

Dimensión

2.2. Teoremas de Cohen–Seidenberg

(2.2.1) Definición. Sea $A \neq \{0\}$ un subanillo de B y sea I un ideal de A . Se dice que un elemento $b \in B$ es *entero sobre I* si existe un polinomio mónico $p(x) = x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$ con $a_i \in I$ para $1 \leq i \leq n$ tal que $f(b) = 0$.

Se dice que el anillo B es *entero sobre el subanillo $A \neq \{0\}$* si todo elemento de B es entero sobre A . También se dice que $A \hookrightarrow B$ es una extensión de anillos *íntegra*.

El siguiente resultado generaliza a (1.3.15):

(2.2.2) Proposición. Si $A \neq \{0\}$ es un subanillo de B e I es un ideal de A , entonces para cada elemento $b \in B$, las siguientes afirmaciones son equivalentes:

(2.2.2.1) b es entero sobre I ;

(2.2.2.2) $A[b]$ es un A -módulo finitamente generado y $b \in \text{Rad}(IA[b])$;

(2.2.2.3) hay un subanillo $A[b] \subseteq C \subseteq B$ finitamente generado como A -módulo y $b \in \text{Rad}(IC)$.

Demostración. (1) $\Rightarrow$ (2) Sea

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$$

un polinomio mónico con $a_i \in I$ para $1 \leq i \leq n$ tal que $f(b) = 0$. Entonces

$$b^n = -a_1b^{n-1} - \cdots - a_{n-1}b - a_n,$$

y por lo tanto, para todo $j \in \mathbb{N}$ existen $a'_1, \dots, a'_n \in A$ tales que

$$b^j = a'_1b^{n-1} + \cdots + a'_{n-1}b + a'_n,$$

con lo que $A[b]$ está generado por $\{b^{n-1}, \dots, b, 1\}$ como A -módulo. Además, dado que $a_1, \dots, a_n \in I$, el elemento

$$b^n = -a_1 b^{n-1} - \dots - a_{n-1} b - a_n$$

pertenece a $IA[b]$, luego $b \in \text{Rad}(IA[b])$.

(2) $\Rightarrow$ (3) $C = A[b]$ es un subanillo de B finitamente generado como A -módulo y $b \in \text{Rad}(IC)$ por hipótesis.

(3) $\Rightarrow$ (1) Sea $\{c_1, \dots, c_m\}$ un sistema generador del subanillo $C \supseteq A[b]$ de B como A -módulo. Entonces, dado que existe $n > 0$ tal que $b^n \in IC$, para cada $i \in \{1, \dots, m\}$ existen $a_{i1}, \dots, a_{im} \in I$ tales que

$$b^n c_i = \sum_{j=1}^m a_{ij} c_j.$$

Luego $(c_1, \dots, c_m)$ es solución del sistema de m ecuaciones lineales con m incógnitas $Hx = 0$, donde H es la matriz

$$H = \begin{pmatrix} a_{11} - b^n & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} - b^n & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} - b^n \end{pmatrix}.$$

Teniendo en cuenta que $(\det H)I_m = H^*H$, donde H^* es la matriz adjunta de la transpuesta de H , se tiene que

$$(\det H) \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = (\det H)I_m \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = H^*H \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = 0,$$

de donde $(\det H)c_i = 0$ para $1 \leq i \leq m$.

Como $1 = \sum_{i=1}^m a_i c_i$, con $a_1, \dots, a_m \in A$, se tiene que $\det H = 0$, pero $(-1)^m \det H$ es un polinomio mónico de grado mn en b con coeficientes en I , así que b es entero sobre I . $\square$

(2.2.3) Corolario. Si B es finitamente generado como A -módulo, entonces B es entero sobre A . En este caso, $b \in B$ es entero sobre I si, y sólo si $b \in \text{Rad}(IB)$.

Demostración. Si $b \in B$ es entero sobre I , por la proposición anterior existe un subanillo $C \supseteq A[b]$ de B finitamente generado como A -módulo y $b \in \text{Rad}(IC) \subseteq \text{Rad}(IB)$.

