Revista INTEGRACION
Departamento de Matemáticas UIS
Vol. 10, No. 2, julio-diciembre 1992

Topología del Espectro en Sistemas Lineales

Arnold Oostra V.*

En esta nota se presenta la prueba de un teorema de Algebra Conmutativa tomada de [1], y en la cual interviene de manera decisiva la topología del espectro primo; la mayor parte del escrito está dedicada a la misma topología del espectro y a describir el contexto en el cual el resultado en cuestión tiene alguna importancia.

Dicho contexto es la teoría de los sistemas lineales sobre anillos conmutativos, actual tema de estudio del Seminario de Algebra de la Universidad Nacional. El resultado mencionado se discutió en el mismo Seminario, y el presente escrito se elaboró para una exposición presentada por el autor en el Encuentro de Topología Nº 6, realizado en la Universidad Javeriana.

R siempre denota un anillo conmutativo con unidad 1.

1. La topología del espectro primo

Un ideal de R es un subgrupo aditivo I tal que si $a \in I$ o $b \in I$, entonces el producto ab pertenece a I. Un ideal primo es un ideal para el cual también es válida la implicación

* Universidad Nacional de Colombia, Bogotá.

recíproca:

$$ab \in I \text{ si y sólo si } a \in I \text{ o } b \in I;$$

además se exige que el ideal primo sea distinto del anillo completo R. Por ejemplo todo ideal maximal respecto a la contenencia (y se entiende, distinto de R) es primo. La colección de ideales primos de R se nota X y recibe el nombre de <u>espectro primo</u> de R.

La <u>dimensión de Krull</u> de R es la longitud máxima posible de cadenas de ideales primos distintos ordenados por inclusión. Así dim R = n si existe una cadena

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \ldots \subsetneq P_n$$

de n + 1 ideales primos de R y no existen cadenas más largas en el conjunto ordenado $(X,\subseteq)$. Como todo ideal distinto de R está contenido en algún ideal maximal, se tiene dim R = 0 si y sólo si todo ideal primo de R es maximal.

Para cada $a \in R$, sea $X_a = \{ P \in X \mid a \notin P \}$ la colección de ideales primos que no contienen a a.

Un elemento de R pertenece a algún ideal primo si y sólo si pertenece a algún maximal, si y sólo si no es invertible; es decir, $X_a = X$ si y sólo si $a \in R^*$ (= elementos invertibles de R), en particular $X_1 = X$. Si $P \in X$, $ab \notin P$ si y sólo si $a \notin P$ y $b \notin P$, de manera que $X_{ab} = X_a \cap X_b$. Además $X_a = \phi$ si y sólo si a pertenece a todos los ideales primos de R, si y sólo si $a \in \eta$ = nilradical de $R = \cap X$, si y sólo si existe $n \in \mathbf{N}$ tal que $a^n = 0$. Esquemáticamente:

<u>Afirmación</u>. i) $X_a = X$ si y sólo si $a \in R^*$; $X_1 = X$.

ii) $X_a \cap X_b = X_{ab}$.

iii) $X_a = \phi$ si y sólo si $a^n = 0$ para algún $n \in \mathbf{N}$.

Ahora (i) y (ii) muestran que la colección

$$\{ X_a \mid a \in R \}$$

es la base de una topología sobre X. La topología generada por esta base recibe el nombre de <u>topología del espectro primo</u> de R, y el espacio resultante se nota $\mathrm{Spec}(R)$.

Esta topología se puede describir también en términos de cerrados: $B \subseteq X$ es cerrado si y sólo si $B^c = \bigcup_{a \in A} X_a$ para algún subconjunto A de R, si y sólo si

$$B = \bigcap_{a \in A} X_a{}^c = \bigcap_{a \in A} \{ P \in X \mid a \in P \} =$$
$$= \{ P \in X \mid A \subseteq P \},$$

de manera que un cerrado de $\mathrm{Spec}(R)$ es el conjunto de ideales primos que contienen un cierto subconjunto de R (del cual no se exige nada: puede o no ser ideal, incluso puede ser vacío).

