Pro Mathematica: Vol. II, No. 3, 1988

PROPIEDADES ALGEBRAICAS CONSIDERADAS EN LA DEMOSTRACION DEL TEOREMA DE LOS CEROS DE HILBERT

Teódulo VERASTEGUI CH. (*)

En esta exposición se presentan diversos conceptos y propiedades del álgebra conmutativa que están relacionados a conceptos básicos de la geometría algebraica. Un resultado importante, en donde se aprecian objetivamente estas relaciones, es el Teorema de los ceros de Hilbert, para cuya demostración se hace una estructuración de conceptos y propiedades referentes al anillo de polinomios con coeficientes en un campo dado, anillos noetherianos, extensiones algebraicas, etc. siguiendo las terminologías y notaciones dadas en [1]:

(*) Profesor Principal de la Sección Matemáticas de la PUCP.

1. Introducción.

Fijado un campo K, se establecen propiedades que relacionan ideales I del anillo de polinomios $K[X_1, X_2, ..., X_n]$ con n indeterminadas y coeficientes en K, con ciertos subconjuntos V del espacio $K^n = K \times K \times ... \times K$, n veces; definiendo los subconjuntos V a partir de los ideales I, y viceversa.

Además, si K es un campo algebraicamente cerrado, se tiene que todo polinomio no constante $F(x)$ en $K[x]$ admite sus raíces o ceros en K; es decir, el conjunto de los ceros de $F(x)$ en K es no vacío; y como $K[x]$ es un dominio de ideales principales, lo anterior significa que para un ideal propio I de $K[x]$ se define el subconjunto V de K formado por los ceros o raíces de todos los elmentos de I, que no es vacío. En el Teorema de los ceros de Hilbert la propiedad anterior se extiende al anillo $K[X_1, X_2, ..., X_n]$ y al espacio K^n: Para cada ideal propio I de $K[X_1, X_2, ..., X_n]$ se define el subconjunto V no vacío de K^n, y si F es un polinomio no constante tal que cada elemento de V es un cero de F, entonces para algún $N > 0$ en Z, F^N está en I. Esto permite establecer una biyección entre los ideales radicales I de $K[X_1, X_2, ..., X_n]$ y los subconjuntos V de K^n definidos por I.

2. Preliminares y Formulación del Problema

Dado un campo K, se tienen:

1) El conjunto $A_n(K) = K \times K \times ... \times K$, n veces, es el n–espacio afín sobre K; a sus elementos $P = (a_1, a_2, ..., a_n)$ llamaremos *puntos* de $A_n(K)$.

2) $K[X_1, X_2, ..., X_n]$ es el anillo de polinomios con n variables sobre K, cuyos elementos F se representan:

$F = F(X_1, X_2, \ldots, X_n) = \sum_{i=0}^{m} \alpha_i X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$, con $\alpha_i \in K$, $\forall i$, $i_1 + i_2 + \ldots + i_n = i$ y $m \geq 0$ en Z

Si $F = F(X_1, X_2, \ldots, X_n) \in K[X_1, X_2, \ldots, X_n]$ y $P = (a_1, a_2, \ldots, a_n) \in A_n(K)$, siendo F un polinomio no constante; el *valor de F en P* es $F(P) = F(a_1, a_2, \ldots, a_n) \in K$.
Si $F(P) = 0$, se dice que "P es un cero de F en K".

3) Para $F \in K[X_1, X_2, \ldots, X_n]$ se tiene:
$V(F) = \{P \in A_n(K) / F(P) = 0\}$, el conjunto de los ceros de F en K, y llamaremos la *hipersuperficie definida por F;* y para $S \subset K[X_1, X_2, \ldots, X_n]$ se tiene:

$V(S) = \{P \in A_n(K) / F(P) = 0, \ \forall F \in S\}$, y se cumple:

$$V(S) = \bigcap_{F \in S} V(F).$$

En base a estas consideraciones, tenemos:

Definición 1.

Un conjunto $X \subset A_n(K)$ se llama *algebraico afín* de $A_n(K)$ o simplemente *algebraico,* si existe $S \subset K[X_1, X_2, \ldots, X_n]$ tal que: $X = V(S)$.

Proposición 1.

Si $S \subset K[X_1, X_2, \ldots, X_n]$, sea I el ideal de $K[X_1, X_2, \ldots, X_n]$ generado por S, o sea $I = \langle S \rangle$. Entonces: $V(S) = V(I)$; es decir, todo conjunto algebraico de $A_n(K)$ es $V(I)$ para algún ideal I de $K[X_1, X_2, \ldots, X_n]$.

Demostración

Vemos que $V(I) \subset V(S)$: Si $P \in V(I)$ entonces $F(P) = 0$, $\forall F \in I$.
Como $I = \langle S \rangle$ se tiene $S \subset I$. Luego $F(P) = 0$, $\forall F \in S$; es decir, $P \in V(S)$. De aquí: $V(I) \subset V(S)$.

Recíprocamente: Si $P \in V(S)$ entonces $F(P) = 0$, $\forall F \in S$. Sea $G \in I = \langle S \rangle$.

Entonces $G = \sum_{F \in S} A_F . F$,
para un número finito de elementos F de S y A_F en $K[X_1, X_2, ..., X_n]$. De aquí:

$$G(P) = \sum_{F \in S} A_F(P) . F(P) = \sum_{F \in S} A_F(P) . 0 = 0;$$ es decir: $P \in V(I)$.

Luego: $V(S) \subset V(I)$.

En consecuencia: Si $I = \langle S \rangle$, se tiene: $V(S) = V(I)$. ♦

Observación 1.

De la definición 1 y la proposición 1, se establece que:
A cada ideal I de $K[X_1, X_2, ..., X_n]$, "objeto" algebraico, le asignamos un conjunto algebraico $V(I)$ de $A_n(K)$, "objeto" geométrico; es decir, se tiene la correspondencia:

$$I \rightarrow V(I)$$

Una propiedad que conduce a la correspondencia recíproca es:

Proposición 2.

Para $X \subset A_n(K)$, el conjunto:

$I(X) = \{F \in K[X_1, X_2, \ldots, X_n] / F(P) = 0, \forall P \in X\}$ de los polinomios de $K[X_1, X_2, \ldots, X_n]$ que se anulan en cada P de X, es un ideal de $K[X_1, X_2, \ldots, X_n]$.

Demostración

Sean F_1 y F_2 en $I(X)$. Entonces: $F_1(P) = 0$ y $F_2(P) = 0$, $\forall P \in X$.

Luego:

i) $(F_1 - F_2)(P) = F_1(P) - F_2(P) = 0$, $\forall P \in X$; es decir, $F_1 - F_2 \in I(X)$.

ii) Para $G \in K[X_1, X_2, \ldots, X_n]$ se cumple: $F_1 . G = G . F_1$ y $(GF_1)(P) = G(P) . F_1(P) = G(P) . 0 = 0$, $\forall P \in X$; es decir, $GF_1 \in I(X)$.

De i) y ii) se concluye que $I(X)$ es un ideal de $K[X_1, X_2, \ldots, X_n]$ ♦

Definición 2.

Para $X \subset A_n(K)$, al ideal $I(X)$ de $K[X_1, X_2, \ldots, X_n]$ llamaremos el *ideal de X*.

En particular, si $X = V$ es un conjunto algebraico de $A_n(K)$, se tiene $I(V)$ el ideal de V.

Observación 2.

De la definición 2 se establece la siguiente correspondencia: A cada conjunto algebraico V de A_n (K) le asignamos un ideal I (V) de $K[X_1, X_2, \ldots, X_n]$; es decir, se tiene:

$$V \rightarrow I(V)$$

De las correspondencias anteriores, si V es un conjunto algebraico de A_n (K), existe un ideal J de $K[X_1, X_2, \ldots, X_n]$ tal que $V = V(J)$; y se tienen que: $I(V) = I(V(J))$ es un ideal de $K[X_1, X_2, \ldots, X_n]$ y $V(I(V)) = V(I(V(J)))$ es un conjunto algebraico de A_n (K).