Recíprocamente, dado que el anillo B es finitamente generado como A -módulo y $b \in \text{Rad}(IB)$, por la proposición anterior b es entero sobre I . $\square$

(2.2.4) Corolario. Si

$$b_1, \dots, b_n \in B$$

son enteros sobre I , entonces $A[b_1, \dots, b_n]$ es finitamente generado como A -módulo y

$$b_i \in \text{Rad}(IA[b_1, \dots, b_n])$$

para $1 \leq i \leq n$.

Demostración. Inducción sobre n .

Para $n = 1$ es cierto por (2.2.2).

Supongamos que es cierto para n elementos enteros sobre I , y sean $b_1, \dots, b_{n+1} \in B$ enteros sobre I . Entonces $A[b_1, \dots, b_n]$ es finitamente generado como A -módulo y

$$b_i \in \text{Rad}(IA[b_1, \dots, b_n]) \subseteq \text{Rad}(IA[b_1, \dots, b_n, b_{n+1}]).$$

Además, b_{n+1} es entero sobre A , y por lo tanto sobre $A[b_1, \dots, b_n]$, así que $A[b_1, \dots, b_n, b_{n+1}]$ es finitamente generado como $A[b_1, \dots, b_n]$ -módulo, y por lo tanto como A -módulo, y

$$b_{n+1} \in \text{Rad}(IA[b_1, \dots, b_n]) \subseteq \text{Rad}(IA[b_1, \dots, b_n, b_{n+1}])).$$

□

(2.2.5) Corolario. Si C es entero sobre el subanillo B y B es entero sobre el subanillo $A \neq \{0\}$, entonces C es entero sobre A .

Demostración. Sea $c \in C$. Como c es entero sobre B , existe un polinomio mónico

$$f(x) = x^n + b_1x^{n-1} + \dots + b_n \in B[x]$$

tal que $f(c) = 0$. Además, dado que $b_1, \dots, b_n$ son enteros sobre A , el anillo $A[b_1, \dots, b_n]$ es finitamente generado como A -módulo.

Luego el anillo $A[b_1, \dots, b_n, c]$ es finitamente generado como A -módulo, y por lo tanto c es entero sobre A . □

(2.2.6) Corolario. Sea $A \neq \{0\}$ un subanillo de B . El conjunto

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

es un subanillo de B .

C es el mayor subanillo de B entero sobre A .

(2.2.7) Definición. Sea $A \neq \{0\}$ un subanillo de B . Al subanillo C del corolario anterior se le denomina *clausura íntegra de A en B* , y se denota por $\overline{A}$.

Se dice que A es *íntegramente cerrado en B* si $\overline{A} = A$.

Un dominio de integridad se dice que es *íntegramente cerrado* si es íntegramente cerrado en su cuerpo de fracciones.

(2.2.8) Ejemplo. Si A es un dominio de factorización única, entonces A es íntegramente cerrado. En particular, $\mathbb{Z}$ y $A[x_1, \dots, x_n]$, con A un dominio de factorización única son íntegramente cerrados.

En efecto, si $z = a/b$, donde a y b no tienen factores comunes, es un elemento del cuerpo de fracciones de A entero sobre A , entonces existe un polinomio mónico

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in A[x]$$

tal que $f(z) = 0$. Multiplicando por b^n se tiene que

$$a^n + a_1a^{n-1}b + \dots + a_{n-1}ab^{n-1} + a_nb^n = 0.$$

Si b no es una unidad, entonces cualquier factor irreducible de b divide a a^n , y por lo tanto a a , lo que contradice que a y b no tienen factores irreducibles en común. Luego b es una unidad y $z \in A$.

Como ejemplos de anillos íntegramente cerrados podemos citar entonces el anillo de los enteros $\mathbb{Z}$ y el anillo de polinomios $A[x_1, \dots, x_n]$, donde A es un dominio de factorización única.

(2.2.9) Lema. Sea B un anillo entero sobre el subanillo A , J un ideal de B e $I = J \cap A$ su contracción en A .

(2.2.9.1) La aplicación $A/I \longrightarrow B/J$; $\bar{a} \longmapsto \bar{a}$ es un monomorfismo de anillos y B/J es entero sobre A/I .

(2.2.9.2) Si en J hay algún elemento que no sea divisor de cero, entonces $I \neq (0)$.

