0.1 Hoja 1

Ejercicio 1 Sea $u \in A$ una unidad y $x \in A$ un elemento nilpotente. Demostrar que $u + x$ es una unidad.

Comenzamos probando que si $x \in \mathfrak{N}_A$, entonces $1 + x \in \mathcal{U}(A)$. Existe $n > 0$ tal que $x^n = 0$, y entonces observamos que $(1 + x)x^{n-1} = x^{n-1}$. Así:

$$\begin{aligned}(1 + x^{n-1})(1 + x) = 1 + 2x^{n-1} &= 1 + 2x^{n-1}(1 + x) \\ = (1 + x^{n-1})(1 + x) &- 2x^{n-1}(1 + x) = 1 \\ = (1 + x^{n-1} &- 2x^{n-1})(1 + x) = 1 \\ &= 1 - x^{n-1})(1 + x) = 1 \quad (1)\end{aligned}$$

Por otra parte, si $u \in \mathcal{U}(A)$, existe $v \in A$ tal que $uv = 1$. Además, por ser $\mathfrak{N}_A$ un ideal, $vx \in \mathfrak{N}_A$ con mismo índice de nilpotencia, y podemos aplicar lo anterior

$$(1 - (vx)^{n-1})(1 + vx) = 1$$

Ahora podemos escribir $1 + vx = v(u + x)$ y por tanto la anterior identidad queda escrita como

$$[v(1 - (vx)^{n-1})](u + x) = 1$$

Ejercicio 2 Sea A, A_1, A_2 anillos y supongamos que $A \cong A_1 \times A_2$.

(i) Sea $\mathfrak{a} \subset A$ un ideal. Demostrar que $\mathfrak{a} \cong \mathfrak{a}' \times \mathfrak{a}''$ para ciertos ideales $\mathfrak{a}' \subset A_1$ y $\mathfrak{a}'' \subset A_2$.

(ii) Sea $\mathfrak{p} \subset A$ un ideal primo. Demostrar que $\mathfrak{p} \cong \mathfrak{p}' \times A_2$ o bien $\mathfrak{p} \cong A_1\mathfrak{p}''$ para ciertos ideales primos $\mathfrak{p}' \subset A_1$ y $\mathfrak{p}'' \subset A_2$.

(i) En general, si $\phi : A \to B$ es un isomorfismo, y $\mathfrak{a} \subset A$ un ideal, entonces $\phi(\mathfrak{a})$ es un ideal de B:

- Para todo $\phi(x), \phi(y) \in \phi(\mathfrak{a})$ tenemos que $\phi(x) + \phi(y) = \phi(\underbrace{x + y}_{\in \mathfrak{a}}) \in \phi(\mathfrak{a})$. - Para todo $\phi(x) \in \phi(\mathfrak{a}), z \in B$ existe $w \in A$ tal que $\phi(w) = z$, y entonces $z\phi(x) = \phi(\underbrace{wx}_{\in \mathfrak{a}}) \in \phi(\mathfrak{a})$.

Y todo ideal del producto $\mathfrak{b} \subset A_1 \times A_2$, es un producto de ideales $\mathfrak{b}_1 \times \mathfrak{b}_2$. Efectivamente, sea

$$\mathfrak{b}_1 = \{x \in A_1 : \exists y \in A_2 // (x, y) \in \mathfrak{b}\}$$

y veamos que es un ideal:

- Para todo $x, x' \in \mathfrak{b}_1$ existen $y, y' \in A_2$ tales que $(x,y), (x',y') \in \mathfrak{b}$ y por ser un ideal tenemos $\mathfrak{b} \ni (x,y) + (x',y') = (x+x', y+y')$ y por tanto $x + x' \in \mathfrak{b}_1$.
- Para todo $x \in \mathfrak{b}_1$ y todo $z \in A_1$ existe $y \in A_2$ tal que $(x,y) \in \mathfrak{b}$, y además $(z,0) \in A_1 \times A_2$, y por ser un ideal se tiene $\mathfrak{b} \ni (x,y)(z,0) = (xz, 0)$ con lo que $xz \in \mathfrak{b}_1$.