La imagen directa de un ideal primo por un homomorfismo de anillos (que respeta la unidad) no necesariamente es un ideal primo, pero la imagen recíproca sí. Además:

<u>Afirmación</u>. Sea $f: R \longrightarrow S$ un homomorfismo de anillos conmutativos.
Para cada $a \in R$,

$$(f^{!})^{-1}(X_a) = X_{f(a)}$$

(siendo $f^{!}: \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(R)$ la imagen recíproca por f).

<u>Prueba</u>

Sea $Q \in \mathrm{Spec}(S)$. $Q \in (f^{!})^{-1}(X_a)$ si y sólo si $f^{!}Q \in X_a$ si y sólo si $a \in f^{!}Q$ si y sólo si $f(a) \in Q$ si y sólo si $Q \in X_{f(a)}$. ∎

Así que $f^{!}$ es continua, y $\mathrm{Spec}: \mathrm{Ani} \longrightarrow \mathrm{Top}$ definido como $\mathrm{Spec}(f) = f^{!}$ (y de la manera obvia en los objetos) es un functor contravariante. Cabe anotar que no conmuta con los functores olvido $\mathrm{Ani} \longrightarrow \mathrm{Conj}$ y $\mathrm{Top} \longrightarrow \mathrm{Conj}$, pues en general X y R son conjuntos distintos.

Se puede probar que para cada $a \in R$, X_a es compacto en $\mathrm{Spec}(R)$ [2]. En particular entonces $\mathrm{Spec}(R) = X_1$ es siempre un espacio compacto.

Sean P, Q ideales primos distintos; sin pérdida de generalidad sea $a \varepsilon R$ tal que $a \varepsilon P$ y $a \notin Q$, entonces $Q \varepsilon X_a$ en tanto que $P \notin X_a$. Es decir, Spec(R) siempre es un espacio T_0.

Ahora $Q \varepsilon \overline{\{P\}}$ si y sólo si P pertenece a cada abierto básico al cual pertenezca Q, si y sólo si para cada $a \varepsilon R$, $Q \varepsilon X_a$ implica $P \varepsilon X_a$, si y sólo si $a \notin Q$ implica $a \notin P$, si y sólo si $P \subseteq Q$, es decir,

$$\overline{\{P\}} = \{ Q \varepsilon X \mid P \subseteq Q \}.$$

Luego: $\overline{\{P\}} = \{P\}$ si y sólo si P es maximal; en general, todo $\{P\}$ es cerrado en Spec(R) si y sólo si todo primo es maximal, es decir:

Afirmación. Spec(R) es T_1 si y solamente si $\dim R = 0$.

Supóngase ahora que Spec(R) es Hausdorff; entonces cada abierto básico X_a es cerrado pues es compacto. Recíprocamente supóngase que cada abierto básico es cerrado y sean $P, Q \varepsilon X$ distintos; sin pérdida de generalidad sea $a \varepsilon P$ tal que $a \notin Q$; entonces $Q \varepsilon X_a$, pero $P \notin X_a$ y X_a es cerrado, luego existe un abierto básico X_b con $P \varepsilon X_b$ y $X_a \cap X_b = \phi$, vale decir, Spec(R) es Hausdorff.

Se puede demostrar que si Spec(R) es T_1 entonces también es Hausdorff [2]. Resultaría entonces:

Afirmación. Son equivalentes para R:

i) $\dim R = 0$ (es decir, todo ideal primo es maximal).

ii) Spec(R) es T_1.

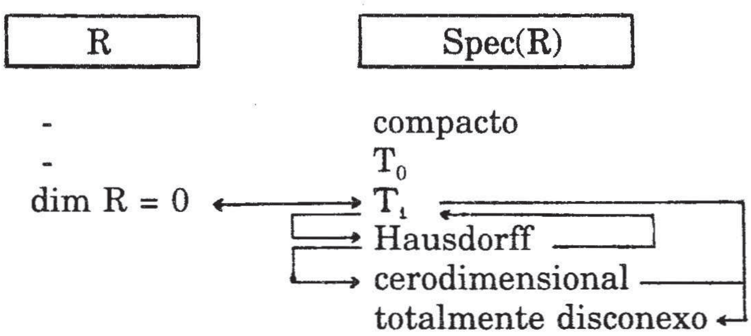
iii) Spec(R) es Hausdorff.

iv) Para cada $a \varepsilon R$, X_a es cerrado en Spec(R).