Demostración. (1) El homomorfismo $A \longrightarrow B/J$; $a \longmapsto \bar{a}$ tiene como núcleo a I , luego la factorización por el cociente A/I es un monomorfismo.

Si $\bar{b} \in B/J$, entonces b es entero sobre A y $A[b]$ es finitamente generado como A -módulo. Luego $A/I[\bar{b}]$ es finitamente generado como A/I -módulo y esto implica que $\bar{b}$ es entero sobre A/I .

(2) Si $b \in J$ no es un divisor de cero y

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in A[x]$$

es un polinomio tal que $f(b) = 0$, podemos asumir que $a_n \neq 0$, ya que si lo fuese, podemos dividir $f(x)$ por la potencia de x necesaria, y dado que b no es divisor de cero, b es una raíz del polinomio resultante.

Luego

$$a_n = -b^n - a_1 b^{n-1} - \cdots - a_{n-1} b \in J,$$

y como $a_n \in A$, se tiene que $0 \neq a_n \in J \cap A = I$. $\square$

(2.2.10) Sea A un subanillo de B . El monomorfismo de anillos inclusión $A \hookrightarrow B$ induce una aplicación continua

$${}^a f : \mathbf{Spec} B \longrightarrow \mathbf{Spec} A; \mathfrak{q} \longmapsto \mathfrak{q} \cap A = \mathfrak{p}.$$

Se dice que $\mathfrak{q}$ *está sobre* $\mathfrak{p}$.

(2.2.11) Proposición. Sea B un anillo entero sobre el subanillo A . Entonces:

(2.2.11.1) ${}^a f : \mathbf{Spec} B \longrightarrow \mathbf{Spec} A$ es sobreyectiva;

(2.2.11.2) ${}^a f$ es cerrada;

(2.2.11.3) Si $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \in \mathbf{Spec} B$, y ${}^a f(\mathfrak{q}_1) = {}^a f(\mathfrak{q}_2)$, entonces $\mathfrak{q}_1 = \mathfrak{q}_2$;

(2.2.11.4) $\mathfrak{q} \in \mathbf{Spec} B$ es maximal si, y sólo si ${}^a f(\mathfrak{q})$ es maximal, y por lo tanto ${}^a f(\mathbf{Max} B) = \mathbf{Max} A$ y ${}^a f^{-1}(\mathbf{Max} A) = \mathbf{Max} B$.

Demostración. (1) Sea $\mathfrak{p} \in \mathbf{Spec} A$ y S la parte multiplicativamente cerrada (de B) $S = A \setminus \mathfrak{p}$.

Si $b \in \mathfrak{p}B$, entonces

$$b = p_1 b_1 + \cdots + p_m b_m,$$

y dado que B es entero sobre A , el anillo $A[b_1, \dots, b_m]$ es finitamente generado como A -módulo. Esto implica que $A[b_1, \dots, b_m, b]$ es finitamente generado como A -módulo y como

$$b \in \text{Rad}(\mathfrak{p}A[b_1, \dots, b_m, b]),$$

por (2.2.2) tenemos que b es entero sobre $\mathfrak{p}$, esto es, existe un polinomio

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

con $a_i \in \mathfrak{p}$ para cada i , tal que $f(b) = 0$.

Si $b \in \mathfrak{p}B \cap S$, entonces

$$b^n = -a_1 b^{n-1} - \cdots - a_{n-1} b - a_n \in \mathfrak{p}$$

ya que $a_i \in \mathfrak{p}$ y $b \in A$, lo que contradice que $b \in S$. Luego $\mathfrak{p}B \cap S = \emptyset$.

Por (1.5.11) existe un elemento maximal del conjunto de ideales de B que contienen a $\mathfrak{p}B$ y no intersectan a S , y ese elemento maximal es un ideal primo $\mathfrak{q}$ de B tal que

$${}^a f(\mathfrak{q}) = \mathfrak{q} \cap A = \mathfrak{p}.$$

(2) Sea $V = V(J)$ un cerrado de $\mathbf{Spec} B$. Por (2.2.9), dado que B es entero sobre A , el anillo cociente B/J es entero sobre el subanillo A/I , donde $I = J \cap A$.