Recíprocamente, si I es un ideal de $K[X_1, X_2, \ldots, X_n]$ entonces $V(I) = V$ es un conjunto algebraico de A_n (K) y $I(V(I)) = I(V)$ es un ideal de $K[X_1, X_2, \ldots, X_n]$.

En base a esto, se trata de establecer relaciones entre ideales I del anillo $K[X_1, X_2, \ldots, X_n]$ y conjuntos algebraicos V de A_n (K), para conocer relaciones exactas entre los ideales $I(V(I))$ e I de $K[X_1, X_2, \ldots, X_n]$ y entre los conjuntos algebraicos $V(I(V))$ y V de A_n (K). Para esto, consideremos:

Proposición 3.

Para $S \subset K[X_1, X_2, \ldots, X_n]$, se cumplen:

i) $S \subset I(V(S))$, y

ii) $V(I(V(S))) = V(S)$. En particular, si $V(S) = V$ es un conjunto algebraico de A_n (K), entonces: $V(I(V)) = V$.

Demostración

i) Si $S \not\subset I(V(S))$, o sea: Existe $F \in S$ y $F \notin I(V(S))$.
De $F \notin I(V(S))$ se tiene que existe $P_0 \in V(S)$
tal que: $F(P_0) \neq 0$.
Además, si $P_0 \in V(S)$ entonces $G(P_0) = 0$, $\forall G \in S$. En particular para $G = F$, se tiene $F(P_0) = 0$, pues $F \in S$, lo que es contradictorio con $F(P_0) \neq 0$.
Luego: $S \subset I(V(S))$.

ii) Veamos que $V(I(V(S))) \subset V(S)$ y $V(S) \subset V(I(V(S)))$:
Si $P \in V(I(V(S)))$ entonces $F(P) = 0$, $\forall F \in I(V(S))$.
Como, por i), $S \subset I(V(S))$, se cumple: $F(P) = 0$, $\forall F \in S$;
es decir, $P \in V(S)$.
Luego: $V(I(V(S))) \subset V(S)$.
También, supongamos que existe P_0 en $A_n(K)$
tal que $P_0 \in V(S)$ y $P_0 \notin V(I(V(S)))$. Si $P_0 \notin V(I(V(S)))$, existe $G \in I(V(S))$ tal que $G(P_0) \neq 0$. Pero de $G \in I(V(S))$ se tiene $G(Q) = 0, \forall Q \in V(S)$.
En particular para $Q = P_0$, $G(P_0) = 0$, que es contrario con
$G(P_0) \neq 0$.
Luego: Si $P \in V(S)$, entonces $P \in V(I(V(S)))$; es decir:
$V(S) \subset V(I(V(S)))$ ♦

Proposición 4.

Para $X \subset A_n(K)$, se cumplen:

i) $X \subset V(I(X))$, y
ii) $I(V(I(X))) = I(X)$. En particular, si $I = I(X)$ es el ideal de X, se tiene $I(V(I)) = I$.

Demostración

i) Suponiendo que existe $P \in X$ y $P \notin V(I(X))$. De $P \notin V(I(X))$ se tiene que existe $F \in I(X)$ tal que $F(P) \neq 0$. Además, si $F \in I(X)$ entonces $F(Q) = 0$, $\forall Q \in X$; y como $P \in X$, en particular para $Q = P$ se tiene que $F(P) = 0$, que es contrario a $F(P) \neq 0$. Luego: $X \subset V(I(X))$.

ii) Sea $F \in I(V(I(X)))$. Entonces $F(P) = 0$, $\forall P \in V(I(X))$. Como, por i), $X \subset V(I(X))$, se tiene $F(P) = 0$, $\forall P \in X$; es decir: $F \in I(X)$. Luego: $I(V(I(X))) \subset I(X)$.

Recíprocamente: si existe $F \in I(X)$ y $F \notin I(V(I(X)))$, entonces $F(P) = 0$, $\forall P \in X$ y existe $P_0 \in V(I(X))$ tal que $F(P_0) \neq 0$.

De $P_0 \in V(I(X))$ se tiene que $G(P_0) = 0$, $\forall G \in I(X)$. En particular para $G = F$ se tiene $F(P_0) = 0$, que conduce a una contradicción. Luego: $I(X) \subset I(V(I(X)))$ ♦

Otra propiedad que caracteriza a los ideales de $X \subset A_n(K)$, que no es común para todo ideal, está contenida en la siguiente:

Proposición 5.

Para $X \subset A_n(K)$, sean $I(X)$ el ideal de X y $F \in K[X_1, X_2, \ldots, X_n]$. Si $F^m \in I(X)$, para algún $m \in Z^+$, entonces $F \in I(X)$.

Este resultado dice que $I(X)$ es un *ideal radical;* es decir:

$I(X) = Rad(I(X))$, donde:

$Rad(I(X)) = \{F \in K[X_1, X_2, \ldots, X_n] / F^m \in I(X),$ para $m \in Z^+\}$, es un ideal de $K[X_1, X_2, \ldots, X_n]$ que contiene a $I(X)$ y se llama el *radical de* $I(X)$.

Demostración

Si para $F \in K[X_1, X_2, \ldots, X_n]$ se cumple: $F^m \in I(X)$ para algún $m \in Z^+$, entonces $F^m(P) = 0$, $\forall P \in X$. Pero $F^m(P) = (F(P))^m = 0$; y como K es un campo, se tiene: $F(P) = 0$, $\forall P \in X$; es decir, $F \in I(X)$. Luego: $Rad(I(X)) \subset I(X)$.

Recíprocamente, si $F \in I(X)$ y como $F = F^1$ se tiene $F \in Rad(I(X))$; o sea: $I(X) \subset Rad(I(X))$.

Por lo tanto: $I(X) = Rad(I(X))$ ♦

Proposición 6.

Si F y G están en $K[X_1, X_2, \ldots, X_n]$, entonces
$V(F.G) = V(F) \cup V(G)$.
Además, $V(F^m) = V(F)$, para $m \in Z^+$.

Demostración

$P \in V(F.G) \Leftrightarrow (F.G)(P) = 0 \Leftrightarrow F(P).G(P) = 0 \Leftrightarrow F(P) = 0$

ó $G(P) = 0 \Leftrightarrow P \in V(F)$ ó $P \in V(G) \Leftrightarrow P \in V(F) \cup V(G)$.

Además:
$V(F^m) = V(F) \cup V(F) \cup \ldots \cup V(F) = V(F)$, para $m \in Z^+$ ♦

De este resultado se tiene:

Definición 3.

Un conjunto algebraico V de A_n (K) se llama *reducible* si existen conjuntos algebraicos V_1 y V_2 de A_n (K) tales que $V_i \neq V$, $i = 1, 2$ y $V = V_1 \cup V_2$. En caso contario se dice que V es *irreducible*.

Proposición 7.

Un conjunto algebraico V de A_n (K) es irreducible si y sólo si $I(V)$ es un ideal primo de $K[X_1, X_2, ..., X_n]$.

Demostración

Si $I(V)$ no es ideal primo de $K[X_1, X_2, ..., X_n]$, existen F_1 y F_2 en $K[X_1, X_2, ..., X_n]$ tal que $F_1 . F_2 \in I(V)$, $F_1 \notin I(V)$ y $F_2 \notin I(V)$.

Como $F_1 . F_2 \in I(V)$, se tiene que $F_1 . F_2(P) = 0$, $\forall P \in V$; es decir: $V = V(I(V)) \subset V(F_1 . F_2)$ y $P \in V(F_1 . F_2)$; y como $V(F_1 . F_2) = V(F_1) \cup V(F_2)$, se tiene que:

$V \subset V(F_1) \cup V(F_2)$. Luego: $V = V \cap (V(F_1) \cup V(F_2)) =$

$(V \cap V(F_1)) \cup (V \cap V(F_2))$, donde $V \cap V(F_i) \neq V$, para $i = 1, 2$;

Pues si $V \cap V(F_i) = V$ se tiene que $V \subset V(F_i)$. De aquí, si $P \in V$ entonces $F_i(P) = 0$, o sea $F_i \in I(V)$, lo que contradice a que $F_i \notin I(V)$, $i = 1, 2$.

