Álgebra conmutativa

Iñaki Garrido and Pedro Montealegre and Miguel Serrano

2021

Capítulo 1

Anillos, ideales y álgebras

1.1 Ideales

Definición 1.1.1. Un *anillo* conmutativo unitario es una terna $(A, +, \cdot)$ de un conjunto con dos operaciones internas, suma $+$ y producto $\cdot$, donde $(A, +)$ es un grupo conmutativo, el producto es asociativo y conmutativo, se cumple la propiedad distributiva, y existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$.

Todos los anillos con los que trabajaremos serán conmutativos y unitarios. Un subconjunto $S \subset A$ de un anillo es un *subanillo* de A si es un anillo con la suma y el producto de A.

Definición 1.1.2. Un *ideal* de un anillo A es un subconjunto $\mathfrak{a} \subset A$ que cumple:

1. Para todo $a, b \in \mathfrak{a}$ se tiene $a + b \in \mathfrak{a}$.
2. Para todo $a \in \mathfrak{a}$ y $x \in A$ se tiene $ax \in \mathfrak{a}$.

Obviamente, si un ideal de un anillo A contiene el $1 \in A$, entonces es el total.

Dado un subconjunto S de un anillo A, se puede considerar $\langle S \rangle$ el menor ideal que lo contiene, que resulta ser

$$\langle S \rangle = \left\{ \sum_{i=1}^{m} s_i a_i \middle| \; s_i \in S, a_i \in A, m \in \mathbb{N} \right\}$$

Dado un ideal $\mathfrak{a}$ se puede definir una relación de equivalencia $x \sim y \iff x - y \in \mathfrak{a}$ y el conjunto cociente resultante $A/\mathfrak{a}$ se dota de estructura de anillo con las operaciones $(a+\mathfrak{a})+(b+\mathfrak{a}) := (a+b)+\mathfrak{a}$ y $(a+\mathfrak{a})\cdot(b+\mathfrak{a}) := ab+\mathfrak{a}$. Es necesario que sea un ideal para que el producto esté bien definido.

Definición 1.1.3. Un anillo A es un dominio de integridad (DI) si para cualesquiera $a, b \in A$ tales que $ab = 0$ se tiene $a = 0$ o bien $b = 0$.

Definición 1.1.4. Sean A, B anillos, un *homomorfismo de anillos* entre A y B es una aplicación $\varphi : A \to B$ que tal que para todo $x, y \in A$ respeta la suma $\varphi(x +_A y) = \varphi x +_B \varphi y$, respeta el producto $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$, y además $\varphi(1_A) = 1_B$.

Dado un homomorfismo de anillos $\varphi : A \to B$ el núcleo $\ker\varphi$ es un ideal de A y la imagen $\mathrm{Im}\varphi$ es un subanillo de B. Además, para todo $\mathfrak{b}$ ideal de B, la preimagen $\varphi^{-1}(\mathfrak{b})$ es un ideal de A.

Teorema 1.1.5. (de isomorfía) *Dado un homomorfismo de anillos $\varphi : A \to B$, se cumple $A/\ker\varphi \cong \mathrm{Im}\varphi$. En particular, si φ es sobreyectivo, entonces $A/\ker\varphi \cong B$.*

Teorema 1.1.6. (de la correspondencia) *Sea A una anillo y $\mathfrak{a}$ un ideal de A. Existe una biyección entre los ideales de A que contienen a $\mathfrak{a}$ y los ideales del cociente $A/\mathfrak{a}$. En particular, todos los ideales de $A/\mathfrak{a}$ son de la forma $\mathfrak{b}/\mathfrak{a} = \{x+\mathfrak{a} : x \in \mathfrak{b}\}$ donde $\mathfrak{b}$ es un ideal que contiene a $\mathfrak{a}$.*

Definición 1.1.7. Un ideal $\mathfrak{p}$ de un anillo A se dice *primo* si es propio y para cualesquiera $a, b \in A$ tales que $ab \in \mathfrak{p}$ se tiene que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Un ideal $\mathfrak{m}$ de A se dice maximal si es propio y no está contenido en ningún otro ideal propio de A.

Comprobar que un ideal $\mathfrak{m}$ de una anillo A es maximal consiste en ver que si $\mathfrak{a} \supset \mathfrak{m}$ para otro $\mathfrak{a}$ ideal propio, entonces $\mathfrak{a} = \mathfrak{m}$.

Tanto la maximalidad como la primalidad se conservan por el teorema de la correspondencia, es decir, $\mathfrak{b}$ es primo / maximal en A si y solo si $\mathfrak{b}/\mathfrak{a}$ es primo / maximal en $A/\mathfrak{a}$.

Proposición 1.1.8. *Un ideal $\mathfrak{p}$ de un anillo A es primo si y solo si $\mathfrak{A}/\mathfrak{p}$ es DI. Un ideal $\mathfrak{m}$ de A es maximal si y solo si $\mathfrak{A}/\mathfrak{m}$ es un cuerpo.*

Como todo cuerpo es dominio de integridad tenemos probado automáticamente que

Corolario 1.1.9. *Todo ideal maximal es primo.*

1.1.1 Operaciones con ideales

Sea A un anillo y sean dos ideales $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$. Se define la *suma* de los ideales como

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \left\{ x + y \middle| \, x \in \mathfrak{a}_1, y \in \mathfrak{a}_2 \right\}$$

y resulta ser el menor ideal que contiene a ambos. La *intersección* de los ideales es la intersección conjuntista con las operaciones heredadas, y es el mayor ideal que está contenido en ambos ideales. El *producto* de los ideales

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_{i=1}^{m} x_i y_i \middle| \, x_i \in \mathfrak{a}_1, y_i \in \mathfrak{a}_2, m \in \mathbb{N} \right\}$$

y también es un ideal.

Observación 1.1.10. Se cumple $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$ (trivial), y se tiene la igualdad si $\mathfrak{a}_1 + \mathfrak{a}_2 = A$. Efectivamente, en tal caso, $1 = a_1 + a_2$ para ciertos $a_i \in \mathfrak{a}_i$, y entonces para todo $t \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, $t = ta_1 + ta_2 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$.

Cuando $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ se dice que los ideales son *comaximales*.

1.1.2 Uso del lema de Zorn en álgebra conmutativa

Definición 1.1.11. Sea un conjunto parcialmente ordenado $(S, \leq)$. Una cadena $T \subset S$ es un subconjunto tal que para cualesquiera $x, y \in T$ se cumple $x \leq y$ o $y \leq x$.

Lema 1.1.12. (de Zorn) *Sea un conjunto parcialmente ordenado $(S, \leq)$. Si toda cadena $T \subset S$ tiene una cota superior, entonces existe un elemento maximal en S.*

Proposición 1.1.13. *Todo anillo $A \neq 0$ tiene un ideal maximal*

Prueba. Consideramos el conjunto Σ de los ideales propios de A, que no es vacío porque $0 \in \Sigma$, y lo ordenamos con la inclusión. Sea $(\mathfrak{a}_i)_{i \in I}$ una cadena en Σ. Veamos que tiene una cota superior. Consideramos $\mathfrak{a}^* = \bigcup_{i \in I} \mathfrak{a}_i$, que es un ideal:

1. Para todos $x, y \in \mathfrak{a}^*$ existen $i, j \in I$ tales que $x \in \mathfrak{a}_i$ e $y \in \mathfrak{a}_j$. Como pertenecen a una cadena, podemos suponer que $\mathfrak{a}_i \subset \mathfrak{a}_j$ y por tanto $x, y \in \mathfrak{a}_j$, que es un ideal, luego $x - y \in \mathfrak{a}_j \subset a^*$.

2. Para todo $x \in \mathfrak{a}^*$ y todo $a \in A$, existe $i \in I$ tal que $x \in \mathfrak{a}_i$ y por tanto $xa \in \mathfrak{a}_i \subset \mathfrak{a}^*$.

Además, es un ideal propio porque $1 \notin \mathfrak{a}_i$ para todo $i \in I$ luego no pertenece a la unión. Entonces $\mathfrak{a}^* \in \Sigma$ y está claro que es una cota superior de la cadena, que es arbitraria. Podemos aplicar el lema de Zorn y concluimos que Σ tiene un elemento maximal, y por tanto A tiene un ideal maximal. □

Corolario 1.1.14. *Para todo ideal* $\mathfrak{a}$ *de un anillo* A *existe un ideal maximal que lo contiene*

Prueba. Se aplica la proposición anteior al anillo ${}^{A}\!/_{\mathfrak{a}}$ teniendo en cuenta que en el teorema de la correspondencia se conservar los ideales maximales. □

Proposición 1.1.15. *Sea* A *anillo, existe un ideal primo minimal*[1] $\mathfrak{p}$.

Prueba. Sabemos que existe un ideal maximal $\mathfrak{p} \subset A$, y este es primo por ser maximal. Consideramos Σ el conjunto de los ideales primos de A, que es no vacío porque $\mathfrak{p} \in \Sigma$, y lo ordenamos parcialmente con la inclusión tal que $\mathfrak{p} \leq \mathfrak{p}' \iff \mathfrak{p} \supset \mathfrak{p}'$. Sea $\{\mathfrak{q}_i\}_{i\in I} \subset \Sigma$ una cadena y consideramos $\mathfrak{q}^* := \bigcap_{i\in I} q_i$. Este es un ideal (la intersección siempre lo es) y $\mathfrak{q}^* \subset \mathfrak{q}_i$ para todo $i \in I$, por tanto es cota superior (para nuestro orden) de la cadena.