Supóngase de nuevo que Spec(R) es T_1 y sean $P, Q \varepsilon X$ distintos; $P \notin \{Q\} = \overline{\{Q\}}$, luego existe un abierto X_a tal que $P \varepsilon X_a$ pero $X_a \cap \{Q\} = \phi$, es decir, $P \varepsilon X_a$ y $Q \notin X_a$ con X_a cerrado - abierto en Spec(R), y de esta manera P no pertenece a la componente conexa de Q. Así que las componentes conexas son unitarias y Spec(R) es totalmente disconexo; esta prueba tiene validez general:

<u>Afirmación</u>. Todo espacio T_1 y cerodimensional (= cada punto posee una base de vecindades cerrado - abiertas) es totalmente disconexo.

En resumen:



Así pues, si dim R = 0 entonces Spec(R) es un espacio de Stone (= Hausdorff, compacto y totalmente disconexo); cabe anotar que ese es el ambiente del espacio de Cantor, que es el único espacio de Stone perfecto y 2 - contable [3].

2. Sistemas lineales

Un <u>sistema lineal</u> de dimensión n sobre R consta de las transformaciones lineales (= matrices) $G: R^m \longrightarrow R^n$ y $F: R^n \rightarrow R^n$ (a veces se añade una salida $H: R^n \longrightarrow R^p$, pero por lo general es irrelevante):

$$\begin{tikzcd} R^m \arrow[r, "G"'] & R^n \arrow[d, "F"] \\ & R^n \end{tikzcd}$$

Los sistemas lineales aparecen en las ecuaciones diferenciales al buscar soluciones al sistema

$$dx/dt = F\,x(t) + G\,u(t).$$

Un sistema lineal (F, G) es <u>accesible</u> si es sobreyectivo en el siguiente sentido: todo vector (columna) de R^n se puede obtener a partir de algún vector de R^m combinando adecuadamente sus imágenes por $G, FG, F^2G, F^3G, \ldots$ Basta considerar n iteraciones, luego (F, G) es accesible si las columnas de $[G, FG, F^2G, \ldots, F^{n-1}G]$ generan a R^n.

Si $G = g$ es un vector (es decir, si $m = 1$), el sistema (F, g) es accesible si $[g, Fg, F^2g, \ldots, F^{n-1}g]$ es invertible (pues resulta cuadrada); en particular,existe un vector (fila) u tal que $ug = 1$, luego las entradas de g generan a R y g es unimodular. Si el sistema (F, g) es accesible se dice que g es un <u>vector cíclico</u> para F.

Ahora bien, considérese de nuevo la ecuación diferencial $dx/dt = F\,x(t)$ ($G = 0$); si $r_1, r_2, \ldots, r_n$ son valores propios distintos de F con vectores propios $v_1, v_2, \ldots, v_n$ respectivamente, entonces la solución general del sistema es

$$x(t) = \sum_{i=1}^{n} C_i e^{r_i t} v_i$$

($C_i \in \mathbf{C}$ arbitrarios),y el comportamiento de x cuando t tiende a infinito depende de $r_1, r_2, \ldots, r_n$: si todos tienen parte real negativa la solución es estable,pero en caso contrario no.

Este ejemplo muestra cómo se llega al problema de la asignación de valores propios o polos a un sistema lineal: se trata de alterar ligeramente la transición F de tal forma que el nuevo sistema tenga ciertos polos predeterminados. Y la única manera de alterar el sistema es regresando al espacio de entrada R^m.

Así,un sistema (F, G) <u>asigna polos</u> si dados r_1, $r_2, \ldots, r_n \in R$ existe una transformación $K: R^n \longrightarrow R^m$ tal que el polinomio característico de $F - GK$ es precisamente

$$(x - r_1)(x - r_2) \ldots (x - r_n):$$

$$\begin{tikzcd} R^m \arrow[r, shift left, "G"'] & R^n \arrow[l, shift left, "K"'] \arrow[d, "F - GK"] \\ & R^n \end{tikzcd}$$

Todo sistema que asigne polos es accesible [4]; por eso el estudio se limita a los sistemas accesibles.