Por (1), la aplicación continua

$$\mathbf{Spec} B/J \longrightarrow \mathbf{Spec} A/I; \mathfrak{q} \longmapsto \mathfrak{q} \cap A/I$$

es sobreyectiva, así que todo ideal primo de A que contenga a I es intersección de A con un ideal primo de B que contiene a J , y recíprocamente, si $\mathfrak{q}$ es un ideal primo de B que contiene a J , entonces $\mathfrak{q} \cap A$ es un ideal primo de A que contiene a I . Luego ${}^a f(V(J)) = V(I)$.

(3) Sea $\mathfrak{p} = \mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$. Entonces $B/\mathfrak{q}_1$ es entero sobre $A/\mathfrak{p}$ y $\mathfrak{Q} = \mathfrak{q}_2/\mathfrak{q}_1$ es un ideal primo de $B/\mathfrak{q}_1$. Como $\mathfrak{Q} \cap A/\mathfrak{p} = (0)$, por (2.2.9) los elementos de $\mathfrak{Q}$ son todos divisores de cero, y por ser $B/\mathfrak{q}_1$ un dominio de integridad, se tiene que $\mathfrak{Q} = (0)$ y por tanto que $\mathfrak{q}_1 = \mathfrak{q}_2$.

(4) Sea $\mathfrak{q} \in \mathbf{Spec} B$ y $\mathfrak{p} = \mathfrak{q} \cap A$. Si $A/\mathfrak{p}$ es un cuerpo, entonces, dado que $B/\mathfrak{q}$ es entero sobre $A/\mathfrak{p}$, para cada elemento $b \neq 0$ de $B/\mathfrak{q}$, existe un polinomio mónico

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

tal que $f(b) = 0$. Como $B/\mathfrak{q}$ es un dominio de integridad, podemos suponer que $a_n \neq 0$. Luego

$$b^{-1} = -a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \in B/\mathfrak{q}.$$

Recíprocamente, si $B/\mathfrak{q}$ es un cuerpo, entonces $\mathbf{Spec}(B/\mathfrak{q}) = \{(0)\}$, y como ${}^a f : \mathbf{Spec}(B/\mathfrak{q}) \longrightarrow \mathbf{Spec} A/\mathfrak{p}$ es sobreyectiva, $A/\mathfrak{p}$ también es un cuerpo. $\square$

(2.2.12) Corolario. Si $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ es una cadena de ideales primos distintos del anillo B entero sobre el subanillo A y $\mathfrak{p}_i = A \cap \mathfrak{q}_i$ para cada i , entonces $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ es una cadena de ideales primos distintos en A .

Demostración. El ideal $\mathfrak{p}_i = \mathfrak{q}_i \cap A = {}^a f(\mathfrak{q}_i)$ es primo para cada i . Además, si existe algún i tal que $\mathfrak{p}_{i-1} = \mathfrak{p}_i$, entonces $\mathfrak{q}_{i-1} = \mathfrak{q}_i$ en virtud de (2.2.11.3), así que la cadena $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ es de longitud n . $\square$

(2.2.13) Corolario. (Teorema del ascenso de Cohen–Seidenberg).

Sea B un anillo entero sobre el subanillo A . Si $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ es una cadena de ideales primos distintos en A y $\mathfrak{q}_0$ es un ideal primo de B que está sobre $\mathfrak{p}_0$, entonces existe una cadena $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ de ideales primos distintos en B tal que $\mathfrak{p}_i = A \cap \mathfrak{q}_i$ para cada i .

Demostración. Supongamos que existe una cadena de ideales primos distintos $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_i$ en B tal que $\mathfrak{q}_j \cap A = \mathfrak{p}_j$ para $1 \leq j \leq i$.

