k[\alpha_1] \hookrightarrow K$ es algebraica. □

(1.3.18) Corolario. *Sea k algebraicamente cerrado. La aplicación que a cada conjunto algebraico afín V le asigna el ideal $I(V)$ de los polinomios que se anulan en todos los puntos de V es una biyección entre los conjuntos algebraicos afines de $\mathbb{A}^n k$ y los ideales radicales de $k[x_1, \ldots, x_n]$.*
Su inversa es la aplicación que a cada ideal radical I le asigna el conjunto $V(I)$ de los ceros de los polinomios de ese ideal.
Esta biyección se puede restrigir a una biyección entre los conjuntos algebraicos irreducibles de $\mathbb{A}^n k$ y los ideales primos de $k[x_1, \ldots, x_n]$, y ésta a su vez a una biyección entre los conjuntos unitarios de $\mathbb{A}^n k$ y los ideales maximales de $k[x_1, \ldots, x_n]$.

(1.3.19) Corolario. *Sea k algebraicamente cerrado. Si $f = f_1^{n_1} \cdots f_r^{n_r}$ es la descomposición de f en irreducibles, entonces*

$$V(f) = V(f_1) \cup \cdots \cup V(f_r)$$

es la descomposición de $V(f)$ en unión de irreducibles, y además

$$I(V(f)) = (f_1 \cdots f_r).$$

Existe una correspondencia biyectiva entre hipersuperficies irreducibles de $\mathbb{A}^n k$ y polinomios irreducibles de $k[x_1, \ldots, x_n]$ (salvo producto por constantes).

(1.3.20) Corolario. *Sea k algebraicamente cerrado. Si I es un ideal de $k[x_1, \ldots, x_n]$, entonces $V(I)$ es finito si, y sólo si $\dim_k k[x_1, \ldots, x_n]/I$ es finita, y en ese caso*

$$\#V(I) \leq \dim_k k[x_1, \ldots, x_n]/I.$$

Demostración. Sea

$$m = \dim_k k[x_1, \ldots, x_n]/I$$

y supongamos que $p_1, \ldots, p_r \in V(I)$ son puntos distintos, con $r > m$. Por (1.8.1), para cada $i \in \{1, \ldots, r\}$ existe un polinomio $f_i \in k[x_1 \ldots, x_n]$ tal que

$$f_i(p_i) = 1 \quad \text{y} \quad f_i(p_j) = 0 \text{ para } j \neq i.$$

El conjunto de vectores

$$\{\overline{f_1}, \ldots, \overline{f_r}\} \subseteq k[x_1, \ldots, x_n]/I$$

es un sistema libre, porque si $\lambda_1, \ldots, \lambda_r \in k$ son tales que $\sum_{i=1}^r \lambda_i \overline{f_i} = 0$, entonces $\sum_{i=1}^r \lambda_i f_i \in I$, y por lo tanto

$$0 = \sum_{i=1}^r \lambda_i f_i(p_j) = \lambda_j$$

para $1 \leq j \leq r$.
Esto está en contradicción con que la dimensión de $k[x_1, \ldots, x_n]/I$ es menor que r.
Luego $V(I)$ es finito y su cardinal es menor que $\dim_k k[x_1, \ldots, x_n]/I$.
Recíprocamente, sea $V(I) = \{p_1, \ldots, p_r\}$, donde $p_i = (a_{i1}, \ldots, a_{in})$ para $1 \leq i \leq r$. Denotemos por f_j al polinomio

$$\prod_{i=1}^{r}(x_j - a_{ij}) \in k[x_j]$$

para $1 \leq j \leq n$. Luego

$$f_j \in I(V(I)) = \mathrm{Rad}I,$$

así que existe $m_j > 0$ tal que $f_j^{m_j} \in I$.
Sea $m = \max\{m_1, \ldots, m_n\}$.
Entonces $f_j^m \in I$, esto es, $\overline{f_j^m} = 0$ en $k[x_1, \ldots, x_n]/I$. Como el grado de f_j^m es rm, tenemos que $\overline{x_j^{rm}}$ es combinación lineal de $\overline{1}, \overline{x_j}, \ldots, \overline{x_j^{rm-1}}$, y por inducción sobre l, que $\overline{x_j^l}$ también lo es para todo $l \geq rm$. Luego

$$\{\overline{x_1^{j_1} \cdots x_n^{j_n}}\}_{0 \leq j_1, \ldots, j_n \leq rm-1}$$

es un sistema generador de $k[x_1, \ldots, x_n]/I$. □