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 $\operatorname{Ker}\varphi$ es un ideal de A y la imagen $\operatorname{Im}\varphi$ 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 $A/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. En particular, si φ es sobreyectivo, entonces $A/\operatorname{Ker}\varphi \cong B$.*

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

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

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 $a \notin \mathfrak{q}_{i_0}$ entonces $b \in \mathfrak{q}_j \forall j \in I$ si $\mathfrak{q}_{i_0} \subseteq \mathfrak{q}_j$, como $b \in \mathfrak{q}_{i_0}$, se tiene que $b \in \mathfrak{q}_j$y. 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

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

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.*

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

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 $\Sigma = \{\mathfrak{a} :$ ideal propio tal que $x_0^n \notin \mathfrak{a}$ 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 $\lambda, a_1, \ldots, a_n$.
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 $S \subset K[X_1, \ldots, X_n]$, 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 $f_i \in S, g_i \in K[X_1, \ldots, X_n]$ para $i = 1, \ldots, m$ 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 $Z(g) = a_1, \ldots, a_n$ 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 $f_1, \ldots, f_r$ sin factores irreducibles en $K[x]$ múltiples tales que $f = f_1 f_2^2 \ldots f_r^r$. [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 $f = f_{i_1} + \dots + f_{i_r}$ 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 $f(a) = f_{i_1}(a) + \dots + f_{i_r}(a) = 0$, 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

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

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

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

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 $\mu \ge \delta$, 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 $\mu_1 = \deg F_1 \ge \delta$, 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.

□

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*

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

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 $A = \{D \in B : \ D \text{ es diagonal con } \operatorname{diag}(D) = (\lambda, \dots, \lambda)\}$.

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 $b_1, \dots, b_r \in B$ tales que para todo $x \in B$ se cumpla

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

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 $b_1, \dots, b_r \in B$ tales que para todo $x \in B$ se escribe $x = \sum_{i_1,\dots,i_r} a_{i_1,\dots,i_r} b_1^{i_1} \dots b_r^{i_r}$.

En el caso particular en que $A \subset B$, entonces B es una A-álgebra finitamente generada si y solo si $B = A[b_1, \dots, b_r]$ para ciertos $b_1, \dots, b_r \in B$, 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 $A \subset A[X_1, \dots, X_n]$ 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 $\{b_1, \dots, b_r\}$. Se puede tomar el anillo de polinomios $A[X_1, \dots, X_r]$ y el homomorfismo evaluación en los b_i:

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

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

$$A[X_1, \dots, X_r] \big/ \operatorname{Ker} \mathrm{eval}_{b_1,\dots,b_r} \cong B$$

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 $f^(k) = f \circ \overset{k)}{\cdots} \circ f$.

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 M.

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

Observación 2.0.7.

1. 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.

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

1. $Anul_A M$ es un ideal de A.

   (a) 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 $(\lambda_1 - \lambda_2) \cdot m = 0 \rightarrow \lambda_1 - \lambda_2 \in Anul_A M$

(b) 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

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

2. 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*

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

Proposición 2.1.6. *Dados M y N dos A-módulos,* $\mathrm{Hom}_A(M, N)$ *tiene estructura de A-módulo.*

Prueba. 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

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

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,

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

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

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

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 2.1.7. . 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 2.1.8. *Sean A un anillo y una familia $\{M_i\}_{i\in I}$ de A-módulos. Entonces $\bigoplus_{i\in I} M_i$ con la suma por coordenadas y el producto por escalares por coordenadas es un A-módulo.*

Observación 2.1.9.

1. 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.

2. Para cada $j \in I$, la inclusión $q_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$ es homomorfismo de anillos.

i)

ii)

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 $x = \sum_{i\in i_{i_1},...i_{i_r}} q_i(x_i)$.

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 $p_i \circ \Phi : N \to M_i$.*

Prueba. 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 $\bigoplus_{i\in I} \Phi_i$

Definición 2.2.4. Se dice que M es un *A-módulo libre* si $M \cong A^{(I)}$ para cierto conjunto I.

Proposición 2.2.5. *M es un A-módulo libre si y solo si 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*

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

. Si dos subconjuntos B y B' cumplen lo anterior, entonces tienen el mismo cardinal.

Prueba. ($2 \Rightarrow 1$) 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 $e_i = (\delta_{ij})_j \in A^{(I)}$. El conjunto $\{ m_i, i \in I \}$ es el que buscamos.

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 $m_i : i \in I$

La unicidad es clara porque estamos usando un isomorfismo, pero podemos detallarlo. Si un elemento tiene dos representaciones en los m_i, al restarlas obtengo una combinación lineal nula de un conjunto de los m_i, basta entonces comprobar que, si una combinación lineal de cualquier subconjunto de los m_i es nula, sus coeficientes son nulos también:

$$\begin{multline} 0_M = \lambda_{i_1} m_{i_1} + \cdots + \lambda_{i_r} m_{i_r} = \Phi(\lambda_{i_1} e_{i_1} + \cdots + \lambda_{i_r} e_{i_r}) \\ \iff \lambda_{i_1} e_{i_1} + \cdots + \lambda_{i_r} e_{i_r} = 0_{A^{(I)}} \iff \lambda_{i_j} = 0_A \quad (2.1) \end{multline}$$

$\forall\ j \in \{1, \ldots, r\}$, lo que concluye la prueba.

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

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

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.

Todo $x \in M$ admite una representación única como combinación lineal finita de elementos de B. Sean las aplicaciones $\psi_i : M \to A$ dadas por $x = \sum_{j \in F} \lambda_j m_j \mapsto \lambda_i$, donde $F \subset I$ finito. Para cada $i \in I$, ψ_i es un homomorfismo de A-módulos y, de forma análoga, la aplicación $\psi : M \longrightarrow A^I$ que verifica $p_i \circ \psi = \psi_i$, 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 $\psi \circ \varphi = Id_{A^{(I)}}$.

Veamos que todas las bases tienen un mismo cardinal. Si $M \cong A^{(I)}$, sean $\mathfrak{m}$ un ideal maximal de A y $\{\, m_i, i \in I \,\}$ una base de M. $\mathfrak{m}M$ es un submódulo de M y, como $\mathfrak{m} \subset \mathrm{Ann}_A \left(M/\mathfrak{m}M \right)$, $M/\mathfrak{m}M$ tiene estructura de $A/\mathfrak{m}$-espacio vectorial.

Tomemos $M = A^{(I)}$ y veamos que $A^{(I)}/\mathfrak{m}A^{(I)} \cong \left(A/\mathfrak{m} \right)^{(I)}$, 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 $\operatorname{Ker} \bigoplus_{i \in I} \tau_i = \mathfrak{m} A^{(I)}$. 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 $(A/\mathfrak{m})^(I) \cong (A/\mathfrak{m})^(J)$ y $\#(I) = \#(J)$. $\square$

Definición 2.2.6. A cualquier conjunto B que cumpla la proposición anterior se le llama base del A-módulo libre M, y a su cardinal se le llama *rango de M*.

Corolario 2.2.7. *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 $\operatorname{Ker}(\Phi_{i+1}) = \operatorname{im}(\Phi_i)$, 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 $\mathrm{im}(f) = \mathrm{Ker}(g)$

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 $\mathrm{Ker}(g) = \mathrm{im}(f)$, 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 $m \in M$, $m - \sigma(g(m)) \in \mathrm{Ker}(g) = im(f)$ 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, $m - \sigma(g(m)) \in \mathrm{Ker}(g) = \mathrm{im}(f)$ 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 $\sigma := \Phi \circ q_{M''}$. □

Denotemos por CRing a la categoría de anillos conmutativos unitarios. Dado $A \in \mathrm{Obj}(\mathrm{CRing})$, denotaremos a su vez por Mod_A a la categoría de A-módulos.

Proposición 2.3.10. *1) Sea*

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \tag{2.2}$$

una sucesión de A-módulos y homomorfismos. Entonces (2.2) es exacta si, y sólo si, para todo $N \in \mathrm{Obj}(\mathrm{Mod}_A)$ la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \overset{\mathrm{Hom}_A(M,f)}{\longrightarrow} \mathrm{Hom}_A(M, N) \overset{\mathrm{Hom}_A(M,g)}{\longrightarrow} \mathrm{Hom}_A(M, N'') \tag{2.3}$$

es también una sucesión exacta.

2) Sea

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 \tag{2.4}$$

una sucesión de A-módulos y homomorfismos. Entonces (2.4) es exacta si, y sólo si, para todo $M \in \mathrm{Obj}(\mathrm{Mod}_A)$ la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \overset{\mathrm{Hom}_A(g,N)}{\longrightarrow} \mathrm{Hom}_A(M, N) \overset{\mathrm{Hom}_A(f,N)}{\longrightarrow} \mathrm{Hom}_A(M', N) \tag{2.5}$$

es también una sucesión exacta.

Prueba. Veamos ($\Rightarrow$) en 1). Denotemos $f_* := \mathrm{Hom}_A(M, f)$ y $g_* := \mathrm{Hom}_A(M, g)$. En primer lugar, por definición de f_* y dado $\varphi \in \mathrm{Hom}_A(M, N')$, si $f \circ \varphi \equiv 0_N$, entonces para toda $x \in M$ se tiene $\varphi(x) = 0$ por la inyectividad de f (si existiera $x \in M$ tal que $\varphi(x) \neq 0_{N'}$, entonces $f(\varphi(x)) \neq 0_N$). Así, vemos que f_* es inyectiva.

Comprobemos ahora que $\mathrm{im}(f_*) = \mathrm{Ker}(g_*)$. En primer lugar, dado que $g_* \circ f_* = (g \circ f)_*$ y $g \circ f = 0_{N''}$ resulta

$$g_* \circ f_* = 0_{\mathrm{Hom}_A(M,N'')},$$

es decir, $\mathrm{im}(f_*) \subset \mathrm{Ker}(g_*)$. Ahora, dado $\psi \in \mathrm{Hom}_A(M, N)$ tal que $g \circ \psi \equiv 0$, se tiene que $\mathrm{im}(\psi) \subset \mathrm{Ker}(g) = \mathrm{im}(f)$. Como f es un isomorfismo sobre su imagen, el homomorfismo de A-módulos

$$\varphi := f^{-1} \circ \psi : \quad M \quad \longrightarrow \quad N'$$

está bien definido. Así, componiendo f por la izquierda tenemos la igualdad $\psi = f \circ \varphi$; de forma equivalente, $\psi \in \mathrm{im}(f_*)$ como queríamos probar.

