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. □

Definición 1.1.15. Dado un anillo A, definimos el *ideal de Jacobson* como

$$\mathfrak{R} := \bigcap_{\substack{\mathfrak{m}\subset A \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$$

Proposición 1.1.16. *Sea A un anillo. Se tiene que para cada $x \in A$, $x \in \mathfrak{R}$ si, y sólo si, $1 - xy$ es unidad para toda $y \in A$.*

Prueba. ($\Rightarrow$) Sea $x \in \mathfrak{R}$ y supongamos que existe $y \in A$ tal que $1 - xy$ no es unidad. Por ser así, existe $\mathfrak{m} \subset A$ maximal tal que $1 - xy \in \mathfrak{m}$, pero por definición de $\mathfrak{R}$ se tiene que $1 - xy + xy = 1 \in \mathfrak{m}$, que es absurdo.

($\Leftarrow$) Supongamos ahora que $x \in A$ verifica las hipótesis pero existe $\subset A$ maximal tal que $x \notin \mathfrak{m}$. Por la maximalidad de $\mathfrak{m}$, $\langle x\rangle \oplus \mathfrak{m} = \langle 1\rangle$; es decir, existen $y \in A$ y $m \in \mathfrak{m}$ tales que

$$xy + m = 1 \Longleftrightarrow m = 1 - xy,$$

pero esto es absurdo. □

Definición 1.1.17. Diremos que un anillo A es un *anillo local* si posee un único ideal maximal.

En vista de lo anterior, tenemos la siguiente caracterización de los anillos locales.

Proposición 1.1.18. *Sea A un anillo. Son equivalentes*

1) A es un anillo local,

2) el único ideal maximal de A es $\mathfrak{R}$,

3) *dado un ideal maximal* $\mathfrak{m} \subset A$*, para cualesquiera* $x \in \mathfrak{m}$ *e* $y \in A$*,* $1 - xy$ *es unidad de* A *y,*

4) *para todo* $x \in A$*,* x *es unidad o* $1 - xy$ *es unidad para cada* $y \in A$*.*

Prueba. $(1 \Rightarrow 2)$, $(2 \Rightarrow 1)$ y $(2 \Rightarrow 3)$ son obvias.

$(3 \Rightarrow 2)$. Dado un ideal maximal $\mathfrak{m} \subset A$ verificando las hipótesis, tenemos por la caracterización del ideal $\mathfrak{R}$ que $\mathfrak{m} \subset \mathfrak{R}$. Como la inclusión $\mathfrak{R} \subset \mathfrak{m}$ se da siempre, tenemos la igualdad. Además, por ser $\mathfrak{m}$ arbitrario, tenemos que $\mathfrak{R}$ es el único ideal maximal de A.

$(3 \Rightarrow 4)$. Sea $x \in A$. Si x no es unidad, entonces pertenece a algún ideal maximal y por la hipótesis tenemos lo que queremos probar.

$(4 \Rightarrow 3)$. Análogamente, dado un ideal maximal $\mathfrak{m} \subset A$ y un elemento $x \in \mathfrak{m}$, se tiene que x no es unidad y por la hipótesis podemos concluir la prueba.

□

Proposición 1.1.19. *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 1.1.20. *Sea* A *anillo y* $\mathfrak{a}$ *ideal de* A*, existe un ideal primo minimal entre los que contienen a* $\mathfrak{a}$*.*

Definición 1.1.21. 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 1.1.22. Sea A un anillo. El *radical* de un ideal $\mathfrak{a}$ de A se define como

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

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

Proposición 1.1.23. *Sea A un anillo, entonces el conjunto $\mathfrak{N}_A$ de todos los elementos nilpotentes de A es un ideal. Se le llama* nilradical *de A.*

Prueba.

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

□

Proposición 1.1.24. *El nilradical de un anillo A verifica $\mathfrak{N}_A = \bigcap_{\mathfrak{p}\ primo} \mathfrak{p}$.*

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

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

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

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

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

Definición 1.1.25. 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 1.1.26. *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 1.1.27. 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 1.1.28. 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

$$Z_{\mathbb{A}_K^n} = \{a \in \mathbb{A}_K^n \big| \; f(a) = 0 \text{ para cada } f \in S\}$$

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

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 $\mathbb{A}_K^1$. Solo hay tres tipos:

1. $Z(0) = \mathbb{A}_K^1$ 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 $\mathfrak{a} = \langle c_1, \dots, c_s \rangle$. Para cada $i = 1, \dots, s$ existe un $f_i \in \mathfrak{I}$ con c_i como coeficiente principal. Sea $\delta = \max_{1 \leq i \leq s} \deg f_i$, y para cada $\gamma \leq \delta$ definimos

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

que también es un ideal de A:

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

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

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

De nuevo, por hipótesis, $\mathfrak{a}_\gamma$ es finitamente generado, así que $\mathfrak{a}_\gamma = \langle d_{\gamma_1}, \ldots, d_{\gamma_m} \rangle$, y para cada $j = 1, \ldots, m_\gamma$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\forall\ m \in M \quad 0_A m = 0_M$$
$$\forall\ \lambda \in A \quad \lambda 0_M = 0_M.$$

   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 $\mathrm{Ker}(f) := \{x \in M \mid f(x) = 0_N\}$ es un submódulo de M y que $\mathrm{im}(f) := \{y \in N \mid \exists\ x \in M \text{ tal que } f(x) = y\}$ 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. 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 $(\lambda_1 - \lambda_2) \cdot m = 0 \to \lambda_1 - \lambda_2 \in Anul_A M$

(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

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

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

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

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

Así,

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

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

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

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

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

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

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

□

2.1.4 Pullbacks

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

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

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

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

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

es un homomorfismo de A-módulos y se denota $\psi_* = \mathrm{Hom}_A(\_\psi)$.