Dado que $B/\mathfrak{q}_i$ es entero sobre $A/\mathfrak{p}_i$, la aplicación

$$\mathrm{Spec}(B/\mathfrak{q}_i) \longrightarrow \mathrm{Spec}(A/\mathfrak{p}_i)$$

es sobreyectiva (ver (2.2.11.1)), y puesto que $\mathfrak{p}_{i+1}/\mathfrak{p}_i \neq (0)$ es un ideal primo de $A/\mathfrak{p}_i$, existe un ideal primo $\mathfrak{Q} \neq (0)$ de $B/\mathfrak{q}_i$ tal que

$$\mathfrak{Q} \cap A/\mathfrak{p}_i = \mathfrak{p}_{i+1}/\mathfrak{p}_i.$$

Luego existe un ideal primo $\mathfrak{q}_{i+1}$ de B tal que $\mathfrak{Q} = \mathfrak{q}_{i+1}/\mathfrak{q}_i$, y que por lo tanto contiene estrictamente a $\mathfrak{q}_i$ y además $\mathfrak{p}_{i+1} = \mathfrak{q}_{i+1} \cap A$.

De esta forma se obtiene una cadena de ideales primos distintos

$$\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_i \subset \mathfrak{q}_{i+1}$$

en B . Estirando la cadena de esta forma, comenzando con $i = 0$, se obtiene al cabo de n estiramientos una cadena $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$ de ideales primos distintos en B tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para cada i . $\square$

(2.2.14) Corolario. Si B es un anillo entero sobre el subanillo A , entonces $\dim A = \dim B$, y si $\mathfrak{q} \in \mathrm{Spec} B$ y $\mathfrak{p} = \mathfrak{q} \cap A$,

(2.2.14.1) la altura de $\mathfrak{q}$ es menor o igual que la altura de $\mathfrak{p}$;

(2.2.14.2) la coaltura de $\mathfrak{q}$ coincide con la coaltura de $\mathfrak{p}$.

Demostración. Supongamos que $n \leq \dim A$, esto es, que existe una cadena de primos distintos $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ en A . Dado que B es entero sobre A , la aplicación

$$^a f : \mathrm{Spec} B \longrightarrow \mathrm{Spec} A$$

es sobreyectiva (ver (2.2.11.1)), así que existe un ideal primo $\mathfrak{q}_0$ de B tal que $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$.

Por (2.2.13), existe una cadena de ideales primos distintos $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$ en B (tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para cada i), luego $n \leq \dim B$.

Recíprocamente, si $n \leq \dim B$ (resp., $n \leq h(\mathfrak{q})$), entonces existe una cadena de ideales primos distintos

$$\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$$

en B (resp., contenidos en $\mathfrak{q}$). Sea $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ para cada i . Si $\mathfrak{p}_i = \mathfrak{p}_{i+1}$, para algún i , entonces por (2.2.11.3) tenemos que $\mathfrak{q}_i = \mathfrak{q}_{i+1}$. Luego

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$$

es una cadena de primos distintos en A (resp., contenidos en $\mathfrak{p}$), y esto implica que $n \leq \dim A$ (resp., $n \leq h(\mathfrak{p})$).

Por otra parte, si $n \leq \dim \mathfrak{p}$, entonces existe una cadena de ideales primos distintos

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$$

en A tal que $\mathfrak{p}_0 = \mathfrak{p}$. Por (2.2.13) existe una cadena de ideales primos distintos $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$ en B con $\mathfrak{q}_0 = \mathfrak{q}$, así que $n \leq \dim \mathfrak{q}$.

Recíprocamente, si $n \leq \dim \mathfrak{q}$ entonces existe una cadena

$$\mathfrak{q} = \mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$$

de ideales primos de B distintos. Por (2.2.11.3), los ideales primos de la cadena $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$, donde $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ para cada i , son distintos, y $\mathfrak{p}_0 = \mathfrak{p}$, luego $n \leq \dim \mathfrak{p}$. $\square$

(2.2.15) Lema. *Si A es un anillo noetheriano, entonces el conjunto de divisores primos minimales de cualquier ideal I de A es finito.*

Demostración. Dado que A es noetheriano, cualquier cadena decreciente de cerrados de $\mathbf{Spec} A$ es estacionaria. En efecto, si $V_1 \supseteq V_2 \supseteq \cdots$ son cerrados, entonces $I(V_1) \subseteq I(V_2) \subseteq \cdots$ son ideales de A , y existe n tal que $I(V_j) = I(V_n)$ para todo $j \geq n$, luego

$$V_j = V(I(V_j)) = V(I(V_n)) = V_n$$

para todo $j \geq n$.