Probemos ahora ($\Rightarrow$) en 2). Sea $\psi \in \mathrm{Hom}_A(M'', N)$ tal que $\psi \circ \psi \equiv 0$. Como g es suprayectiva, la suposición anterior implica que $M'' = \mathrm{im}(g) \subset \mathrm{Ker}\,\psi$; es decir, $\psi \equiv 0_{\mathrm{Hom}_A(M'',N)}$ y g^* es inyectiva.

Veamos ahora que $\mathrm{im}(g^*) = \mathrm{Ker}(f^*)$. En primer lugar, si $\psi \in \mathrm{im}(g^*)$, existe $\varphi \in \mathrm{Hom}_A(M'', N)$ tal que $\psi = \varphi \circ g$. Por ser esto así, se tiene

$$f^*(\psi) = \psi \circ f = (\varphi \circ g) \circ f = \varphi \circ (g \circ f) = \varphi \circ 0_{\mathrm{Hom}_A(M',M'')} = 0_{\mathrm{Hom}_A(M',N)},$$

es decir, $\mathrm{im}(g^*) \subset \mathrm{Ker}(f^*)$.

Ahora, sea $\psi \in \mathrm{Ker}(f^*)$, i.e, $\psi \circ f \equiv 0_{\mathrm{Hom}_A(M',N)}$. Por un lado, $\mathrm{Ker}(g) = \mathrm{im}(f) \subset \mathrm{Ker}(\psi)$. Por otro, como g es sobreyectiva, para todo $x \in M''$ existe $m_x \in M$ tal que $g(m_x) = x$. Podemos definir así la siguiente aplicación

$$\begin{array}{rccc} \varphi & M'' & \longrightarrow & N \\ & x & \longmapsto & \psi(m_x) \end{array}.$$

Veamos que está bien definida. Supongamos que existen $m_x, {m_x}' \in M$ distintos de forma que $g(m_x) = g({m_x}') = x$. Por darse $\mathrm{Ker}(g) \subset \mathrm{Ker}(\psi)$ y ser g homomorfismo de A-módulos, $m_x - {m_x}' \in \mathrm{Ker}(g) \subset \mathrm{Ker}(\psi)$, es decir, $\psi(m_x) = \psi({m_x}')$. Tras comprobar que φ es un homomorfismo de A-módulos, tenemos que para cada $x \in M$ se verifica

$$\varphi(g(x)) = \psi(x);$$

es decir, $\psi = \varphi \circ g$.

Ahora vamos a probar las implicaciones ($\Leftarrow$) tanto en 1) como en 2). Comenzamos con la de 2). Para ver que g es suprayectiva, tomamos en primer lugar $N := {}^{M''}\!\diagup_{\mathrm{im}(g)}$ en (2.5). Si consideramos la aplicación cociente $c : M'' \longrightarrow N$, se tiene que $g^*(c) = c \circ g = 0_{\mathrm{Hom}_A(M,N)}$; es decir, como g^* es inyectiva, $c \equiv 0_{\mathrm{Hom}_A(M'',N)}$ y $M'' = \mathrm{im}(g)$.

Tomemos ahora $N := {}^{M}\!\diagup_{\mathrm{im}(f)}$. De nuevo, si consideramos la aplicación cociente $c : M \longrightarrow N$, se tiene que $f^*(c) = c \circ f = 0_{\mathrm{Hom}_A(M',N)}$ y $c \in \mathrm{Ker}(f^*)$. Por esto último, existe $\varphi \in \mathrm{Hom}_A(M'', N)$ tal que $c = \varphi \circ g$. Si $x \in M$ es tal que $g(x) = 0$, entonces $c(x) = 0_N$ y $x \in \mathrm{im}(f)$. Así, $\mathrm{Ker}(g) \subset \mathrm{im}(f)$. Para ver que $\mathrm{Ker}(g) \supset \mathrm{im}(f)$ basta tomar $N := M''$ y observar que

$$g^*(1_{M''}) = g \in \mathrm{Ker}(f^*);$$

es decir, $g \circ f = 0_{\mathrm{Hom}_A(M',M'')}$ y se tiene lo que buscábamos.

Comprobemos por último la suficiencia en 1). Para ver que f es inyectiva, tomemos $M := \mathrm{Ker}(f)$ y la inclusión $i : M \longrightarrow N'$, que es inyectiva. Por esta elección, tenemos que

$$f_*(i) = f \circ i = 0_{\mathrm{Hom}_A(M,N')}$$

y , como por hipótesis f_* es inyectiva, $i \equiv 0_{\mathrm{Hom}_A(M,N')}$. Ahora, como i es inyectiva, se tiene que $\mathrm{Ker}(f) = \{0_{N'}\}$, es decir, f es inyectiva.

Para ver $\mathrm{Ker}(g) = \mathrm{im}(f)$, veamos las dos inclusiones. En primer lugar, tomando $M := N'$ y $1_{N'} \in \mathrm{Hom}_A(M, N')$, se tiene que

$$f_*(1_{N'}) = f \in \mathrm{im}(f_*) = \mathrm{Ker}(g_*),$$

es decir, $g \circ f = 0_{\mathrm{Hom}_A(N',N'')}$ y $\mathrm{Ker}(g) \supset \mathrm{im}(f)$. Para el otro contenido, definamos de forma análoga al caso anterior $M := \mathrm{Ker}(g)$ y consideremos la inclusión $i \in \mathrm{Hom}_A(M, N)$. Por esta elección tenemos que

$$g_*(i) = g \circ i = 0_{\mathrm{Hom}_A(M,N'')},$$

es decir, $i \in \mathrm{Ker}(g_*) = \mathrm{im}(f_*)$ y por lo tanto existe $\varphi \in \mathrm{Hom}_A(M, N')$ de forma que $i = f \circ \varphi$. Es por esto que, dado $x \in M$ se verifica

$$x = i(x) = f(\varphi(x)) \in \mathrm{im}(f).$$

Así, $\mathrm{Ker}(g) \subset \mathrm{im}(f)$. □

2.4 Módulos proyectivos y módulos inyectivos

Supongamos $M \in \mathrm{Obj}(\mathrm{Mod}_A)$ tal que, siempre que se tenga una sucesión exacta

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0,$$

se tuviera que la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \overset{\mathrm{Hom}_A(M,f)}{\longrightarrow} \mathrm{Hom}_A(M, N) \overset{\mathrm{Hom}_A(M,g)}{\longrightarrow} \mathrm{Hom}_A(M, N'') \longrightarrow 0$$

también es exacta. Por 2.3.10, esto es equivalente a que para cualesquiera $N, N'' \in \mathrm{Obj}(\mathrm{Mod}_A)$ y todo $\varphi \in \mathrm{Hom}_A(M, N')$ existiría $h \in \mathrm{Hom}_A(M, N)$ tal que $g \circ h = \varphi$. Esta observación motiva la siguiente definición.

Definición 2.4.1. Sea $M \in \mathrm{Obj}(\mathrm{Mod}_A)$ tal que para toda $g \in \mathrm{Hom}_A(N, N')$ suprayectiva y toda $\varphi \in \mathrm{Hom}_A(M, N')$ existe $h \in \mathrm{Hom}_A(M, N)$ verificando $g \circ \varphi = h$. En estas condiciones, decimos que M es un A-*módulo proyectivo*.

Observación 2.4.2. Todo módulo libre es un módulo proyectivo. Sea $A^{(I)}$ un A-módulo libre con sistema de generadores $\{a_i\}_{i \in I}$. Sean también $g \in \mathrm{Hom}_A(N, N')$ suprayectiva y $\varphi \in \mathrm{Hom}_A(A^{(I)}, N')$ arbitrarias. Por ser g sobreyectiva, para cada $i \in I$ existe $n_i \in N$ tal que $g(n_i) = \varphi(a_i)$. Es por esto que podemos definir

$$\begin{array}{rccc} h: & A^{(I)} & \longrightarrow & N \\ & a_i & \longmapsto & n_i \end{array}.$$

Por lo ya comentado, h está bien definido. Además, como $\{a_i\}_{i\in I}$ es un sistema de generadores, para cada $x \in A^{(I)}$ existe $F_x \subset I$ finito tal que $x = \sum_{i\in F_x} \lambda_i a_i$, donde $\lambda_i \in A$ para cada $i \in F_x$. Es por esto que tomando $x \in A^{(I)}$ arbitrario se verifica

$$g(h(x)) = g\left(\sum_{i\in F_x} \lambda_i h(a_i)\right) = \sum_{i\in F_x} \lambda_i g(n_i) = \sum_{i\in F_x} \lambda_i \varphi(a_i) = \varphi\left(\sum_{i\in F_x} \lambda_i a_i\right) = \varphi(x).$$

Tenemos así que $g \circ h = \varphi$.

Proposición 2.4.3. *M es un A-módulo proyectivo si, y sólo si, M es suma directa de un A-módulo libre.*

Prueba. ($\Rightarrow$) Sabemos que existe $I \subset M$ tal que

$$\begin{array}{rrcl} \pi: & A^{(I)} & \longrightarrow & M \\ & e_i & \longmapsto & m_i \end{array}$$

es un homomorfismo bien definido y suprayectivo (basta tomar al propio M como sistema de generadores). Surge así de manera natural la siguiente sucesión exacta

$$0 \to \operatorname{Ker}\pi \overset{i}{\hookrightarrow} A^{(I)} \overset{\pi}{\to} M \to 0.$$

Por hipótesis, M es A-módulo proyectivo, es decir, tomando $\pi \in \operatorname{Hom}_A(A^{(I)}, M)$ suprayectivo y $1_M \in \operatorname{Hom}_A(M, M)$, existe $h \in \operatorname{Hom}_A(M, A^{(I)})$ tal que $\pi \circ h = 1_M$; es decir, por 2.3.9 la sucesión anterior es escindida y $A^{(I)} \cong \operatorname{Ker}\pi \oplus M$. □

Ahora, supongamos que $N \in \operatorname{Obj}(\operatorname{Mod}_A)$ es tal que, si la sucesión

$$0 \longrightarrow M' \overset{f}{\longrightarrow} M$$

es exacta, entonces la sucesión

$$\operatorname{Hom}_A(M, N) \overset{\operatorname{Hom}_A(f,N)}{\longrightarrow} \operatorname{Hom}_A(M', N) \longrightarrow 0$$

también lo es; es decir, para cualquier $\varphi \in \operatorname{Hom}_A(M', N)$, existe $\Phi \in \operatorname{Hom}_A(M, N)$ de forma que $\varphi = \Phi \circ f$. Por ser f inyectiva, podemos interpretar M' como un submódulo de M (entender f como una inclusión) y, por esto, nuestro problema se trata de un problema de extensión.