Con esto queda probado que todo $\mathfrak{a} \subset A$ es isomorfo a un producto de ideales.

(ii) En general, si $\phi : A \to B$ es un isomorfismo, y $\mathfrak{p} \subset A$ un ideal primo, entonces $\phi(\mathfrak{p})$ es un ideal primo de B:

- Sean $x', y' \in B$ tales que $x' = \phi(x), y' = \phi(y) \in \phi(\mathfrak{p})$, entonces $\phi(\mathfrak{p}) \ni x'y' = \phi(x)\phi(y) = \phi(xy)$ por tanto $xy \in \mathfrak{p}$ y como es un ideal primo, $x \in \mathfrak{p}$ o $y \in \mathfrak{p} \iff x' \in \phi(\mathfrak{p})$ o $y' \in \phi(\mathfrak{p})$.

Si $\mathfrak{p} \subset A_1 \times A_2$ es un ideal primo, entonces sabemos de a) que $\mathfrak{p} = \mathfrak{a}_1 \times \mathfrak{a}_2$ producto de ideales. Veamos que o bien $\mathfrak{p} = \mathfrak{p}_1 \times A_2$ con $\mathfrak{p}_1$ primo, o bien $\mathfrak{p} = A_1 \times \mathfrak{p}_2$ con $\mathfrak{p}_2$ primo. Supongamos $\mathfrak{p}_1 \neq A_1$:

- Para todo $x, y \in A_1$ tales que $xy \in \mathfrak{p}_1$ existe $z \in A_2$ tal que $(xy, z) \in \mathfrak{p}$. Entonces se tiene $\mathfrak{p} \ni (xy, z) = (x,z)(y,1)$ y por lo tanto $(x,z) \in \mathfrak{p}$ o bien $(y,1) \in \mathfrak{p}$ lo que implica que $x \in \mathfrak{p}_1$ o $y \in \mathfrak{p}_1$. Por tanto $\mathfrak{p}_1$ es un ideal primo. - Más aún, dado $x \in \mathfrak{p}_1$, obviamente se cumple $1 \cdot x \in \mathfrak{p}_1$. Siguiendo lo de arriba, $(1,z)(x,1) \in \mathfrak{p}$, y como $\mathfrak{p}_1 \neq A_1$ no puede ser que $(1,z) \in \mathfrak{p}$, luego necesariamente $(x,1) \in \mathfrak{p}$ y por lo tanto $1 \in \mathfrak{p}_2$ y así $\mathfrak{p}_2 = A_2$.

Ejercicio 3 Sea $\mathfrak{a} \subset A$ un ideal. Demostrar que:

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(A) \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p}$$

Utilizando la caracterización que conocemos del nilradical de un anillo aplicado al cociente, y teniendo en cuenta que la biyección del teorema de la correspondencia conserva la primalidad, tenemos que:

$$\begin{aligned} x \in \sqrt{\mathfrak{a}} \iff x + \mathfrak{a} \in \mathfrak{N}_{A/\mathfrak{a}} = \bigcap_{\bar{\mathfrak{p}} \in \operatorname{Spec}(A/\mathfrak{a})} \bar{\mathfrak{p}} \iff \\ \forall \bar{\mathfrak{p}} \in \operatorname{Spec}(A/\mathfrak{a}),\ x + \mathfrak{a} \in \bar{\mathfrak{p}} \iff \\ \forall \mathfrak{p} \in \operatorname{Spec}(A),\ x \in \mathfrak{p} \end{aligned} \quad (2)$$

Ejercicio 4 Sea A un anillo y $f = a_nX^n + \ldots + a_1X + a_0 \in A[X]$. Demostrar que f es una unidad en $A[X]$ si y solo si a_0 es unidad y todos los a_i son nilpotentes.