Veamos que $\mathfrak{q}^*$ es primo. Sean $ab \in \mathfrak{q}^*$, por ser así, $ab \in \mathfrak{q}_i$ para toda $i \in I$. Si $a \in \mathfrak{q}_i \forall i \in I$, entonces $a \in \mathfrak{q}^*$. Por otra parte, si existe $i_0 \in I$ tal que $a \notin \mathfrak{q}_{i_0}$

$$\begin{aligned} &\text{entonces } b \in \mathfrak{q}_j \forall j \in I: \\ &\qquad \text{si } \mathfrak{q}_{i_0} \subseteq \mathfrak{q}_j, \text{ como } b \in \mathfrak{q}_{i_0}, \text{ se tiene que } b \in \mathfrak{q}_j \text{y,} \end{aligned}$$

Así se tiene $\mathfrak{q}^* \in \Sigma$ y aplicando el lema de Zorn, existe un elemento maximal para el orden dado, equivalemente, minimal en sentido de la inclusión. □

Corolario 1.1.16. *Sea* A *anillo y* $\mathfrak{a}$ *ideal de* A*, existe un ideal primo minimal entre los que contienen a* $\mathfrak{a}$.

Definición 1.1.17. Sea A un anillo. Un elemento $x \in A$ se dice *nilpotente* si existe un $n \in \mathbb{N} \setminus \{0\}$ tal que $x^n = 0$.

Definición 1.1.18. Sea A un anillo. El *radical* de un ideal $\mathfrak{a}$ de A se define como

$$\sqrt{\mathfrak{a}} = \{x \in A : \exists n > 0 \text{ tal que } x^n \in \mathfrak{a}\}$$

[1] Un ideal primo que no contiene a ningún otro ideal primo.

Proposición 1.1.19. *Sea A un anillo, entonces el conjunto $\mathfrak{N}_A$ de todos los elementos nilpotentes de A es un ideal. Se le llama* nilradical *de A.*

Prueba.

1. Si $x \in \mathfrak{N}_A$ y $a \in A$, existe $n > 0$ tal que $x^n = 0$ y por tanto $(xa)^n = x^n a^n = 0$.
2. Si $x, y \in \mathfrak{N}_A$, existen $m, n > 0$ tales que $x^n = y^m = 0$. Utilizando el binomio de Newton se tiene que $(x+y)^{n+m-1}$ es una suma de multiplos de productos de la forma $x^r y^s$ con $r + s = m + n - 1$, y por tanto no se puede tener a la vez $r < n$ y $s < m$, de manera que cada uno de los sumandos es 0 y $(x+y)^{n+m-1} = 0$.

□

Proposición 1.1.20. *El nilradical de un anillo A verifica $\mathfrak{N}_A = \bigcap_{\mathfrak{p} \text{ primo}} \mathfrak{p}$.*

Prueba. Denotamos por $\mathfrak{N}$ a la intersección. Si $x \in \mathfrak{N}_A$ entonces existe $n > 0$ con $x^n = 0$. El cero pertenece a todo ideal, en particular para todo $\mathfrak{p}$ primo $0 = x^n = xx^{n-1} \in \mathfrak{p}$, lo que implica que $x \in \mathfrak{p}$ (porque o bien $x \in \mathfrak{p}$ o bien $x^{n-1} \in \mathfrak{p}$ y repetimos). Por tanto $x \in \mathfrak{N}$ y $\mathfrak{N}_A \subset \mathfrak{N}$.

Para ver el otro contenido, comprobamos que si $x_0 \notin \mathfrak{N}_A$ entonces existe $\mathfrak{p}$ primo tal que $x \notin \mathfrak{p}$. Sea $\Sigma = \{\mathfrak{a} : \text{ ideal propio tal que } x_0^n \notin \mathfrak{a} \text{ para todo } n > 0\}$, que es un conjunto no vació porque pertenece el 0, ya que si x_0 no es nilpotente, ninguna de sus potencias es 0, así que $x_0^n \notin \{0\}$ para todo n. Argumentamos igual que en la proposición 1.1.13 y obtenemos un elemento maximal de $\mathfrak{p}^* \in \Sigma$.

Veamos que $\mathfrak{p}^*$ es primo, equivalentemente, que si $x, y \notin \mathfrak{p}^*$, entonces $xy \notin \mathfrak{p}^*$. Sean entonces $x, y \notin \mathfrak{p}^*$, y consideramos $\mathfrak{p}^* + (x)$ y $\mathfrak{p}^* + (y)$ ideales que contienen a $\mathfrak{p}^*$ estrictamente. Como $\mathfrak{p}^*$ es un elemento maximal de Σ, esos dos ideales no pueden pertenecer a Σ, así que por definición existen $m, n > 0$ tales que $x_0^n \in \mathfrak{p}^* + (x)$ y $x_0^m \in \mathfrak{p}^* + (y)$. Entonces existen $p, q \in \mathfrak{p}^*$ tales que

$$x_0^{m+n} = x_0^n x_0^m = (p+x)(q+y) = \underset{\in\mathfrak{p}}{pq} + \underset{\in(xy)}{py} + \overset{\in(xy)}{qx} + \overset{\in(xy)}{xy} \in \mathfrak{p}^* + (xy)$$

Por tanto $\mathfrak{p}^* + (xy) \notin \Sigma$, y como $\mathfrak{p}^* \in \Sigma$, entonces $xy \notin \mathfrak{p}^*$. □

Definición 1.1.21. Un ideal $\mathfrak{q}$ de un anillo A se dice *primario* si cumple que, si $ab \in \mathfrak{q}$, entonces $a \in \mathfrak{q}$ o bien existe n con $b^n \in \mathfrak{q}$.

Proposición 1.1.22. *Un ideal $\mathfrak{q}$ es primario si y solo si $\mathfrak{N}_{A/\mathfrak{q}}$ coincide con el conjunto de divisores de* 0 *de $A/\mathfrak{q}$.*

Prueba. $\Rightarrow$) Obviamente todos los elementos de $\mathfrak{N}_{A/\mathfrak{q}}$ son divisores de 0. Supongamos que $(a+\mathfrak{q})(b+\mathfrak{q}) = 0+\mathfrak{q}$, entonces $ab \in \mathfrak{q}$. Por tanto $a \in \mathfrak{q}$ y entonces $a+\mathfrak{q} = 0+\mathfrak{q} \in \mathfrak{N}_{A/\mathfrak{q}}$, o bien existe n tal que $b^n \in \mathfrak{q}$ y así $b^n+\mathfrak{q} = (b+\mathfrak{q})^n = 0+\mathfrak{q}$ y por tanto $b+\mathfrak{q} \in \mathfrak{N}_{A/\mathfrak{q}}$.

$\Leftarrow$) Si $ab \in \mathfrak{q}$ y supongamos que $a \notin \mathfrak{q}$, entonces $0+\mathfrak{q} = ab+\mathfrak{q} = (a+\mathfrak{q})(b+\mathfrak{q})$. Como $a+\mathfrak{q} \neq 0+\mathfrak{q}$, o bien $b \in \mathfrak{q}$, o bien $b+\mathfrak{q}$ es un divisor de 0, y por tanto está en el nilradical del cociente, y existe n tal que $(b+\mathfrak{q})^n = b^n+\mathfrak{q} = 0+\mathfrak{q}$, es decir, $b^n \in \mathfrak{q}$ como queríamos. □

1.1.3 Extensión y contracción de ideales

Definición 1.1.23. Sea $\phi : A \to B$ un homomorfismo de anillos y sea $\mathcal{I}(A), \mathcal{I}(B)$ los conjuntos de ideales de A y B. Se define la *extensión de ideales* como la aplicación

$$\begin{aligned} e : \mathcal{I}(A) &\to \mathcal{I}(B) \\ \mathfrak{a} &\mapsto \mathfrak{a}^e = \left\{ \sum_{i=1}^{m} \phi(a_i)b_i \;\middle|\; a_i \in \mathfrak{a}, b_i \in B, m \in \mathbb{N} \right\} \end{aligned}$$

y la *contracción de ideales* como

$$\begin{aligned} c : \mathcal{I}(B) &\to \mathcal{I}(A) \\ \mathfrak{b} &\mapsto \phi^{-1}(\mathfrak{b}) \end{aligned}$$

Observación 1.1.24. Propiedades de la extensión y la contracción

1. La contracción conserva ideales primos: si $\mathfrak{p}$ es un ideal primo de B, entonces $\mathfrak{p}^c$ es un ideal primo de A.
2. El comportamiento de e y c respecto de las operaciones anteriores es el siguiente

$$\begin{aligned} (\mathfrak{a}_1+\mathfrak{a}_2)^e &= (\mathfrak{a}_1)^e + (\mathfrak{a}_2)^e & (\mathfrak{b}_1+\mathfrak{b}_2)^c &\subseteq (\mathfrak{b}_1)^c + (\mathfrak{b}_2)^c \\ (\mathfrak{a}_1\cap\mathfrak{a}_2)^e &\subseteq (\mathfrak{a}_1)^e \cap (\mathfrak{a}_2)^e & (\mathfrak{b}_1\cap\mathfrak{b}_2)^c &= (\mathfrak{b}_1)^c \cap (\mathfrak{b}_2)^c \\ (\mathfrak{a}_1\mathfrak{a}_2)^e &= (\mathfrak{a}_1)^e(\mathfrak{a}_2)^e & (\mathfrak{b}_1\mathfrak{b}_2)^c &\subseteq (\mathfrak{b}_1)^c(\mathfrak{b}_2)^c \end{aligned}$$

1.2 Lenguaje geométrico en álgebra conmutativa

Definición 1.2.1. Sea K un cuerpo, se dice que es *algebraicamente cerrado* si se cumple cualquiera de las condiciones equivalentes:

1. Para todo $f \in K[x] \setminus \{0\}$ existe $a \in K$ tal que $f(a) = 0$.
2. Todo $f \in K[x] \setminus \{0\}$ se descompone en factores de primer grado, es decir, si $\deg f = n$, $f(x) = \lambda \prod_{i=1}^{n}(x - a_i)$ para ciertos $\lambda, a_1, \dots, a_n$.
3. Toda extensión algebraica $L|K$ es trivial: $L = K$.