Luego: V es reducible.

Recíprocamente: si V es reducible, existen V_1 y V_2 conjuntos algebraicos de $A_n(K)$ tal que $V_i \subsetneq V$, $i = 1, 2$ y $V_1 \cup V_2 = V$.
De $V_i \subsetneq V$, $i = 1, 2$, se tiene: $I(V) \subsetneq I(V_i)$, $i = 1, 2$.
Precisando que la inclusión es propia: si $I(V) = I(V_i)$, entonces $V(I(V)) = V(I(V_i))$; pero V y V_i son conjuntos algebraicos y por la proposición 3 se tiene: $V(I(V)) = V$ y $V(I(V_i)) = V_i$; o sea:
$V = V_i$, $i = 1, 2$, lo cual no es cierto.
Luego existe $F_i \in I(V_i)$ y $F_i \notin I(V)$; y como $\forall P \in V$ se tiene:
$P \in V_1$ o $P \in V_2$, entonces: $F_i(P) = 0$, $i = 1, 2$; es decir: $F_1 F_2 \in I(V)$, con $F_i \notin I(V)$, $i = 1, 2$. De aquí: $I(V)$ no es ideal primo de $K[X_1, X_2, \ldots, X_n]$ ♦

En los resultados anteriores, los conjuntos algebraicos de $A_n(K)$ se han definido a partir de ideales generados por subconjuntos de $K[X_1, X_2, \ldots, X_n]$; por lo que las propiedades dadas son entre conjuntos algebraicos V de $A_n(K)$, donde $V = V(I)$ para algún ideal I de $K[X_1, X_2, \ldots, X_n]$, con $I = I(X)$ para $X \subset A_n(K)$.

Falta establecer relaciones más generales entre ideales I de $K[X_1, X_2, \ldots, X_n]$ y conjuntos algebraicos V de $A_n(K)$: Dado el ideal I de $K[X_1, X_2, \ldots, X_n]$, se tiene $I \subset I(V(I))$. Sin embargo, $I \neq I(V(I))$, en general.

Así por ejemplo:

a) En $A_1(R)$, sea $I = \langle x^2 \rangle$ el ideal de $R[x]$ generado por $S = \{x^2\}$
Entonces: $V(I) = V(x^2) = V(x)$. De aquí:
$I(V(I)) = I(V(x)) = \langle x \rangle \neq I$.

b) En $A_3(R)$, sea $I = \langle (x^2 + y^2)^2, z^4 \rangle$ el ideal de $R[x, y, z]$ generado por $S = \{(x^2 + y^2)^2, z^4\}$. Entonces $V(I) = V(x^2 + y^2, z)$.
De aquí: $I(V(I)) = \langle x^2 + y^2, z \rangle \neq I$.

Un resultado que caracteriza a $V(I)$ y a $I(V(I))$, para un ideal I de $K[X_1, X_2, \ldots, X_n]$, a través de los polinomios que determinan a $V(I)$, es el Teorema de los ceros de Hilbert, considerando K *un campo algebraico cerrado.*

Antes de la formulación del Teorema mencionado, veamos algunos resultados algebraicos que se usarán en la demostración del mismo.

3. Propiedades algebraicas.

Definición 4.

Un anillo conmutativo A se llama *noetheriano* si todo ideal I de A es finitamente generado; es decir, existen $a_1, a_2, \ldots, a_r$ en A *tal que:*

$$I = (\sum_{i=1}^{r} \alpha_i a_i, \text{ con } \alpha_i \in A \text{ para } i = 1, 2, \ldots, r) = \langle a_1, a_2, \ldots, a_r \rangle$$

Así, si A es un dominio de ideales principales, entonces A es anillo noetheriano; pues cada ideal I de A es generado por un elemento; o sea $I = \langle a \rangle$.

También, si A es un campo, sus únicos ideales son $A = \langle 1 \rangle$ y $0 = \langle 0 \rangle$, los que son finitamente generados; luego, A es un anillo noetheriano.

Lema 1.

En un anillo noetheriano A, toda familia $S = (I_\alpha)_\alpha$ no vacía de

ideales I_α de A, admite un elemento maximal; es decir, existe un ideal $I\alpha_0$ en S tal que $I\alpha_0 \not\subset I\alpha$, $\forall \alpha \neq \alpha_0$.

Demostración

Como $S \neq \phi$, por el axioma de elección, de cada subconjunto de S se fija un elemento con una propiedad determinada:

Sea $I_0 \in S$ y sea $S_1 = \{I_\alpha \in S \,/\, I_0 \subsetneq I_\alpha\}$. Si $S_1 = \phi$, entonces I_0 es un elemento maximal de S; y si $S_1 \neq \phi$, sea $I_1 \in S_1$ y sea:

$S_2 = \{I_\alpha \in S_1 \,/\, I_1 \subsetneq I_\alpha\}$. Como en el caso anterior, si $S_2 = \phi$, entonces I_1 es un elemento maximal de S; y si $S_2 \neq \phi$ se tiene $I_2 \in S_2$ y sea: $S_3 = \{I_\alpha \in S \,/\, I_2 \subsetneq I_\alpha\}$. Continuando con el proceso, se obtiene una cadena ascendente de ideales de A : $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$ Afirmamos que dicha sucesión es estacionaria; es decir, existe $n \in N$ tal que $S_{n+1} = \phi$, pues A es un anillo noetheriano. De aquí, sea $I\alpha_0 = I_n$. Entonces $I\alpha_0$ es un elemento maximal de S.

Por el contrario, si $\forall n$, $S_{n+1} \neq \phi$, sea $I = \bigcup_{n=0}^{\infty} I_n$, que es un ideal de A.

Como A es anillo noetheriano, existen $u_1, u_2, \ldots, u_r$ en A tal que: $I = \langle u_1, u_2, \ldots, u_r \rangle$. Para n suficientemente grande, $u_i \in I_{n+1}$, $\forall_i = 1, 2, \ldots, r$. Luego: $I = I_{n+1} = I_{n+2} = \ldots$, que contradice a la definición de los conjuntos S_j. ♦

Proposición 8.

(Teorema de la Base de Hilbert). Si A es un anillo noetheriano, entonces el anillo de polinomios $A[x]$ es también noetheriano. En particular, si K es un campo, $K[x]$ es un anillo noetheriano.

De aquí: $K[X, Y] = K[X][Y]$ también es noetheriano; y por un proceso inductivo, $K[X_1, X_2, ..., X_n]$ es anillo noetheriano.

Demostración

Dado el ideal I de $A[x]$, hay que probar: I es finitamente generado. En efecto: Para $j \geq 0$ en Z, sea:

$I_j = \{0\} \cup \{r \in A / a_0 + a_1 x + ... + r x^j \in I\}$; es decir, I_j está formado por el elemento 0 de A y los coeficientes principales de los polinomios de grado j en I.

Afirmación 1.

$\forall j \geq 0$, en Z, I_j es un ideal de A y $I_j \subseteq I_{j+1}$.

En efecto: para r y t en I_j y $a \in A$. Si $r - t = 0$, se tiene: $r - t \in I_j$.

Si $r - t \neq 0$, sean

$$f(x) = a_0 + a_1 x + ... + r x^j \text{ y } g(x) = b_0 + b_1 x + ... + t x^j \text{ en } I.$$

Entonces: $f(x) - g(x) = (a_0 - b_0) + (a_1 - b_1) x + ... + (r - t) x^j \in I$.

De aquí $r - t \in I_j$. Por otro lado:

$$a.f(x) = (a a_0) + (a a_1) x + ... + (ar) x^j \in I, \text{ o sea: } ar \in I_j.$$

Luego, I_j es un ideal de A, $\forall j = 0, 1, ...$

Para ver que $I_j \subseteq I_{j+1}$, sea $r \in I_j$. Si $r = 0$, entonces $r \in I_{j+1}$.