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

Respectivamente, dados N_1, N_2 y N_3 A-módulos y $\varphi \in \mathrm{Hom}_A(N_1, N_2)$ y $\psi \in \mathrm{Hom}_A(N_2, N_3)$, entonces $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$.

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 A-módulos.

3. 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 A-módulos.

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. 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:

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

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

Recíprocamente, 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 $\mathfrak{m} \subset \operatorname{Ann}_A \left(M/\mathfrak{m}M \right)$, $M/\mathfrak{m}M$ tiene estructura de $A/\mathfrak{m}$-espacio vectorial.

Tomemos $M = A^{(I)}$ y veamos que $A^{(I)}/\mathfrak{m}A^{(I)} \cong \left(A/\mathfrak{m} \right)^{(I)}$, 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

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

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 $\operatorname{im}(f) = \operatorname{Ker}(g)$

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:

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

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

3) $M \cong M' \oplus M''$ 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. Con abuso de notación y siempre que no lleve a confusión, si $M \in \mathrm{Obj}(\mathrm{Mod}_A)$, escribiremos $M \in \mathrm{Mod}_A$, e igual con el resto de categorías.

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 $M \in \mathrm{Mod}_A$ la sucesión

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

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 $M \in \mathrm{Mod}_A$ *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

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

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

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

Así, $\operatorname{Ker}(g) \subset \operatorname{im}(f)$. $\square$

2.4 Módulos proyectivos y módulos inyectivos

Supongamos $M \in \operatorname{Mod}_A$ 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

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

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

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

$$\begin{tikzcd}
N \arrow[r, two heads, "g"] & N' \\
M \arrow[u, "h"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

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 $g \in \operatorname{Hom}_A(N, N')$ suprayectiva y $\varphi \in \operatorname{Hom}_A(A^{(I)}, N')$ 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

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

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 $A^{(I)} \cong \operatorname{Ker}\pi \oplus M$. $\square$

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

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

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 $N \in \mathrm{Mod}_A$ es un A-módulo inyectivo si, para cualesquiera $M, M' \in \mathrm{Mod}_A$, $f \in \mathrm{Hom}_A(M', M)$ 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

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

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 $A^{(M\times N)}$

$$S = \{e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}, e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')},\\ e_{(m,\lambda n)} - \lambda e_{(m,n)}, e_{(\lambda m,n)} - \lambda e_{(m,n)}\} \quad (2.6)$$

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

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

□

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 $M_1, \ldots, M_r$, 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

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

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

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

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

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

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

$$\begin{array}{ccc} \mathrm{Mod}_A & \xrightarrow{M\times_A\_} & \mathrm{Mod}_A \\ N & \longmapsto & M\otimes_A N \end{array}$$

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

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

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

es también una sucesión exacta.

Prueba. Sabemos que (2.10) es exacta si, y sólo si, para todo P A-módulo se tiene que la sucesión

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

es exacta.

Consideramos la sucesión

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

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

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

Por otro lado, definamos

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

Hay que comprobar que la aplicación está bien definida, esto es, que F_φ es bilineal. 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
- $\varphi_{\lambda m}(n) = (\lambda\varphi)_m(n) = \lambda\varphi_m(n) = \varphi_m(\lambda n)$.

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

Con esto queda demostrado el isomorfismo.

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.

$$\begin{array}{cccccc} 0 \to & \mathrm{Hom}_A(M \otimes_A N'', P) \to & \mathrm{Hom}_A(M \otimes_A N, P) \to & \mathrm{Hom}_A(M \otimes_A N', P) \\ & \Phi''_N \downarrow & \Phi_N \downarrow & \Phi'_N \downarrow \\ 0 \to & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \to & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \to & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P)) \end{array} \tag{2.12}$$

Estos isomorfismos implican que por ser (**??**) exacta (2.11) es también exacta. Para probar esto es suficiente ver que cada uno de los diagramas de (2.12) conmutan, es decir, que

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

y

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

Sea $F \in \mathrm{Hom}_A(M \otimes N'', P)$, y cualquier $m \otimes n \in M \otimes_A N$. Entonces $\Phi_{N''}(F(m \otimes n)) = \varphi_F(m)(n)$ y componiendo ahora con $(g^*)_*$

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

Por último,

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

El caso de la f es análogo. □

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 $\{ \text{rel}_1, \ldots, \text{rel}_s \} \subset \Sigma$ tales que

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

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

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

$$0 \longrightarrow M \otimes_A N_{\text{red}}{}' \xrightarrow{1 \otimes f_{|N_{\text{red}}{}'}} M \ M \otimes N_{\text{red}}$$

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

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

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

$\square$

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 $\{ m_1, \ldots, m_r \}$. La inclusión antes mencionada implica $m_i | 2$ para toda $i \in \{ 1, \ldots, r \}$, es decir, $m_i = 1$ o $m_i = 2$. Por esto, existe $i \in \{ 1, \ldots, r \}$ 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*

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

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

$$m_i = \sum_{j=1}^{s} \mu_{ij} m_j{}' \quad \forall\, i \in \{\, 1, \dots, r \,\} \tag{2.13}$$

y

$$\sum_{i \in F} \mu_{ij} n_i = 0_N \quad \forall\, j \in \{\, 1, \dots, s \,\}\,. \tag{2.14}$$

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

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

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

$$m_i = \sum_{j=1}^{s} \mu_{ij} m_j{}' \quad \forall\, i \in \{1, \ldots, r\}. \tag{2.15}$$

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

$$0_N = f(k_j) = \sum_{i=1}^{r} \mu_{ij} f(e_i) = \sum_{i=1}^{r} \mu_{ij} n_i \quad \forall\, j \in \{1, \ldots, s\}. \tag{2.16}$$

□

Teorema 2.5.19. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes.*

1) M es un A-módulo plano.

