

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

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 $\phi : A \rightarrow B$ 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:

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

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:

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

Ejercicio 4 Sea A un anillo y $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$. 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 $\sum_{j=1}^n a_j X^j \in \mathfrak{N}_A$, y como $a_0 \in \mathcal{U}(A)$, en virtud del ejercicio 1 se tiene que $\sum_{j=1}^n a_j X^j + a_0 = f \in \mathcal{U}(A)$.

\Rightarrow) Como f es una unidad, existe $g = \sum_{j=1}^m b_j X^j \in A[X]$ tal que $fg = 1$. En primer lugar, esto implica que $a_0 b_0 = 1$ 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 $m = \text{lcm}(a, b)$.

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 $\Phi : A \rightarrow A_1 \times \dots \times A_n$ via un isomorfismo de anillos y los conjuntos de idempotentes ortogonales de A , ie. $\{e_1, \dots, e_n\} \subset A$ 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 $A = A_1 \times \dots \times A_n = \bigoplus_{i=1}^n A_i$, entonces podemos tomar la proyección $A \rightarrow A_i$ compuesta con la inclusión $A_i \rightarrow A$ que resulta en un endomorfismo de A que denotamos e_i . Este endomorfismo es idempotente. Efectivamente, si tomamos $x = (x_1, \dots, x_n) \in A = \bigoplus_{i=1}^n A_i$ entonces $e_i \circ e_i(x) = e_i(0, \dots, 0, x_i, 0, \dots, 0) = (0, \dots, 0, x_i, 0, \dots, 0)$. Son ortogonales porque $e_j(0, \dots, 0, x_i, 0, \dots, 0) = (0, \dots, 0)$. Y también tenemos que suman la identidad porque para cualquier $x \in A$:

$$\begin{aligned} e_1(x) + \dots + e_i(x) + e_j(x) + \dots + e_n(x) &= \\ = (x_1, 0, \dots, 0) + \dots + (0, \dots, x_i, 0, \dots, 0) + (0, \dots, 0, x_j, \dots, 0) + (0, \dots, 0, x_n) &= \\ = (x_1, \dots, x_i, x_j, \dots, x_n) = x \end{aligned} \quad (3)$$

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 $\Phi : \bigoplus A_i \rightarrow A$, este determina un conjunto de idempotentes según a donde envíe a los elementos siguientes:

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

Efectivamente, por ser homomorfismo ha de cumplirse que

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

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

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

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 $x e_i = e_i x = e_i e_i a = e_i a = x$.

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

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

$$\phi_i(xy) = x y e_i = x y e_i e_i = (x e_i)(y e_i) = \phi_i(x) \phi_i(y) \quad (8)$$

Finalmente podemos coger $\Phi : A \rightarrow \bigoplus \mathfrak{a}_i$ 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 $0 = \Phi(x) = (x e_1, \dots, x e_n)$ entonces $0 = \sum_i x e_i = x \sum_i e_i = x$. Por lo tanto Φ es el isomorfismo que buscábamos.

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

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

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

No es un subanillo porque carece del elemento unidad de $A_1 \times \dots \times A_n$ que es la tupla con todos 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 $\Phi : A_1 \times A_2 \rightarrow A$ 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

$$[\mu m] + [\nu n] = [1_{\mathbb{Z}}] = 1_{\mathbb{Z}_{mn}} \quad (11)$$

$$[\mu m][\nu n] = [\mu \nu][nm] = [0] \quad (12)$$

$$[\mu m][\mu m] = [\mu m][1 - \nu n] = [\mu m] \quad (13)$$

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 $\frac{\mu m x}{mn} = \frac{\mu x}{n}$, 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 $[\mu m x] = [\mu m y]$ 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

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

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

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

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 $z_j \in \mathfrak{a} \setminus \bigcup_{i \neq j} \mathfrak{p}_i \neq \emptyset$. 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 $z = z_1 \cdot \dots \cdot z_n + z_{n+1} \in \mathfrak{a}$ no pertenece a la unión.

Si perteneciese, a algún \mathfrak{p}_j para $j \leq n$, entonces $z_{n+1} = z - z_1 \cdot \dots \cdot z_n \in \mathfrak{p}_j$, en contra de la construcción. Por otro lado, si $z \in \mathfrak{p}_{n+1}$, entonces $z_1 \cdot \dots \cdot z_n = z - z_{n+1} \in \mathfrak{p}_{n+1}$ 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 $\text{eval}_{a_1, \dots, a_n} : A[X_1, \dots, X_n] \rightarrow A$ cuyo núcleo son los polinomios de la forma $\sum_i (x_i - a_i) f$, pues todos sus términos deben anularse, y entonces $\ker \text{eval}_{a_1, \dots, a_n} = I$ 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 $\lambda_0^i, \dots, \lambda_m^i \in K$ tales que $\lambda_0^i + \lambda_1^i x_i + \dots + \lambda_m^i x_i^m = 0$, es decir, que el polinomio no nulo $f_i(T) = \lambda_0^i + \lambda_1^i T + \dots + \lambda_m^i T^m \in K[T]$ tiene a x_i por raíz.