Si $r \neq 0$, sea $f(x) = a_0 + a_1 x + ... + r x^j \in I$; y como $x \in A[x]$ se tiene:

$h(x) = x f(x) = a_0 x + a_1 x^2 + ... + r x^{j+1} \in I$; es decir: $r \in I_{j+1}$. Luego:

$I_j \subseteq I_{j+1}$, $\forall j$. Lo que completa la afirmación.

De la afirmación 1 y considerando el Lema 1, para la cadena $I_o \subseteq I_1 \subseteq I_2 \subseteq \ldots$ de ideales del anillo noetheriano A, existe $m \geq 0$ en Z tal que $I_h = I_m$, $\forall h \geq m$ en Z; y los ideales I_o, I_1, ..., I_m son finitamente generados; es decir existen $a_{i_1}, a_{i_2}, \ldots, a_{in_i}$ en A para cada $i = 0, 1, 2, \ldots, m$; tal que: $I_i = \langle a_{i_1}, a_{i_2}, \ldots, a_{in_i} \rangle$ donde cada a_{ij} es 0 ó es coeficiente principal de polinomios $f_{ij}(x)$, para $i = 0, 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n_i$; y $f_{ij}(x) \in I$ de grado i.

Afirmación 2

El ideal I es generado por los polinomios $f_{ij}(x)$, con $i = 0, 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n_i$; es decir: $I = \langle f_{ij}(x) \rangle$.

En efecto: como $f_{ij}(x) \in I$, $\forall i$ y $\forall j$, se tiene:

$$\langle f_{ij}(x),\ i = 0, 1, \ldots, m;\ j = 1, 2, \ldots, n_i \rangle \subset I.$$

Recíprocamente: sea $f(x) = b_o + b_1 x + \ldots + b_d x^d \in I$ de grado d.

Considerando inducción sobre d, se tiene:

Para $d = 0$, $f(x) = b_o \in I_o \subset \langle f_{ij}(x) \rangle$

Asumiendo que todo polinomio de grado no mayor que $d-1$ en I es combinación de los polinomios $f_{ij}(x)$, $i = 0, 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n_i$; *Si* $d > m$, entonces $I_d = I_m$. De aquí, cada coeficiente b_d en I_d es de la forma: $b_d = c_1 a_{m_1} + c_2 a_{m_2} + \ldots + c_{n_m} a_{mn_m}$, con $c_1, c_2, \ldots, c_{n_m}$ en A.

Luego:

$$F(x) = f(x) - x^{d-m}(c_1 f_{m_1}(x) + c_2 f_{m_2}(x) + \ldots + c_{n_m} f_{mn_m}(x)) \in I,$$

pues $f(x)$ y $f_{ij}(x)$ están en I; además, el coeficiente de x^d en $F(x)$

es:

$$b_d - \sum_{j=1}^{n_m} c_j a_{mn_j} = 0,$$

por lo que el grado de $F(x)$ es menor que d.

Por el proceso inductivo, se tiene que $F(x)$ es combinación de los polinomios $f_{ij}(x)$. De aquí:

$$f(x) = F(x) + x^{d-m}\,(c_1 f_{m_1}(x) + c_2 f_{m_2}(x) + \ldots + c_{n_m} f_{mn_m}(x));$$

es decir: $f(x) \in \langle f_{ij}(x) \rangle$.

Si $d \leq m$, para b_d en I_d, existen $e_1, e_2, \ldots, e_{n_d}$ en A tal que:

$b_d = e_1 a_{d_1} + e_2 a_{d_2} + \ldots + e_{n_d} a_{dn_d}$ Luego:

$G(x) = f(x) - (e_1 f_{d_1}(x) + e_2 f_{d_2}(x) + \ldots + e_{n_d} f_{n_d}(x)) \in I$ y tiene grado menor que d. De aquí, por proceso de inducción, $G(x)$ es combinación de los $f_{ij}(x)$; por lo que:

$$f(x) = G(x) + e_1 f_{d_1}(x) + e_2 f_{d_2}(x) + \ldots + e_{n_d} f_{n_d}(x)$$

es combinación de los $f_{ij}(x)$.

En consecuencia, $I = \langle f_{ij}(x), i = 0, 1, 2, \ldots, m \text{ y } j = 1, 2, \ldots, n_i \rangle$;

con lo que se asegura el resultado del teorema. ♦

Definición 5.

Dado un anillo A, sea B un subanillo de A. Se tienen:

1) A es un *módulo de tipo finito sobre* B, si A, como B–módulo, es de generación finita; es decir, existen $v_1, v_2, \ldots, v_t$ en A tal que:

$$A = \sum_{j=1}^{t} Bv_j = \{ \sum_{j=1}^{t} b_j v_j \,/\, b_j \in B\}$$

2) A es un *anillo de tipo finito sobre* B, si existen $v_1, v_2, \ldots, v_n$ en A tal que:

$$A = B[v_1, v_2, \ldots, v_n] = \{ \sum_i b_i \, v_1^{i1} \, v_2^{i2} \ldots v_n^{in}, \text{ con } b_i \in B\}$$

3) Un elemento v de A se llama *entero sobre* B si existe $f(x) \in B[x]$ tal que $f(v) = 0$, con $f(x) = x^n + b_{n-1} x^{n-1} + \ldots + b_0$. En particular, si A y B son campos y $v \in A$ es entero sobre B, se dice que v *es algebraico sobre* B.

4) Si cada $v \in A$ es entero sobre B, se dice que A *es entero sobre* B.
En particular, si A y B son campos y A es entero sobre B, se dice que A *es extensión algebraica sobre* B.

Considerando los conceptos anteriores, se tienen los siguientes resultados:

Proposición 9.

Sean A un dominio de integridad, B un subanillo de A y $v \in A$. Entonces, las condiciones siguientes son equivalentes:

i) v es un entero sobre B.
ii) $B[v]$ es un módulo de tipo finito sobre B.
iii) Existe un subanillo B' de A tal que $B[v] \subset B'$ y B' es un módulo de tipo finito sobre B.

Demostración

i) $\Rightarrow$ *ii):* si $v \in A$ es un elemento entero sobre B, existe

$f(x) = x^n + b_{n-1}\, x^{n-1} + \ldots + b_o$ en $B[x]$ tal que
$f(v) = v^n + b_{n-1}\, v^{n-1} + \ldots + b_1 v + b_o = 0$. De aquí:

$$v^n = -\sum_{i=0}^{n-1} b_i v^i;$$ es decir: $v^n \in B[v]$. También: $v, v^2, \ldots, v^{n-1}$

están en $B[v]$. Además:

$$v^{n+1} = vv^n = v\left(-\sum_{j=0}^{n-1} b_j v^j\right) = -\sum_{j=0}^{n-1} b_j\, v^{j+1} = -\sum_{j=0}^{n-2} b_j v^{j+1} - b_{n-1} v^n$$

$$= -\sum_{j=0}^{n-2} b_j v^{j+1} - b_{n-1}\left(-\sum_{j=0}^{n-1} b_j v^j\right) =$$

$$= \sum_{j=1}^{n-1} (b_{n-1} b_j - b_{j-1})\, v^j + b_{n-1} b_o \in B[v]$$

Luego, por un proceso inductivo, $\forall t$, $v^t \in B[v]$; es decir, $B[v]$ es un módulo de tipo finito sobre B generado por $1, v, v^2, \ldots, v^{n-1}$

ii) $\Rightarrow$ *iii):* considerando $B' = B[v]$, se tiene el resultado.

iii) $\Rightarrow$ *i):* Sea B' un subanillo de A tal que $B[v] \subset B'$ y B' es un módulo de tipo finito sobre B. Entonces existen $\omega_1, \omega_2, \ldots, \omega_r$ en B' tal que:

$B' = \sum_{i=1}^{r} B\omega_i$. Como $B[v] \subset B'$ se tiene que $v \in B'$ y también:

$v\omega_i \in B'$, $\forall i = 1, 2, \ldots, r$. Luego:

$v\omega_i = \sum_{i=1}^{r} b_{ij}\,\omega_j$, con $b_{ij} \in B$. De aquí:

$\sum_{j=1}^{r} (v\,\delta_{ij} - b_{ij})\,\omega_j = 0$, $\forall i = 1, 2, \ldots, r$, es un sistema de r ecuaciones

con r incógnitas en $\omega_1, \omega_2, \ldots, \omega_r$. Si $\Delta = det\,(v\delta_{ij} - b_{ij})$, por la fórmula de Crammer se tiene:

$\Delta\,\omega_j = 0$, $\forall j$. Luego:

$\Delta B' = \Delta.\ \sum_{j=1}^{r} B\omega_j = \sum_{j=1}^{r} B\,\Delta\,\omega_j = 0$. Como $1 \in B'$ se tiene:

$$\Delta 1 = \Delta = 0.$$

Por otro lado, al desarrollar Δ y como v aparece sólo en la diagonal principal, se tiene:

$$\Delta = \prod_{j=1}^{r} (v - b_{ij}) = v^r + c_{r-1}\,v^{r-1} + \ldots + c_1 v + c_o = 0$$

con $c_j \in B$. De aquí, v es un elemento entero sobre B. ♦

Proposición 10.

Sean: A un anillo, B un subanillo de A y $(v_i)_i$ con $i = 1, 2, \ldots, n$, una familia finita de elementos $v_i \in A$ tal que para cada i, v_i es entero sobre $B\,[v_1, v_2, \ldots, v_{i-1}]$; en particular, cada v_i es entero sobre B. Entonces:

$B[v_1, v_2, \ldots, v_n]$ es un módulo de tipo finito sobre B y todo elemento de $B[v_1, v_2, \ldots, v_n]$ es entero sobre B.

Demostración

Considerando inducción sobre n:
Para $n = 1$, si v_1 es entero sobre B, entonces, por la proposición anterior, se tiene que $B[v_1]$ es un módulo de tipo finito sobre B.

Supongamos que para $1 \leq r < n$ se cumple que $B[v_1, v_2, \ldots, v_r]$ es un módulo de tipo finito sobre B. Entonces $M = B[v_1, v_2, \ldots, v_{n-1}]$ es un módulo de tipo finito sobre B; es decir, existen $\omega_1, \omega_2, \ldots, \omega_p$ en M tal que:

$$M = \sum_{j=1}^{p} B\omega_j$$

y como v_n es entero sobre M, entonces:

$M[v_n] = B[v_1, v_2, \ldots, v_n]$ es un módulo de tipo finito sobre M, por la proposición 9. De aquí, existen $u_1, u_2, \ldots, u_q$ en $M[v_n]$ tal que:

$M[v_n] = \sum_{h=1}^{q} Mu_h$ Luego:

$$B[v_1, v_2, \ldots, v_n] = M[v_n] = \sum_{h=1}^{q} \left(\sum_{j=1}^{p} B\omega_j \right) u_h = \sum_{j,h} B\omega_j u_h \ ;$$

es decir, $\{\omega_j u_h,\ j = 1, 2, \ldots, p \ y \ h = 1, 2, \ldots, q\}$ genera a

$B[v_1, v_2, \ldots, v_n]$ sobre B como B–módulo. De aquí, $B[v_1, v_2, \ldots, v_n]$ es un módulo de tipo finito sobre B.

Además, si $v \in B[v_1, v_2, \ldots, v_n]$, se tiene:

$v = \sum_j a_j v_1^{j_1} v_2^{j_2} \ldots v_n^{j_n}$, con $a_j \in B$. Luego, $B[v] = \sum_{i=1}^{t} B v^i$,

es un subanillo de $B[v_1, v_2, \ldots, v_n]$ que contiene a B y que es un módulo de tipo finito sobre B; y por la proposición 9 se tiene que v es un entero sobre B. De aquí, todo v de $B[v_1, v_2, \ldots, v_n]$ es un entero sobre B. ♦

Proposición 11. (Teorema de Zariski).

Dados L un campo, K un subcampo de L tal que L es un anillo de tipo finito sobre K; entonces: L es un módulo de tipo finito sobre K. De aquí, L es una extensión algebraica sobre K.

Demostración

Por ser L un anillo de tipo finito sobre K, existen $v_1, v_2, \ldots, v_n$ en L tal que $L = K[v_1, v_2, \ldots, v_n]$. Por la proposición anterior, es suficiente probar que cada v_i, $i = 1, 2, \ldots, n$, sea entero sobre K.

Para esto, considerando inducción sobre n:

Para $n = 1$, sea $v = v_1$. Como $L = K[v]$ es un campo y $v \in K[v]$, entonces $v^{-1} \in K[v]$; es decir:

$v^{-1} = \sum_{i=1}^{m} a_i v^i$, con $a_i \in K$ y $a_m \neq 0$. Luego:

$$1 = \sum_{i=1}^{m} a_i v^{i+1} \in K; \text{ o sea:}$$

$a_m v^{m+1} + a_{m-1} v^m + \ldots + a_1 v^2 + a_0 v - 1 = 0$; y como: $a_m \neq 0$ se tiene:

$$v^{m+1} + \frac{a_{m-1}}{a_m} v^m + \ldots + \frac{a_1}{a_m} v^2 + \frac{a_o}{a_m} v + (-\frac{1}{a_m}) = 0;$$

$$\text{con} \quad \frac{a_{m-1}}{a_m}, \frac{a_{m-2}}{a_m}, \ldots, \frac{a_1}{a_m}, \frac{a_o}{a_m} \quad \text{y} - \frac{1}{a_m} \quad \text{en } K;$$

por lo que v es entero sobre K. Por la proposición 9 se concluye que $L = K[v]$ es un módulo de tipo finito sobre K.

Para $n \geq 2$, supongamos que exista algún $v_i \in L$ tal que v_i no es entero sobre K. Reordenando, sea $v_i = v_1$, que no es entero sobre K, y sea $K_1 = K(v_1) \subset L$ el campo de fracciones de $K[v_1]$.

Por inducción: $v_2, v_3, \ldots, v_n$ son enteros sobre K_1; o sea,

$L = K_1[v_2, v_3, \ldots, v_n]$ es módulo de tipo finito sobre K_1; y como

$K \subset K_1 \subset L$, se tiene:

Afirmación:

K_1 es anillo de tipo finito sobre K.
En efecto: Por ser L módulo de tipo finito sobre K_1, existen $\omega_1, \omega_2, \ldots, \omega_m$ en L tal que:

$$L = \sum_{j=1}^{m} K_1 \omega_j = \{ \sum_{j=1}^{m} b_j \omega_j / b_j \in K_1 \}; \text{ y como } v_i \in L, \text{ se tiene:}$$

$$v_i = \sum_{j=1}^{m} b_{ij} \omega_j \quad \text{con } b_{ij} \in K_1; \text{ y para } \omega_i \text{ y } \omega_j \text{ en } L \text{ se tiene:}$$

$\omega_i\,\omega_j \in L$ y $\omega_i\,\omega_j = \sum_{h=1}^{m} b_{ijh}\,\omega_h$, con $b_{ijh} \in K_1$.

Como los elementos b_{ij} y b_{ijh} están en K_1 y $K \subset K_1$, entonces dichos elementos generan un anillo $K_0 \subset K_1$ de tipo finito sobre K, a través del homomorfismo de anillos:

$\varphi: K[x_1, \ldots, x_{ij}, \ldots, x_{ijh}, \ldots, x_n] \to K_1$, tal que: $\varphi(x_{ij}) = b_{ij}$,

$\varphi(x_{ijh}) = b_{ijh}$ y $\varphi(K) \approx K$; es decir: $K_0 = K[\ldots, b_{ij}, \ldots, b_{ijh}, \ldots] \subset K_1$.