$\Leftarrow$) Sabemos que $\mathfrak{N}_A$ es un ideal, así que $\sum_{j=1}^{n} a_jX^j \in \mathfrak{N}_A$, y como $a_0 \in \mathcal{U}(A)$, en virtud del ejercicio 1 se tiene que $\sum_{j=1}^{n} a_jX^j + a_0 = f \in \mathcal{U}(A)$.

$\Rightarrow$) Como f es una unidad, existe $g = \sum_{j=1}^{m} b_jX^j \in A[X]$ tal que $fg = 1$. En primer lugar, esto implica que $a_0b_0 = 1$ luego $a_0 \in \mathcal{U}(A)$.

FALTA LA SEGUNDA PARTE

Ejercicio 5 *Sea A un DIP. Si $\mathfrak{a}$ es un ideal propio, demostrar que son equivalentes*

a) $\mathfrak{a}$ es un ideal primo,

b) $\mathfrak{a}$ es un ideal maximal,

c) existe $f \in A$ irreducible tal que $\mathfrak{a} = \langle f \rangle$.

Si $a, b \in A \setminus \{0\}$ no son unidades, y $d, m \in A$ tales que $\langle a \rangle + \langle b \rangle = \langle d \rangle$, $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$, demostrar que $d = \gcd(a, b)$ y $m = \operatorname{lcm}(a, b)$.

a) $\iff$ *b)* La implicación $\Leftarrow$ se tiene siempre. Sea $\mathfrak{a} = aA$ un ideal primo, y supongamos que existe $\mathfrak{b} = bA$ tal que $\mathfrak{a} \subsetneq \mathfrak{b}$. Existe $x \in A$ tal que $bx = a \in \mathfrak{a}$ primo, luego $b \in \mathfrak{a}$ o $x \in \mathfrak{a}$. No puede ser que $b \in \mathfrak{a}$ porque en tal caso existiría un $z \in A$ tal que $az = b$ y entonces para todo $t \in A$ se tendría que $bt = a(zt) \in aA = \mathfrak{a}$ y por tanto $\mathfrak{b} \subseteq \mathfrak{a}$, en contra de nuestra hipótesis. Por tanto $x \in \mathfrak{a}$, y existe $w \in A$ tal que $x = aw$, entonces $a(bw) = a$ y por tanto $1 = bw \in \mathfrak{b}$, con lo que $\mathfrak{b} = A$. Así $\mathfrak{a}$ es maximal.

b) $\iff$ *c)* Sea $\mathfrak{a} = aA$ un ideal, y supongamos que a se puede expresar como $a = uv$ con $u, v \notin \mathcal{U}(A)$. Entonces $\mathfrak{a} \subseteq uA$ y, además, $uA \neq A$ porque u no es unidad. Veamos que $uA \not\subseteq \mathfrak{a}$, o equivalentemente, $u \notin \mathfrak{a}$. Si $u \in \mathfrak{a}$ existe un w tal que $u = aw = u(vw)$ y por tanto $u(1 - vw) = 0$ luego $1 = vw$, ya que $u \neq 0$ pues si no $\mathfrak{a} = 0$ que no es maximal. Esto va en contra de la suposición de que $v \notin \mathcal{U}(A)$. Así que $\mathfrak{a} \subsetneq uA \subsetneq A$ y por tanto no es un ideal maximal.

Supongamos ahora que a es irreducible, y existe $\mathfrak{b} = bA \supset \mathfrak{a}$. Existe $w \in A$ tal que $a = bw$, y como a es irreducible entonces $b \in \mathcal{U}(A)$ o $w \in \mathcal{U}(A)$, en cualquier caso $\mathfrak{b} = A$, y por tanto $\mathfrak{a}$ es maximal.

Ejercicio 6

(i) Sea A un anillo, demostrar que existe una biyección entre las descomposiciones $\Phi : A \to A_1 \times \ldots \times A_n$ via un isomorfismo de anillos y los conjuntos de idempotentes ortogonales de A, ie. $\{e_1, \ldots, e_n\} \subset A$ tales que $\sum_{i=1}^n e_i = 1_A$ y $e_i e_j = \delta_{ij} e_i$.