Proposición 1.2.2. *Para todo cuerpo K existe una extensión $L|K$ algebraicamente cerrada.*

Prueba. Ver teorema II.2.4 en [FG17]. □

Ejemplo 1.2.3.

1. $\mathbb{F}_p := \mathbb{Z}/\langle p \rangle$, $p \in \mathbb{Z}$ primo
2. $\mathbb{F}_{p^e} := \mathbb{F}_p[x]/\langle f(x) \rangle$ donde $f(x)$ es irreducible en $\mathbb{F}_p$ y de grado e. Se verifica que $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^{e'}}$ si, y sólo si, $e|e'$.

Definición 1.2.4. Si K es un cuerpo y $S \subset K[X_1, \dots, X_n]$, entonces se dice que

$$Z_{\mathbb{A}^n_K} = \{a \in \mathbb{A}^n_K \,|\, f(a) = 0 \text{ para cada } f \in S\}$$

es un *conjunto algebraico* en $\mathbb{A}^n_K$.

El estudio de los conjuntos de ceros de polinomios está íntimamente relacionado con el estudio de ideales porque $Z(S) = Z(\langle S \rangle)$. Efectivamente, si $a \in Z(\langle S \rangle)$, como $S \subset \langle S \rangle$, entonces en particular a anula a todo polinomio de S, luego $Z(S) \supset Z(\langle S \rangle)$. Recíprocamente, sea $a' \in Z(S)$ y $g \in \langle S \rangle$ entonces existen $f_i \in S, g_i \in K[X_1, \dots, X_n]$ para $i = 1, \dots, m$ tales que $g(a') = \sum_{i=1}^{m} f_i(a')g_i(a') = 0$, así que $Z(S) \subset Z(\langle S \rangle)$.

Ejemplo 1.2.5. Sea un cuerpo K algebraicamente cerrado y estudiemos los conjuntos algebraicos de $K[X]$ en $\mathbb{A}^1_K$. Solo hay tres tipos:

1. $Z(0) = \mathbb{A}^1_K$ porque el 0 se anula en todas partes.
2. $Z(K[X]) = \varnothing$ porque hay polinomios constantes no nulos.
3. Si $g(x) = \langle \prod_{i=1}^{n}(x - a_i) \rangle$, entonces $Z(g) = a_1, \dots, a_n$ porque un f se anula en todos los a_i si y solo si es múltiplo de $\prod_{i=1}^{n}(x - a_i)$.

Si K es un cuerpo, para todo $f \in K[x]$ se pueden encontrar $f_1, \dots, f_r$ sin factores irreducibles en $K[x]$ múltiples tales que $f = f_1 f_2^2 \dots f_r^r$. [2] En particular, $f_{\text{red}} =$

[2] Ver apéndice

$f_1 f_2 \dots f_r$ es un polinomio con mismos ceros que f pero de multiplicidad 1 [3]. Esto es útil, porque como $K[X]$ es un DIP, todo ideal es de la forma $\mathfrak{a} = fK[x]$. Dicho f puede ser en principio más complejo de lo que es necesario, por ejemplo, para definir el conjunto algebraico $\{x \in \mathbb{R} | \ x^2 = 0\}$ podemos usar, en vez de x^2, el polinomio x.

Lema 1.2.6. *Sea K un cuerpo, si $\mathfrak{a} \subset \mathfrak{b}$ son ideales de $K[X_1, \dots, X_n]$, entonces $Z(\mathfrak{a}) \supset Z(\mathfrak{b})$.*

Proposición 1.2.7. *Sea K un cuerpo y $A = K[X_1, \dots, X_n]$*

1. *Si $\{\mathfrak{a}_i\}_{i \in I}$ una familia arbitraria de ideales de A, entonces $Z(\sum_i \mathfrak{a}_i) = \bigcap_i Z(\mathfrak{a}_i)$.*
2. *Si $\{\mathfrak{b}_j\}_{j=1}^m$ una familia finita de ideales de $K[X_1, \dots, X_n]$, entonces $\bigcup_{j=1}^m Z(\mathfrak{b}_j) = Z(\mathfrak{b}_1 \dots \mathfrak{b}_m)$.*

Prueba. Por orden

1. Sea $a \in Z(\sum_i \mathfrak{a}_i)$. Cualquier $f_i \in \mathfrak{a}_i$ es en particular un elemento de $\sum_i \mathfrak{a}_i$ así que $f_i(a) = 0$. Como i es arbitrario y f_i también, entonces $a \in \bigcap_i Z(\mathfrak{a}_i)$.

Denotando $\mathfrak{a}^* = \sum\limits_{i \in I} \mathfrak{a}_i$, dado $f \in \mathfrak{a}^*$ tenemos que $f = f_{i_1} + \cdots + f_{i_r}$ para ciertos $\{i_1, \dots, i_r\} \subseteq I$ y donde $f_{i_j} \in \mathfrak{a}_{i_j}$. Si tomamos $a \in \bigcap Z(\mathfrak{a}_i)$, entonces $f(a) = f_{i_1}(a) + \cdots + f_{i_r}(a) = 0$, es decir, $a \in Z(\mathfrak{a}^*)$.

2. Comprobamos el doble contenido. Primero, como $\mathfrak{a} \cdot \mathfrak{b} \subset (\mathfrak{a} \cap \mathfrak{b})$ y este está contenido en ambos $\mathfrak{a}$ y $\mathfrak{b}$, entonces por el lema 1.2.6 $\mathcal{Z}(\mathfrak{a}), \mathcal{Z}(\mathfrak{b}) \subset \mathcal{Z}(\mathfrak{a} \cdot \mathfrak{b})$, y así su unión también está contenida.

El otro contenido lo hacemos por contrarrecíproco. Si $a \notin \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$, entonce es que $a \notin \mathcal{Z}(\mathfrak{a})$ y $a \notin \mathcal{Z}(\mathfrak{b})$. Existen $f \in \mathfrak{a}$ y $g \in \mathfrak{b}$ tales que $f(a) \neq 0$ y $g(a) \neq 0$, por tanto $fg(a) = f(a)g(a) \neq 0$, y entonces $a \notin \mathcal{Z}(\mathfrak{a} \cdot \mathfrak{b})$.

□

De acuerdo a lo que hemos visto, los conjuntos algebraicos en $\mathbb{A}_K^n$ son una colección $\mathcal{A}$ de subconjuntos que cumplen:

1. $\varnothing, \mathbb{A}_K^n \in \mathcal{A}$,
2. la intersección arbitraria de conjuntos de $\mathcal{A}$ pertenece a $\mathcal{A}$,

[3] Ver apéndice.

3. la unión finita de conjuntos de $\mathcal{A}$ pertenece a $\mathcal{A}$.

Estos son los tres axiomas que debe cumplir una familia de conjuntos para ser los cerrados de una *topología*.

Ejemplo 1.2.8. $\mathbb{A}^1_K$ es un espacio topológico con la topología de los complementarios finitos.

Teorema 1.2.9. (de la base de Hilbert) *Si A es un anillo tal que todo ideal de A está finitamente generado, entonces $A[X]$ también cumple esa propiedad.*

Prueba. Sea $\mathfrak{I} \subset A[x]$ un ideal, y formamos el conjunto de los coeficientes principales de polinomios en $\mathfrak{I}$.

$$\mathfrak{a} = \{c \in A \setminus \{0\} |\ \exists r \in \mathbb{N} \text{ con } cx^r + \text{tmg} \in \mathfrak{i}\} \cup \{0\}^4$$

Comprobamos que $\mathfrak{a}$ es un ideal.

1. Sean $c, d \in \mathfrak{a}$. Si $c = d$ entonces $c - d = 0 \in \mathfrak{a}$. Si $c \neq d$, entonces existen r, s tales que $f = cx^r + \text{tmg}, g = dx^s + \text{tmg} \in \mathfrak{I}$. Entonces por ser $\mathfrak{I}$ un ideal tenemos que
$$\mathfrak{I} \ni f - x^{r-s}g = (c-d)x^r + \text{tmg}$$
con lo que $c - d \in \mathfrak{a}$ también.

2. Sean $c \in \mathfrak{a}$ y $\lambda \in A$. Si $\lambda = 0$ es trivial. Si no, existe $f \in \mathfrak{I}$ con c de coeficiente principal, y $\lambda f \in \mathfrak{I}$ tiene a λc de coeficiente principal, luego $\lambda c \in \mathfrak{a}$.

Por hipótesis, $\mathfrak{a}$ está finitamente generado $\mathfrak{a} = \langle c_1, \ldots, c_s \rangle$. Para cada $i = 1, \ldots, s$ existe un $f_i \in \mathfrak{I}$ con c_i como coeficiente principal. Sea $\delta = \max_{1 \leq i \leq s} \deg f_i$, y para cada $\gamma \leq \delta$ definimos

$$\mathfrak{a}_\gamma = \{d \in A \setminus \{0\} |\ \exists f \in \mathfrak{I} \text{ con } \deg f = \gamma \text{ y con } d \text{ como coeficiente principal}\} \cup \{0\}$$

que también es un ideal de A:

1. Sean $c, d \in \mathfrak{a}_\gamma$. Si $c = d$ entonces $c - d = 0 \in \mathfrak{a}$. Si $c \neq d$, entonces existen $f, g \in \mathfrak{I}$ de grado γ con coeficientes principales c, d respectivamente, entonces $f - g \in \mathfrak{I}$ es de grado γ y tiene a $c - d$ por coeficiente principal.

[4] Aquí tmg significa términos de menor grado. Expresamos así el polinomio porque no será necesario prestar atención al resto.

2. Si $c \in \mathfrak{a}$ y $\lambda \in A$. Si $\lambda = 0$ es trivial. Si no, existe $f \in \mathfrak{I}$ de grado γ con c de coeficiente principal, y $\lambda f \in \mathfrak{I}$ es de grado γ y tiene a λc de coeficiente principal.