Por otro lado, para $v \in L$, se tiene:

$$v = \sum_{i=1}^{m} \alpha_i\, v_1^{i1}\, v_2^{i2} \ldots v_n^{in}, \text{ con } \alpha_i \in K,$$

por ser L un anillo de tipo finito sobre K. Luego:

$$v = \sum_{i=1}^{n} \alpha_i \Big(\sum_{j=1}^{m} b_{1j}\,\omega_j\Big)^{i1} \Big(\sum_{j=1}^{m} b_{2j}\,\omega_j\Big)^{i2} \ldots \Big(\sum_{j=1}^{m} b_{nj}\,\omega_j\Big)^{in},$$

de donde, efectuando las potencias y multiplicaciones y considerando:

$\omega_i\,\omega_j = \sum_{h=1}^{m} b_{ijh}\,\omega_h$, se tiene que v es una combinación de:

$\omega_1, \omega_2, \ldots, \omega_m$ con coeficientes en K_0; es decir, $v = \sum_{j=1}^{m} \beta_j\,\omega_j$, con

$\beta_j \in K_0$; y como $K_0 \subset K_1 \subset L$, considerando K_1 submódulo de L sobre K_0, se tiene que K_1 es un módulo de tipo finito sobre K_0.

Luego, como K_1 es módulo de tipo finito sobre K_o y K_o es anillo de tipo finito sobre K, existen elementos $u_1, u_2, \ldots, u_p$ en K_1 tal que:

$K_1 = \sum_{j=1}^{p} K_o u_j$, y existen elementos $s_1, s_2, \ldots, s_t$ en $K_o \subset K_1$ tal que:

$K_o = \sum_{h} K s_1^{h1} s_2^{h2} \ldots s_t^{ht}$. De esto:

$$K_1 = \sum_{j=1}^{p} \left(\sum_{h} K s_1^{h1} s_2^{h2} \ldots s_t^{ht} \right) u_j = \sum_{j,h} K s_1^{h1} s_2^{h2} \ldots s_t^{ht} u_j =$$

$K[u_1, u_2, \ldots, u_p, s_1, s_2, \ldots, s_t]$; es decir, K es un anillo de tipo finito sobre K; lo que prueba la afirmación.

Considerando: $K_1 = K[y_1, y_2, \ldots, y_s]$, para $y_1, y_2, \ldots, y_s$ en K_1 y como $K_1 = K(v_1)$, se tiene: $y_j = (f_j/g_j)$, con f_j y g_j en $K[v_1] \approx K[x]$, $j = 1, 2, \ldots, s$. Sea d el mínimo común múltiplo de los g_j en $K[v_1]$. Entonces: $dy_j = d.\ (f_j/g_j) = (d/g_j)\ .\ f_j = h_j f_j$, con $h_j \in K[v_1]$, para $j = 1, 2, \ldots, s$; o sea: $\forall j,\ dy_j \in K[v_1]$.

Por otro lado, para $z \in K_1$ se tiene: $z = \sum_{j} b_j y_1^{j1} y_2^{j2} \ldots y_s^{js}$, con

$b_j \in K$; y sea $N_j = j_1 + j_2 + \ldots + j_s$. Si $N \geq N_j\ \forall_j$ se tiene:

$$zd^N = \sum_{j} b_j y_1^{j1} y_2^{j2} \ldots y_s^{js} d^N = \sum_{j} b_j' (y_1 d)^{j1} (y_2 d)^{j2} \ldots (y_s d)^{js}$$

$$= \sum_{j} b_j' (h_j f_j), \text{ con } b_j' \in K \text{ y } h_j f_j \in K[v_1].$$

De aquí: $\forall z \in K_1,\ zd^N \in K[v_1]$, para algún $N > 0$.

También, sea $h \in K[v_1]$, donde h es irreducible y primo relativo con d. Entonces $1/h \in K_1$ y existe $N > 0$ tal que $d^N . (1/h) = (d^N/h) \in K[v_1]$; es decir, h divide a d^N; y como h es irreducible, se concluye que h divide a d, que contradice a que h es primo relativo con d.

En consecuencia: v_1 es entero sobre K; de aquí, cada v_i es entero sobre K.
Luego: $L = K[v_1, v_2, ..., v_n]$ es módulo finito sobre K. Además, como K y L son campos y cada elemento de $K[v_1, v_2, ..., v_n]$ es entero sobre K, se cncluye que L es extensión algebraica sobre K. ♦

Proposición 12

Sea K un campo algebraicamente cerrado y sea L una extensión de K, (K es subcampo de L), tal que L es módulo de tipo finito sobre K. Entonces: $L = K$.

Demostración

Como L y K son campos y L es módulo de tipo finito sobre K, se tienen que L es extensión algebraica de K; es decir, todo elemento $z \in L$ es algebraico sobre K. De aquí, existe $f(x) \in K[x]$, tal que $f(z) = 0$. Pero por ser K un campo algebraicamente cerrado, todas las raices de $f(x)$ están en K; es decir: $z \in K$. Luego: $L = K$. ♦

Para concluir, veamos el enunciado y la demostración del Teorema de los ceros de Hilbert.

4. El Teorema de los Ceros de Hilbert

Teorema

Sea K un campo algebraicamente cerrado y sea I un ideal propio de $K[x_1, x_2, ..., x_n]$. Entonces:

1) (Versión "Débil"): $V(I) \neq \phi$; es decir, existe $P \in A_n(K)$ tal que $F(P) = 0$, $\forall F \in I$.

2) (Versión "Fuerte"): $I(V(I)) = Rad(I)$; es decir, si para $F \in K[x_1, x_2, ..., x_n]$ se cumple $F(P) = 0$, $\forall P \in V(I)$, entonces $F^N \in I$, para algún $N > 0$ en Z, y recíprocamente.

Demostración

1) Como $K[x_1, x_2, ..., x_n]$ es anillo noetheriano e I es un ideal propio, para la familia $(J_\alpha)_\alpha$ de ideales J_α de $K[x_1, x_2, ..., x_n]$ tal que $I \subseteq J_\alpha$ $\forall \alpha$, existe un ideal maximal J tal que $I \subseteq J$, según el Lema 1. Luego, si $F(P) = 0$, $\forall F \in J$, entonces $F(P) = 0$, $\forall F \in I$; es decir, $V(J) \subseteq V(I)$. De aquí, es suficiente que $V(J) \neq \phi$ para asegurar que $V(I) \neq \phi$.

Por lo anterior, asumiendo que I es un ideal maximal de $K[x_1, x_2, ..., x_n]$ se tiene en consecuencia, que $K[x_1, x_2, ..., x_n]/I$ es un campo; y si Π: $K[x_1, x_2, ..., x_n] \rightarrow K[x_1, x_2, ..., x_n]/I$ es el epimorfismo canónico, tal que $\Pi(F) = F + I$ y $Ker(\Pi) = I$, y como también $K \subset K[x_1, x_2, ..., x_n]$, considerando la restricción $\overline{\Pi}$ de Π a K se tiene que $\overline{\Pi}$ es un monomorfismo de anillos, es decir, $\overline{\Pi}(K) \approx K$. De aquí, $K \subset K[x_1, x_2, ..., x_n]/I$ como subcampo. Además, sea $\Pi(x_i) = v_i$, $i = 1, 2, ..., n$. Entonces:

$\Pi(K[x_1, x_2, \ldots, x_n]) = \overline{\Pi}(K)[v_1, v_2, \ldots, v_n] \approx K[v_1, v_2, \ldots, v_n]$ y por la suryectividad de Π se tiene que $K[x_1, x_2, \ldots, x_n]/I \approx K[v_1, v_2, \ldots, v_n]$ es un anillo de tipo finito sobre K. Por la proposición 11 se concluye que $K[x_1, x_2, \ldots, x_n]/I$ es un módulo de tipo finito sobre K; y siendo K campo algebraicamente cerrado, por la proposición 12, se tiene que $K[x_1, x_2, \ldots, x_n]/I = K$.