Una condición ligeramente más fuerte es la siguiente: un sistema (F, G) <u>asigna coeficientes</u> si dado cualquier polinomio mónico $p(x) \in R[x]$, existe $K: R^n \longrightarrow R^m$ tal que el polinomio característico de $F - GK$ es precisamente $p(x)$.

Un sistema accesible donde $G = g$ es un vector (o sea, $m = 1$) siempre asigna coeficientes [4]. Con este resultado, bajo ciertas condiciones se puede pasar a sistemas con $m > 1$: pues supóngase que para el sistema (F, G) existe un vector u de R^m tal que (F, Gu) es accesible; dado $p(x) \in R[x]$ mónico, existe $K: R^n \longrightarrow R$ tal que el polinomio característico de $F - GuK$ es $p(x)$, pero entonces (F, G) también asigna coeficientes. Claramente el resultado no se altera si inicialmente se reemplaza F por $F - GL$ (pues

F - GL - GuK = F - G(L - uK)), y así se llega a la siguiente definición.

Un sistema (F, G) se retroalimenta a un vector cíclico si existen $L: R^n \longrightarrow R^m$ y $u \in R^m$ tales que (F - GL, Gu) es accesible (es decir, Gu es vector cíclico para F - GL, de ahí el nombre).

Según lo dicho antes, si un sistema (F, G) se retroalimenta a un vector cíclico entonces asigna coeficientes y por lo tanto, polos. Además Gu es unimodular, es decir, G tiene un vector unimodular en su imagen.

3. Anillos con propiedades especiales

Se dice que el anillo R:

tiene la propiedad PA si todo sistema accesible sobre R asigna polos;

tiene la propiedad CA si todo sistema accesible sobre R asigna coeficientes;

tiene la propiedad FC si todo sistema accesible sobre R se retroalimenta a un vector cíclico;

tiene la propiedad GCU si toda matriz G sobre R para la cual exista alguna matriz F tal que (F, G) es un sistema accesible, posea un vector unimodular en su imagen (es decir, existe un vector u tal que Gu es unimodular).

De acuerdo con la discusión del inciso anterior, se tienen las siguientes implicaciones (FC $\longrightarrow$ CA significa: si R tiene la propiedad FC entonces tiene la propiedad CA):

$$\begin{tikzcd} \boxed{\text{GCU}} & \boxed{\text{FC}} \arrow[l] \arrow[d] \\ \boxed{\text{PA}} & \boxed{\text{CA}} \arrow[l] \end{tikzcd}$$

Se puede demostrar que la propiedad GCU implica la PA, pero eso no es relevante cuando se indaga acerca de las condiciones bajo las cuales la condición GCU implica la FC.

Hay un caso en el cual se tiene esta implicación, y es cuando el anillo R satisface la siguiente condición: dados a, b ε R tales que aR + bR = R (aquí aR + bR es el ideal generado por { a, b }), entonces se puede encontrar un elemento c ε R tal que a + bc ε R^* (a + bc es invertible), o lo que es lo mismo, existen x ε R^*, y ε R tales que ax + by = 1 (o sea, 1 ε aR^* + bR). Esto se expresa diciendo que R <u>tiene el uno en el rango estable</u>.

<u>Afirmación</u> [5] Sea R un anillo que tiene el uno en el rango estable.

R tiene la propiedad GCU si y sólo si tiene la propiedad FC.

4. <u>Anillos locales y locales - globales</u>

Un ejemplo de un anillo que tiene el uno en el rango estable es aquel que tiene un solo ideal maximal M. Pues en este caso, un elemento es invertible si y sólo si no pertenece a M (R^* = R - M); si aR + bR = R entonces a y b no pueden pertenecer simultáneamente al ideal M por ser éste distinto de R: si a $\notin$ M entonces a + b0 ε R^*, y si b $\notin$ M entonces a + $b(b^{-1}(1 - a))$ ε R^*.