(ii) Demostrar que dada una descomposición, los A_i se identifican con ideales de A, no con subanillos. ¿Qué descomposición corresponde al conjunto de idempotentes $\{0_A, 1_A\}$.

(i) Veamos este apartado de dos formas: una donde los idempotentes son endomorfismos y otra donde son elementos de A.

1. Si tenemos $A = A_1 \times \cdots \times A_n = \bigoplus_{i=1}^n A_i$, entonces podemos tomar la proyección $A \to A_i$ compuesta con la inclusión $A_i \to A$ que resulta en un endomorfismo de A que denotamos e_i. Este endomorfismo es idempotente. Efectivamente, si tomamos $x = (x_1, \ldots, x_n) \in A = \bigoplus_{i=1}^n A_i$ entonces $e_i \circ e_i(x) = e_i(0, \ldots, 0, x_i, 0, \ldots, 0) = (0, \ldots, 0, x_i, 0, \ldots, 0)$. Son ortogonales porque $e_j(0, \ldots, 0, x_i, 0, \ldots, 0) = (0, \ldots, 0)$. Y también tenemos que suman la identidad porque para cualquier $x \in A$:

$$\begin{multline} e_1(x) + \ldots + e_i(x) + e_j(x) + \ldots + e_n(x) = \\ = (x_1, 0, \ldots, 0) + \cdots + (0, \ldots, x_i, 0, \ldots, 0) + (0, \ldots, 0, x_j, \ldots, 0) + (0, \ldots, 0, x_n) = \\ = (x_1, \ldots, x_i, x_j, \ldots, x_n) = x \quad (3) \end{multline}$$

Por otra parte, si tenemos un subconjunto $\{e_i\}_{i=1}^r$ tal que $\sum_{i=1}^r e_i = 1$ y $e_i e_j = \delta_{ij} e_i$ podemos definir una descomposición de A tomando A_i las imágenes de los e_i.

2. Dado el isomorfismo $\Phi : \bigoplus A_i \to A$, este determina un conjunto de idempotentes según a donde envíe a los elementos siguientes:

$$\begin{aligned} \Phi : A_1 \times \ldots \times A_n &\to A \\ (1, 0, \ldots, 0) &\mapsto e_1 \\ (0, 1, \ldots, 0) &\mapsto e_2 \\ &\vdots \\ (0, 0, \ldots, 1) &\mapsto e_n \end{aligned}$$

Efectivamente, por ser homomorfismo ha de cumplirse que

$$1_A = \Phi(1,1,\ldots,1) = \Phi(1,0,\ldots,0) + \cdots + \Phi(0,0,\ldots,1) = e_1 + e_2 + \ldots e_n \quad (4)$$

$$0_A = \Phi(0,0,\ldots,0) = \Phi((0,\ldots,\overset{i)}{0},\ldots,0)\cdot(0,\ldots,\overset{j)}{0},\ldots,0)) \quad i \neq j \quad (5)$$

$$e_i = \Phi((0,\ldots,\overset{i}{1},\ldots,0)\cdot(0,\ldots,\overset{i}{1},\ldots,0)) = e_i e_i \quad (6)$$

Recíprocamente, dados $\{e_i\}_{i=1}^r$ tomemos los ideales $\mathfrak{a}_i = e_i A$ de A. Estos tienen estructura de anillo conmutativo unitario con las operaciones heredadas y tomando $1_{\mathfrak{a}_i} = e_i$. En efecto, todo el resto de propiedades se cumple automáticamente y comprobamos que esa es la unidad: para todo $x \in \mathfrak{a}_i$ existe $a \in A$ tal que $x = e_i a$ y entonces $xe_i = e_i x = e_i e_i a = e_i a = x$.