\Leftarrow) Lo probamos por inducción. Escribimos solo el caso base $A = K[x_1]$. Consideramos el homomorfismo evaluación $\text{eval}_{x_1} : K[T] \rightarrow A$. El núcleo $\ker \text{eval}_{x_1}$ 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 $\ker \text{eval}_{x_1}$ es un ideal maximal, está generado por un elemento irreducible f , y entonces por la caracterización de maximales $K[T]/\langle f \rangle \cong \text{Im } \text{eval}_{x_1}$ 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, $1 + \langle f \rangle, \dots, T^{n-1} + \langle f \rangle$ 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 $\text{Im } \text{eval}_{x_1}$ es un isomorfismo de K -espacios vectoriales porque deja fijos todos los elementos de K . Entonces $1, x_1, \dots, x_1^{n-1}$ es una base de $A = K[x_1]$.

Ejercicio 17 Sea A un anillo y $f, g \in A[T]$ dos polinomios primitivos. Probar que fg es un polinomio primitivo.

Supongamos que fg no es primitivo. Entonces el ideal \mathfrak{a} que generan sus coeficientes no es el total. Sea \mathfrak{m} un ideal maximal que contiene a \mathfrak{a} .

Consideramos $A/\mathfrak{m}[T] \cong (A/\mathfrak{m})[T]$. Esto es cierto, podemos definir el homomorfismo suprayectivo $A[T] \rightarrow (A/\mathfrak{m})[T]$ dado por $f = \sum a_i T^i \mapsto \sum (a_i + \mathfrak{m}) T^i$, cuyo núcleo es $\mathfrak{m}[T]$. Ese cociente es un cuerpo, en particular un dominio de integridad. La clase de fg se anula en el cociente, pero no las clases de f, g porque sus coeficientes generan todo A , y si se anulasen significaría que $\mathfrak{m} = A$. Y esto es absurdo porque $[fg] = [f][g]$.

Ejercicio 18 Sea A un anillo y M un A -módulo. Definimos en $A \times M$ la multiplicación $(a, m)(b, n) = (ab, an + bm)$ con la suma natural y el producto de A -módulo. Probar que $A \times M$ es una A -álgebra con la suma natural y ese producto. ¿Es el homomorfismo $a \mapsto (a, 0_M)$ inyectivo?

Para ver que es A -álgebra solo hay que demostrar que $A \times M$ es un anillo (conmutativo unitario). Como $(A, +)$ y $(M, +)$ son grupos abelianos, $(A \times M, +)$ donde la suma es por coordenadas, también es un grupo abeliano.

El producto es conmutativo $(b, n)(a, m) = (ba, bm + an) = (ab, an + bm) = (a, m)(b, n)$ y distributivo:

$$\begin{aligned} (a, m)[(b, m) + (c, k)] &= (a, m)(b+c, m+k) = (a(b+c), a(n+k) + (b+c)m) = (ab+ac, an+ak+bm+cm) \\ &= (ab, an+bm) + (ac, ak+cm) = (a, m)(b, n) + (a, m)(c, k) \end{aligned} \quad (14)$$

y tiene unidad $(a, m)(1_A, 0) = (a1_A, a0 + 1_A m) = (a, m)$.

Obviamente la inclusión de un factor en un producto cartesiano es siempre inyectiva.

Ejercicio 19

Ejercicio 17 del Atiyah Comprobamos las dos condiciones para ser base. En primer lugar $\bigcup_{f \in A} X_f = \bigcup_{f \in A} \text{Spec } A \setminus V(f) = \text{Spec } A \setminus \bigcap_{f \in A} V(f) = \text{Spec } A$. Esto último es porque $V(f) \cap V(g) = V(\langle f, g \rangle)$ para cualesquiera $f, g \in A$, luego $\bigcap_{f \in A} V(f) = V(A) = V(\langle 1 \rangle) = \emptyset$. En segundo lugar, sean $f, g \in A$ y $\mathfrak{p} \in X_f \cap X_g = \text{Spec } A \setminus (V(f) \cup V(g))$. Entonces $f, g \notin \mathfrak{p}$, y por ser primo $fg \notin \mathfrak{p}$, luego $\mathfrak{p} \in X_{fg}$. Y si $\mathfrak{q} \in X_{fg}$, entonces $fg \notin \mathfrak{q}$, y por ser ideal esto implica que $f \notin \mathfrak{q}$ y $g \notin \mathfrak{q}$, por tanto $X_{fg} \subset X_f \cap X_g$, lo que termina la demostración de que ese conjunto es base de la topología. Además tenemos los dos contenidos lo que demuestra (i).