Un argumento similar al utilizado para descomponer un conjunto algebraico afín en irreducibles muestra que todo cerrado $V(I)$ de $\mathbf{Spec} A$ se descompone como unión de un número finito de componentes irreducibles, y estas se corresponden biyectivamente con los divisores primos minimales de I . $\square$

(2.2.16) Observación. El resultado anterior se puede demostrar de una manera más directa, sin hacer referencia a la descomposición de un cerrado en componentes irreducibles.

Sea

$$\mathcal{I} = \{I; I \text{ ideal de } A, I \text{ tiene infinitos divisores primos minimales}\}.$$

Supongamos que $\mathcal{I} \neq \emptyset$. Como A es noetheriano, existe un elemento I maximal de $\mathcal{I}$.

Si I fuese primo, entonces I sería el único divisor primo minimal de I , lo que contradice que $I \in \mathcal{I}$.

Luego I no es primo, esto es, existe dos ideales J y K de A tales que $JK \subseteq I$ pero $J, K \not\subseteq I$. Se puede suponer sin pérdida de generalidad que $I \subseteq J, K$, o si no, se pueden tomar $J + I$ y $K + I$.

Por la maximalidad de I , dado que I está contenido estrictamente en J y en K , se tiene que $J, K \notin \mathcal{I}$. Sean entonces $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ los divisores primos minimales de J y $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ los de K .

Si $\mathfrak{p}$ es un divisor primo minimal de I , entonces o bien $\mathfrak{p} = \mathfrak{p}_i$ para algún i , o bien $\mathfrak{p} = \mathfrak{q}_j$ para algún j , porque

$$\prod_{i=1}^n \mathfrak{p}_i \prod_{j=1}^m \mathfrak{q}_j \subseteq \bigcap_{i=1}^n \mathfrak{p}_i \cap \bigcap_{j=1}^m \mathfrak{q}_j = \text{Rad}J \cap \text{Rad}K \subseteq \text{Rad}JK \subseteq \text{Rad}I \subseteq \mathfrak{p},$$

y por ser primo, o bien $\mathfrak{p}_i \subseteq \mathfrak{p}$ para algún i , o bien $\mathfrak{q}_j \subseteq \mathfrak{p}$ para algún j . Supongamos que $\mathfrak{p}_i \subseteq \mathfrak{p}$. Entonces, dado que $\mathfrak{p}$ es un divisor primo minimal de I e $I \subseteq J \subseteq \mathfrak{p}_i$, se puede concluir que en efecto $\mathfrak{p} = \mathfrak{p}_i$. En el caso de que $\mathfrak{q}_j \subseteq \mathfrak{p}$ para algún j , por un razonamiento similar $\mathfrak{p} = \mathfrak{q}_j$.

Luego todos los divisores primos minimales de I están en

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} \cup \{\mathfrak{q}_j, \dots, \mathfrak{q}_m\},$$

lo que contradice que $I \in \mathcal{I}$.

Por lo tanto $\mathcal{I} = \emptyset$.

(2.2.17) Corolario. *Si el anillo B es noetheriano y entero sobre el subanillo A , entonces la imagen inversa por ${}^a f$ de cualquier $\mathfrak{p} \in \mathbf{Spec}A$ es un conjunto finito no vacío.*

Demostración. Por (2.2.11.1), existe $\mathfrak{q} \in \mathbf{Spec}B$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$. Además, cualquier ideal primo $\mathfrak{q}$ de B tal que ${}^a f(\mathfrak{q}) = \mathfrak{p}$ es un divisor primo minimal del ideal $\mathfrak{p}B$, porque dado que $\mathfrak{p} \subseteq \mathfrak{q}$ y $\mathfrak{q}$ es un ideal de B , tenemos que $\mathfrak{p}B \subseteq \mathfrak{q}$, y por otra parte si $\mathfrak{q}' \subseteq \mathfrak{q}$ es otro divisor primo de $\mathfrak{p}$, entonces

$$\mathfrak{p} \subseteq {}^a f(\mathfrak{q}') \subseteq {}^a f(\mathfrak{q}) = \mathfrak{p},$$

y por (2.2.11.3) $\mathfrak{q}' = \mathfrak{q}$.