Esta extensión no va a ser posible en general como muestra el siguiente ejemplo.

Ejemplo 2.4.4. Sea $n \in \mathbb{Z}$ y consideremos $\langle n \rangle \subset \mathbb{Z}$ submódulo. Si definimos la aplicación

$$\begin{array}{rcl} \langle n \rangle & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & 1_{\mathbb{Z}} \\ \lambda n & \longmapsto & \lambda \end{array},$$

se comprueba que no puede extenderse a $\mathbb{Z}$.

Surge la siguiente definición.

Definición 2.4.5. Diremos que $N \in \mathrm{Obj}(\mathrm{Mod}_A)$ es un A-módulo inyectivo si, para cualesquiera $M, M' \in \mathrm{Obj}(\mathrm{Mod}_A)$, $f \in \mathrm{Hom}_A(M', M)$ inyectiva y $\varphi \in \mathrm{Hom}_A(M', N)$, se tiene que existe $\Phi \in \mathrm{Hom}_A(M, N)$ de forma que $\varphi = \Phi \circ f$.

2.5 Producto tensorial de módulos

La motivación de la construcción que vamos a desarrollar en esta sección es poder estudiar formas bilineales (multilineales) a través de formas lineales, cuyas propiedades conocemos mejor. Para ello, vamos a construir una estructura relacionada con el producto cartesiano de módulos llamada *producto tensorial.* Antes de proseguir, recordamos definiciones.

Definición 2.5.1. Sean M, N y P A-módulos. Una aplicación$\Phi : M \times N \longrightarrow P$ se dice A-bilineal si se verfican las siguientes condiciones.

1) Para cada $m_1, m_2 \in M$, $n \in N$, $\Phi(m_1 + m_2, n) = \Phi(m_1, n) + \Phi(m_2, n)$

2) Para cada $m \in M$, $n_1, n_2 \in N$, $\Phi(m, n_1 + n_2) = \Phi(m, n_1) + \Phi(m, n_2)$

3) Para cada $m \in M$, $n \in N$, $\lambda \in A$, $\Phi(\lambda m, n) = \Phi(m, \lambda n) = \lambda\Phi(m, n)$

Observación 2.5.2. Análogamente, podemos definir el concepto de aplicaciones multilineales de la siguiente forma. Dados $M_1, \ldots, M_r$ A-módulos,

$$\Phi : M_1 \times \cdots \times M_r \longrightarrow P$$

se dice multilineal si para cada $i \in \{1, \ldots, r\}$

- $\Phi(m_1, \ldots, m_i + m_i', \ldots, m_r) = \Phi(m_1, \ldots, m_i, \ldots, m_r) + \Phi(m_1, \ldots, m_i', \ldots, m_r)$
- $\Phi(m_1, \ldots, \lambda m_i, \ldots, m_r) = \lambda\Phi(m_1, \ldots, m_i, \ldots, m_r)$

Con $\lambda \in A$ y $m_j \in M_j$ para cada $j \in \{1, \ldots, r\}$

Observación 2.5.3. Si M, M' son A-módulos, $g : M \to M'$ es suprayectiva, y $N \subset \operatorname{Ker} g$, entonces el siguiente diagrama conmuta

$$\begin{tikzcd}
m \arrow[d, mapsto] & M \arrow[d, two heads] \arrow[drr, "g"] & & & \\
m + \operatorname{Ker} g & M/\operatorname{Ker} g \arrow[rr] & & M' & g(m) \\
m + N \arrow[u, mapsto] & M/N \arrow[u, two heads] \arrow[urr] & & &
\end{tikzcd}$$

Proposición 2.5.4. *Dados dos A-módulos M y N, existe un A-módulo $M \otimes_A N$ y una aplicación A-bilineal $\delta : M \times N \to M \otimes_A N$ tal que para cada A-módulo P y para cada $F : M \times N \to P$ A-bilineal, existe una única aplicación A-lineal $f : M \otimes_A N :\to P$ tal que $f \circ \delta = F$.*

Además, el par $(\delta, M \otimes_A N)$ es único, en el sentido que de existir otro par (δ', T) que verifique las condiciones del enunciado, se tiene que $T \cong M \otimes_A N$.

Prueba. Para ver la unicidad, supongamos que (δ, T) y (δ', T') cumplen las condiciones de la proposición. Poniendo a T' como P y a δ' como F, el resultado garantiza la existencia de $j : T \to T'$ tal que $\delta' = j \circ \delta$. Intercambiando los roles de T y T', se tiene $j' : T' \to T$ tal que $\delta = j' \circ \delta'$. Entonces, cada una de las composiciones $j \circ j'$ y $j' \circ j$ son la identidad, lo cual garantiza que j sea un isomorfismo.

Para la existencia, procedemos como sigue. Consideremos $A^{(M \times N)}$, la suma directa de A tantas veces como elementos tenga $M \times N$. Definimos el siguiente subconjunto de $A^{(M \times N)}$

$$\begin{aligned} S = \{ & e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}, e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}, \\ & e_{(m,\lambda n)} - \lambda e_{(m,n)}, e_{(\lambda m,n)} - \lambda e_{(m,n)} \} \end{aligned} \tag{2.6}$$

con $m, m' \in M$, $n, n' \in N$ y $\lambda \in A$.

Ahora tomamos Σ el submódulo generado por S. Se cumple $\Sigma \subset A^{(M \times N)}$, luego podemos definir el cociente $A^{(M \times N)}/\Sigma$, que es un A-módulo:

$$\begin{array}{ccc} M \times N & \xrightarrow{\delta} & M \otimes_A N := A^{(M \times N)} / \Sigma \\ (m, n) & \longmapsto & [e_{(m,n)}] \end{array}$$

La aplicación δ es bilineal por construcción. Además, $\{[e_{(m,n)}] : (m,n) \in M \times N\}$ es un sistema de generadores de $M \otimes_A N$.

Cada aplicación $f : M \times N \to P$ se extiende por linealidad a un homomorfismo de A-módulos $f : A^{(M\times N)} \to P$, tomando $f(e_{(m,n)}) = f(m,n)$, $f(e_{(m,n)} + e_{(m,n)}) = f(m,n) + f(m',n')$, y $f(\lambda e_{(m,n)}) = \lambda f(m,n)$. En particular, dada $F : M \times N \to P$ es bilineal, definimos el homomorfismo de A-módulos

$$\begin{array}{rrcl} f_0 : & A^{M\times N} & \longrightarrow & P \\ & e_{(m,n)} & \longmapsto & F(m,n) \end{array}$$

Para poder pasar al cociente solo hemos de comprobar que $\Sigma \subset ker(f_0)$. Como Σ está generado por S, basta ver $S \subset ker(f_0)$. Pero esto es directo por ser F bilineal y la definición de S. Por ejemplo,

$$f_0(e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}) = F(e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}) = 0$$

. Así, la siguiente aplicación está bien definida y cumple las condiciones del teorema

$$\begin{array}{rrcl} \tilde{f}_0 : & A^{M\times N}/\Sigma & \longrightarrow & P \\ & [e_{(m,n)}] & \longmapsto & F(m,n) \end{array}$$

$\square$

Definición 2.5.5. Al A-módulo $M \otimes N$ se le llama *producto tensorial* de M y N.

Observación 2.5.6. Observamos que la construcción es de lo más natural. Otra forma de escribir la construcción es pensar que hemos tomado todos los elementos del producto cartesiano de la forma $(m+m',n) - (m,n) - (m',n), (m,n+n') - (m,n) - (m,n'), (m,\lambda n) - \lambda(m,n), \lambda(m,n) - \lambda(m,n)$, es decir, hemos seleccionado unas relaciones que queremos que se cumplan (de bilinealidad). Al cocientar por el módulo que generan, estamos imponiendo que cada uno de esos elementos sea 0, que $[(m+m',n)] = [(m,n)] + [(m',n)]$, etc.

Observación 2.5.7. De ahora en adelante omitiremos el subíndice de $\otimes_A$, escribiendo $M \otimes N$ siempre que no de lugar a confusión. Entonces

1. A las clases $[e_{(m,n)}]$ se les denota $m \otimes n$.

   Todo elemento de $M \otimes N$ es suma $\sum_{i=1}^{r} m_j \otimes n_j$, para ciertos $m_j \in M$, $n_j \in N$ y $r \in \mathbb{N}$, ya que $[\lambda e_{(m,n)}] = [e_{(\lambda m,n)}] = [e_{(m,\lambda n)}]$ por la definición inicial de S.

2. Las aplicaciones bilineales de $M \times N$ en P, $\mathrm{Bil}_A(M \times N, P)$ están en correspondencia biyectiva con $\mathrm{Hom}_A(M \otimes N, P)$.