De nuevo, por hipótesis, $\mathfrak{a}_\gamma$ es finitamente generado, así que $\mathfrak{a}_\gamma = \langle d_{\gamma_1}, \dots, d_{\gamma_m} \rangle$, y para cada $j = 1, \dots, m_\gamma$ existe un polinomio $g_{\gamma_j} \in \mathfrak{I}$ que tiene a d_{γ_j} por coeficiente principal.

Vamos a comprobar que $\mathfrak{I} = \mathfrak{H}$ donde

$$\mathfrak{H} = \langle \{f_1, \dots, f_s\} \cup \{g_{\gamma_j}\}_{\substack{1 \leq \gamma \leq \delta \\ 1 \leq j \leq m_\gamma}} \rangle \subset \mathfrak{I}$$

El contenido $\supset$ se tiene por construcción. Para el otro, sea $F \in \mathfrak{I} \setminus \{0\}$ (si $\mathfrak{I} = \{0\}$, es trivial) y sea $\mu = \deg F$. Distinguimos dos casos.

Caso 1 Supongamos $\mu \geq \delta$, en caso contrario pasamos al caso 2. Sea $b \in \mathfrak{a}$ el coeficiente principal de F, entonces $b = \sum_{i=1}^{s} \lambda_i c_i$ para ciertos $\lambda_i \in A$. Resulta entonces que

$$F_1 = F - \underbrace{\sum_{i=1}^{s} \lambda_i x^{\mu - r_i} f_i}_{\in \mathfrak{H}} \in \mathfrak{I}, \qquad r_i = \deg f_i$$

es un polinomio de grado $< \mu$ por construcción. Además basta demostrar que $F_1 \in \mathfrak{H}$ para que $F \in \mathfrak{H} \subset \mathfrak{I}$.

Si $\mu_1 = \deg F_1 \geq \delta$, repetimos lo anterior para F_1 y obtenemos otro polinomio $F_2 \in \mathfrak{I}$ de grado estrictamente menor que μ_1. Se cumple entonces que $F =$ (polinomio en $\mathfrak{H} + F_2$. Continuamos repitiendo hasta que obtenemos $F^* \in \mathfrak{I}$ de grado ν estrictamente menor que δ. Entonces

$$F = (\text{polinomio en } \mathfrak{H}) + F^* \tag{1.1}$$

y basta ver que F^* está en $\mathfrak{H}$ para que $F \in \mathfrak{H} \subset \mathfrak{I}$. Pasamos al caso 2.

Caso 2 Como $\nu < \delta$, el coeficiente principal de F^*, u, está en $\mathfrak{a}_\nu$, o bien $F^* = 0$ en cuyo caso hemos terminado por (1.1). Como ese ideal está finitamente generado, tenemos $u = \sum_{j=1}^{m_\nu} t_j d_{\nu_j}$ para ciertos $t_j \in A$. Por definición de $\mathfrak{a}_\nu$, existen $g_{\nu_j}(x) \in \mathfrak{H}$ con d_{ν_j} como coeficiente principal para cada $j = 1, \dots, m_\nu$. Podemos imitar el caso 1 y formar

$$F_1^* = F^* - \underbrace{\sum_{j=1}^{m_\nu} t_j g_{\nu_j}}_{\in \mathfrak{H}}$$

que por construcción es un polinomio de grado menor que ν. Basta ver que $F_1^* \in \mathfrak{H}$ para que $F^* \in \mathfrak{H}$. Podemos repetir este paso para F_1^* y obtendremos otro polinomio $F_2^* \in \mathfrak{I}$, de manera que $F_1^* \in \mathfrak{H}$ si $F_2^* \in \mathfrak{H}$. Como los grados de cada uno de los polinomios que obtenemos son cada vez menores, necesariamente en algún momento obtendremos un polinomio $F^{**} = 0 \in \mathfrak{H}$ y hemos terminado.

$\square$

Corolario 1.2.10. *Si A es tal que todo ideal está finitamente generado, entonces $A[X_1, \ldots, X_n]$ también cumple es propiedad.*

Lema 1.2.11. *Sea K un cuerpo y $f \in K[x]$. Se verifica que*

$$\sqrt{\langle f(x) \rangle} = \langle f_{red}(x) \rangle.$$

Demostración. Denotemos

$$f(x) := f_1(x) f_2(x)^2 \cdots f_r(x)^r$$

donde f_i es libre de cuadrados y $\mathrm{mcd}(f_i, f_j) = 1$ para cada par $i \neq j$. Si $g(x) \in K[x]$ es tal que existe $\nu \in \mathbb{N}$ de forma que $g(x)^\nu \in \lambda(x) f(x)$ para cierto $\lambda(x) \in K[x]$, entonces $f_i(x) | g(x)$. Más aún, por las propiedades de los f_i se verifica que $\prod f_i(x) | g(x)$; es decir, $f_{\mathrm{red}}(x) | g(x)$.

Teorema 1.2.12. (Nullstellensatz) *Sea K un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$, entonces*

$$\mathfrak{I}(\mathcal{Z}(\mathfrak{a})) = \{ f \mid f(a) = 0 \text{ para todo } a \in \mathcal{Z}(\mathfrak{a}) \} = \sqrt{\mathfrak{a}}$$

Corolario 1.2.13. *El mayor ideal $\mathfrak{b}$ de $K[x_1, \ldots, x_n]$ tal que $Z_K(\mathfrak{b}) = Z_K(\mathfrak{a})$, para un $\mathfrak{a}$ dado, es $\mathfrak{I} Z_K(\mathfrak{a})$.*

1.3 Álgebras

Definición 1.3.1. Sea $\varphi : A \to B$ homomorfismo de anillos (conmutativos unitarios). Se dice que B es una A-álgebra.

Ejemplo 1.3.2.

1. Si A es un subanillo de B, entonces B tiene estructura de A-álgebra via la inclusión $i : A \to B$.

2. En concreto, si $\mathbb{K}$ es un cuerpo, tenemos el ejemplo anterior para $B = \mathcal{M}_n(\mathbb{K})$ y $A = \{D \in B : \ D \text{ es diagonal con } \operatorname{diag}(D) = (\lambda, \ldots, \lambda)\}$.

3. Si consideramos un cociente de un anillo A por un ideal suyo $\mathfrak{a}$, entonces la proyección canónica $p : A \to A/\mathfrak{a}$ dota al cociente de estructura de A-álgebra.

4. Si K es un cuerpo, entonces una extensión suya $L|K$ es una K-álgebra.

Observación 1.3.3. En estos ejemplos se ve que el homomorfismo de anillos que da la estructura de álgebra no debe cumplir nada en particular: puede o no ser inyectivo, sobreyectivo, etc.

Definición 1.3.4. Sean A un anillo y B, C dos A-álgebras. Se dice que $f : B \to C$ es un homomorfismo de A-álgebras si es un homomorfismo de anillos que hace conmutativo el diagrama siguiente:

$$\begin{tikzcd} A \arrow[r, "\varphi_B"] \arrow[dr, "\varphi_C"'] & B \arrow[d, "f"] \\ & C \end{tikzcd}$$

Definición 1.3.5. Sea B una A-álgebra mediante $f : A \to B$. Se dice que B está finitamente generada si existen $b_1, \ldots, b_r \in B$ tales que para todo $x \in B$ se cumpla

$$x = \sum_{i_1,\ldots,i_r} f(a_{i_1,\ldots,i_r}) b_1^{i_1} \ldots b_r^{i_r}$$

Observación 1.3.6. Sea B una A-álgebra, si utilizamos la caracterización de la observación 2.0.3, entonces B es finitamente generada si y solo si existen $b_1, \ldots, b_r \in B$ tales que para todo $x \in B$ se escribe $x = \sum_{i_1,\ldots,i_r} a_{i_1,\ldots,i_r} b_1^{i_1} \ldots b_r^{i_r}$.

En el caso particular en que $A \subset B$, entonces B es una A-álgebra finitamente generada si y solo si $B = A[b_1, \ldots, b_r]$ para ciertos $b_1, \ldots, b_r \in B$, es decir, el menor anillo que contiene a A y a los b_i.

Ejemplo 1.3.7.

1. Si A es un anillo, entonces $A \subset A[X_1, \ldots, X_n]$ y el anillo de polinomios es una A-álgebra finitamente generada.

2. Sean A subanillo de B, con B una A-álgebra finitamente generada por $\{b_1, \ldots, b_r\}$. Se puede tomar el anillo de polinomios $A[X_1, \ldots, X_r]$ y el homomorfismo evaluación en los b_i:

$$\begin{aligned} \mathrm{eval}_{b_1,\ldots,b_r} : A[X_1, \ldots, X_r] &\to B \\ X_i &\mapsto b_i \\ A \ni a &\mapsto a \end{aligned}$$

   El homomorfismo $\mathrm{eval}_{b_1,\ldots,b_r}$ es suprayectivo porque los elementos de B son expresiones polinomiales en $b_1, \ldots, b_r$. Aplicando el primer teorema de isomorfía tenemos

$$A[X_1, \ldots, X_r] \big/ \ker \mathrm{eval}_{b_1,\ldots,b_r} \cong B$$

3. Más generalmente, si B es una A-álgebra finitamente generada, también es una $f(A)$-álgebra finitamente generada y se puede repetir el ejemplo anterior con $f(A)$, que es subanillo de B.

Capítulo 2

Módulos

Definición 2.0.1. Sea A un anillo, se llama A-módulo a cualquier grupo abeliano $(M, +)$ sobre el que A actúa linealmente, es decir, un grupo M con junto con una operación externa $A \times M \to M$ que cumple que para todo $m, n \in M, a, b \in A$:

1. $a(m + n) = am + an$
2. $(a + b)m = am + bm$
3. $(ab)m = a(bm)$
4. $1_A m = m$.

Ejemplo 2.0.2.