Por (2.2.15), el número de divisores primos minimales de $\mathfrak{p}B$ es finito, así que la antimagen de $\mathfrak{p}$ por ${}^a f$ es un conjunto finito. $\square$

(2.2.18) Lema. Si I es un ideal del subanillo A de B y $\overline{A}$ es la clausura íntegra de A en B , entonces $\text{Rad}(I\overline{A})$ es el conjunto de elementos de B que son enteros sobre I .

Demostración. Si $b \in B$ es entero sobre I , entonces $A[b]$ es finitamente generado como A -módulo y $b \in \text{Rad}(IA[b])$. Por lo tanto $b \in \text{Rad}(I\overline{A})$, dado que $A[b] \subseteq \overline{A}$ al ser $b \in \overline{A}$.

Recíprocamente, si

$$b \in \text{Rad}(I\overline{A}),$$

entonces existen $b_1, \dots, b_n \in \overline{A}$ tales que $b \in \text{Rad}(IA[b_1, \dots, b_n])$. En particular, existe $m > 0$ tal que $b^m \in A[b_1, \dots, b_n]$, así que b es entero sobre $A[b_1, \dots, b_n]$ por lo que $A[b_1, \dots, b_n, b]$ es finitamente generado como $A[b_1, \dots, b_n]$ -módulo

Como $b_1, \dots, b_n$ son enteros sobre A , $A[b_1, \dots, b_n]$ es finitamente generado como A -módulo, luego $A[b_1, \dots, b_n, b]$ es finitamente generado como A -módulo. Por (2.2.2), b es entero sobre I . $\square$

(2.2.19) Lema. Sea A un anillo íntegramente cerrado, K su cuerpo de fracciones, L una extensión de cuerpos de K e I un ideal radical de A . Si $c \in L$ es entero sobre I , entonces el polinomio mínimo $m(x)$ de c sobre K es de la forma

$$m(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n, \text{ con } a_i \in I, \forall i \in \{1, \dots, n\}.$$

Demostración. Sea

$$m(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

el polinomio mínimo de c , que es algebraico sobre K porque es entero sobre $I \subseteq A \subseteq K$. Sean $c_1, c_2, \dots, c_n$ las raíces de $m(x)$ en la clausura algebraica $\overline{K}$ de K . Si $f(x) \in A[x]$ es un polinomio mónico con coeficientes en I tal que $f(c) = 0$, dado que para cada $i \in \{1, \dots, n\}$ existe un K -automorfismo α_i de $\overline{K}$ tal que $\alpha_i(c) = c_i$, tenemos que

$$0 = \alpha_i(f(c)) = f(\alpha_i(c)) = f(c_i),$$

así que c_i es también entero sobre I .

Los coeficientes de $m(x)$ son

$$a_i = (-1)^i \sum_{\substack{1 \leq j_1, \dots, j_i \leq n \\ j_k \neq j_{k'}}} c_{j_1} \cdots c_{j_i}$$

para $1 \leq i \leq n$, y son enteros sobre I porque $A[c_1, \dots, c_n]$ es un subanillo de $\overline{K}$ que los contiene y $a_i \in \text{Rad}(IA[c_1, \dots, c_n])$ dado que

$$c_1, \dots, c_n \in \text{Rad}(IA[c_1, \dots, c_n]).$$

Además, los coeficientes a_i pertenecen a K , así que por (2.2.18) a_i es un elemento de $\text{Rad}(I\overline{A})$, donde $\overline{A}$ es la clausura íntegra de A en K , que por hipótesis es $\overline{A} = A$. Luego $a_i \in \text{Rad} I = I$. $\square$

(2.2.20) Teorema. (Teorema del descenso de Cohen–Seidenberg).

Sea B un dominio de integridad entero sobre el subanillo A , de manera que A es íntegramente cerrado (en su cuerpo de fracciones). Si $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$ son ideales primos distintos en A y $\mathfrak{q}_1$ es un ideal primo de B tal que $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$, entonces existe un ideal primo $\mathfrak{q}_0$ de B contenido (estrictamente) en $\mathfrak{q}_1$ tal que $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$.

Demostración. Los conjuntos $S_0 = A \setminus \mathfrak{p}_0$, $S_1 = B \setminus \mathfrak{q}_1$ y

$$S = S_0 S_1 = \{rs; r \in S_0, s \in S_1\}$$

son partes multiplicativamente cerradas y $S_0, S_1 \subseteq S$.