   En particular, si tomamos A como K cuerpo y M y N K-espacios vectoriales,

$$\mathrm{Hom}_A(M \otimes_K N, K) = (M \otimes_K N)^* = \mathrm{Bil}_K(M \times N, K)$$

3. La construcción del producto tensorial de módulos se puede generalizar. Dados unos A-módulos $M_1, \dots, M_r$, existe un A-módulo $M_1 \otimes \cdots \otimes M_r$ y $\delta : M_1 \times \cdots \times, M_r \longrightarrow M_1 \otimes \cdots \otimes M_r$ multilineal tal que para cualquier aplicación A-multilineal $\Phi : M_1 \times \cdots \times, M_r \longrightarrow P$, existe una única $f : M_1 \otimes \cdots \otimes M_r \longrightarrow P$ A-lineal tal que $f \circ \delta = F$

Lema 2.5.8. *Sean Z y Z' dos A-módulos. Sea $\{z_i\}_{i\in I}$ un sistema de generadores de Z y sea $\{z'_j\}_{j\in J}$ un sistema de generadores de Z'. Entonces, $\{z_i \otimes z_j : (i,j) \in I \times J\}$ es un sistema de generadores de $Z \otimes Z'$.*

Proposición 2.5.9. *Sea A un anillo conmutativo unitario. Se cumple:*

1. *Dados M, N y P A-módulos,*

$$M \otimes N \otimes P \cong (M \otimes N) \otimes P$$

2. $M \otimes N = N \otimes M$

3. *Dados $f : M_1 \to M_2$ y $g : N_1 \to N_2$ A-lineales, existe $f \otimes g : M_1 \otimes N_1 \to M_2 \otimes N_2$ A-lineal tal que si tenemos $f' : M_2 \to M_3$ y $g' : N_2 \to N_3$ homomorfismos de A-módulos,*

$$M_1 \otimes N_1 \xrightarrow{f\otimes g} M_2 \otimes N_2 \xrightarrow{f'\otimes g'} M_3 \otimes N_3$$

   se cumple

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$$

4. *Si B es un A-álgebra, $B \otimes M$ es un B-módulo*

5. *Si B y C son A-álgebras, $B \otimes C$ es un A-álgebra, un B-módulo y un C-módulo*

6. *Para todo P A-módulo, se verifica $P \otimes_A A \cong P$ mediante el siguiente isomorfismo de A-módulos*

$$\begin{array}{rcl} P & \longrightarrow & P \otimes_A A \\ p & \longmapsto & p \otimes_A 1_A \end{array}$$

7. *Sean $\{ N_i \}_{i\in I}$ y M A-módulos. Se cumple que*

$$M \otimes_A \left(\bigoplus_{i\in I} N_i \right) \cong \bigoplus_{i\in I} (M \otimes_A N_i).$$

En particular,

$$M \otimes_A A^{(I)} \cong \bigoplus_{i\in I} (M \otimes_A A) \cong M^{(I)}.$$

Prueba. Comprobamos cada cosa.

1. Definimos la aplicación A-trilineal

$$\begin{array}{rccc} F: & M \times N \times P & \longrightarrow & (M \otimes N) \otimes P \\ & (m,n,p) & \longmapsto & (m \otimes n) \otimes p \end{array}$$

Existe una única $f : M \otimes N \otimes P \to (M \otimes N) \otimes P$ tal que $f(m \otimes n \otimes p) = F(m,n,p) = (m \otimes n) \otimes p$,

$$\begin{tikzcd} M \times N \times P \arrow[r, "F"] \arrow[d] & (M \otimes N) \otimes P \\ M \otimes N \otimes P \arrow[ur, "f"'] & \end{tikzcd}$$

Veamos como definir la flecha en sentido contrario. Para cada $p \in P$ definimos la aplicación A-bilineal

$$\begin{array}{rccc} \Phi_p: & M \times N & \longrightarrow & M \otimes N \otimes P \\ & (m,n) & \longmapsto & m \otimes n \otimes p \end{array}$$

Existe una única $\varphi_p : M\otimes N \to M\otimes N\otimes P$ tal que $\varphi_p(m\otimes n) = \Phi_p(m,n) = m\otimes n\otimes p$

$$\begin{tikzcd} M \times N \arrow[r, "\Phi_p"] \arrow[d] & M \otimes N \otimes P \\ M \otimes N \arrow[ur, "\varphi_p"'] & \end{tikzcd}$$

Observamos que si $p, p' \in P$, entonces $\varphi_p + \varphi_{p'} = \varphi_{p+p'}$ por unicidad ya que ambas completan el diagrama: $\varphi_p(m \otimes n) + \varphi_{p'}(m \otimes n) = m \otimes n \otimes p + m \otimes n \otimes p' = m \otimes n \otimes (p + p') = \varphi_{p+p'}(m \otimes n)$. Lo mismo ocurre con $\lambda\varphi_p = \varphi_{\lambda p}$.

Sea entonces la aplicación A-bilineal

$$\begin{array}{rrcl} G: & (M \otimes N) \times P & \longrightarrow & M \otimes N \otimes P \\ & (z, p) & \longmapsto & \varphi_p(z) \end{array}$$

Existe una única $g : (M \otimes N) \otimes P \to M \otimes N \otimes P$ aplicación A-lineal que hace conmutativo el diagrama siguiente

$$\begin{tikzcd} (M \otimes N) \times P \arrow[r, "G"] \arrow[d] & M \otimes N \otimes P \\ (M \otimes N) \otimes P \arrow[ur, "g"'] & \end{tikzcd}$$

Veamos entonces que la composición de ambas es la identidad. Para ello solo hace falta ver que deja los generadores de cada A-módulo invariantes. Efectivamente,

$$\begin{array}{c} M \otimes N \otimes P \xrightarrow{f} (M \otimes N) \otimes P \xrightarrow{g} M \otimes N \otimes P \\ m \otimes n \otimes p \longmapsto (m \otimes n) \otimes p \longmapsto m \otimes n \otimes p \end{array}$$

Por tanto, $g \circ f = Id_{M \otimes N \otimes P}$

Por otro, $\{m \otimes n : (m, n) \in M \times N\}$ es sistema de generadores de $M \otimes N$. Por el lema 2.5.8, $\{(m \otimes n) \otimes p : (m, n, p) \in M \times N \times P\}$ es sistema de generadores de $(M \otimes N) \otimes P$. Evaluando, $(f \circ g)((m \otimes n) \otimes p) = (m \otimes n) \otimes p)$ y concluimos $f \circ g) = Id_{(M \otimes N) \otimes P}$.

2. Siguiendo el esquema de *1*, solo hay que definir las aplicaciones naturales $M \times N \to N \otimes M$ que llevan $(m, n) \mapsto n \otimes m$ y la análoga en la otra dirección, que pasan al producto tensorial, y cuya composición resulta en la identidad. Para comprobar esto último solo hay que verlo para los generadores que es trivial.

3. Definimos la aplicación A-bilineal $M_1 \times N_1 \to M_2 \times N_2$ dada por $(m_1, n_1) \mapsto f(m_1) \otimes g(n_1)$. Entonces existe una única $M_1 \otimes N_1 \to M_2 \otimes N_2$ lineal que completa el diagrama conmutativo habitual.

Lo mismo sucede con $M_2 \times N_2 \to M_3 \times N_3$, de forma que obtenemos el diagrama

$$\begin{tikzcd}
M_1 \otimes N_1 \arrow[r, "f_1 \otimes g_1"] \arrow[rr, bend right, "(f_2 \otimes g_2) \circ (f_1 \otimes g_1)"'] & M_2 \times N_2 \arrow[r, "f_2 \otimes g_2"] & M_3 \times N_3
\end{tikzcd}$$

Podemos definir la aplicación A-bilineal $M_1 \times N_1 \to M_3 \otimes N_3$ dada por $(m_1, n_1) \mapsto (f_2 \circ f_1)(m_1) \otimes (g_2 \circ g_1)(n_1)$, y así existe una única aplicación $M_1 \otimes N_1 \to M_3 \otimes N_3$ que cierra el diagrama conmutativo, y por unicidad ha de coincidir con la composición de arriba.

4. Queremos definir un producto externo. Empezamos definiendo para cada $b \in B$ la aplicación A-lineal $\Phi_b : B \times M \to B \otimes M$ dada por $(b', m) \mapsto bb' \otimes m$. Entonces existe una única aplicación lineal del producto tensorial que cierra el diagrama

$$\begin{tikzcd}
B \times M \arrow[r, "\Phi_p"] \arrow[d] & B \otimes M \\
B \otimes M \arrow[ur, "\varphi_p"'] &
\end{tikzcd}$$

Se cumple que $\varphi_{b_1+b_2} = \varphi_{b_1} + \varphi_{b_2}$ y que $\varphi_{b_1 b_2} = \varphi_{b_1} \circ \varphi_{b_2}$ por la unicidad. De esta forma podemos definir la aplicación

$$\Phi : B \times (B \otimes M) \to B \otimes M \tag{2.7}$$
$$(b, z) \mapsto \varphi_b(z) \tag{2.8}$$

que está bien definida y con la cual $B \otimes M$ cumple los axiomas de A-módulo.

7. Denotemos por $n_i \in \oplus_{i \in I} N_i$ al elemento tal que tiene a $n \in N_i$ por i-ésima coordenada y 0 en el resto. Definamos la aplicación

$$\begin{array}{rccc} F: & M \times (\oplus_{i \in I}) & \longrightarrow & \oplus_{i \in I}(M \otimes_A N_i) \\ & (m, n_i) & \longmapsto & (m \otimes n)_i \end{array}.$$

Esta aplicación es bilineal por serlo para el sistema de generadores

$$\begin{aligned}
F(\lambda m, n_i) = (\lambda m \otimes n)_i =& (m \otimes \lambda n)_i = F(m, \lambda n) \\
=& \lambda(m \otimes n)_i = \lambda F(m, n_i), \\
F(m_1 + m_2, n_i) =& ((m_1 + m_2) \otimes n)_i = \\
=& (m_1 \otimes n)_i + (m_2 \otimes n)_i = F(m_1, n_i) + F(m_2, n_i) \quad \text{y} \\
F(m, (n_1 + n_2)_i) =& (m \otimes (n_1 + n_2))_i = \\
=& (m \otimes n_1)_i + (m \otimes n_2)_i = F(m, n_{1i}) + F(m, n_{2i}).
\end{aligned}$$

Es por esto que existe

$$f: \quad M \otimes_A (\oplus_{i \in I} N_i) \quad \longrightarrow \quad \oplus_{i \in I}(M \otimes_A N_i)$$

aplicación A-lineal. En el otro sentido comenzamos definiendo para cada $i \in I$ las aplicaciones

$$\begin{array}{rccc} G_i: & M \times N_i & \longmapsto & M \otimes (\oplus_{i \in I} N_i) \\ & (m, n) & \longmapsto & m \otimes n_i \end{array},$$

que son A-bilineales de nuevo por la propia definición. Así, surgen las apliciones A-lineales

$$g_i \quad M \otimes N_i \quad \longrightarrow \quad M \otimes (\oplus_{i \in I} N_i) \ ,$$

que nos permiten definir a su vez la siguiente aplicación A-lineal

$$g := \oplus_{i \in I} g_i : \quad \oplus(M \otimes_A N_i) \quad \longrightarrow \quad M \otimes_A (\oplus_{i \in I} N_i) \ .$$

Se comprueba que $g \circ f = 1_{M \otimes_A (\oplus N_i)}$ y $f \circ g = 1_{\oplus(M \otimes_A N_i)}$ y se tiene el resultado.