1. Si $\mathbb{K}$ es un cuerpo, todo $\mathbb{K}$-espacio vectorial es un $\mathbb{K}$-módulo..
2. Si V es un $\mathbb{K}$-espacio vectorial de dimensión finita y $f : V \to V$ un endomorfismo, entonces V es un $\mathbb{K}[x]$-módulo via la aplicación

$$\begin{aligned} \mathbb{K}[x] \times V &\to V \\ (p(x), v) &\mapsto p(f) = a_n f^{(n)} + \cdots + a_1 f + a_0 \end{aligned}$$

   siendo $p(x) = a_n x^n + \cdots + a_1 x + a_0$ y $f^(k) = f \circ \overset{k)}{\ldots} \circ f$.

3. Toda A-álgebra B de un anillo A es un A-módulo. B es un anillo luego $(B, +)$ es un grupo abeliano. Por ser A-álgebra, existe un homomorfismo $\varphi : A \to B$, y entonces podemos definir la operación externa de la definición 2.0.1 como $A \times B \to B$ que hace corresponder $(a, b) \mapsto \varphi(a)b$.

Observación 2.0.3. Atendiendo al último ejemplo resulta que dados dos anillos A, B, dar a B estructura de A-álgebra es equivalente a darle estructura de A-módulo junto con la propiedad adicional de que

$$\forall b, b' \in B,\ \forall a \in A \quad a \cdot_{\text{ext}} (bb') = (a \cdot_{\text{ext}} b)b'$$

Definición 2.0.4. . Dado un anillo A y un A-módulo M, diremos que $S \subset M$ es un *submódulo de* M si es un subgrupo de M cerrado para la multiplicación por elementos de A.

Observación 2.0.5. Si A es un anillo, $\mathfrak{a} \subseteq A$ un ideal, y M un A-módulo entonces el conjunto

$$\mathfrak{a}M := \left\{ \sum_{i=1}^{r} a_i m_i \mid r \in \mathbb{N},\ a_i \in \mathfrak{a},\ m_i \in \mathbb{N} \right\}$$

es un submódulo de A.

Definición 2.0.6. . Sean $(A, +, \cdot)$ anillo, M y N A-módulos. Una aplicación $f : M \longrightarrow N$ se dice que es un homomorfismo de A-módulos o, simplemente, que es una aplicación A-lineal si verifica

i) $\forall\ m_1, m_2 \in M \quad f(m_1 + m_2) = f(m_1) + f(m_2)$ y

ii) $\forall\ \lambda \in A,\ \forall\ m \in M \quad f(\lambda m) = \lambda f(m)$.

Observaciones. *i)* En un A-módulo M se tiene que

$$\begin{aligned} &\forall\ m \in M \quad 0_A m = 0_M \\ &\forall\ \lambda \in A \quad \lambda 0_M = 0_M. \end{aligned}$$

Para ver lo primero basta observar que para todo $m \in M$ se tiene que $0_A m + m = (0_A + 1_A)m = 1_A m = m$, es decir, $0_A m = 0_M$. De aquí se desprende también que

$$(-1_A)(1_M) = -1_M = (1_A)(-1_M)$$

puesto que $0_M = 0_A 1_M = (1_A - 1_A)1_M = 1_A 1_M + (-1_A)(1_M) = 1_M + (-1_A)(1_M)$.

También se desprende que, para $\lambda \in A$ y $m \in M$ fijados (arbitrarios), $\lambda 0_M = \lambda(0_A m) = (\lambda 0_A)m = 0_A m = 0_M$; esto es, la segunda propiedad.

ii) Dado un homomorfismo de A-módulos, $f : M \longrightarrow N$, se tiene que $\ker(f) := \{x \in M \mid f(x) = 0_N\}$ es un submódulo de M y que $\operatorname{im}(f) := \{y \in N \mid \exists\ x \in M \text{ tal que } f(x) = y\}$ es un submódulo de N.

2.1 Construcciones con A-módulos

2.1.1 Módulos cociente

Dados $(A, +, \cdot)$ un anillo, M un A-módulo y $N \subset M$ un submódulo. Denotemos para cada $m \in M$ como $[m]_N$ a la clase de m en M/N. Tras esta consideración, se tiene que M/N junto a la aplicación

$$\begin{array}{rcl} M/N \times M/N & \longrightarrow & M/N \\ ([m_1]_N, [m_2]_N) & \longmapsto & [m_1 + m_2]_N. \end{array}$$

tiene estructura de grupo abeliano. Esto es así puesto que $(M, +)$ es un grupo abeliano y, por lo tanto, todo subgrupo suyo también lo es; es decir, todo subgrupo suyo será normal y el cociente será de nuevo abeliano.

Definición 2.1.1. . Sean $(A, +, \cdot)$ un anillo, M un A-módulo y $N \subseteq M$ un submódulo. Definiendo la aplicación

$$\begin{array}{rcl} A \times M/N & \longrightarrow & M/N \\ (\lambda, [m]) & \longmapsto & \lambda[m]_N := [\lambda m]_N \end{array}$$

dotamos a M/N de estructura de A-módulo y lo denominamos *módulo cociente.*

Observación 2.1.2. La aplicación natural

$$\begin{array}{rcl} M & \longrightarrow & M/N \\ m & \longmapsto & [m]_N \end{array}$$

es un homomorfismo de A-módulos.

2.1.2 Anuladores

Definición 2.1.3. Dados A un anillo y M un A-módulo, definimos el anulador de A en M como

$$Anul_A M = \{\lambda \in A \mid \lambda \cdot m = 0, \forall m \in M\}$$

Observación 2.1.4. *i)* $Anul_A M$ es un ideal de A:

1) Dados $\lambda_1, \lambda_2 \in Anul_A M$, para cada $m \in M$, $\lambda_1 \cdot m = \lambda_2 \cdot m = 0$. Restando, se obtiene $(\lambda_1 - \lambda_2) \cdot m = 0 \to \lambda_1 - \lambda_2 \in Anul_A M$

2) Dado $\lambda \in Anul_A M$, para cada $\alpha \in A$ y para cada $m \in M$ se tiene $(\alpha \cdot \lambda) \cdot m = \alpha \cdot (\lambda \cdot m) = \alpha \cdot 0 = 0$, luego $\alpha \cdot \lambda \in Anul_A M$

Por tanto, $A/Anul_A M$ tiene estructura de anillo. Además, podemos ver a M como un $A/Anul_A M$-módulo mediante la aplicación

$$\begin{array}{rcl} {}^{A}\!\diagup_{Anul_A M} \times M & \longrightarrow & M \\ (\lambda + Anul_A M) \cdot m & \longmapsto & \lambda \cdot m \end{array}$$

ii) Dado un ideal $\mathfrak{a} \subset Anul_A M$, M es un $A/\mathfrak{a}$-módulo. Los submódulos de M como $A/\mathfrak{a}$-módulo son los submódulos de M como A-módulo.

2.1.3 Aplicaciones A-lineales

Definición 2.1.5. . Dados M y N dos A-módulos, definimos *el conjunto de aplicaciones A-lineales entre M y N*

$$\mathrm{Hom}_A(M,N) := \{f : M \longrightarrow N \mid f \text{ es aplicación } A\text{-lineal}\}$$

Proposición. Dados M y N dos A-módulos, $\mathrm{Hom}_A(M,N)$ tiene estructura de A-módulo.

Demostración. En primer lugar, definamos para cada $\lambda \in A$ y cada $f \in \mathrm{Hom}_A(M,N)$ la aplicación

$$\begin{array}{rrcl} \lambda f : & M & \longrightarrow & N \\ & m & \longmapsto & \lambda(f(m)) \end{array}$$

y veamos de nuevo que $\lambda f \in \mathrm{Hom}_A(M,N)$, de forma que

$$\begin{array}{rcl} A \times \mathrm{Hom}_A(M,N) & \longrightarrow & \mathrm{Hom}_A(M,N) \\ (\lambda, f) & \longmapsto & \lambda f \end{array}$$

esté bien definida. Sean $m, m_1, m_2 \in M$ y $\mu \in A$:

$$\begin{aligned} (\lambda f)(m_1 + m_2) &= \lambda(f(m_1 + m_2)) = \\ &= \lambda(f(m_1) + f(m_2)) = \\ &= \lambda(f(m_1)) + \lambda(f(m_2)) = (\lambda f)(m_1) + (\lambda f)(m_2). \end{aligned}$$

$$\begin{aligned} (\lambda f)(\mu m) &= \lambda(f(\mu m)) = \lambda(\mu(f(m))) = (\lambda\mu)(f(m)) = \\ &= (\mu\lambda)(f(m)) = \mu(\lambda(f(m))) = (\mu(\lambda f))(m). \end{aligned}$$

Ahora, dadas $f, g \in \mathrm{Hom}_A(M,N)$ definamos la aplicación

$$\begin{array}{rrcl} f + g : & M & \longrightarrow & N \\ & m & \longmapsto & f(m) + g(m) \end{array}$$

Veamos que $f+g \in \mathrm{Hom}_A(M,N)$. Dados $m, m_1, m_2 \in M$ y $\lambda \in A$ arbitrarios, tenemos efectivamente

$$\begin{aligned}(f+g)(m_1+m_2) &= f(m_1+m_2)+g(m_1+m_2) = \\ &= f(m_1)+f(m_2)+g(m_1)+g(m_2) = (f+g)(m_1)+(f+g)(m_2).\end{aligned}$$

$$\begin{aligned}(f+g)(\lambda m) &= f(\lambda m)+g(\lambda m) = \lambda f(m)+\lambda g(m) = \\ &= \lambda(f(m)+g(m)) = \lambda((f+g)(m)) = (\lambda(f+g))(m).\end{aligned}$$

Así,

$$\begin{array}{rrcl} + : & \mathrm{Hom}_A(M,N)\times \mathrm{Hom}_A(M,N) & \longrightarrow & \mathrm{Hom}_A(M,N) \\ & (f,g) & \longmapsto & f+g, \end{array}$$

está bien definida y dota a $\mathrm{Hom}_A(M,N)$ de estructura de grupo abeliano.