Ahora consideramos $\phi_i : A \to \mathfrak{a}_i$ dado por $x \mapsto \phi_i(x) = xe_i$ que es un homomorfismo suprayectivo (esto segundo es obvio porque $\mathfrak{a}_i = e_i A$):

$$\phi_i(x+y) = (x+y)e_i = xe_i + ye_i = \phi_i(x) + \phi_i(y) \quad (7)$$

$$\phi_i(xy) = xye_i = xye_ie_i = (xe_i)(ye_i) = \phi_i(x)\phi_i(y) \quad (8)$$

Finalmente podemos coger $\Phi : A \to \bigoplus \mathfrak{a}_i$ como $\Phi = \bigoplus_i \phi_i$ que es homomorfismo suprayectivo por serlo cada una de las coordendas, y además es inyectivo porque si $x \in A$ es tal que $0 = \Phi(x) = (xe_1,\ldots,xe_n)$ entonces $0 = \sum_i xe_i = x\sum_i e_i = x$. Por lo tanto Φ es el isomorfismo que buscabamos.

(ii) Claramente $A_i \cong 0 \times \ldots \times A_i \times \ldots \times 0$ y este es un ideal de $A_1 \times \ldots \times A_n \cong A$ lo que demuestra la identificación. Efectivamente dados $a, b \in A_i$, y $(x_1,\ldots,x_n) \in A_1 \times \ldots \times A_n$ tenemos

$$(0,\ldots,\overset{i)}{a},\ldots,0) - (0,\ldots,\overset{i)}{b},\ldots,0) = (0,\ldots,\overset{i)}{a-b},\ldots,0) \in 0\times\ldots\times A_i\times\ldots\times 0 \quad (9)$$

$$(x_1,\ldots,x_n)\cdot(0,\ldots,\overset{i)}{a},\ldots,0) = (0,\ldots,\overset{i)}{x_i a},\ldots,0) \in 0\times\ldots\times A_i\times\ldots\times 0 \quad (10)$$

No es un subanillo porque carece del elemento unidad de $A_1 \times \ldots \times A_n$ que es la tupla con todo unos.

Finalmente, si tomamos el conjunto de idempotentes $0_A, 1_A$ obtenemos la descomposición trivial $A = \{0_A\} \times A$. Si seguimos la forma 2. de proceder, el isomorfismo $\Phi : A_1 \times A_2 \to A$ debería asignar $(1,0) \mapsto 0_A$ y $(0,1) \mapsto 1_A$. Está bien definido porque se cumple que $1_A = 0_A + 1_A = \Phi(1,0) + \Phi(0,1) = \Phi(1,1)$ como debe ser.

Ejercicio 7 *Encontrar un sistema de idempotentes ortogonales no trivial y una descomposición asociada para*

(i) $\mathbb{Z}_{nm}$ *con* $\gcd(n,m)=1$.

(ii) $\mathbb{Q}[X]/\langle x^2(x-1)\rangle$.

(iii) $K[X]/\langle fg\rangle$ *con* $\gcd(f,g)=1$.

(i) Sabemos que si m,n son coprimos entonces $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$. Esta es nuestra descomposición. Para sacar los idempotentes ortogonales nos valemos de la identidad de Bezout: por ser coprimos existen μ,ν tales que $\mu m+\nu n=1_{\mathbb{Z}}$. Además tenemos que

$$[\mu m]+[\nu n]=[1_{\mathbb{Z}}]=1_{\mathbb{Z}_{mn}} \tag{11}$$
$$[\mu m][\nu n]=[\mu\nu][nm]=[0] \tag{12}$$
$$[\mu m][\mu m]=[\mu m][1-\nu n]=[\mu m] \tag{13}$$

Por tanto, $e_1=[\mu m]$ y $e_2=[\nu n]$ son los elementos que buscamos. La descomposición viene dada por los ideales $[\mu m]\mathbb{Z}_{mn}$ y $[\nu n]\mathbb{Z}_{mn}$. Veamos que son precisamente $\mathbb{Z}_n$ y $\mathbb{Z}_m$ respectivamente. Los elementos del ideal $[\mu m]\mathbb{Z}_{mn}$ son los restos de la división $\frac{\mu mx}{mn}=\frac{\mu x}{n}$, es decir, son restos que determina una clase en $\mathbb{Z}_n$, por tanto $[\mu m]\mathbb{Z}_{mn}\subset\mathbb{Z}_n$. Pero además, si $[x],[y]\in\mathbb{Z}_{mn}$ son tales que $[\mu mx]=[\mu my]$ en $\mathbb{Z}_{mn}$, entonces $\mu m(x-y)\in mn\mathbb{Z}$ por lo tanto $x-y\in n\mathbb{Z}$. Es decir, que hay exactamente n clases en nuestro ideal, por tanto $[\mu m]\mathbb{Z}_{mn}=\mathbb{Z}_n$.