Luego, para $i = 1, 2, \ldots, n$ se tiene: $\Pi(x_i) = v_i \in K$; o sea: $x_i + I = v_i$ y de aquí: $x_i - v_i \in I$.

Sea $I^1 = \langle x_i - v_i,\ i = 1, 2, \ldots, n \rangle$ el ideal de $K[x_1, x_2, \ldots, x_n]$ generado por los polinomios $x_i - v_i$, para $i = 1, 2, \ldots, n$; o sea $I^1 \subset I$.

Afirmación:

I^1 es un ideal maximal de $K[x_1, x_2, \ldots, x_n]$.

En efecto: Sea J un ideal de $K[x_1, x_2, \ldots, x_n]$ tal que $I^1 \subset J$.

Si $I^1 \neq J$, existe $F \in K[x_1, x_2, \ldots, x_n]$ tal que $F \in J$ y $F \notin I^1$. Como K es un campo y $v_1, v_2, \ldots, v_n$ están en K, se tiene:

$$F = F(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{n} \alpha_i x_1^{i1} x_2^{i2} \ldots x_n^{in} =$$

$$\sum_{i=0}^{n} \alpha_i (x_1 - v_1 + v_1)^{i1} \ldots (x_n - v_n + v_n)^{in}$$

$$= \sum_{i=0}^{n} \lambda_i (x_1 - v_1)^{i1} (x_2 - v_2)^{i2} \ldots (x_n - v_n)^{in} = \lambda_0 + \sum_{i=1}^{n} \gamma_i (x_i - v_i),$$

donde en cada caso: $\alpha_i \in K$, $\lambda_i \in K$ y $\gamma_i \in K[x_1, x_2, \ldots, x_n]$; y como

$\sum \gamma_i (x_i - v_i) \in I^1 \subset J$ y $F \in J$, se tiene que $\lambda_0 \in J$ y $\lambda_0 \neq 0$,

pues $F \notin I^1$.

De aquí: $\lambda_0^{-1} \in K$ y $1 = \lambda_0^{-1} \lambda_0 \in J$; es decir:

$J = K[x_1, x_2, \ldots, x_n]$. Por lo que se asegura que I^1 es ideal maximal.

De la afirmación anterior, como I es un ideal propio de

$K[x_1, x_2, \ldots, x_n]$ y $I^1 \subset I$, se tiene que $I^1 = I$, o sea:

$I = \langle x_1 - v_1, x_2 - v_2, \ldots, x_n - v_n \rangle$; y por la proposición 1, se tiene

$V(I) = V((x_1 - v_1, x_2 - v_2, \ldots, x_n - v_n))$. Luego:

$P \in V(I) \Leftrightarrow P \in V((x_1 - v_1, x_2 - v_2, \ldots, x_n - v_n)) \Leftrightarrow$

$(x_i - v_i)(P) = 0, \ \forall i = 1, 2, \ldots, n.$

$\Leftrightarrow x_i(P) = v_i, \ \forall i = 1, 2, \ldots, n \Leftrightarrow P = (v_1, v_2, \ldots, v_n)$.

De aquí: $V(I) = \{(v_1, v_2, \ldots, v_n)\} \neq \phi$.

2) Veamos que: i) $Rad(I) \subset I(V(I))$ y ii) $I(V(I)) \subset Rad(I)$.

i) Si $F \in Rad(I)$, existe $N > 0$ en Z tal que $F^N \in I$.

Luego, para $P \in V(I)$ se tiene que $G(P) = 0$, $\forall G \in I$; y como $F^N \in I$, también se tiene: $F^N(P) = 0$. De aquí: $P \in V(F^N)$. Luego: $V(I) \subset V(F^N)$.

Pero $V(F^N) = V(F)$, por la proposición 6; es decir, $V(I) \subset V(F)$. Además, si $G \in I(V(F))$, entonces $G(P) = 0$, $\forall P \in V(F)$, y también: $G(P) = 0$, $\forall P \in V(I)$, pues $V(I) \subset V(F)$, o sea: $G \in I(V(I))$. Luego: $I(V(F)) \subset I(V(I))$; y por la proposición 3i), $F \in I(V(F))$; es decir, $F \in I(V(I))$.

Por lo tanto: si $F \in Rad(I)$, entonces $F \in I(V(I))$; esto es: $Rad(I) \subset I(V(I))$.

ii) Como I es ideal del anillo noetheriano $K[x_1, x_2, \ldots, x_n]$, se tiene que I es finitamente generado, o sea existen $F_1, F_2, \ldots, F_r$ en I tal que: $I = \langle F_1, F_2, \ldots, F_r \rangle$. De aquí, para $G \in I$ y $P \in A_n(K)$, si $F_i(P) = 0$, $\forall i = 1, 2, \ldots, r$, entonces: $G(P) = 0$.

Luego, sea $F \in I(V(I))$. Si $F = 0$; entonces $F \in Rad(I)$, por ser $Rad(I)$ un ideal de $K[x_1, x_2, \ldots, x_n]$. Si $F \neq 0$, sea u un elemento en alguna extensión de K tal que $(x_1, x_2, \ldots, x_n, u)$ sea trascendente sobre K; en $K[x_1, x_2, \ldots, x_n]$ sea J el ideal generado por I y $uF - 1$; o sea,
$J = \langle I, uF - 1 \rangle = \langle F_1, F_2, \ldots, F_r, uF - 1 \rangle$.
Como $F \in I(V(I))$, se tiene que $F(P) = 0$, $\forall P \in V(I)$, siendo:
$P = (a_1, a_2, \ldots, a_n) \in A_n(K)$.
Si $\overline{P} = (a_1, a_2, \ldots, a_n, d) \in A_{n+1}(K)$, entonces:
$(uF - 1)(\overline{P}) = d.F(P) - 1 = d.0 - 1 = -1 \neq 0$, $\forall d \in K$.
De aquí, si $\overline{Q} = (c_1, c_2, \ldots, c_n, q) \in A_{n+1}(K)$ y $\forall H \in J$,
se cumple: $H(Q) = 0$; y como:
$I \subset J$ y $K[x_1, x_2, \ldots, x_n] \subset K[x_1, x_2, \ldots, x_n, u]$, también se cumple: $H(Q) = 0$, $\forall H \in I$, siendo: $Q = (c_1, c_2, \ldots, c_n)$ y

$H = \sum_{i=1}^{r} \alpha_i F_i$ con $\alpha_i \in K[x_1, x_2, \ldots, x_n]$; donde $F_i(Q) = 0$,

$\forall i = 1, 2, \ldots, r$. Luego $F(Q) = 0$; y para

$\tilde{H} = \sum_{i=1}^{r} \alpha_i F_i + \beta(uF - 1) \in J$, con $\beta = 1 \in K[x_1, x_2, \ldots, x_n, u]$, se tiene:

$$\tilde{H}(\bar{Q}) = \sum_{i=1}^{r} \alpha_i(Q) F_i(Q) + \beta(\bar{Q})(q.F(Q) - 1) = 0 + 1(q.0 - 1) = -1 \neq 0,$$

lo que es una contradicción con $H(\bar{Q}) = 0$, $\forall H \in J$. Por lo tanto se concluye que $V(J) = \phi$. Luego, por la parte 1), se tiene que:

$J = \langle 1 \rangle = K[x_1, x_2, \ldots, x_n, u]$. De aquí:

$$1 = \sum_{i=1}^{r} G_i F_i + G_{r+1}(uF - 1),$$ para ciertos $G_i \in K[x_1, x_2, \ldots, x_n, u]$,

$i = 1, 2, \ldots, r, r + 1$. Considerando $K(x_1, x_2, \ldots, x_n)$, el campo de fracciones de $K[x_1, x_2, \ldots, x_n]$ y como $F \neq 0$, para x_i y $(1/F)$ en $K(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$, considerando el homomorfismo de sustitución:

$\phi : K[x_1, x_2, \ldots, x_n, u] \rightarrow K(x_1, x_2, \ldots, x_n)$, donde

$\phi(x_i) = x_i$, $i = 1, 2, \ldots, n$, $\phi(u) = (1/F)$ y $\phi(K) = K$, se tiene:

$K[x_1, x_2, \ldots, x_n, u] \approx K[x_1, x_2, \ldots, x_n, (1/F)]$. Luego:

$$1 = \sum_{i=1}^{r} \overline{G}_i(x_1, x_2, \ldots, x_n, 1/F).F_i + \overline{G}_{r+1}(x_1, x_2, \ldots, x_n, 1/F)((1/F)F-1)$$

$$= \sum_{i=1}^{r} \overline{G}_i(x_1, x_2, \ldots, x_n, 1/F).F_i.$$

Sea F^N el común denominador de los términos en $1/F$ de cada G_i, para algún $N > 0$ en Z suficientemente grande. Entonces:

$$1 = 1/F^N(\sum_{i=1}^{r} \overline{G}_i(x_1, x_2, \ldots, x_n).F_i), \text{ o sea:}$$

$$F^N = \sum_{i=1}^{r} \overline{G}_i(x_1, x_2, \ldots, x_n).F_i = \sum_{i=1}^{r} \overline{G}_i F_i, \text{ con } \overline{G}_i \in K[x_1, x_2, \ldots, x_n]$$

De aquí: $F^N \in I$; es decir: $F \in Rad\ (I)$. Luego: $I\ (V\ (I)) \subset Rad\ (I)$. De i) y ii) se concluye: $I\ (V\ (I)) = Rad\ (I)$. ♦

Del teorema anterior se tienen ciertas consecuencias. Entre éstas tenemos:

Colorario 1

Si I es un ideal radical de $K[x_1, x_2, \ldots, x_n]$, entonces: $I\ (V\ (I)) = I$. De aquí, existe una biyección entre los conjntos algebraicos V de $A_n(K)$ y los ideales radicales I de $K[x_1, x_2, \ldots, x_n]$.

Demostración

Por la parte 2) del teorema anterior, como I es un ideal radical, o

sea: *Rad (I) = I, se tiene: I (V (I)) = I.*

Además, si V es un conjunto algebraico, se tiene que $V = V(I)$ para algún ideal I de $K[x_1, x_2, \ldots, x_n]$. Luego: $I(V) = I(V(I)) = Rad(I) = I$, donde I es ideal radical. ♦

Corolario 2

Si I es un ideal primo de $K[x_1, x_2, \ldots, x_n]$, entonces $V(I)$ es irreducible.

De aquí, existe una biyección entre conjuntos algebraicos irreducibles V y los ideales primos I de $K[x_1, x_2, \ldots, x_n]$; en donde, a los ideales maximales le corresponden puntos.

Demostración

Si I es un ideal primo de $K[x_1, x_2, \ldots, x_n]$, se tiene: $I \subset Rad(I)$, $\forall$ ideal I.

Sea $F \in Rad(I)$. Entonces $F^m \in I$ para algún $m > 0$. Pero

$F^m = F.F^{m-1} \in I$; y como I es ideal primo, se tiene:

$F \in I$ o $F^{m-1} \in I$. También: $F^{m-1} = F.F^{m-2}$, y se tiene

$F \in I$ o $F^{m-2} \in I$. Continuando un número finito de veces, se tiene que $F \in I$; es decir, $Rad(I) \subset I$.

Luego: $Rad(I) = I$, para I ideal primo.

Además, $I(V(I)) = I$ es un ideal primo; luego, por la proposición

7, se tiene que $V(I)$ es irreducible.

También, si V es irreducible, entonces $I(V)$ es ideal primo; lo que permite establecer la biyección.

Por otro lado, si $I_o \subsetneqq I_1 \subsetneqq I_2 \subsetneqq \ldots \subsetneqq I_m \neq K[x_1, x_2, \ldots, x_n]$

es una cadena ascendente de ideales propios, con I_m el ideal maximal, se tiene:

$V(I_o) \supsetneqq V(I_1) \supsetneqq \ldots \supsetneqq V(I_m) \supsetneqq \phi$; donde, por 1) del teorema,

$V(I_m) \neq \phi$. Luego existe $P \in A_n(K)$ tal que $(P) \subset V(I_m)$. De aquí: $I(V(I_m)) = Rad(I_m) \subset I((P))$; y como $I_m \subset Rad(I_m)$, se tiene: $I_m \subset I((P))$. Por ser I_m ideal maximal se tiene: $I_m = I((P))$ o $I((P)) = K[x_1, x_2, \ldots, x_n]$. Si $I((P)) = K[x_1, x_2, \ldots, x_n]$, entonces: $F(P) = 0$, $\forall F \in K[x_1, x_2, \ldots, x_n]$, lo cual no es verdad.

Luego $I_m = I((P))$. De aquí, como todo conjunto finito de $A_n(K)$ es algebraico, se tiene: $V(I_m) = (P)$. ♦

Corolario 3

Para $F \in K[x_1, x_2, \ldots, x_n]$, sea $F = F_1^{n1} F_2^{n2} \ldots F_r^{nr}$ la descomposición de F en sus factores irreducibles. Entonces:

$V(F) = \bigcup_{i=1}^{r} V(F_i)$, donde cada $V(F_i)$ es irreducible. Además

$I(V(F)) = \langle F_1, F_2, \ldots, F_r \rangle$.
De aquí, existe una biyección entre polinomios irreducibles F de $K[x_1, x_2, \ldots, x_n]$ y las hipersuperficies irreducibles de

$A_n(K)$, salvo factores no nulos en K.

Demostración

Por la proposición 6 se tiene: $V(F) = V(F_1) \cup V(F_2) \cup \ldots \cup V(F_r)$. Además, como F_i es irreducible en $K[x_1, x_2, \ldots, x_n]$ se tiene que $\langle F_i \rangle$ es ideal primo, $\forall i$.

Luego, por corolario 2, $V(F_i)$ es irreducible; y $I(V(F_i)) = Rad(\langle F_i \rangle) = \langle F_i \rangle$. De aquí:

$$I(V(F)) = I\left(\bigcup_{i=1}^{r} V(F_i)\right) = \bigcap_{i=1}^{r} I(V(F_i)) = \bigcap_{i=1}^{r} \langle F_i \rangle \supset \langle F_1 . F_2 . \ldots . F_r \rangle;$$

y si $G \in \bigcap_{i=1}^{r} \langle F_i \rangle$, entonces: $G = H_i F_i$, $\forall i = 1, 2, \ldots, r$, con $H_i \in K[x_1, x_2, \ldots, x_n]$; o sea F_i divide a G, $\forall i$; de donde: $F_1 . F_2 . \ldots . F_r$ divide a G, por lo que $G = H(F_1 . F_2 . \ldots . F_r)$, con $H \in K[x_1, x_2, \ldots, x_r]$; es decir, $G \in \langle F_1, F_2 . \ldots . F_r \rangle$.

De aquí: $I(V(F)) = \langle F_1 . F_2 . \ldots . F_r \rangle$

Finalmente, para $F \in K[x_1, x_2, \ldots, x_n]$, irreducible, se tiene que $\langle F \rangle$ es ideal primo; o sea $V(F)$ es irreducible. También, para $V(F)$ irreducible, se tiene que $I(V(F)) = Rad(\langle F \rangle) = \langle F \rangle$ es ideal primo. ♦

Bibliografía

[1]: *W. Fulton:* Curvas Algebraicas.– Editorial Reverté S.A. España. 1971.

[2]: *M. F. Atiyah & I. G. Macdonald.*– Introducción to Commutative Algebra.– Addison-Wesley Pub. Co. Londres. 1969.

[3]: *P. Samuel.*– Teoría Algebraica de Números.– Ediciones Omega. Barcelona. 1972.

[4]: *J. K. Golhaber & G. Ehrlich.*– Algebra.– The MacMillan Co. Maryland. 1970.