Comprobemos por último que el producto exterior cumple los cuatro axiomas de la definición de A-módulo. Sean $m \in M$, $f, g \in \mathrm{Hom}_A(M,N)$ y $\lambda, \mu \in A$ arbitrarios:

i) $(\lambda(f+g))(m) = \lambda((f+g)(m)) = \lambda(f(m)+g(m)) = \lambda(f(m))+\lambda(g(m)) = (\lambda f)(m)+(\lambda g)(m) = (\lambda f+\lambda g)(m)$,

ii) $((\lambda+\mu)f)(m) = (\lambda+\mu)(f(m)) = \lambda(f(m))+\mu(f(m)) = (\lambda f)(m)+(\mu f)(m) = (\lambda f+\mu f)(m)$,

iii) $((\lambda\mu)f)(m) = (\lambda\mu)(f(m)) = \lambda(\mu(f(m)) = \lambda((\mu f)(m)) = (\lambda(\mu f))(m)$ y

iv) $(1_A f)(m) = 1_A(f(m)) = f(m)$.

2.1.4 Pullbacks

Dados M_1, M_2 y N A-módulos y dada $\varphi \in \mathrm{Hom}_A(M_1,M_2)$, podemos definir

$$\begin{array}{rrcl} \varphi^* : & Hom_A(M_2,N) & \longrightarrow & Hom_A(M_1,N) \\ & g & \longmapsto & g\circ\varphi \end{array}$$

que resulta ser un homomorfismo de A-módulos y se denota $\varphi^* = Hom_A(\varphi\_)$.

Análogamente, dados M, N_1 y N_2 A-módulos y dada $\psi \in \mathrm{Hom}_A(N_1,N_2)$,

$$\begin{array}{rrcl} \psi^* : & Hom_A(M,N_1) & \longrightarrow & Hom_A(M,N_2) \\ & g & \longmapsto & \psi\circ g \end{array}$$

es un homomorfismo de A-módulos.

Nótese que si tenemos M_1, M_2 y M_3 A-módulos y $\varphi \in Hom_A(M_1,M_2)$ y $\psi \in Hom_A(M_2,M_3)$, entonces $(\psi\circ\varphi)^* = \varphi^*\circ\psi^*$

2.1.5 Suma directa

Definición 2.1.6. . Sean $(A,+,\cdot)$ un anillo conmutativo unitario y $\{M_i\}_{i\in I}$ una familia no vacía de A-módulos. Definimos el conjunto

$$\bigoplus_{i\in I} M_i := \left\{(m_i)_{i\in I} \in \prod_{i\in I} M_i \mid m_i = 0_{M_i}, \forall\ i \in I \setminus F,\ F \subseteq I \text{ finito}\right\}$$

y lo llamamos *suma directa* de los A-módulos $\{M_i\}_{i\in I}$.

Proposición. Sean A un anillo y una familia $\{M_i\}_{i\in I}$ de A-módulos. Definamos las aplicaciones

$$\begin{array}{rrcl} + : & \bigoplus_{i\in I} M_i \times \bigoplus_{i\in I} M_i & \longrightarrow & \bigoplus_{i\in I} M_i \\ & ((m_i)_i, (m_i')_i) & \longmapsto & (m_i)_i + (m_i')_i := (m_i + m_i')_i, \end{array}$$

y

$$\begin{array}{rcl} A \times \bigoplus_{i\in I} M_i & \longrightarrow & \bigoplus_{i\in I} M_i \\ (\lambda, (m_i)_i) & \longmapsto & \lambda(m_i)_i := (\lambda m_i)_i. \end{array}$$

Se tiene que $(\bigoplus_{i\in I} M_i, +)$ es un grupo abeliano y $\bigoplus_{i\in I} M_i$ es un A-módulo mediante el producto exterior definido.

Observaciones. *i)* Para cada $j \in I$, tenemos definida $p_j : \bigoplus_{i\in I} M_i \to M_j$, la proyección a cada M_j. No es más que la restricción a $\bigoplus_{i\in I} M_i$ de la proyección Π_j definida sobre el producto cartesiano $\Pi_{i\in I} M_i$. p_j es un homomorfismo de A-módulos.

ii) Para cada $j \in I$, definimos la inclusión

$$\begin{array}{rrcl} q_j : & M_j & \longrightarrow & \bigoplus_{i\in I} M_i \\ & x & \longmapsto & (x) := \begin{cases} 0 & \text{si } i \neq j; \\ x & \text{si } i = j. \end{cases} \end{array}$$

q_j es un homomorfismo de anillos.

iii) Para cada $x = (x_i) \in \bigoplus_{i\in I} M_i$, existe un número finito de índices $i_1, ..., i_r$ tal que $x_{i_r} \neq 0$. Entonces, expresamos $x = \sum_{i\in i_{i_1},\dots i_{i_r}} q_i(x_i)$.

Notación. Dado A un anillo, I un conjunto no vacío, denotamos $A^{(I)} = \bigoplus_{i\in i} A_i$, donde para cada $i \in I$, $A_i = A$. $A^{(I)}$ es un submódulo de $A^I = \prod_{i\in I} A_i$, con $A_i = A$ para cada $i \in I$.

2.2 A-módulos libres

Definición 2.2.1. . Dado un homomorfismo de A-módulos, $f : M \to N$, se dice que es un isomorfismo de A-módulos si existe $g : N \to M$ homomorfismo de A-módulos tal que $g \circ f = Id_M$ y $f \circ g = Id_N$, es decir, una inversa de f.

Observación 2.2.2. $f : M \longrightarrow N$ es isomorfismo de A-módulos si, y sólo si, es inyectivo y sobreyectivo. Esto significa que es suficiente que f sea biyectivo como A-aplicación.

Lema 2.2.3. *Sean $M_i : i \in I$ un conjunto de A-módulos y sea N otro A-módulo. Un homomorfismo $\Phi : \bigoplus_{i\in I} M_i \to N$ viene unívocamente determinado por los homomorfismos $\Phi \circ q_i : M_i \to N$. Análogamente, los homomorfismos $\Phi : N \to \bigoplus_{i\in I} M_i$ vienen unívocamente determinados por los homomorfismos $p_i \circ \Phi : N \to M_i$.*

Demostración. Sea $\Phi : \bigoplus_{i\in I} M_i \to N$ un homomorfismo de A-módulos. Para cada $i \in I$, $\Phi \circ q_i$ es una composición de homomorfismos, luego es un homomorfismo de anillos.

Recíprocamente, dados $\Phi_i : M_i \to N$ homomorfismo de A-módulos, para cada $i \in I$, definimos $\Phi : \bigoplus_{i\in I} M_i \to N$ de la siguiente forma:

Para cada $\omega \in \bigoplus_{i\in I} M_i$, existen unos únicos $i_1, ..., i_r$, todos ellos distintos, tales que $\omega = q_{i_1}(\omega_{i_1}) + \cdots q_{i_r}(\omega_{i_r})$. Entonces, ponemos $\Phi(\omega) = \Phi_{i_1}(\omega_{i_1}) + ... + \Phi_{i_r}(\omega_{i_r})$. En el caso en el que ω sea 0, ponemos $\Phi(\omega) = 0$. Φ es un homomorfismo de anillos que cumple $\Phi \circ q_i = \Phi_i$, para cada $i \in I$.

Notación. Denotamos al Φ de la demostración anterior como $\bigoplus_{i\in I} \Phi_i$

Proposición 2.2.4. *Sea A un anillo y M un A-módulo. Son equivalentes*

1) *Existe $B := \{m_i\}_{i\in I} \subseteq M$ tal que para cada $x \in M$ existe $F \subseteq I$ cumpliendo que x se puede expresar de forma única como*

$$x = \sum_{\substack{j\in F \\ \lambda_j \in A}} \lambda_j m_j$$

   y

2) *$M \approx A^{(I)}$.*

Si se da cualquiera de ellas se dice que M es un A-módulo libre y B es una base. Además, en estas condiciones, dos bases B y B' de M tienen el mismo cardinal, que se llama rango de M.

Demostración. ($1 \Rightarrow 2$) En primer lugar, para cada $i \in I$ definimos las aplicaciones

$$\begin{array}{rccc} \varphi_i : & A & \longrightarrow & M \\ & 1_A & \longmapsto & m_i. \end{array}$$

por definición, para cada $i \in I$ y cada $\lambda \in A$ se verifica $\varphi_i(\lambda) = \lambda m_i$. De esta forma, φ_i es un homomorfismo de A-módulos entre A y M para cada $i \in I$ y, por el lema previo, $\varphi := \bigoplus_{i\in I} \varphi_i : A^{(I)} \longrightarrow M$ es a su vez un homomorfismo de A-módulos.

Por otro lado, dado que por hipótesis todo $x \in M$ admite una representación única como combinación lineal finita de elementos de B, definimos para cada $i \in I$ las aplicaciones

$$\begin{array}{rccc} \psi_i : & M & \longrightarrow & A \\ & x & \longmapsto & \lambda_i, \end{array}$$

donde λ_i es el correspondiente escalar asociado al elemento m_i en la representación de x. De nuevo, para cada $i \in I$, ψ_i es un homomorfismo de A-módulos y, de forma análoga, la aplicación

$$\psi : \quad M \longrightarrow A^I$$

verificando $p_i \circ \psi = \psi_i$ es un homomorfismo de A-módulos y es único. Más aún, para cada $x \in M$ existe $F \subseteq I$ finito de forma que, $\psi_i(x) = 0_A$ si $i \in I \setminus F$; es decir, $\psi(M) \subseteq A^{(I)}$.

Por último, es claro por definición de los homomorfismos que $\varphi \circ \psi = Id_M$ y $\psi \circ \varphi = Id_{A^{(I)}}$.