(i) $X_f \cap X_g = X_{fg}$.

(ii) $\emptyset = \text{Spec } A \setminus V(f) \iff V(f) = \text{Spec } A \iff f \in \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p} = \mathfrak{N}_A$.

(iii) Sabemos que si $f \notin \mathcal{U}(A)$, entonces existe un ideal maximal que lo contiene, en particular existe un ideal primo que lo contiene. Luego si ningún ideal primo lo contiene, no existe maximal que lo contenga, entonces no es unidad: $\emptyset = V(f) \Rightarrow pf \notin \mathfrak{p} \forall \mathfrak{p} \in \text{Spec } A \Rightarrow f \notin \mathcal{U}(A)$. Por otra parte, si f es unidad, no puede estar contenido en ningún ideal que no sea el total, y por tanto no hay primo (un ideal propio) que lo contenga.

(iv) $X_f = X_g \iff V(f) = V(g)$, y $\langle f \rangle$ es el menor radical que contiene a f , luego $\forall \mathfrak{p} \in V(f)$ se tiene $\langle f \rangle \subset \mathfrak{p}$ y que $\sqrt{\langle f \rangle} = \bigcap_{\mathfrak{p} \in V(f)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in V(g)} \mathfrak{p} = \sqrt{\langle g \rangle}$. Recíprocamente, si $\bigcap_{\mathfrak{p} \in V(f)} \mathfrak{p} = \bigcap_{\mathfrak{q} \in V(g)} \mathfrak{q}$, dado $\mathfrak{p} \in V(f)$, $\bigcap_{\mathfrak{q} \in V(g)} \mathfrak{q} \subset \mathfrak{p}$ y por ende $g \in \mathfrak{p}$ luego $\mathfrak{p} \in V(g)$; el otro contenido es análogo. Luego $V(f) = V(g)$ y por tanto $X_f = X_g$.

(v) Basta comprobarlo para un recubrimiento por abiertos de la base. Sea $\{X_{f_i}\}_{i \in I}$ recubrimiento de $\text{Spec } A$, y comprobemos que $\langle \{f_i\}_{i \in I} \rangle = \langle 1 \rangle$. Efectivamente, como $\text{Spec } A = \bigcup i \in IX_{f_i}$, entonces

$$\emptyset = \bigcap_{i \in I} V(f_i) = V(\{f_i\}_{i \in I}) = V(\langle \{f_i\}_{i \in I} \rangle) \quad (15)$$

lo que quiere decir que no hay ningún primo que contenga a $\langle \{f_i\}_{i \in I} \rangle$, en particular no hay ningún maximal que lo contenga, es decir, que $\langle \{f_i\}_{i \in I} \rangle = \langle 1 \rangle$. Entonces existe $J \subset I$ finito y existen $\{\lambda_j\}_{j \in J}$ tales que $1 = \sum_{j \in J} \lambda_j f_j$. Por tanto $\langle \{f_j\}_{j \in J} \rangle = \langle 1 \rangle$ y así $V(\langle \{f_j\}_{j \in J} \rangle) = \emptyset$ lo que implica $\bigcup_{j \in J} X_{f_j} = \text{Spec } A$. Con lo que $\{X_{f_j}\}_{j \in J}$ es subrecubrimiento finito de $\{X_{f_i}\}_{i \in I}$.

(vi) Consideramos $(X_{g_i})_{i \in I}$ recubrimiento de X_f . Podemos suponer spg. que $X_f = \bigcup_{i \in I} X_{f_i}$ por ser abierto. Entonces tenemos $V(f) = V(\langle f_i \rangle_{i \in I})$ y por tanto $f \in \sqrt{\langle f_i \rangle_{i \in I}}$ de forma que existe un $n > 0$ tal que $f^n \in \langle f_i \rangle_{i \in I}$. Por tanto, existe $J \subset I$ finito y $\{a_j\}_{j \in J}$ tales que $f^n = \sum_{j \in J} a_j f_j$.