Un anillo con un solo ideal maximal se denomina <u>local</u>; se acaba de mostrar que todo anillo local tiene el uno en el rango estable, y también se puede probar que un anillo local tiene la propiedad GCU, de modo que tiene la propiedad FC (de hecho, en [4] se prueba directamente que todo anillo local tiene la propiedad FC).

El ejemplo trivial de anillo local es un campo, cuyo único ideal maximal es $\{ 0 \}$. Pero todo anillo conmutativo "contiene" anillos locales.

En efecto, para cualquier ideal primo $P \varepsilon X$ sea

$$R_P = \{ a/s \mid a \varepsilon R, s \varepsilon R - P \}$$

con las operaciones definidas como entre los números racionales, y la regla de simplificación $at/st = a/s$ (para cada $t \varepsilon R - P$). Fácilmente se verifica que

$$P_P = \{ x/s \mid x \varepsilon P, s \varepsilon R - P \}$$

es un ideal primo de R_P; ahora si $a/r \varepsilon R_P - P_P$ entonces $a \varepsilon P$, es decir, $a \varepsilon R - P$ de donde $r/a \varepsilon R_P$. Pero claramente r/a es el inverso de a/r, así que $R_P - P_P \subseteq R_P^*$, $R_P - R_P^* \subseteq P_P$ y en consecuencia P_P contiene todos los ideales propios de R_P, en particular es el único ideal maximal de R_P.

Así pues, en cada una de las "localizaciones" R_P, el anillo R tiene las propiedades requeridas para la propiedad FC, y para que R tuviera la misma propiedad, sería suficiente que esas dos propiedades (GCU y uno en el rango estable) se pudieran levantar al anillo total. Cabe anotar que es esta una técnica muy utilizada en el Algebra Conmutativa.

Ahora bien, ambas propiedades se pueden expresar en términos de polinomios: pues existe $c \varepsilon R$ tal que $a + bc \varepsilon R^*$ si y sólo si la evaluación del polinomio $f(x) = a + bx$ toma un valor invertible; y G tiene un vector unimodular en su imagen si y sólo si la evaluación del polinomio

$$g(x_1, ..., x_n, y_1, ..., y_m) = [x_1, ..., x_n]\, G \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}$$

toma un valor invertible.

Que la evaluación de un polinomio tome un valor invertible se expresa diciendo que admite unidades:
$f(x_1, ..., x_k) \varepsilon R[x_1, ..., x_k]$ <u>admite unidades</u> si existen $u_1, ..., u_k \varepsilon R$ tales que $f(u_1, ..., u_k) \varepsilon R^*$.

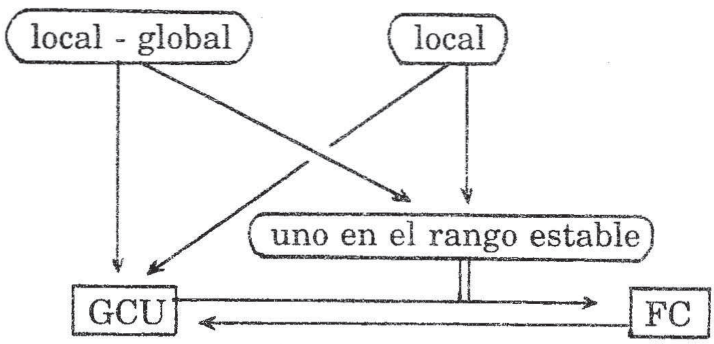
Y así para levantar las dos propiedades de los R_P a R basta que se pueda levantar la admisión de unidades. Por ejemplo, si $aR + bR = R$, ciertamente $(a/1)R_P + (b/1)R_P = R_P$ de donde $(a/1) + (b/1)x \varepsilon R_P[x]$ admite unidades en R_P. Si esto último implica que $a + bx \varepsilon R[x]$ también admite unidades, entonces R tiene el uno en el rango estable.

Exigiendo a la fuerza lo que se desea, nace el siguiente concepto:

<u>Definición</u> Un anillo R es <u>local - global</u> si todo polinomio de $R[x_1, \ldots, x_k]$ que admite unidades localmente, admite unidades.