($2 \Rightarrow 1$) Supongamos que existe $\phi : A^{(I)} \to M$ un isomorfismo de A-módulos, para cierto conjunto de índices I. Sea, para cada $i \in I$, $m_i := \phi(e_i)$, donde $e_i \in A^{(I)}$ viene dado por

$$e_i = \begin{cases} e_{ij} = 0 & \text{si } i \neq j; \\ e_{ii} = 1_A \end{cases}$$

Veamos que $m_i : i \in I$ verifica 1). Para cada $m \in M$, por ser ϕ sobreyectiva, existe un $\underline{x} \in A^{(I)}$ tal que $\phi(\underline{x}) = m$. A su vez, existen $i_1, ..., i_r \in I$ tales que $\underline{x} = q_{i_1}(x_{i_1}) + ... + q_{i_r}(x_{i_r}) = x_{i_1} q_{i_1}(1_A) + ... + x_{i_r} q_{i_r}(1_A)$. Por tanto, $\phi(\underline{x}) = x_{i_1}\phi(e_{i_1}) + ... + x_{i_r}\phi(e_{i_r}) = x_{i_1} m_{i_1} + ... + x_{i_1} m_{i_r} = m$. Hemos escrito m como una combinación lineal de elementos $m_i : i \in I$

Supongamos ahora que para ciertos $\{i_j\}_{j\in\{1,\dots,r\}} \subset I$

$$\lambda_{i_1} m_{i_1} + \cdots + \lambda_{i_r} m_{i_r} = 0_M, \qquad \lambda_{i_j} \in A.$$

Por ser así, tenemos

$$\Phi(\lambda_{i_1} e_{i_1} + \cdots + \lambda_{i_r} e_{i_r}) = 0_M \Longleftrightarrow \lambda_{i_1} e_{i_1} + \cdots + \lambda_{i_r} e_{i_r} = 0_{A^{(I)}} \Longleftrightarrow \lambda_{i_j} = 0_A \quad \forall\, j \in \{1, \dots, r\}.$$

Falta ver que todas las bases tienen un mismo cardinal. Para ello, usaremos las observaciones previas a la proposición.

Supongamos $M \approx A^{(I)}$. Sean $\mathfrak{m}$ un ideal maximal de A (sabemos que existe) y $\{m_i\}_{i\in I}$ una base de M. Tenemos que $\mathfrak{m}M$ es un submódulo de M y, como $\mathfrak{m} \subset \operatorname{Ann}_A \left(M/\mathfrak{m}M \right)$, $M/\mathfrak{m}M$ tiene estructura de $A/\mathfrak{m}$-espacio vectorial.

Tomemos $M = A^{(I)}$ y veamos que $A^{(I)}/\mathfrak{m}A^{(I)} \approx \left(A/\mathfrak{m}\right)^{(I)}$, que es un $A/\mathfrak{m}$-espacio vectorial de dimensión $\#(I)$.

En primer lugar, definamos para cada $i \in I$ las siguientes aplicaciones

$$
\begin{array}{rccl}
\tau_i : & A & \longrightarrow & \left(A/\mathfrak{m}\right)^{(I)} \\
& 1_A & \longmapsto & \tau_i(1_A) = (a_j + \mathfrak{m})_{j\in I} := \begin{cases} a_j + \mathfrak{m} = \mathfrak{m} & \text{si } i \neq j \\ a_j + \mathfrak{m} = 1 + \mathfrak{m} & \text{si } i = j \end{cases}
\end{array}.
$$

Se comprueba que, para cada $i \in I$, τ_i es homomorfismo de A-módulos y, por lo tanto, $\bigoplus_{i\in I} \tau_i : A^{(I)} \longrightarrow \left(A/\mathfrak{m}\right)^{(I)}$ es también un homomorfismo de A-módulos.

Además, $\bigoplus_{i\in I} \tau_i$ es sobreyectivo y $\ker \bigoplus_{i\in I} \tau_i = \mathfrak{m}A^{(I)}$. Así, por el Primer Teorema de Isomorfía, $\bigoplus_{i\in I} \tau_i$ induce un isomorfismo de $A/\mathfrak{m}$-módulos, $\widehat{\bigoplus_{i\in I} \tau_i} : A^{(I)}/\mathfrak{m}A^{(I)} \longrightarrow \left(A/\mathfrak{m}\right)^{(I)}$

Ahora, dados dos conjuntos de índices no vacíos I y J, supongamos que existe un isomorfismo de A-módulos $\Phi : A^{(I)} \longrightarrow A^{(J)}$. Por ser así, en concreto se tiene que $\Phi(\mathfrak{m}A^{(I)}) = \mathfrak{m}A^{(J)}$ y Φ induce otro isomorfismo de $A/\mathfrak{m}$-módulos, $\widehat{\Phi} : A^{(I)}/\mathfrak{m}A^{(I)} \longrightarrow A^{(J)}/\mathfrak{m}A^{(J)}$. De esta forma, resulta que $(A/\mathfrak{m})^(I) \approx (A/\mathfrak{m})^(J)$ y $\#(I) = \#(J)$.

Corolario. Sea M es un A-módulo libre, es decir, existe un conjunto I tal que $M \cong A^{(I)}$, y sea N otro A-módulo. Dados $n_i : i \in I \subset N$, existe un único homomorfismo de A-módulos $f : M \to N$ tal que $f(m_i) = n_i$ para cada $i \in I$, donde $m_i : i \in I$ es una base de M

2.3 Sucesiones exactas

Definición 2.3.1. Una sucesión de homomorfismos de A-módulos

$$
\ldots \longrightarrow M_{i-1} \xrightarrow{\Phi_{i-1}} M_i \xrightarrow{\Phi_i} M_{i+1} \longrightarrow \ldots
$$

se dice exacta si $ker(\Phi_{i+1}) = im(\Phi_i)$, donde para cada i, M_i es un A-módulo y $\Phi_i : M_i \to M_{i+1}$ es un homomorfismo de A-módulos.

Definición 2.3.2. Decimos que una sucesión de homomorfismos de A-módulos es corta si es de la forma

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

Observación 2.3.3. Una sucesión corta es exacta si y sólo si $f : M_1 \to M_2$ es inyectiva, $g : M_2 \to M_3$ es suprayectiva y $im(f) = ker(g)$

Ejemplo 2.3.4. *1)* Dados $N \subset M$ A-módulos,

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

es una sucesión corta exacta.

2) Dados M y N A-módulos,

$$0 \longrightarrow M \xrightarrow{q_M} M \oplus N \xrightarrow{p_N} N \longrightarrow 0$$

es una también una sucesión corta exacta.

Observación 2.3.5. Toda sucesión de homomorfismos de A-módulos se puede descomponer en varias sucesiones cortas.

Definición 2.3.6. Dado M un A-módulo, un subconjunto $S \subset M$ es un sistema de generadores de M si para cada $x \in M$ existen $\{s_1, ..., s_n\} \subset S$ tales que

$$x = \lambda_1 s_1 + ... + \lambda_n s_n$$

con $\lambda_i \in A$ para cada $i \in \{1, ..., n\}$.

Es decir, el menor submódulo de M que contiene a S es el propio M.

Definición 2.3.7. Dado un conjunto de A-módulos ζ, una aplicación $\lambda : \zeta \to \mathbb{N}$ se dice aditiva si para cada M, M' y $M'' \in \zeta$ y para cada sucesión corta y exacta

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

se verifica $\lambda(M) = \lambda(M') + \lambda(M'')$.

Ejemplo 2.3.8. Dado K cuerpo, los K-módulos son los K-espacios vectoriales. Tomando ζ como los K-espacios vectoriales de dimensión finita,

$$\begin{array}{ccc} \zeta & \longrightarrow & \mathbb{N} \\ M & \longmapsto & dim(M) \end{array}$$

es una aplicación aditiva.

Proposición 2.3.9. *Sea*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una sucesión corta y exacta de A-módulos. Son equivalentes:

i) Existe $\pi : M \longrightarrow M'$ homomorfismo de A-módulos tal que $\pi \circ f = 1_{M'}$

ii) Existe $\sigma : M'' \longrightarrow M$ homomorfismo de A-módulos tal que $g \circ \sigma = 1_{M''}$

iii) $M \cong M' oplus M''$ vía f y g, es decir, existe $\Phi : M \longrightarrow M' \oplus M''$ isomorfismo de A-módulos tal que los diagramas son conmutativos.

En tal caso, se dice que la sucesión corta es escindida.

Prueba. ($1 \Rightarrow 2$) Dado $m'' \in M''$, por ser g sobreyectiva existe $m \in M$ tal que $g(m) = m''$. Considero

$$m^* := m - f \circ \tau(m) \in M$$

y afirmo que m^* no depende de la elección hecha de $m \in M$ de forma que $g(m) = m''$. Supongamos que existe otro $m_1 \in M$ tal que $g(m_1) = m''$. Por ser así,

$$g(m - m_1) = g(m) - g(m_1) = 0_{M''}.$$

Como $\ker(g) = \operatorname{im}(f)$, existe $m' \in M'$ tal que $f(m') = m - m_1$. Dado que por hipótesis $\tau \circ f = \mathrm{id}_{M'}$, tenemos

$$m - m_1 = f(m') = f \circ \tau(m - m_1) = f \circ \tau(m) - f \circ \tau(m_1)$$

y

$$m - f \circ \tau(m) = m_1 - f \circ \tau(m_1).$$

Vemos así que m^* no depende del $m \in M$ escogido con tal de que se tenga $g(m) = m''$.

Por esto que acabamos de ver, la aplicación

$$\begin{array}{rccl} \sigma : & M'' & \longrightarrow & M \\ & m'' & \longmapsto & m^* = m - f \circ \tau(m) \end{array},$$

donde m verifica $g(m) = m''$, está bien definida. Además, para cada $m'' \in M''$,

$$g \circ \sigma(m'') = g(\sigma(m'')) = g(m - f \circ \tau(m)) = g(m) = m'',$$

es decir, $g \circ \sigma = \mathrm{id}_{M''}$.