2) 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

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

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

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

es inyectiva. Es decir, $\mathfrak{a} \otimes M \cong \mathfrak{a}M$

Prueba. Vamos probando cada una de las implicaciones.

($2 \Rightarrow 1$). Tenemos que ver que si $0 \to N' \to N$ es exacta entonces $0 \to M \otimes N' \to M \otimes N$ es exacta. Por resultados anteriores, podemos suponer N y N' finitamente generados.

Sea así

$$N' = \langle n'_1, \dots, n'_t \rangle$$

y

$$N = \langle n'_1, \dots, n'_t, n_{t+1}, \dots, n_r \rangle$$

Aquí estamos haciendo un abuso de notación. Al suponer la sucesión exacta, la aplicación $N' \to N$ es inyectiva, luego es un isomorfismo sobre su imagen. Luego podemos suponer $N' \subset N$ y los generadores de N' generadores de N también.

Sea, para cada $j = 1, \dots r - t$,

$$N'_j = \langle n'_1, \dots, n'_t, n_{t+1}, \dots, n_{t+j} \rangle$$

Se cumple $n'_{r-t} = N$. $0 \to M \otimes N' \to M \otimes N$ descompone en

$$0 \longrightarrow M \otimes N' \longrightarrow M \otimes N'_1 \longrightarrow \cdots \longrightarrow M \otimes N'_{r-t} = M \otimes N$$

Por tanto, para ver que es inyectiva, basta verlo para cada una de las flechas anteriores. Es decir, podemos restringirnos al caso

$$N' = \langle n'_1, \dots, n'_t \rangle$$

y

$$N = \langle n'_1, \dots, n'_t, n \rangle$$

y ver que $M \otimes N' \xrightarrow{1_M \otimes i}$ es inyectiva.

Sea $z \in M \otimes N'$ tal que $(1_M \otimes i)(z) = 0_{M\otimes N}$. Veamos que $z = 0_{M\otimes N'}$. Utilizando las propiedades de multilinealidad, $z = \sum_{i=1}^t m_i \otimes n'_i$. Aplicando $1_M \otimes i$, $\sum_{i=1}^t m_i \otimes n'_i = 0_{M\otimes N}$ Es decir, $0_{M\otimes N} = \sum_{i=1}^t m_i \otimes n'_i + 0_M \otimes n$. Como $N = \langle n'_1, \dots, n'_t, n_{t+1}, \dots, n_r \rangle$ es generador de N, estamos en condiciones de aplicar el lema anterior. Este nos dice que existen $\{m'_j : j = 1, \dots, s\}$ tal que

$$m_i = \sum_{j=1}^s \lambda_{ij} m'_j, i = 1, \dots, t \tag{2.17}$$

,

$$m_{t+1} = 0 = \sum_{j=1}^s \lambda_{t+1,j} m'_j \tag{2.18}$$

y

$$\sum_{i=1}^t (\lambda_{ij} n'_i + \lambda_{t+1,j} n) = 0 \tag{2.19}$$

Aplicado la hipótesis del Teorema a (2.18), se tiene que existen $m''_h \in M$, $\gamma_{j_h} \in A$, con $h = 1, \dots, q$ tal que

$$m'_j = \sum_{h=1}^q \gamma_{j_h} m''_h, j = 1, \dots, s \tag{2.20}$$

y

$$\sum_{j=1}^s \lambda_{t+1,j} \gamma_{j_h} = 0, h = 1, \dots, q \tag{2.21}$$

Ahora se cumple

$$\begin{aligned} z &= \sum_{i=1}^t m_i \otimes n'_i \overset{(2.17)}{=} \sum_{i=1}^t (\sum_{j=1}^s \lambda_{ij} m'_j) \otimes n'_i \sum_{j=1}^s m'_j \otimes (\sum_{i=1}^t \lambda_{ij} n'_i) \\ &\overset{(2.19)}{=} \sum_{j=1}^s m'_j \otimes (-\lambda_{t+1,j} n) \overset{(2.20)}{=} \sum_{j=1}^s (\sum_{j=1}^q \gamma_{j_h} m''_h) \otimes (-\lambda_{t+1,j} n) \\ &= \sum_{h=1}^q m''_h \otimes (-\sum_{j=1}^s \gamma_{j_h} \lambda_{t+1,j} n) \end{aligned}$$

Ahora bien, esto último pertenece a N', y como sabemos que es 0 en N', necesariamente es 0 en N' ($1 \Rightarrow 3$) es claro. ($3 \Rightarrow 2$). Sea M un A-módulo, sean $a_i \in A$ tales que $\sum_{i=1}^r a_i m_i = 0$. Consideramos el ideal $\mathfrak{a} = \langle a_1 \dots a_r \rangle$. Por la hipótesis,

$$\begin{array}{rcl} M \otimes \mathfrak{a} & \longrightarrow & M \\ m \otimes a & \longmapsto & am \end{array}$$

es inyectiva. De esta forma, $\sum_{i=1}^r am_i = 0_M$ implica que $\sum_{i=1}^r m_i \otimes a_i = 0_{M \otimes \mathfrak{a}}$.