Es decir, dado $f(x) = \Sigma\, a_i x^i \varepsilon R[x]$, si para cada ideal primo $P \varepsilon X$ el polinomio $\Sigma\, (a_i/1)x^i \varepsilon R_P[x]$ admite unidades en R_P, entonces $f(x)$ admite unidades en R (y análogamente para polinomios con varias indeterminadas).

De acuerdo con lo que se ha dicho antes, todo anillo local - global tiene la propiedad GCU y el uno en el rango estable, y en consecuencia tiene la propiedad FC (que a su vez entraña la propiedad PA):



Ahora se llega a la afirmación alrededor de la cual gira esta discusión:

5. Todo anillo de dimensión cero es local - global

Informalmente, el razonamiento seguido en la prueba es el siguiente:

Para cierto polinomio $f(x)$ que admita unidades localmente, se busca un elemento $c \varepsilon R$ tal que $f(c) \varepsilon R - P$ para cada ideal primo P, pues en tal caso $f(c) \varepsilon R^*$ y $f(x)$ admite unidades.

Pues bien, obsérvese que si $f(a/s) \varepsilon R_P^* = R_P - P_P$, al agrupar los "denominadores" se encuentra un $b \varepsilon R$ tal que $f(b) \varepsilon R - P$. Luego del hecho de que $f(x)$ admita unidades localmente se concluye que para cada $P \varepsilon X$ existe un elemento b_P tal que $f(b_P) \varepsilon R - P$; y todo el problema consiste en intercambiar un cuantificador universal con un existencial.

Claramente basta encontrar un elemento c congruente con b_P módulo P (es decir, $c - b_P \varepsilon P$) para cada P. Esto sugiere utilizar el teorema chino de residuos, pero ese resultado sólo es válido para sistemas

$$x \equiv a_1 \ (I_1)$$

$$x \equiv a_k \ (I_k)$$

que sean finitos y donde además los I_i son ideales "primos entre sí" en el sentido de que $I_i + I_j = R$ si $i \neq j$.

Para reducir el caso a las hipótesis del teorema chino, sería suficiente encontrar una partición finita del espectro primo X tal que las intersecciones de las clases sean ideales primos entre sí, pues entonces al escoger el b_P correspondiente a algún primo P de la clase, si c es congruente con cada b_P módulo la intersección, lo es módulo cada primo del paquete y así c es el elemento buscado.

La búsqueda de la partición conduce de manera natural a considerar la topología del espectro. Precisamente la compacidad de Spec(R) permite encontrar un cubrimiento finito, y si

Spec(R) es cerodimensional este cubrimiento se puede refinar hasta una partición constituida por conjuntos cerrado - abiertos, con lo cual todo queda resuelto.

A continuación se escribe la prueba con un poco más de rigor; se han separado con guiones los razonamientos puramente algebraicos de los topológicos.

<u>Teorema</u>. Si $\dim R = 0$ entonces R es local - global.

<u>Demostración</u>

Sea R un anillo de dimensión cero y supóngase que $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ admite unidades localmente.

Sea P un ideal primo de R; entonces existen $a_1/s_1, \ldots, a_n/s_n \in R_P$ tales que $f(a_1/s_1, \ldots, a_n/s_n) \in R_P^*$, es decir, $f(a_1/s_1, \ldots, a_n/s_n) = a/s$ para ciertos
$a, s \in R - P$. Fácilmente se verifica que entonces existen $b_1, \ldots, b_n \in R$ tales que $f(b_1, \ldots, b_n) \in R - P$, es decir, $f(b_P) \notin P$ donde b_P denota el "vector" $(b_1, \ldots, b_n)$.

- - - - -

Es decir, $P \in X_{f(b_P)}$; en consecuencia
$X \subseteq \bigcup_{P \in X} X_{f(b_P)}$ y como Spec(R) es compacto, existen $b^{(1)}, \ldots, b^{(m)}$ tales que $X \subseteq \bigcup_{k=1}^{m} X_{f(b^{(k)})}$. Haciendo

$$A_1 = X_{f(b^{(1)})},$$
$$A_2 = X_{f(b^{(2)})} - A_1,$$

y en general

$$A_k = X_{f(b^{(k)})} - A_{k-1}$$

$(1 < k \leq m)$, se tiene

$$X \subseteq \bigcup_{k=1}^{m} A_k \ ,$$

donde los A_k son disyuntos dos a dos. Más aún: como
$\dim R = 0$, Spec(R) es un espacio de Hausdorff y cada compacto $X_{f(b^{(k)})}$ es a la vez cerrado y abierto; por construcción, los A_k son

también cerrados de Spec(R).