(ii) $A=\mathbb{Q}[x]/\langle x^2(x-1)\rangle$. Este ejemplo es el mismo que el anterior pero en un anillo de polinomios. En ambos casos tenemos un dominio euclídeo y por tanto una identidad de Bezout para el máximo común divisor. En concreto, $\gcd(x^2,x-1)=1$ que sale en la primera división $x^2=x(x-1)+1$ o equivalentemente $x^2+x(1-x)=1$, y podemos tomar como conjunto de idempotentes ortogonales $\{x^2,x(1-x)\}$ que cumplirán, análogamente a lo dicho en a), que $A=\mathbb{Q}[x]/\langle x^2\rangle\times\mathbb{Q}[x]/\langle x(1-x)\rangle$.

(iii) Literalmente lo mismo que el (ii) pero ahora genérico. Se cumple exactamente lo mismo.

Ejercicio 9 *Sea* A *un anillo y* $\mathfrak{a}\subset A$ *un ideal. Denotamos*

$$\mathfrak{a}[X]=\{f\in A[X]|\ f \textit{ tiene sus coeficientes en } \mathfrak{a}\}$$

Demostrar que $\mathfrak{a}[X]$ *es el extendido de* $\mathfrak{a}$ *via la inclusión. Si* $\mathfrak{p}$ *es ideal primo de* A*, ¿es* $\mathfrak{p}[X]$ *un ideal primo de* $A[X]$*?*

Estamos considerando la extensión de $\mathfrak{a}$ por la inclusión $i : A \hookrightarrow A[X]$, entonces

$$\mathfrak{a}^e = \langle \mathfrak{i}(a) \rangle \equiv \langle \mathfrak{a} \rangle_{A[X]} = \left\{ \sum_{i=0}^{n} a_i g_i \middle| \, a_i \in \mathfrak{a}, g_i \in A[X], n \in \mathbb{N} \right\}$$

Ahora bien, $\sum_{i=0}^n a_i g_i = \sum_{i=0}^n a_i \sum_{j=0}^m b_j^i X^j = \sum_{i,j} (a_i b_j^i) X^j$ y se cumple $a_i b_j^i \in \mathfrak{a}$ para todo i, j por ser un ideal.

Ejercicio 11 *Sea A un anillo, $\mathfrak{a}$ un ideal, y $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ ideales primos. Si $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, entonces $\mathfrak{a} \subset \mathfrak{p}_i$ para algún $i \in \{1, \dots, n\}$.*

Probamos el contrarrecíproco por inducción sobre n. El caso $n = 1$ es obvio. Supongamos que si tenemos n ideales primos y $\mathfrak{a} \not\subset \mathfrak{p}_i$ para ningún i, entonces $\mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$, y estudiamos el caso $n+1$. Vamos a encontrar un elemento de $\mathfrak{a}$ que no pertenece a ningún $\mathfrak{p}_i$.

Para cada j consideramos un $z_j \in \mathfrak{a} \setminus \bigcup_{i \neq j} \mathfrak{p}_i \neq \varnothing$. La diferencia conjuntista es efectivamente no vacía por hipótesis de inducción, pues hay n ideales primos en esa unión. Además, podemos suponer que $z_j \in \mathfrak{p}_j$ para cada j, pues en caso contrario existe algún z_j que no pertenece a ninguno de los ideales primos y hemos terminado. Afirmamos que el elemento $z = z_1 \cdot \ldots \cdot z_n + z_{n+1} \in \mathfrak{a}$ no pertenece a la unión.