Por el lema, tomando $N = \mathfrak{a}$, existen $\lambda_{ij} \in A, m'_i \in M$ tales que

$$m_i = \sum_{j=1}^s \lambda_{ij} m'_j, i = 1, \dots, r$$

y

$$\sum_{i=1}^r \lambda_{ij} a_i = 0, j = 1, \dots, s$$

lo que prueba el resultado □

Observación 2.5.20. Gracias el Teorema, se tiene la siguiente interpretación de la platitud de A-álgebras.

La condición 3 nos dice que tomando B un A-álgebra, $A \xrightarrow{\varphi} B$ y $\mathfrak{a}$ un ideal de A, si B es un A-módulo plano, $\mathfrak{a} \otimes B \cong \mathfrak{a}B = \varphi(\mathfrak{a})B$

La condición 2 nos dice que, bajo las mismas condiciones sobre B, si se tiene

$$\sum_{i=1}^r a_i x_i = 0, x_i \in B, a_i \in A$$

entonces existen $y_j \in B, \lambda_{ij} \in A$, con $x_i = \sum_{j=1}^s \lambda_{ij} y_j$ para cada $i \in \{1, \dots, r\}$ y $\sum_{i=1}^r \lambda_{ij} a_i = 0$ para cada $j \in \{1, \dots, s\}$.

Esto es, dado un sistema de ecuaciones lineales homogéneo con coeficientes en A, $\sum_{i=1}^r a_i X_i = 0$ cada solución $(x_1, \dots, x_r)$ en B se puede expresar como una combinación lineal

$$(x_1, \dots, x_r) = \sum_{j=1}^s Y_j (\lambda_{1j}, \dots, \lambda_{rj})$$

donde cada $(\lambda_{1j}, \dots, \lambda_{rj}) \in A^r$ son soluciones de $\sum_{i=1}^r a_i X_i = 0$.

Definición 2.5.21. Sea M un A-módulo.

1) Diremos que M es *finitamente generado* si existen $r \in \mathbb{N}$ y una sucesión

$$A^{(r)} \xrightarrow{f} M \longrightarrow 0 \tag{2.22}$$

exacta.

2) Diremos que M es *finitamente presentado* si existen $r, t \in \mathbb{N}$ y una sucesión

$$A^{(t)} \xrightarrow{g} A^{(r)} \xrightarrow{f} M \longrightarrow 0 \tag{2.23}$$

exacta.

Observación 2.5.22. Supongamos M A-módulo y una sucesión como en (2.23). En primer lugar, M es finitamente generado porque también la sucesión

$$A^{(r)} \xrightarrow{f} M \longrightarrow 0$$

es exacta. Más aún, dado que $\operatorname{im}(g) = \operatorname{Ker}(f)$, la sucesión

$$A^{(t)} \xrightarrow{g} \operatorname{Ker}(f) \longrightarrow 0$$

es también exacta e implica que $\operatorname{Ker}(f)$ es finitamente generado.

Recíprocamente, supongamos que tenemos un A-módulo M, una sucesión como (2.22) y que además $\operatorname{Ker}(f)$ es finitamente generado. Veamos que M es finitamente generado. Por ser $\operatorname{Ker}(f)$ finitamente generado, existen $t \in \mathbb{N}$ y

$$A^{(t)} \xrightarrow{g} \operatorname{Ker}(f) \longrightarrow 0$$

exacta. De igual forma la sucesión

$$\operatorname{Ker}(f) \xhookrightarrow{i} A^{(r)} \xrightarrow{f} M \longrightarrow 0$$

es también exacta, luego basta considerar $G := i \circ g$ y ver que

$$A^{(t)} \xrightarrow{G} A^{(r)} \xrightarrow{f} M \longrightarrow 0$$

es exacta para concluir que M es finitamente presentado.

Capítulo 3

Anillos de fracciones

En el siguiente capitulo generalizaremos la construcción del cuerpo de los números racionales desde el anillo de los enteros a cualquier dominio de integridad. Para ello, necesitaremos el siguiente concepto.

Definición 3.0.1. Sea A un anillo conmutativo unitario, donde $0_A \neq 1_A$. $S \subset A$ se dice *multiplicativamente cerrado* si se verifica

1. $0_A \notin S$
2. $1_A \in S$
3. $s_1 \cdot s_2 \in S, \forall s_1, s_2 \in S$

Ejemplo 3.0.2.

1. $S = \{1_A\}$ es multiplicativamente cerrado
2. Denotemos como $\mathrm{Div}_0(A)$ al conjunto de los divisores de 0 de A. $S = A \setminus \mathrm{Div}_0(A)$ es multiplicativamente cerrado. En efecto,
   - $0_A \in \mathrm{Div}_0(A)$, pues cualquier $a \in A$ verifica que $a \cdot 0_A = 0_A$. Por tanto, $0_A \notin S$
   - Para cada $a \in A \setminus \{0\}$, $1_A \cdot a = a \neq 0$, luego $a \notin \mathrm{Div}_0(A)$, es decir, $1_A \in S$
   - Dados $s_1, s_2 \in S$ y $x \in A \setminus \{0\}$, $(s_1 \cdot s_2) \cdot x = s_1 \cdot (s_2 \cdot x)$. Como $s_1 \notin \mathrm{Div}_0(A)$, $s_2 \cdot x = 0$, pero como $s_2 \notin \mathrm{Div}_0(A)$, necesariamente $x = 0$, lo que implica $s_1 \cdot s_2 \in S$.
3. Dado $\mathfrak{p}$ un ideal primo de A, $A \setminus \mathfrak{p}$ es un conjunto multiplicativamente cerrado. En efecto,

- Por ser ideal, $0 \in \mathfrak{p}$
- Por ser primo, $1 \notin \mathfrak{p}$
- Por ser primo, si $s_1 \cdot s_2 \in \mathfrak{p}$, necesariamente alguno tiene que estar en $\mathfrak{p}$.