Para ver el caso particular, basta aplicar lo que acabamos de probar y la propiedad 6 del producto tensorial.

□

En estas construcciones se tienen las siguientes propiedades.

1) Dados M_1, M_2 y M_3 A-módulos, $M_1 \otimes M_2 \otimes M_3 \cong (M_1 \otimes M_2) \otimes M_3 \cong M_1 \otimes (M_2 \otimes M_3)$

2) $M \otimes N = N \otimes M$

3) Dados $f: M_1' \to M_1$ y $g: M_2' \to M_2$ A-lineales, existe $f \otimes g: M_1' \otimes M_2' \to M_1 \otimes M_2$ A-lineal tal que el diagrama es conmutativo.

   En particular, si $M \in Obj(Mod_A)$, $M \otimes \_$ es un funtor covariante de Mod_A en Mod_A (Véase Apéndice A)

Ahora, dado un A-módulo M, consideremos el funtor

$$\begin{array}{ccc} Mod_A & \overset{M\oplus_A\_}{\longrightarrow} & Mod_A \\ N & \longmapsto & M \oplus_A N \end{array}$$

y estudiemos su comportamiento respecto de sucesiones exactas. Antes de comenzar, cabe destacar que estudiar este funtor es equivalente a estudiar el funtor $\_ \oplus_A M$ debido al isomorfismo existente $M \oplus_A N \cong N \oplus_A M$.

Proposición 2.5.10. *Sea M un A-módulo y sea*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0 \tag{2.9}$$

una sucesión exacta. Se cumple que

$$M \otimes_A N' \overset{1_M \otimes f}{\longrightarrow} M \otimes_A N \overset{1_M \otimes g}{\longrightarrow} M \otimes_A N'' \longrightarrow 0 \tag{2.10}$$

es también una sucesión exacta.

Prueba. Sabemos que (2.9) es exacta si, y sólo si, para todo P A-módulo se tiene que la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(M \oplus_A N'', P) \overset{(1_M \oplus g)^*}{\longrightarrow} \mathrm{Hom}_A(M \oplus_A N, P) \overset{(1_M \oplus f)^*}{\longrightarrow} \mathrm{Hom}_A(M \oplus_A N', P) \tag{2.11}$$

es exacta.

La sucesión

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \overset{(g^{*_P})_{*_M}}{\longrightarrow} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \overset{(f^{*_P})_{*_M}}{\longrightarrow} \\ \overset{(f^{*_P})_{*_M}}{\longrightarrow} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)), \end{aligned}$$

donde $(f^{*_P})_{*_M} := \mathrm{Hom}_A(M, \mathrm{Hom}_A(f, P))$ y $(g^{*_P})_{*_M} := \mathrm{Hom}_A(M, \mathrm{Hom}_A(g, P))$, surge de aplicar en primer lugar el funtor $\mathrm{Hom}_A(\_, P)$ a la sucesión 2.9 y, después, aplicar el funtor $\mathrm{Hom}_A(M, \_)$ al resultado anterior. Así, 2.3.10 nos dice que es exacta.

Observemos ahora que, para cada $X \in \{ N, N', N'' \}$ se tiene la cadena de isomorfismos de A-módulos

$$\mathrm{Hom}_A(M \otimes_A X, P) \cong \mathrm{Bil}_A(M \times X, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P)).$$

El primero de los isomorfismos es inmediato atendiendo a la propia definición del producto tensorial: Dada $F \in \mathrm{Bil}_A(M \times X, P)$, existe una única $\bar{F} \in \mathrm{Hom}_A(M \otimes$

$X, P)$ de forma que para cada par $(m, x) \in M \times X$ se verifica $\bar{F}(m \otimes_A x) = F(m, x)$. Comprobemos el segundo de los isomorfismos. En primer lugar, definamos

$$\begin{array}{rcl} \mathrm{Bil}_A(M \times X, P) & \longrightarrow & \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P)) \\ F(m, n) & \longmapsto & (\varphi_F(m))(n) := F(m, n) \end{array}.$$

Dados $F, G \in \mathrm{Bil}_A(M \times X, P)$ y $\lambda \in A$ tenemos

- $(F + G)(n, m) = F(m, n) + G(m, n)$ y
- $(\lambda F)(m, n) = \lambda F(m, n)$.

Por otro lado, definamos

$$\begin{array}{rcl} \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P)) & \longrightarrow & \mathrm{Bil}_A(M \times X, P) \\ \varphi(m)(n) & \longmapsto & F_\varphi(m, n) := \varphi(m)(n) \end{array}.$$

Veamos que la aplicación es bilienal. Sean $\varphi \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P))$, $\{ m, m_1, m_2 \} \subset M$, $\{ n, n_1, n_2 \} \subset X$ y $\lambda \in A$. Tenemos

- $\varphi(m_1 + m_2)(n) = (\varphi(m_1) + \varphi(m_2))(n) = \varphi(m_1)(n) + \varphi(m_2)(n)$,
- $\varphi(m)(n_1 + n_2) = \varphi(m)(n_1) + \varphi(m)(n_2)$ y
- $\varphi(\lambda m)(n) = (\lambda\varphi)(m)(n) = \lambda\varphi(m)(n) = \varphi(m)(\lambda n)$.

Vemos así que ambas aplicaciones son A-lineales. Por último, sean $F \in \mathrm{Bil}_A(M \times X, P)$ y $\varphi \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P))$ y veamos que la una es la inversa de la otra. Se tiene

- $\varphi_{F_\varphi}(m)(n) = F_\varphi(m, n) = \varphi(m)(n)$ y
- $F_{\varphi_F}(m, n) = \varphi_F(m)(n) = F(m, n)$.

Denotemos $\Phi_X : \mathrm{Hom}_A(M \otimes_A X, P) \longrightarrow \mathrm{Hom}_A(M, \mathrm{Hom}_A(X, P))$, para cada $X \in \{N, N', N''\}$, a cada uno de los isomorfismos definidos. Estos isomorfismos implican que por ser (**??**) exacta (2.11) es también exacta. Para probar esto es suficiente ver que se tienen las igualdades

$$(1_M \otimes g)^* = {\Phi_N}^{-1} \circ (g^*)_* \circ \Phi_{N''}$$

y

$$(1_M \otimes f)^* = {\Phi'_N}^{-1} \circ (f^*)_* \circ \Phi_N.$$

Probemos la primera de las igualdades. Dado $F \in \mathrm{Hom}_A(M \oplus N'', P)$, $\Phi_{N''}(F) := \varphi_F \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N'', P))$ y

$$(g^*)_*(\varphi_F(m)(n)) = g^*(\varphi_F(m))(n) = \varphi_F(m)(g(n))$$

para cada $m \oplus n \in M \oplus_A N$. Por último,

$${\Phi_N}^{-1}(\varphi_F(m)(g(n))) = F(m \oplus g(n))$$

y

$$F(m \oplus g(n)) = F((1_M \oplus g)(m \oplus n)).$$

Dado que $m \oplus n \in M \oplus_A N''$ era arbitrario, tenemos la igualdad que buscábamos. El caso de la f es análogo. $\square$

Definición 2.5.11. Se dice que un A-módulo M es plano si, y sólo si, el funtor $M \otimes_A \_\_$ es exacto, i.e, conserva sucesiones exactas.

Antes de continuar con la siguiente proposición, observemos lo siguiente: dados M, N A-módulos y $N' \subset N$ submódulo, un elemento $m \otimes_A n' \in M \otimes_A N'$ puede considerarse como un elemento en $M \otimes_A N'$ y como un elemento en $M \otimes_A N$ haciendo uso de la inclusión

$$M \otimes_A N' \overset{i}{\hookrightarrow} M \otimes_A N;$$

sin embargo, de la pertenencia $m \otimes_A n' \in M \otimes_A N'$ no se sigue necesariamente la igualdad $i(m \otimes_A n') = m \otimes_A n$.

Ejemplo 2.5.12. Consideremos los $\mathbb{Z}$-módulos $M := \mathbb{Z}$, $N = N' := \mathbb{Z}/2\mathbb{Z}$ y $M' := 2\mathbb{Z}$ (submódulo de $\mathbb{Z}$). Tomemos $x \in N \setminus \{0\}$:

- por un lado, $2 \otimes_{\mathbb{Z}} x = 1 \otimes_{\mathbb{Z}} 2x = 0_{M \otimes N}$,
- sin embargo, por otro lado el elemento $2 \otimes_{\mathbb{Z}} x$ no es $0_{M' \otimes N'}$.

Proposición 2.5.13. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes.*

1. *M es un A-módulo plano.*
2. *Para toda sucesión corta exacta*

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0,$$

la sucesión

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1 \otimes f} M \otimes_A N \xrightarrow{1 \otimes g} M \otimes_A N'' \longrightarrow 0$$

es exacta.

3. *Para cualesquiera dos A-módulos N y N' y cualquier sucesión exacta corta*

$$0 \longrightarrow N' \xrightarrow{f}, N$$

la sucesión

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1\otimes f} M \otimes_A N$$

es exacta.

4. *Para cualesquiera dos A-módulos N y N' finitamente generados y cualquier sucesión exacta corta*

$$0 \longrightarrow N' \xrightarrow{f}, N$$

la sucesión

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1\otimes f} M \otimes_A N$$

es exacta.