Falta por comprobar que σ es homomorfismo de A-módulos. Sean $\lambda, \mu \in A$ y $m_1'', m_2'' \in M''$ arbitrarios. Usamos que f, g y τ son homomorfismos de A-módulos. en primer lugar, es claro que, si $m_1, m_2 \in M$ verifican $g(m_i) = m_i''$, entonces $g(\lambda m_1) = \lambda m_1''$, $g(\mu m_2) = \mu m_2''$ y $g(\lambda m_1 + \mu m_2) = \lambda m_1'' + \mu m_2''$. Teniendo esto en cuenta,

$$\begin{aligned}\sigma(\lambda m_1'' + \mu m_2'') &= (\lambda m_1 + \mu m_2) - f \circ \tau(\lambda m_1 + \mu m_2) = \\ &= \lambda m_1 - f \circ \tau(\lambda m_1) + \mu m_2 - f \circ \tau(\mu m_2) = \sigma(\lambda m_1'') + \sigma(\mu m_2'')\end{aligned}$$

como queríamos.

$(2 \Rightarrow 1)$ Partiendo ahora de la existencia de $\sigma : M'' \longrightarrow M$ verificando $g \circ \sigma = \mathrm{id}_{M''}$, buscamos definir $\tau : M \longrightarrow M'$ cumpliendo $\tau \circ f = \mathrm{id}'_M$. Dado $m \in M$, $m - \sigma(g(m)) \in \ker(g) = im(f)$ y, como antes, existe $m' \in M'$ tal que $f(m') = m - \sigma(g(m))$ único por la inyectividad de f. Así, la aplicación

$$\begin{array}{rccc}\tau : & M & \longrightarrow & M' \\ & m & \longmapsto & m'\end{array},$$

donde m' es el único elemento en M' tal que $f(m') = m - \sigma(g(m))$, está bien definida. Además, es claro que para cada $m' \in M'$ se cumple $\tau \circ f(m') = m'$. La comprobación de que τ es homomorfismo de A-módulos es análoga al caso anterior.

$(2 \Rightarrow 3)$ En primer lugar, como se verifica 2) también tenemos 1); es decir, contamos con las aplicaciones τ y σ verificando las condiciones del enunciado.

Definimos así $\Phi : M' \oplus M'' :\longrightarrow M$ como el único homomorfismo de A-módulos que hace $\Phi \circ q_{M'} = f$ y $\Phi \circ q_{M''}$. Φ está bien definido por la propia contrucción de la suma directa $M' \oplus M''$. Veamos que es sobreyectivo. Sea $m \in M$ y tomemos $m' := \tau(m - \sigma(g(m))$ y $m'' := g(m)$. De nuevo, $m - \sigma(g(m)) \in \ker(g) = \mathrm{im}(f)$ y existe $m^* \in M'$ tal que $f(m^*) = m - \sigma(g(m))$. Por esto,

$$\begin{aligned}\Phi(m', m'') =& \Phi((m', 0) + (0, m'')) = \Phi \circ q_{M'}(m') + \Phi \circ q_{M''}(m'') = \\ =& f(\tau(m - \sigma(g(m)))) + \sigma(g(m)) = f \circ \tau \circ f(m^*) + \sigma \circ g(m) = \\ =& f(m^*) + \sigma \circ g(m) = m - \sigma(g(m)) + \sigma(g(m)) = m.\end{aligned}$$

Veamos ahora que Φ es inyectiva. Supongamos que $\Phi(m', m'') = 0_M$, es decir, $f(m') + \sigma(m'') = 0_M$. Aplicando g tenemos que $m'' = g \circ \sigma(m'') = 0_{M''}$. Por su parte, como f es inyectiva, $f(m') = 0_{M'}$ implica $m' = 0_{M'}$.

Por último, si $m \in M$, $\Phi^{-1}(m) = (m', m'')$, con $m'' = g(m)$. Así, ${p_{M''}}^{-1} = g$.

$(3 \Rightarrow 2)$ Basta tomar $\sigma := \Phi \circ q_{M''}$. $\square$

Apéndice A

Ejemplo factorización polinomio

Factorizamos el siguiente polinomio f como $F_1(F_2)^2 \dots (F_r)^r$ para ciertos polinomios F_i que tienen todos sus factores irreducibles de multiplicidad 1.

$$f(x) = (x-3)^4(x-2)^2(x+7)^2(x^2+1)$$

Calculamos su derivada formal, que comparte con f los factores irreducibles múltiples de f. El máximo común divisor f_1 entre f y f' tiene como factores irreducibles exactamente a los factores irreducibles con multiplicidad mayor o igual a 2 de f, pero ahora con multiplicidad 1 menos que en f.

$$f_1 = \gcd(f, f') = (x-3)^3(x-2)(x+7)$$

Por lo tanto, al dividir f entre f_1 nos queda un polinomio con todos los factores irreducibles de f pero ahora con multiplicidad 1.

$$g_1 = \frac{f}{f_1} = (x-3)(x-2)(x+7)(x^2+1)$$

Ahora tomamos f_1 y repetimos el proceso. Este comparte con su derivada sus factores irreducibles múltiples, que son los factores irreducibles de multiplicidad mayor o igual a 3 de f. Esos son exactamente los factores irreducibles del máximo común divisor f_2 entre ambos, en el cual aparecen con multiplicidad 1 menos que en f_1, es decir, con multiplicidad 2 menos que en f.

$$f_2 = \gcd(f_1, f_1') = (x-3)^2$$

Ahora al calcular el cociente $\frac{f_1}{f_2}$ obtenemos un polinomio que tiene por factores irreducibles exactamente los de f de multiplicidad mayor o igual a 2, pero ahora son simples.

$$g_2 = \frac{f_1}{f_2} = (x-3)(x-2)(x+7)$$

Finalmente, podemos sacar F_1, el primero de los polinomios que necesitamos para la factorización, sin más que dividir g_1 entre g_2. Efectivamente, g_1 tiene por factores irreducibles todos los de f pero con multiplicidad 1, y g_2 todos los múltiples de f pero con multiplicidad 1. Así al dividir solo quedarán los factores irreducibles simples.

$$F_1 = \frac{g_1}{g_2} = x^2 + 1$$

Ahora repetimos el proceso para f_1, es decir, en lo anterior hacer $f = f_1$. De esta forma obtendremos un polinomio que tiene por factores irreducibles exactamente a los factores irreducibles simples de f_1, que son los factores irreducibles dobles de f. Observamos que ya tenemos calculados el primer paso $\gcd(f_1, f_1') = f_2$, y el segundo $\frac{f_1}{f_2} = g_2$, así que sacamos

$$\begin{aligned} f_3 &= \gcd(f_2, f_2') = x-3 \\ g_3 &= \frac{f_2}{f_3} = x-3 \\ F_2 &= \frac{g_2}{g_3} = (x-2)(x+7) \end{aligned}$$

Repetimos dos veces más

$$\begin{aligned} f_4 &= \gcd(f_3, f_3') = 1 \\ g_4 &= \frac{f_3}{f_4} = x-3 \\ F_3 &= \frac{g_3}{g_4} = 1 \end{aligned}$$

$$\begin{aligned} f_5 &= \gcd(f_3, f_3') = 1 \\ g_5 &= \frac{f_3}{f_4} = 1 \\ F_4 &= \frac{g_3}{g_4} = x-3 \end{aligned}$$

¿Cómo sabemos cuando parar? Precisamente si intentamos repetir una vez más, obtenemos $f_6 = g_6 = F_5 = 1$, y como las siguientes etapas las construimos a partir de estos polinomios, quiere decir que todo lo que obtendremos a partir de ahora serán 1, así que debemos concluir el proceso con F_4. Esto nosotros lo sabíamos de antemano porque hemos escrito el polinomio factorizado en sus factores irreducibles y 4 era la mayor multiplicidad que teníamos, pero el criterio anterior es un criterio de parada general.

De esta forma tenemos$f$ factorizado como

$$f = F_1(F_2)^2(F_3)^3(F_4)^4$$

Además, el producto $f_{\text{red}} = F_1F_2F_3F_4$ es un polinomio que tiene mismos ceros que f pero todos ellos simples.

Apéndice B

Ejercicios

B.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:

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

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:

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

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 $x \in A$:

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

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

$$1_A = \Phi(1, 1, \ldots, 1) = \Phi(1, 0, \ldots, 0) + \cdots + \Phi(0, 0, \ldots, 1) = e_1 + e_2 + \ldots e_n \tag{B.4}$$

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

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

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 $\mathfrak{a}_i = e_i A$):

$$\phi_i(x + y) = (x + y)e_i = xe_i + ye_i = \phi_i(x) + \phi_i(y) \tag{B.7}$$

$$\phi_i(xy) = xye_i = xye_i e_i = (xe_i)(ye_i) = \phi_i(x)\phi_i(y) \tag{B.8}$$

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

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

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

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

$$[\mu m]+[\nu n]=[1_{\mathbb{Z}}]=1_{\mathbb{Z}_{mn}} \tag{B.11}$$

$$[\mu m][\nu n]=[\mu\nu][nm]=[0] \tag{B.12}$$

$$[\mu m][\mu m]=[\mu m][1-\nu n]=[\mu m] \tag{B.13}$$

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*

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

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

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

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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos. Si $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, entonces $\mathfrak{a} \subset \mathfrak{p}_i$ para algún $i \in \{1, \ldots, n\}$.*

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 $I \subset A[X_1, \ldots, X_n]$ un ideal. Demostrar que $A[X_1, \ldots, X_n]/I \cong A$ 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 supra-yectivo $\mathrm{eval}_{a_1,\ldots,a_n} : A[X_1, \ldots, X_n] \to A$ cuyo núcleo son los polinomios de la forma $\sum_i (x_i - a_i)f$, pues todos sus términos deben anularse, y entonces $\ker \mathrm{eval}_{a_1,\ldots,a_n} = I$ 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 $1, x_i, \ldots, x_i^m$ 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 $A = K[x_1]$.