Esto implica que para todo $\mathfrak{p} \in V(\langle f_j \rangle_{j \in J})$ se cumple $\langle f \rangle \subset \mathfrak{p}$, y a su vez $f \in \mathfrak{p}$, de manera que $V(\langle f_j \rangle_{j \in J}) \subset V(f)$. Los complementarios cumplen la inclusión contraria

$$X_f = \text{Spec } A \setminus V(f) \subset \text{Spec } A \setminus V(\langle f_j \rangle_{j \in J}) = \bigcup_{j \in J} X_{f_j}$$

y por tanto $\{X_{f_j}\}_{j \in J}$ es un subrecubrimiento finito.

(vii) \Rightarrow) Supongamos que A es abierto y compacto. Por ser abierto es unión de abiertos de la base, $A = \bigcup_{i \in I} X_{f_i}$, estos forman un recubrimiento y por ser compacto podemos quedarnos con un subrecubrimiento finito: $A = \bigcup_{i=1}^n X_{f_i}$.

\Leftarrow) Si $A = \bigcup_{i=1}^n X_{f_i}$, entonces es abierto por ser unión de abiertos. Sea $(X_{g_j})_{j \in J}$ un recubrimiento de A , en particular recubren cada X_{f_i} . Para cada $i = 1, \dots, n$ por ser compacto existe $F_i \subset J$ finito tal que $X_{f_i} \subset \bigcup_{j \in F_i} X_{g_j}$. Por tanto $A \subset \bigcup_{i=1}^n \bigcup_{j \in F_i} X_{g_j}$.

Ejercicio 20 Sea A un anillo y \mathfrak{a}_i con $i = 1, \dots, n$ ideales tales que si $i \neq j$, entonces $\mathfrak{a}_i + \mathfrak{a}_j = A$.

- (i) Sea $\mathfrak{b}_i = \bigcap_{j \neq i} \mathfrak{a}_j$, probar que $\mathfrak{b}_i + \mathfrak{a}_i = A$.
- (ii) Demostrar que la aplicación $A \rightarrow \prod_{i=1}^n A/\mathfrak{a}_i$ es supreyectiva y su núcleo es $\bigcap_{j=1}^n \mathfrak{a}_j$.
- (iii) Encontrar el conjunto de idempotentes ortogonales que describe la descomposición anterior.

(i) Por inducción sobre n . Si $n = 2$, es trivial. Supongamos cierto para $1, \dots, n$ y consideremos $n + 1$ ideales cumpliendo las hipótesis del enunciado. Cualquier subconjunto suyo cumple las hipótesis también.

Fijamos i, j y construimos $\mathfrak{b}_{ij} = \bigcap_{k \neq i, j} \mathfrak{a}_k$. Si pensamos en $\{\mathfrak{a}_k\}_{k \neq i}$, este es un conjunto de n ideales y \mathfrak{b}_{ij} es intersección de todos menos 1, entonces por hipótesis de inducción tenemos que $\mathfrak{b}_{ij} + \mathfrak{a}_i = A$. Análogamente para $\{\mathfrak{a}_k\}_{k \neq j}$ y por eso $\mathfrak{b}_{ij} + \mathfrak{a}_j = A$. Además, por la hipótesis original, $\mathfrak{a}_i + \mathfrak{a}_j = A$.

Entonces tenemos tres ideales $\mathfrak{b}_{ij}, \mathfrak{a}_i, \mathfrak{a}_j$ que cumplen las hipótesis del enunciado. Por tanto, por hipótesis de inducción, $\mathfrak{b}_i = \mathfrak{b}_{ij} \cap \mathfrak{a}_j = (\bigcap_{k \neq i, j} \mathfrak{a}_k) \cap \mathfrak{a}_j = \bigcap_{k \neq i} \mathfrak{a}_k$ cumple $\mathfrak{b}_i + \mathfrak{a}_i = A$.

(ii) Para cada i , la proyección canónica $\pi_i : A \rightarrow A/\mathfrak{a}_i$ es un homomorfismo sobreyectivo. Realmente, $\prod_{i=1}^n A/\mathfrak{a}_i = \bigoplus_{i=1}^n A/\mathfrak{a}_i$. Sabemos que en tal caso, $\pi = \bigoplus_{i=1}^n \pi_i$ es también homomorfismo, y como tiene todas sus componentes sobreyectivas, es sobreyectivo. Finalmente, si $0 = \pi(a)$, entonces $0 = \pi_i(a) = a + \mathfrak{a}_i$ o equivalente $a \in \mathfrak{a}_i$ para todo $i = 1, \dots, n$, y por tanto $a \in \bigcap_{i=1}^n \mathfrak{a}_i$.

(iii)