3.1 Construcción del anillo de fracciones

Sea A un anillo conmutativo y unitario. Sea $S \subset A$ un conjunto multiplicativamente cerrado. Definimos en $A \times S$ la siguiente relación

$$(a, s_1) \sim (b, s_2) \iff \exists s' \in S : s'(as_2 - bs_1) = 0$$

Proposición 3.1.1. *La relación '$\sim$' es de equivalencia*

Prueba. Las propiedades reflexiva y simétrica son inmediatas. Para ver la transitiva, supongamos

$$(a, s_1) \sim (b, s_2) \iff \exists s' \in S : s'(as_2 - bs_1) = 0 \tag{3.1}$$

y

$$(b, s_2) \sim (c, s_3) \iff \exists s'' \in S : s''(bs_3 - cs_2) = 0 \tag{3.2}$$

Multiplicamos la primera ecuación por $s''s_3$ y la segunda por $s's_1$. Sumando ambas expresiones queda

$$0_A = s_2 s' s''(as_3 - cs_1)$$

lo que es equivalente a $(a, s_1) \sim (c, s_3)$ □

Observación 3.1.2. Es necesario incluir la existencia del $s' \in S$ para que se cumpla la transitividad, no basta con pedir únicamente que se anule la resta entre los paréntesis.

Al conjunto $A \times S/\sim$ se le suele denotar como $S^{-1}A$. A los elementos $[(a, s)]$ se les denota a su vez como $\frac{a}{s}$. Definimos en este conjunto las siguientes operaciones:

- $[(a, s)] + [(b, t)] := [(at + bs, st)]$
- $[(a, s)] \cdot [(b, t)] := [(ab, dt)]$

Nótese que no son más que las operaciones para fracciones normales.

Proposición 3.1.3. *Las operaciones + y · están bien definidas y $(S^{-1}A,+,\cdot)$ es un anillo conmutativo unitario tal que*

$$\begin{array}{rccc} \delta_S: & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & [(a,1)] \end{array}.$$

es un homomorfismo de anillos.

Prueba. Veamos que + está bien definida. Supongamos

$$(a_1,s_1)\sim(a_1',s_1') \iff \exists s_1^*\in S: s_1^*(a_1s_1'-a_1's_1)=0 \tag{3.3}$$

y

$$(a_2,s_2)\sim(a_2',s_2') \iff \exists s_2^*\in S: s_2^*(a_2s_2'-a_2's_2)=0 \tag{3.4}$$

Multilpicamos (3.3) por $s_2s_2's_2^*$ y (3.4) por $s_1s_1's_1^*$ y sumando ambas expresiones queda

$$s_1^*s_2^*((s_1's_2')(a_1s_2+a_2s_1)-(s_1s_2)(a_1's_2'+a_2's_1'))=0$$

Esto se traduce en que

$$\frac{a_1}{s_1}+\frac{a_2}{s_2}=\frac{a_1'}{s_1'}+\frac{a_2'}{s_2'}.$$

+ verifica la propiedad asociativa:

$$\left(\frac{a_1}{s_1}+\frac{a_2}{s_2}\right)+\frac{a_3}{s_3}=\frac{a_1s_2+a_2s_1}{s_1s_2}+\frac{a_3}{s_3}=\frac{a_1s_2s_3+a_2s_1s_3+a_3s_1s_2}{s_1s_2s_3}=$$
$$\frac{a_1}{s_1}+\frac{a_2s_3+a_3s_2}{s_2s_3}=\frac{a_1}{s_2}+\left(\frac{a_2}{s_2}+\frac{a_3}{s_3}\right).$$

La propiedad conmutativa se comprueba fácilmente.

Comprobemos ahora que · está bien definida. Tomemos dos pares $(a_1,s_1)\sim(a_1',s_1')$ y $(a_2,s_2)\sim(a_2',s_2')$. Existen $s_1^*,\ s_2^*\in S$ tales que

$$s_1^*(a_1s_1'-a_1's_1)=0 \tag{3.5}$$

y

$$s_2^*(a_2s_2'-a_2's_2)=0. \tag{3.6}$$

Basta multiplicar (3.5) y (3.6) por $a_2s_2's_2^*$ y $a_1's_1s_1^*$ respectivamente y sumarlas para obtener $(a_1a_2,s_1s_2)\sim(a_1'a_2',s_1's_2')$, es decir,

$$\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}=\frac{a_1'}{s_1'}\cdot\frac{a_2'}{s_2'}.$$

Es sencillo comprobar que $\cdot$ verifica las propiedades asociativa y conmutativa.