Sea ahora

$I_k = \cap A_k = \{ a \in R \mid a \in P \text{ para cada } P \in A_k \}$

$(1 \leq k \leq m)$; nótese que si $A_k = \phi$, sencillamente $I_k = R$. En estas condiciones, para cada ideal primo $Q \in X$ se tiene: $Q \supseteq I_k$ si y sólo si $Q \in A_k$. En efecto:

$\leftarrow$ Si $Q \in A_k$ claramente $\cap A_k \subseteq Q$.

$\rightarrow$ Si $Q \notin A_k$, como A_k es cerrado existe un abierto X_q tal que $Q \in X_q$ y $X_q \cap A_k = \phi$.

Pero $Q \in X_q$ si y sólo si $q \notin Q$; y $X_q \cap A_k = \phi$ si y sólo si $A_k \subseteq X_q^c$ si y sólo si $J \in A_k$ implica $q \in J$ si y sólo si $q \in I_k$.

Así $Q \in X_q$ y $X_q \cap A_k = \phi$ significa que $q \in I_k - Q$ y por lo tanto $Q \not\supseteq I_k$.

- - - - -

Cada A_k es una colección de ideales de R luego $I_k = \cap A_k$ es un ideal. Además si $i = j$ entonces $I_i + I_j = R$; pues en caso contrario, existiría un ideal maximal M tal que $I_i + I_j \subseteq M$: en particular se tendría $I_i \subseteq M$, luego $M \in A_i$ (pues todo maximal es también ideal primo) y del mismo modo $I_j \subseteq M$ implicaría $M \in A_j$, resultando $M \in A_i \cap A_j$ lo cual es absurdo.

Por el teorema chino de residuos, teniendo ideales $I_1, ..., I_m$ que satisfacen $I_i + I_j = R$ para $i = j$, dados $b^{(1)}, ..., b^{(m)}$ existe $c = (c_1, ..., c_n)$ tal que

$$b^{(k)} \equiv c \ (I_k),$$

$1 \leq k \leq m$ (aquí realmente se utiliza el teorema n veces, una para cada componente).

Y entonces $f(c) \in R^*$ al no pertenecer a ningún ideal primo. Pues supóngase por el contrario que $f(c) \varepsilon N$ para algún primo $N \varepsilon X$; N pertenece a cierta familia A_t de manera que $I_t \subseteq N$.

De $b^{(t)} \equiv c \ (I_t)$ se sigue $f(b^{(t)}) \equiv f(c) \ (I_t)$, es decir, $f(b^{(t)}) - f(c) \varepsilon I_t$ y así $f(b^{(t)}) - f(c) \varepsilon N$. Puesto que $f(c) \varepsilon N$, también $f(b^{(t)}) \varepsilon N$.

- - - - -

Pero esto contradice el hecho de que $N \varepsilon A_t \subseteq X_{f(b^{(t)})}$. ∎

6. Bibliografía

[1] McDonald B. R., Waterhouse W. Projective modules over rings with many units. Proc. Amer. Math. Soc. 83, pp. 455-458, 1981.

[2] Atiyah M. F., MacDonald I. G. Introduction to Commutative Algebra. Reading (Massachusetts), Addison - Wesley Publishing Company, 1969.

[3] Acosta L. Una demostración algebraica de la unicidad del conjunto de Cantor. Tesis de Magister, Bogotá, Universidad Nacional, 1988.

[4] Brewer J., Bunce J., VanVleck F. S. Linear systems over commutative rings. New York, Marcel Dekker, Inc., 1986.

[5] Brewer J., Katz D., Ullery W. Pole assignability in polinomial rings, power series rings, and Prüfer domains, Journal of Algebra, Vol 106, Nº 1, pp.265 -286, 1985.