Prueba. En primer lugar, $(1 \Leftrightarrow 2)$ basta con aplicar la definición de módulo plano para $(1 \Rightarrow 2)$ y tener en cuenta que toda sucesión exacta larga se puede escindir en sucesiones exactas cortas para $(2 \Rightarrow 1)$. También son claras las implicaciones $(2 \Rightarrow 3)$ y $(3 \Rightarrow 4)$. Probemos $(3 \Rightarrow 2)$ y $(4 \Rightarrow 3)$.

$(3 \Rightarrow 2)$. Sean M, N y N' A-módulos y consideremos una sucesión exacta arbitraria

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0.$$

En primer lugar, aplicando (**??**) tenemos que $\mathrm{im}(1 \otimes f) = \mathrm{Ker}\,(1 \otimes g)$ y que $1 \otimes g$ es sobreyectiva. Por otro lado, del hecho de que la sucesión que hemos tomado sea exacta se desprende que, en concreto,

$$0 \longrightarrow N' \xrightarrow{f} N$$

es también exacta; así, por hipótesis tenemos que $1 \otimes f$ es inyectiva.

Con todo, resulta que la sucesión

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1\otimes f} M \otimes_A N \xrightarrow{1\otimes g} M \otimes_A N'' \longrightarrow 0$$

es también exacta.

$(4 \Rightarrow 3)$. Sean N, N' A-módulos y $f : N' \longrightarrow N$ una aplicación A-lineal e inyectiva. Tomemos $z := \sum_{i=1}^{r} m_i \otimes_A n_i \in M \otimes_A N'$ tal que $f(z) = 0_{M\otimes_A N}$, esto ocurre si, y sólo si, $\sum_{i=1}^{r} m_i \otimes_A f(n_i) = 0_{M\otimes_A N}$ o, lo que es lo mismo

$$e_{(m_1,f(n_1))} + \cdots + e_{(m_r,f(n_r))} \in \Sigma.$$

Esta pertenencia nos garantiza la existencia de ciertos $\{\, \mathrm{rel}_1, \dots, \mathrm{rel}_s \,\} \subset \Sigma$ tales que

$$e_{(m_1, f(n_1))} + \cdots + e_{(m_r, f(n_r))} = \sum_{i=1}^{s} \lambda_i \mathrm{rel}_i \qquad \lambda_i \in A \ \forall\ i \in \{1, \dots, s\}$$

Definamos ahora los menores submódulos de N y de N' que contengan a los conjuntos $\{\, \mathrm{rel}_1, \dots, \mathrm{rel}_s, f(n_1), \dots, f(n_r) \,\}$ y $\{\, n_1, \dots, n_r \,\}$ respectivamente. Denotemos al primero por N_{red} y al segundo, $N_{\mathrm{red}}{}'$.

Es claro que $f_{|N_{\mathrm{red}}{}'} : N_{\mathrm{red}}{}' \longrightarrow N_{\mathrm{red}}$ está bien definida y es inyectiva. Así, por la hipótesis, se tiene que la sucesión

$$0 \longrightarrow M \otimes_A N_{\mathrm{red}}{}' \overset{1\otimes f_{|N_{\mathrm{red}}{}'}}{\longrightarrow M} \; M \otimes N_{\mathrm{red}}$$

es exacta. Así, denotando por z_{red} al elemento z visto en $M \otimes_A N_{\mathrm{red}}{}'$, se tiene que $f(z_{\mathrm{red}}) = 0_{M \otimes_A N_{\mathrm{red}}}$, es decir, $z_{\mathrm{red}} = 0_{M \otimes_A N_{\mathrm{red}}{}'}$. Si ahora consideramos el homomorfismo inclusión

$$M \otimes_A N_{\mathrm{red}}{}' \overset{i}{\hookrightarrow} M \otimes_A N',$$

en este caso, por ser homomorfismo sí se puede concluir que $i(z_{\mathrm{red}}) = z = 0_{M \otimes_A N'}$.

$\square$

Observación 2.5.14. *1)* Sean M y N dos A-módulos. El mismo argumento empleado en la implicación ($4 \Rightarrow 3$) de la prueba anterior prueba que, tras la adaptación necesaria, si $\sum_{i=1}^{r} m_i \otimes_A n_1 = 0_{M \otimes_A N}$, existen $M' \subset M$ y $N' \subset N$ submódulos finitamente generados que contienen a los conjutos $\{\, m_i \,\}$ y $\{\, n_i \,\}$ respectivamente, tales que $\sum_{i=1}^{r} m_i \otimes_A n_i = 0_{M' \otimes N'}$. De nuevo, hay que destacar que no necesariamente se tiene $M' \otimes_A N' \subset M \otimes_A N$.

Ejemplo 2.5.15. Denotemos respectivamente por M_0 y N_0 a los submódulos M' y N' de la observación anterior y mantengamos la notación de **??**.

Es claro que $M_0 \supset M'$ y $N_0 \supset N'$ pues si $z = 0_{M_0 \otimes N_0}$ y $M_0 \subset M'$ y $N_0 \subset N'$ también debe ser $0_{M' \otimes N'}$. En primer lugar, si $x \neq 0_N$, el menor submódulo generado por x es el propio N. Así, $N_0 = N = N'$. Supongamos ahora M_0 generado por los elementos $\{\, m_1, \dots, m_r \,\}$. La inclusión antes mencionada implica $m_i | 2$ para toda $i \in \{\, 1, \dots, r \,\}$, es decir, $m_i = 1$ o $m_i = 2$. Por esto, existe $i \in \{\, 1, \dots, r \,\}$ tal que $m_i = 1$ y $\mathbb{Z} = \langle 1 \rangle \subset M_0$.

Así, los únicos submódulos M_0 y N_0 que verifican las condiciones del consecuente de la observación anterior son $\mathbb{Z}$ y $\mathbb{Z}/2\mathbb{Z}$.

Teorema 2.5.16. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes.*

1. M es un A-módulo plano.

2. Para cualesquiera N' y N A-módulos y $f : N' \longrightarrow N$ inyectiva,

$$1_M \otimes f : M \otimes N' \longrightarrow M \otimes N$$

es inyectiva.

2'. Para cualesquiera N' y N A-módulos finitamente generados y $f : N' \longrightarrow N$ inyectiva,

$$1_M \otimes f : M \otimes N' \longrightarrow M \otimes N$$

es inyectiva.

3. Si

$$\sum_{i=1}^{n} a_i m_i = 0_A$$

para ciertos $a_i \in A$ y $m_i \in N$, entonces existen ${m_j}' \in M$ de forma que para cada i se tiene

$$m_i = \sum_{j=1}^{s} \lambda_{ij} {m_j}', \qquad \lambda_{ij} \in A$$

y para cada j se verifica

$$\sum_{i=1}^{n} \lambda_{ij} a_i = 0.$$

4. Si $\mathfrak{a} \in A$ es un ideal, entonces la aplicación

$$\begin{array}{ccll} \mathfrak{a} \otimes_A M & \longrightarrow & M & \textit{entendido como } A \otimes_A M \\ \sum_{i\in F} a_i \otimes_A m_i & \longmapsto & \sum_{i \in F} a_i m_i & \end{array}$$

es inyectiva.

Observación 2.5.17. *1.* Sean A un anillo conmutativo y unitario, I un conjunto de índices, N y N' A-módulos y $f : N' \longrightarrow N$ una aplicación A-lineal inyectiva. Se verifica que la aplicación

$$1_{A^{(I)}} \otimes_A f : A^{(I)} \otimes N \longrightarrow A^{(I)} \otimes_A N$$

es también inyectiva.

Dado que $A^{(I)} \otimes_A N \cong \oplus_{i\in I} N$ y $A^{(I)} \otimes_A N' \cong \oplus_{i \in I} N'$, basta comprobar que la aplicación

$$\oplus_{i\in I} f : \oplus_{i\in I} N' \longrightarrow \oplus_{i\in I} N$$

es inyectiva.

2. Si B es plano y $\mathfrak{a} \subset A$ un ideal, entonces la cuarta afirmación del teorema anterior nos da el isomorfismo de A-módulos

$$\mathfrak{a}^e \cong \mathfrak{a} \otimes_A B.$$

Lema 2.5.18. *Sean M y N A-módulos, donde $N := \langle n_1, \dots, n_r \rangle_A$. Si se tiene una relación en $M \otimes_A N$ de forma que*

$$\sum_{i=1}^{r} m_i \otimes n_i = 0_{M \otimes_A N},$$

entonces existen elementos $m_j{}' \in M$ y $\mu_{ij} \in A$, para $j \in \{1, \dots, s\}$ y $s \in \mathbb{N}$, de forma que

$$m_i = \sum_{j=1}^{s} \mu_{ij} m_j{}' \quad \forall\, i \in \{\, 1, \dots, r \,\} \tag{2.12}$$

y

$$\sum_{i \in F} \mu_{ij} n_i = 0_N \quad \forall\, j \in \{\, 1, \dots, s \,\}. \tag{2.13}$$

Prueba. Probemos primero un caso base: consideremos N como A-módulo libre generado por el conjunto $\{\, n_1, \dots, n_r \,\}$; es decir, existe un isomorfismo de A-módulos

$$\begin{array}{rccc} \sigma: & N & \longrightarrow & A^{(r)} \\ & n_i & \longmapsto & e_i \end{array}.$$

Así, tenemos la cadena de isomorfismos de A-módulos

$$\begin{array}{ccccc} M \otimes N & \xrightarrow{1 \otimes \sigma} & M \otimes A^{(r)} & \longrightarrow & M^{(r)} \\ (m \otimes n_i) & \longmapsto & (m \otimes e_i) & \longmapsto & (m)_i \end{array}$$

y se desprende que

$$\sum_{i=1}^{r} m_i n_i = 0_{M \otimes N} \Leftrightarrow (m_1, \dots, m_r) = 0_{M^{(r)}} \Leftrightarrow m_i = 0_M \quad \forall\, i \in \{1, \dots, r\}.$$

Tras esto, basta tomar $s = r$ y definir $m_j{}' := m_j$, $\mu_{ij} := 0_A$ para $i, j \in \{\, 1, \dots, r \,\}$.