Veamos que se cumple la propiedad distributiva:

$$\frac{a_1}{s_1}\left(\frac{a_2}{s_2}+\frac{a_3}{s_3}\right)=\frac{a_1a_2s_3+a_1a_3s_2}{s_1s_2s_3}=\frac{a_1s_1a_2s_3+a_1a_3s_1s_2}{s_1^2s_2s_3}=\frac{a_1a_2}{s_1s_2}+\frac{a_1a_3}{s_1s_3}.$$

Finalmente, que $\delta_S(a)=[(a,1)]$ es un homomorfismo de anillos se sigue sencillamente de la definición. $\square$

Observación 3.1.4. 1) El elemento neutro para $+$ en $S^{-1}A$ es $0_{S^{-1}A}=[(0,1)]$. Además, para cada $s\in S$, se tiene que $[(0,1)]=[(0,s)]$. En efecto, dado $\frac{a}{s}\in S^{-1}A$,

$$0_{S^{-1}A}+\frac{a}{s}=\frac{0_A}{1}+\frac{0\cdot s+a}{s}=\frac{a}{s}$$

y para cada $s\in S$ se tiene trivialmente $1_A(0_As-0_A1_A)=0_A$, es decir, $[(0,1)]=[(0,s)]$.

2) Análogamente, el elemento neutro para $\cdot$ en $S^{-1}A$ es $1_{S^{-1}A}=[(1,1)]$ y, para cada $s\in S$, se tiene que $[(1,1)]=[(s,s)]$.

3) El núcleo de δ_S es el conjunto $\{a\in A:[(a,1)]=[(0,s)],s\in S\}$, esto es, existe un s^* tal que $s^*(a-0)=s^*a=0$. Una condición suficiente para que δ_S sea inyectiva es que A sea dominio de integridad. Concretamente, δ_S es inyectiva si, y sólo si, $S\cap\mathrm{Div}_0(A)=\varnothing$.

3.1.1 Propiedad universal del anillo de fracciones

Teorema 3.1.5. ***(Propiedad universal del anillo de fracciones)*** *Sean A y B anillos, $S\subset A$ un subconjunto multiplicativamente cerrado de A y $\varphi:A\longrightarrow B$ de forma que $\varphi(s)$ es unidad en B para toda $s\in S$. Bajo estas hipótesis, existe un único homomorfismo $\Phi:S^{-1}A\longrightarrow B$ que cumple*

$$\varphi=\Phi\circ\delta_S$$

Prueba. Supongamos en primer lugar la existencia de tal homomorfismo y probemos su unicidad. Para todo $a\in A$ se tiene que $\Phi(\frac{a}{1})=\Phi\circ\delta_S(a)=\varphi(a)$. Por otra parte, dado $s\in S$, se tiene

$$1_B=\Phi\left(\frac{1_A}{1_A}\right)=\Phi\left(\frac{s}{s}\right)=\Phi\left(\frac{s}{1_A}\frac{1_A}{s}\right)=\Phi\left(\frac{s}{1_A}\right)\Phi\left(\frac{1_A}{s}\right)=\varphi(s)\Phi\left(\frac{1_A}{s}\right),$$

es decir, $\Phi(\frac{1_A}{s}) = \varphi(s)^{-1}$. Con todo, para todo $\frac{a}{s} \in S^{-1}A$ se tiene $\Phi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$; es decir, Φ está unívocamente determinado por φ.

Teniendo en cuenta lo anterior, vamos a definir para cada $\frac{a}{s} \in S^{-1}A$

$$\Phi\left(\frac{a}{s}\right) := \varphi(a)\varphi(s)^{-1}.$$

Veamos que está bien definido. Dados dos elementos $\frac{a}{s}$ y $\frac{a'}{s'}$ en la misma clase de equivalencia, existe $s^* \in S$ tal que $s^*(as' - a's) = 0_A$. Aplicando φ a ambos miembros de la igualdad resulta $\varphi(s^*)(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)) = 0_B$ y, dado que $\varphi(s^*)$ es unidad por hipótesis, tenemos que $\varphi(a)\varphi(s') - \varphi(a')\varphi(s) = 0_B$. De esto se desprende

$$\varphi\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1} = \Phi\left(\frac{a'}{s'}\right).$$

Esta última igualdad también se apoya en el hecho de que $\varphi(s)$ y $\varphi(s')$ son unidades. □

Observación 3.1.6. 1) El enunciado del teorema se puede reescribir pidiendo que B sea una A-álgebra mediante un homomorfismo φ.

2) De la Propiedad universal del anillo de fracciones se deduce que, en el caso de que A sea un DI y $S = \mathrm{Div}_0(A)$, $S^{-1}A$ es el menor cuerpo que contiene a A.

Supongamos K cuerpo tal que $A \subset K$. Como ya hemos comentado en (3.1.4), δ_S es un homomorfismo inyectivo, luego también se tiene $A \subset S^{-1}A$. Además, por ser $S^{-1}A$ un cuerpo, Φ (definido como en el teorema) es de igual forma inyectivo, por lo que $S^{-1}A \subset K$.

3) Si S_1 y S_2 son conjuntos multiplicativamente cerrados de A tales que $S_1 \subset S_2$, todo $s \in S_1$ verifica que $\delta_{S_2}(s)$ es unidad en ${S_2}^{-1}A$. Así, podemos aplicar el Principio universal del anillo de fracciones y tener que $\delta_{S_2} = \Phi \circ \delta_{S_1}$, de forma que todo elemento $\frac{a}{s}$ de ${S_1}^{-1}A$ se puede ver como uno de ${S_2}^{-1}A$.

Hay que destacar igualmente que Φ no es necesariamente inyectiva, puede existir cierto elemento $\frac{a}{s} \in {S_1}^{-1}A$ tal que $\frac{a}{s} \neq 0_{{S_1}^{-1}A}$ y cumpla $\frac{a}{s} = 0_{{S_2}^{-1}A}$ visto como elemento de ${S_2}^{-1}A$. Una condición suficiente para la inyectividad de Φ es que se tenga $S_2 \cap \mathrm{Div}_0(A) = \varnothing$.