Sea $b \in \mathfrak{p}_0 B \cap S$. Entonces b es entero sobre $\mathfrak{p}_0$, y por (2.2.19) los coeficientes a_i del polinomio mínimo

$$m(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

de b en el cuerpo de fracciones K de A pertenecen a $\mathfrak{p}_0$. Como $b \in S$, existen $r \in S_1$ y $s \in S_2$ tales que $b = rs$. El elemento $s = br^{-1} \in L$, donde L es el cuerpo de fracciones de B , es entero sobre A porque pertenece a B . Además, su polinomio mínimo en K es

$$x^n + a_1 r^{-1} x^{n-1} + \dots + a_{n-1} r^{-n+1} x + a_n r^{-n},$$

así que, de nuevo por (2.2.19), $a_i r^{-i} = a'_i \in A$ para cada i . Entonces $a'_i \in \mathfrak{p}_0$, ya que $\mathfrak{p}_0 \ni a_i = a'_i r^i$, y $r \notin \mathfrak{p}_0$. Luego s es entero sobre $\mathfrak{p}_0$, y por (2.2.2)

$$s \in \text{Rad}(\mathfrak{p}_0 B) \subseteq \text{Rad}(\mathfrak{p}_1 B) \subseteq \text{Rad} \mathfrak{q}_1 = \mathfrak{q}_1,$$

lo que contradice que $s \in S_1$.

Luego $\mathfrak{p}_0 B \cap S = \emptyset$, y por (1.5.11) existe un elemento maximal $\mathfrak{q}_0$ de

$$\{J \leq B; \mathfrak{p}_0 B \subseteq J, J \cap S = \emptyset\}$$

y $\mathfrak{q}_0$ es un ideal primo. Como $\mathfrak{p}_0 B \subseteq \mathfrak{q}_0$ y

$$\mathfrak{q}_0 \cap S_0 \subseteq \mathfrak{q}_0 \cap S = \emptyset,$$

se tiene $\mathfrak{p}_0 = \mathfrak{q}_0 \cap A$. Como

$$\mathfrak{q}_0 \cap S_1 \subseteq \mathfrak{q}_0 \cap S = \emptyset,$$

se tiene $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$, y este contenido es estricto porque $\mathfrak{p}_0 \neq \mathfrak{p}_1$. $\square$

(2.2.21) Corolario. *Sea B un dominio de integridad entero sobre el subanillo A , de manera que A es íntegramente cerrado (en su cuerpo de fracciones). Si $\mathfrak{q} \in \text{Spec} B$, entonces $h(\mathfrak{q}) = h(\mathfrak{q} \cap A)$.*

Demostración. Sea $\mathfrak{p} = A \cap \mathfrak{q}$. Como hemos visto en (2.2.14), $h(\mathfrak{q}) \leq h(\mathfrak{p})$. Recíprocamente, si $n \leq h(\mathfrak{p})$, entonces existe una cadena $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ de primos distintos en A tal que $\mathfrak{p}_n = \mathfrak{p}$. Veamos que existe una cadena de ideales primos distintos en B que termina en $\mathfrak{q}$ y tal que cada primo de la cadena es un primo sobre el $\mathfrak{p}_i$ correspondiente.

Sea $i \in \{1, \dots, n\}$ y supongamos que

$$\mathfrak{q}_i \subset \cdots \subset \mathfrak{q}_n = \mathfrak{q}$$

es una cadena de primos distintos de B tales que $\mathfrak{q}_j \cap A = \mathfrak{p}_j$ par $i \leq j \leq n$. Por (2.2.20), existe un ideal primo primo $\mathfrak{q}_{i-1}$ en B estrictamente contenido en $\mathfrak{q}_i$ tal que

$$\mathfrak{q}_{i-1} \cap A = \mathfrak{p}_{i-1}.$$

Repitiendo este razonamiento para cada i , comenzando por $i = n$, tenemos una cadena de ideales primos distintos

$$\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n = \mathfrak{q}$$

en B con lo que $n \leq h(\mathfrak{q})$.

Luego $h(\mathfrak{p}) \leq h(\mathfrak{q})$. $\square$