Ahora, de forma más general, sea

$$0 \longrightarrow K := \mathrm{Ker}(f) \hookrightarrow A^{(r)} \xrightarrow{F} N \longrightarrow 0$$

una sucesión exacta, donde F verifica $F(e_i) = n_i$ para cada $i \in \{ 1, \ldots, r \}$. Sabemos que la sucesión

$$M \otimes_A K \overset{h:=1_m \otimes i}{\longrightarrow} M \otimes_A A^{(r)} \overset{f:=1_M \otimes F}{\longrightarrow} M \otimes N \longrightarrow 0$$

es exacta.

De esta forma, si un elemento $z := \sum m_i \otimes e_i$ verifica $f(z) = 0_{M \otimes_A N}$, entonces existe $w := \sum_{j=1}^{s} m_j{}' \otimes k_j \in M \otimes_A K$ de forma que $h(w) = z$; esto supone

$$\sum_{j=1}^{s} m_j{}' \otimes k_j - \sum_{i=1}^{r} m_i \otimes e_i = 0_{M \otimes_A A^{(r)}}.$$

Además, para cada $j \in \{ 1, \ldots, s \}$ existen $\mu_{ij} \in A$ tales que

$$k_j = \sum \mu_{ij} e_i.$$

Resulta así lo siguiente. Por un lado se tiene

$$\begin{aligned}\sum_{j=1}^{s} m_j{}' \otimes k_j - \sum_{i=1}^{r} m_i \otimes e_i &= \sum_{j=1}^{s} m_j{}' \otimes \sum_{i=1}^{r} \mu_{ij} e_i - \sum_{i=1}^{r} m_i \otimes e_i = \\ &= \sum_{i=1}^{r} (\sum_{j=1}^{s} \mu_{ij} m_j{}') \otimes e_i - \sum_{i=1}^{r} m_i \otimes e_i = \\ &= \sum_{i=1}^{r} (\sum_{j=1}^{s} \mu_{ij} m_j{}' - m_i) \otimes e_i = 0_{M \otimes_A A^{(r)}},\end{aligned}$$

de donde se desprenden las igualdades

$$m_i = \sum_{j=1}^{s} \mu_{ij} m_j{}' \quad \forall\, i \in \{ 1, \ldots, r \}. \tag{2.14}$$

Por otro lado, como para cada $j \in \{ 1, \ldots, s \}$ se tiene $k_j \in K$, resulta

$$0_N = f(k_j) = \sum_{i=1}^{r} \mu_{ij} f(e_i) = \sum_{i=1}^{r} \mu_{ij} n_i \quad \forall\, j \in \{ 1, \ldots, s \}. \tag{2.15}$$

□

Apéndice A

Teoría de categorías

Una categoría ζ viene dada por:

- La *clase* de sus objetos $Obj(\zeta)$.
- Para cada par de objetos A, $B \in Obj(\zeta)$ un conjunto llamado $Hom_\zeta(A, B)$, las "flechas" de A en B.
- Para cada A, B, $C \in Obj(\zeta)$ una aplicación

$$\begin{array}{rcl} Hom_\zeta(A,B) \times Hom_\zeta(B,C) & \longrightarrow & Hom_\zeta(A,C) \\ (f,g) & \longmapsto & g \circ f \end{array}$$

  siendo dichas aplicaciones asociativas.

Definición A.0.1. Un funtor covariante entre dos categorías ζ y ζ' es una aplicación entre sus objetos

$$\begin{array}{rcl} F : Obj(\zeta) & \longrightarrow & Obj(\zeta') \\ A & \longmapsto & F(A) \end{array}$$

y para cada $A, B \in Obj(\zeta)$ una aplicación

$$\begin{array}{rcl} F : Hom_\zeta(A,B) & \longrightarrow & Hom_{\zeta'}(F(A),F(B)) \\ f & \longmapsto & F(f) \end{array}$$

tal que se verifica

1) Para cada $C \in Obj(\zeta)$ y para cada $f \in Hom_\zeta(A, B)$ y $g \in Hom_{\zeta'}(B, C)$, $F(g \circ f) = F(g) \circ F(f)$
2) Para cada cada $A \in Obj(\zeta)$, $F(1_A) = 1_{F(A)}$

Nótese que hemos empleado la misma notación, F, para definir dos funciones en principio distintas, pero se permite este abuso de notación ya que se puede distinguir muy fácilmente sobre qué conjunto está actuando la F en cada momento.

Ejemplo A.0.2. *1)* Sea ζ_{TOP} la categoría de los espacios topológicos y ζ_{SET} la categoría de los conjuntos. Definimos en funtor *olvido* como

$$\begin{array}{rcl} F : \mathrm{Obj}(\zeta_{TOP}) & \longrightarrow & \mathrm{Obj}(\zeta_{SET}) \\ X & \longmapsto & X \end{array}$$

2) Sea G_T la categoría de grupos, podemos definir un funtor

$$F : Obj(\zeta_{SET}) \longrightarrow Obj(G_T)$$

asociando a cada conjunto X el grupo libre generado por X, es decir, el conjunto de palabras generado por X.

3) Sea Ann la categoría de anillos conmutativos unitarios. Dado $A \in Obj(Ann)$, consideramos Mod_A la categoría de A-módulos. Dado $M \in Obj(Mod_A)$, definimos el funtor covariante

$$\begin{array}{rcl} Hom_A(M, \_) : Mod_A & \longrightarrow & Mod_A \\ N & \longmapsto & Hom_A(M, N) \end{array}$$

A su vez, dados N_1, N_2 A-módulos y $f : N_1 \to N_2$ homomorfismo, podemos definir

$$\begin{array}{rcl} f_* : Hom_A(M, N_1) & \longrightarrow & Hom_A(M, N_2) \\ \varphi & \longmapsto & f \circ \varphi \end{array}$$

Si tenemos la secuencia de homomorfismo de A-módulos

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$$

se tiene la siguiente secuencia

$$Hom_A(M, N_1) \xrightarrow{f_*} Hom_A(M, N_2) \xrightarrow{g_*} Hom_A(M, N_3)$$

que verifica $(g \circ f)_* = g_* \circ f_*$

Definición A.0.3. Un funtor contravariante entre dos categorías ζ y ζ' consiste en la aplicación

$$\begin{array}{rcl} F : Obj(\zeta) & \longrightarrow & Obj(\zeta') \\ A & \longmapsto & F(A) \end{array}$$

y para cada $A, B \in Obj(\zeta)$ una aplicación

$$\begin{array}{rcl} F : Hom_\zeta(A, B) & \longrightarrow & Hom_{\zeta'}(F(B), F(A)) \\ f & \longmapsto & F(f) \end{array}$$

tal que se verifica

1) Para cada $C \in Obj(\zeta)$ y para cada $f \in Hom_{\zeta}(A,B)$ y $g \in Hom_{\zeta'}(B,C)$, $F(g \circ f) = F(f) \circ F(g)$

2) Para cada cada $A \in Obj(\zeta)$, $F(1_A) = 1_{F(A)}$

Al igual que antes, hacemos un abuso de notación al usar F para denotar funciones distintas.

Ejemplo A.0.4. Consideremos ζ_{TOP} la categoría de espacios topológicos con aplicaciones continuas. Tomamos

$$\begin{array}{rcl} F : Obj(\zeta_{TOP}) & \longrightarrow & Obj(Ann) \\ (X,T) & \longmapsto & Cont(X,\mathbb{R}) \end{array}$$

donde $Cont(X,\mathbb{R})$ es el conjunto de las aplicaciones continuas de X a $\mathbb{R}$. Este conjunto es un anillo conmutativo y unitario con las operaciones $(f+g)(x) = f(x)+g(x)$ y $(f \cdot g)(x) = f(x) \cdot g(x)$

Dado $f : X \to Y$ continua, le asociamos el funtor contravariante

$$\begin{array}{rcl} Cont(Y,\mathbb{R}) & \longrightarrow & Cont(X,\mathbb{R}) \\ \varphi & \longmapsto & \varphi \circ f \end{array}$$

Definición A.0.5. Sea ζ una categoría.

1) Sea $O \in Obj(\zeta)$ tal que para cada $A \in Obj(\zeta)$, $Hom_{\zeta}(O,A)$ es un único elemento. Entonces a O se le llama objeto inicial de una categoría

2) Sea $O \in Obj(\zeta)$ tal que para cada $A \in Obj(\zeta)$, $Hom_{\zeta}(A,O)$ es un único elemento. Entonces a O se le llama objeto final de una categoría

Ejemplo A.0.6. *1)* $\varnothing$ es un objeto inicial.

2) {x} es un objeto final

3) Dado $A \in$ Obj(Ann), Mod_A tiene a $\{0\}$ como objeto inicial y final

Definición A.0.7. Dadas una categoría ζ, $A, A', B, B' \in Obj(\zeta)$ y $u \in \mathrm{Hom}_{\zeta}(A,B)$,

1) Decimos que u es un monomorfismo si $u \circ f = i \circ g$ implica que $f = g$, donde f y g pertenecen a $\mathrm{Hom}_{\zeta}(A',A)$

2) Decimos que u es un epimorfismo si $f \circ u = g \circ u$ implica que $f = g$, donde f y g pertenecen a $\mathrm{Hom}_{\zeta}(B,B')$

Observación A.0.8. *1)* Si tomamos las categorías de anillos y módulos, los conceptos de monomorfismo e inyectividad son equivalentes.

2) En la categoría de módulos, el concepto de epimorfismo es equivalente al de homomorfismo suprayectivo. Sean A un anillo y $M, N \in \mathrm{Mod}_A$. Tomemos $u \in \mathrm{Hom}_A(M, N)$ un epimorfismo. Se verifica que u es suprayectivo si, y sólo si

$$N/\mathrm{im}(u) = \{\, 0 \,\}\,.$$

En vista de esto, tomemos $N' := N/\mathrm{im}(u)$ y los homomorfismos f y g definidos como

$$\begin{array}{cccc} f & N & \longrightarrow & N' \\ & n & \longmapsto & [n]_{N'} \end{array}$$

y

$$\begin{array}{cccc} g & N & \longrightarrow & N' \\ & n & \longmapsto & [0]_{N'} \end{array}\,.$$

Se corresponden con la proyección canónica y el homomorfismo idénticamente nulo respectivamente. Ahora, tomando $x \in M$ arbitrario se tiene

$$(f \circ u)(x) = f(u(x)) = [0]_{N'} = g(u(x)) = (g \circ u)(x).$$

Así, por hipótesis $f(x) = g(x)$ para cada $x \in M$; es decir, $f \equiv [0]_{N'}$ y $N/\mathrm{im}(u) = \{0\}$.