3.2 Módulo de fracciones

De forma similar a como hemos procedido, consideremos A un anillo, $S \subset A$ un conjunto multiplicativamente cerrado y M un A-módulo. Consideremos el conjunto $M \times S$ y definamos en él la siguiente relación de equivalencia $\sim$: dados $(m_1, s_1), (m_2, s_2) \in M \times S$ se tiene

$$(m_1, s_1) \sim (m_2, s_2) \Longleftrightarrow \exists s \in S \; s(s_2 m_1 - s_1 m_2) = 0_M.$$

donde el producto que estamos considerando es el exterior de M como A-módulo.

Denotemos $S^{-1}M := M \times S/\sim$ y veamos que lo podemos dotar de una estructura tanto de A-módulo como de $S^{-1}A$-módulo. Definamos las siguientes operaciones:

$$\begin{array}{rrcl} + : & S^{-1}M \times S^{-1}M & \longrightarrow & S^{-1}M \\ & ([(m_1, s_1)], [(m_2, s_2)]) & \longmapsto & [(s_2 m_1 + s_1 m_2, s_1 s_2)] \end{array},$$

$$\begin{array}{rrcl} \cdot : & A \times S^{-1}M & \longrightarrow & S^{-1}M \\ & (a, [(m, s)]) & \longmapsto & [(am, s)] \end{array}$$

y

$$\begin{array}{rrcl} * : & S^{-1}A \times S^{-1}M & \longrightarrow & S^{-1}M \\ & ([(a, s_1)], [(m, s_2)]) & \longmapsto & [(am, s_1 s_2)] \end{array}.$$

Proposición 3.2.1. *Las aplicaciones $+$, $\cdot$ y $*$ están bien definidas.*

Prueba. La prueba para $+$ es análoga al caso de los anillos de fracciones. Veamos las otras dos.

Sean $(m, s), (m', s') \in M \times S$ tales que $(m, s) \sim (m', s')$. Existe $s^* \in S$ tal que $s^*(s'm - sm') = 0_M$. Así, dado $a \in A$, tenemos que

$$0_M = a(s^*(s'm - sm') = s^*(s'(am) - s(am')),$$

es decir, $(am, s) \sim (am', s')$ y $\cdot$ está bien definida.

Sean ahora $(a, s_1), (a', s_1') \in S^{-1}A$ y $(m, s_2), (m', s_2') \in M \times S$ tales que $(a, s_1) \sim (a, s_1')$ y $(m, s) \sim (m', s')$. Existen $s_3, s_3' \in S$ tales que

$$s_3(as_1' - a's_1) = 0_A \tag{3.7}$$

y

$$s_3'(s_2'm - s_2 m') = 0_M. \tag{3.8}$$

A partir de estas igualdades obtenemos las siguientes

$$s_3(as_1' - a's_1)(s_2' s_3 m) = 0_A(s_2' s_3 m) = 0_M \tag{3.9}$$

y

$$(a's_1 s_3)s_3'(s_2'm - s_2 m') = 0_M \tag{3.10}$$

y sumándolas resulta

$$s_3s_3'(s_1's_2'am - s_1s_2a'm') = 0_M,$$

es decir, $(am, s_1s_2) \sim (a'm', s_1's_2')$ y $*$ está bien definida. $\square$

Observación 3.2.2. En la prueba de $*$ hay que tener la precaución en este caso (y en comparación con las pruebas anteriores) de que el producto que se considera es el exterior de M. Más aún, los elementos de (3.7) son elementos de A y los de (3.8) lo son de M. El paso a (3.9) y (3.10) permite sumarlas.

De aquí en adelante, siempre que no haya posibilidad de confusión se omitirá el símbolo $*$.

Corolario 3.2.3. *$(S^{-1}M, +)$ dotado con el producto exterior $\cdot$ es un A-módulo.*

Corolario 3.2.4. *$(S^{-1}M, +)$ dotado con el producto exterior $*$ es un $S^{-1}A$-módulo.*

Prueba. Comprobemos que se verifican los cuatro axiomas de la definición de $S^{-1}A$-módulo.

i) En primer lugar, claramente se tiene

$$1_{S^{-1}A}\frac{m}{s} = \frac{1_A}{1_A}\frac{m}{s} = \frac{1_Am}{1_As} = \frac{m}{s}, \quad \text{para todo } \frac{m}{s} \in S^{-1}M.$$

ii) Sean $\frac{a}{s} \in S^{-1}M$ y $\frac{m_1}{s_1}, \frac{m_2}{s_2} \in S^{-1}M$. Tenemos

$$\begin{aligned}\frac{a}{s}\left(\frac{m_1}{s_1} + \frac{m_2}{s_2}\right) &= \frac{a}{s}\frac{s_2m_1 + s_1m_2}{s_1s_2} = \frac{as_2m_1 + as_1m_2}{ss_1s_2} \\ &\overset{i)}{=} \frac{s}{s}\frac{s_2m_1 + s_1m_2}{ss_1s_2} = \frac{as_2sm_1 + as_1sm_2}{ss_1ss_2} = \frac{am_1}{ss_1} + \frac{am_2}{ss_2}.\end{aligned}$$

iii) Ahora, dados $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}A$ y $\frac{m}{s} \in S^{-1}M$ se tiene

$$\begin{aligned}\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right)\frac{m}{s} &= \frac{a_1s_2 + a_2s_1}{s_1s_2}\frac{m}{s} = \frac{a_1s_2m + a_2s_1m}{s_1s_2s} \\ &\overset{i)}{=} \frac{s}{s}\frac{a_1s_2m + a_2s_1m}{s_1s_2s} = \frac{a_1s_2sm_1 + a_2s_1sm_2}{s_1ss_2s} = \frac{a_1m}{s_1s} + \frac{a_2m}{s_2s}\end{aligned}$$

iv) Por último, sean $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in S^{-1}A$ y $\frac{m}{s} \in S^{-1}M$. Resulta

$$\left(\frac{a_1}{s_1}\frac{a_2}{s_2}\right)\frac{m}{s} = \frac{(a_1a_2)m}{(s_1s_2)s} = \frac{a_1(a_2m)}{s_1(s_2s)} = \frac{a_1}{s_1}\left(\frac{a_2}{s_2}\frac{m}{s}\right).$$