Si perteneciese, a algún $\mathfrak{p}_j$ para $j \leq n$, entonces $z_{n+1} = z_j - z_1 \cdot \ldots \cdot z_n \in \mathfrak{p}_j$, en contra de la construcción. Por otro lado, si $z \in \mathfrak{p}_{n+1}$, entonces $z_1 \cdot \ldots \cdot z_n = z - z_{n+1} \in \mathfrak{p}_{m+1}$ y por ser este un ideal primo alguno de los z_i, con $1 \leq i \leq n$, pertenece a $\mathfrak{p}_{n+1}$, de nuevo en contra de la construcción de z.

Ejercicio 13 Sea A un anillo e $I \subset A[X_1, \dots, X_n]$ un ideal. Demostrar que $A[X_1, \dots, X_n]/I \cong A$ y que si A es un cuerpo, I es maximal.

La última afirmación es evidente, porque un ideal es maximal si y solo si el cociente es un cuerpo. Para ver el isomorfismo solo hace falta coger el homomorfismo suprayectivo $\mathrm{eval}_{a_1,\dots,a_n} : A[X_1, \dots, X_n] \to A$ cuyo núcleo son los polinomios de la forma $\sum_i (x_i - a_i) f$, pues todos sus términos deben anularse, y entonces $\ker \mathrm{eval}_{a_1,\dots,a_n} = I$ y hemos terminado.

Ejercicio 15 Se trata de repetir las demostraciones sobre extensiones finitas de cuerpos y la algebricidad de los generadores.

$\Rightarrow$) Si A es un K-espacio vectorial de dimensión finita m, entonces para cada i las potencias $1, x_i, \dots, x_i^m$ son $m+1$ vectores del espacio y por tanto son linealmente dependientes. Esto implica que existen $\lambda_0^i, \ldots, \lambda_m^i \in K$ tales que $\lambda_0^i + \lambda_1^i x_i + \ldots + \lambda_m^i x_i^m = 0$, es decir, que el polinomio no nulo $f_i(T) = \lambda_0^i + \lambda_1^i T + \ldots + \lambda_m^i T^m \in K[T]$ tiene a x_i por raíz.

$\Leftarrow$) Lo probamos por inducción. Escribimos solo el caso base $A = K[x_1]$. Consideramos el homomorfismo evaluación $\mathrm{eval}_{x_1} : K[T] \to A$. El núcleo $\ker \mathrm{eval}_{x_1}$ es un ideal primo de $K[T]$. Efectivamente, si $f, g \in K[T]$ son tales que $0 = fg(x_1) = f(x_1)g(x_1)$ entonces por ser A un DI, $f(x_1) = 0$ ó $g(x_1) = 0$, como queríamos probar. Por ser K un cuerpo, $K[T]$ es un DIP (es dominio euclídeo) y así $\ker \mathrm{eval}_{x_1}$ es un ideal maximal, está generado por un elemento irreducible f, y entonces por la caracterización de maximales $K[T]/\langle f \rangle \cong \mathrm{Im}\, \mathrm{eval}_{x_1}$ es un cuerpo. Dado que la imagen es un cuerpo que contiene a K y a x_1 y está contenida en A, debe coincidir con A.

Tomamos f el único polinomio mónico irreducible que genera el núcleo. Resulta que el grado n de f es la dimensión de $K[x_1]$. Efectivamente, $1 + \langle f \rangle, \ldots, T^{n-1} + \langle f \rangle$ es una base de $K[T]/\langle f \rangle$ (demostración en el libro de Gamboa). Además el isomorfismo $g + \langle f \rangle \mapsto g(x_1)$ entre $K[T]/\langle f \rangle$ e $\mathrm{Im}\, \mathrm{eval}_{x_1}$ es un isomorfismo de K-espacios vectoriales porque deja fijos todos los elementos de K. Entonces $1, x_1, \ldots, x_1^{n-1}$ es una base de $A = K[x_1]$.