Sin embargo, en la categoría de anillos homomorfismo suprayectivo sí implica epimorfismo, pero no se tiene la otra implicación. En efecto,

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \xrightarrow{f,g} C$$

con C anillo verifica las condiciones de epimorfismo $f \restriction_{\mathbb{Z}} = g \restriction_{\mathbb{Z}}$ implica $f = g$, pero la inclusión de $\mathbb{Z}$ sobre $\mathbb{Q}$ no es sobreyectiva.

Apéndice B

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

$$\begin{aligned} f_4 &= \gcd(f_3, f_3') = 1 \\ g_4 &= \frac{f_3}{f_4} = x-3 \\ F_3 &= \frac{g_3}{g_4} = 1 \end{aligned} \qquad \begin{aligned} f_5 &= \gcd(f_3, f_3') = 1 \\ g_5 &= \frac{f_3}{f_4} = 1 \\ F_4 &= \frac{g_3}{g_4} = x-3 \end{aligned}$$

¿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 C

Ejercicios

C.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:

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

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

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

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

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

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

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

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

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

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

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

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

y veamos que es un ideal:

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

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

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

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

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

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

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

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

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

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

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.*

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 $uA \nsubseteq \mathfrak{a}$, 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 $x \in A$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 8 (a) Dado que $\langle x-1, y\rangle \supset \langle x^2+y^2-1\rangle$ los Teoremas de Isomorfía nos dan

$$\left.{\mathbb{R}[x,y]}\middle/{\langle x^2+y^2-1\rangle}\right/\left.{\langle x-1,y\rangle}\middle/{\langle x^2+y^2-1\rangle}\right. \simeq \mathbb{R}[x,y]/\langle x-1,y\rangle \simeq \mathbb{R};$$

es decir, $\mathfrak{a}$ es maximal en A.

Por otra parte, sea $p \in \mathbb{R}[x,y]$ de grado positivo y supongamos que $\{x, y\} \subset \langle p\rangle$. Se sigue de esto que existen $h, g \in \mathbb{R}[x,y]$ tales que

$$\begin{aligned} ph &= x \quad \text{y} \\ pg &= y. \end{aligned}$$

De ser así, los grado de p respecto de x y de y deben ser ambos menores o iguales que 1, es decir, $p = ax + by + c$ para ciertos $a, b, c \in \mathbb{R}$. Si $a = 0$ y $b \neq 0$, necesariamente el grado de g respecto de y debe ser 0, lo que supone

$$pg = (by+c)\left(\sum_{i\in F}\lambda_i x^{r_i}\right) = \sum_{i\in F} b\lambda_i x^{r_i} y + \sum_{i\in F} c\lambda_i x^{r_i} = y,$$

pero esto es absurdo. Si $c \neq 0$, entonces $g = 0$. Por otro lado, si $c = 0$, entonces podemos considerar $p = y$ y el grado de ph respecto de y es mayor que 0. El caso $a \neq 0$ y $b = 0$ es análogo.

Ahora, si $\mathfrak{a}$ fuera principal, se podría expresar como $\langle [p]\rangle$ para cierto $[p] \in A$. Sin embargo, por el mismo argumento dado al principio del apartado, se tendría que $\langle p\rangle$ es maximal en $\mathbb{R}[x,y]$, pero por lo que acabamos de ver $x \notin \langle p\rangle$ o $y \notin \langle p\rangle$. Suponiendo $x \notin \langle p\rangle$, $\langle p\rangle \subset \langle x\rangle + \langle p\rangle \subsetneq \mathbb{R}[x,y]$

(b) Comprobemos ahora que $\langle [x-(1+iy)]\rangle = \mathfrak{b}$. En primer lugar, teniendo en cuenta

$$\begin{aligned}\left(\left[\frac{-1}{2i}\right][x+(1+iy)]\right)[x-(1+iy)] &= \left[\frac{-1}{2i}\right][x^2-(1+iy)^2] = \\ &= \left[\frac{-1}{2i}\right][x^2-1-2iy+y^2] = \\ &= \left[\frac{-1}{2i}\right][-2iy] = [y] \in \langle [x-(1+iy)]\rangle,\end{aligned}$$

tenemos que

$$[-x-iy][x-1-iy] = [x-x^2-y^2+iy] = [x-1] \in \langle [x-(1+iy)]\rangle.$$

Por otra parte, como

$$[x-1-iy] = [x-1]-i[y]$$

podemos concluir $\langle [x-(1+iy)]\rangle = \mathfrak{b}$.

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

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

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

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

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

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

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

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

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

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

Ejercicio 13 Sea A un anillo e $I \subset A[X_1, \ldots, X_n]$ 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 suprayectivo $\mathrm{eval}_{a_1,\ldots,a_n} : A[X_1, \ldots, X_n] \to A$ cuyo núcleo son los polinomios de la forma $\sum_i (x_i - a_i) f$, pues todos sus términos deben anularse, y entonces $\operatorname{Ker} \mathrm{eval}_{a_1,\ldots,a_n} = I$ 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 $\operatorname{Ker} \mathrm{eval}_{x_1}$ 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 $\operatorname{Ker} \mathrm{eval}_{x_1}$ es un ideal maximal, está generado por un elemento irreducible f, y entonces por la caracterización de maximales $K[T]/\langle f \rangle \cong \operatorname{Im} \mathrm{eval}_{x_1}$ 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 $\operatorname{Im} \mathrm{eval}_{x_1}$ 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 $A[x]/\mathfrak{m}[T] \cong (A/\mathfrak{m})[T]$. Esto es cierto, podemos definir el homomorfismo suprayectivo $A[T] \to (A/\mathfrak{m})[T]$ dado por $f = \sum a_i T^i \mapsto \sum (a_i + \mathfrak{m}) T^i$, cuyo núcleo es $\mathfrak{m}[T]$. Por ser $(A/\mathfrak{m})$ un cuerpo, tanto $(A/\mathfrak{m})[x]$ como $A[x]/\mathfrak{m}[x])$ son dominios de integridad.

Ahora bien, por un lado $[fg] = [0]$ por tenerse la inclusión $\mathrm{cf}(fg) \subset \mathfrak{m}$. Sin embargo, por otro, como f y g son primitivos sus coeficientes generan A y, si $[f] = [0]$ o $[g] = [0]$, se tendría $A = \mathfrak{m}$. Llegamos así al absurdo de que $[f]$ y $[g]$ sean divisores de $[0]$ en $A[x]/[x]$

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:

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

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, a saber:

1) $\bigcup_{f\in A} X_f = \operatorname{Spec} A$ y
2) para cualesquiera X_f y X_g, existe $h \in A$ tal que $X_h \subset X_f \cap X_g$.

En primer lugar $\bigcup_{f\in A} X_f = \bigcup_{f\in A} \operatorname{Spec} A \setminus V(f) = \operatorname{Spec} A \setminus \bigcap_{f\in A} V(f) = \operatorname{Spec} A$. Esto último es porque $V(f) \cap V(g) = V(\{f,g\})$ para cualesquiera $f, g \in A$, luego $\bigcap_{f\in A} V(f) = V(A) = V(\langle 1\rangle) = \varnothing$. En segundo lugar, sean $f, g \in A$ y $\mathfrak{p} \in X_f \cap X_g = \operatorname{Spec} A \setminus (V(f) \cup V(g))$. Entonces $f, g \notin \mathfrak{p}$, y por ser primo $fg \notin \mathfrak{p}$, luego $\mathfrak{p} \in X_{fg}$. Más aún, si $\mathfrak{q} \in X_{fg}$, entonces $fg \notin \mathfrak{q}$, lo que implica que $f \notin \mathfrak{q}$ y $g \notin \mathfrak{q}$, i.e., $X_{fg} \subset X_f \cap X_g$. Esto termina la demostración de que ese conjunto es base de la topología; además, tenemos los dos contenidos que prueban (i) $X_f \cap X_g = X_{fg}$.

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

(iii) Sabemos que, si $f \notin \mathcal{U}(A)$, entonces existe un ideal maximal que lo contiene que es a su vez primo. Por ser esto así, $V(f) \neq \varnothing$ y $X_f \neq \operatorname{Spec} A$. Por otra parte, si f es unidad, no puede estar contenido en ningún ideal propio de A; en concreto, no puede estar contenido en ningún ideal primo.

(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 $\operatorname{Spec} A$, y comprobemos que $\langle \{f_i\}_{i\in I}\rangle = \langle 1\rangle$. Efectivamente, como $\operatorname{Spec} A = \bigcup_{i\in I} X_{f_i}$, entonces

$$\varnothing = \bigcap_{i\in I} V(f_i) = V(\{f_i\}_{i\in I}) = V(\langle \{f_i\}_{i\in I}\rangle), \tag{C.15}$$

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 $\langle \{f_i\}_{i\in I}\rangle = \langle 1\rangle$. Por ser así, 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 $V(\langle \{f_j\}_{j\in J}\rangle) = \varnothing$ lo que implica $\bigcup_{j\in J} X_{f_j} = \operatorname{Spec} A$. 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:

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

y, así, $\{\, X_{f_j} \,\}_{j\in J}$ 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 $A \to \prod_{i=1}^n A/\mathfrak{a}_i$ 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 construirmos $\mathfrak{b}_{ij} = \bigcap_{k\neq i,j} \mathfrak{a}_k$. 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 $\pi_i : A \to A/\mathfrak{a}_i$ 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 compontentes 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 $i = 1, \ldots, n$, y por tanto $a \in \bigcap_{i=1}^n \mathfrak{a}_i$.

(iii)