□

En vista de este último resultado, parece natural definir un funtor, S^{-1}, entre las categorías Mod_A y $\mathrm{Mod}_{S^{-1}A}$ de tal manera que:

- $S^{-1}(M) := S^{-1}M$ para cada M A-módulo y,
- dados M y N A-módulos, para cada $f \in \mathrm{Hom}_A(M,N)$

$$S^{-1}(f) := S^{-1}f : \begin{array}{ccc} S^{-1}M & \longrightarrow & S^{-1}N \\ \frac{m}{s} & \longmapsto & \frac{f(m)}{s} \end{array}.$$

Lema 3.2.5. *Dados M_1, M_2 y M_3 A-módulos, $f \in \mathrm{Hom}_A(M_1,M_2)$ y $g \in \mathrm{Hom}_A(M_2,M_3)$ se verifica*

$$S^{-1}(g\circ f) = S^{-1}g \circ S^{-1}f.$$

Prueba. Dado $\frac{m}{s} \in M_1$ se tiene

$$S^{-1}(g\circ f)\left(\frac{m}{s}\right) = \frac{(g\circ f)(m)}{s} = \frac{g(f(m))}{s} = S^{-1}g\left(\frac{f(m)}{s}\right) = (S^{-1}g\circ S^{-1}f)\left(\frac{m}{s}\right).$$

□

Proposición 3.2.6. *Si $M' \xrightarrow{f} M \xrightarrow{g} M''$ es una sucesión exacta, entonces la sucesión*

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

también lo es.

Prueba. Veamos en primer lugar la inyectividad y la sobreyectividad de $S^{-1}f$ y $S^{-1}g$ respectivamente. Sea $\frac{m'}{s} \in S^{-1}M'$ tal que $S^{-1}f\left(\frac{m}{s}\right) = 0_{S^{-1}M}$. Por ser así, existe $t \in S$ de forma que $tf(m') = 0_M$ y, como $f \in \mathrm{Hom}_A(M',M)$ y es inyectiva, $tm' = 0_{M'}$, es decir, $\frac{m'}{s} = 0_{S^{-1}M'}$. Consideremos ahora $\frac{m''}{s} \in S^{-1}M''$. Dado $m'' \in M''$ y por ser g sobreyectiva existe $m \in M$ tal que $g(m) = m'$, es decir, $S^{-1}g\left(\frac{m}{s}\right) = \frac{m''}{s}$.

Comprobemos ahora que $\mathrm{im}(S^{-1}f) = \mathrm{Ker}(S^{-1}g)$. En primer lugar, como $g\circ f \equiv 0_{M''}$, el lema anterior nos dice que

$$0_{S^{-1}M''} \equiv S^{-1}(g\circ f) = S^{-1}g\circ S^{-1}f,$$

es decir, $\mathrm{im}(S^{-1}f) \subseteq \mathrm{Ker}(S^{-1}g)$. Por otra parte, dado $\frac{m}{s} \in \mathrm{Ker}(S^{-1}g)$, tenemos que existe $t \in S$ tal que $tg(m) = 0_{M''}$ y por ser g homomorfismo esto implica que $tm \in \mathrm{Ker}(g)$, es decir, existe a su vez $m' \in M'$ tal que $f(m') = tm$. Es por esto que basta considerar el elemento $\frac{m'}{ts}$ de forma que $f(\frac{m'}{ts}) = \frac{tm}{ts} = \frac{m}{s}$ y $\mathrm{Ker}(g) \subseteq \mathrm{im}(f)$. □

Podemos demostrar que el funtor S^{-1} es exacto de una forma alternativa. Para ello, probemos antes algunos resultados.

Proposición 3.2.7. *Dado un anillo A y un subconjunto multiplicativamente cerrado $S \subset A$ se tiene que $S^{-1}A$ es un A-módulo plano.*

Prueba. Para probarlo vamos a usar la caracterización por ecuaciones. Sean $a_i \in A$ y $\frac{\alpha_i}{s_i} \in S^{-1}A$, $i \in \{1, \dots, n\}$ tales que

$$\sum_{i=1}^{n} a_i \frac{\alpha_i}{s_i} = 0_{S^{-1}A}.$$

Denotando $s^* := \prod_{j=1}^{n} s_j$ y $s_i^* := \prod_{j \neq i} s_j$ resulta

$$0_{S^{-1}A} = \sum_{i=1}^{n} a_i \frac{\alpha_i}{s_i} = \sum_{i=1}^{n} a_i \frac{s_i^* \alpha_i}{s^*} = \frac{\sum_{i=1}^{n} a_i s_i^* \alpha_i}{s^*},$$

es decir, existe $t \in S$ tal que

$$t(\sum_{i=1}^{n} a_i s_i^* \alpha_i) = 0_A.$$

De esta forma, basta considerar $m_i' := \frac{1}{ts^*} \in S^{-1}A$ y $\lambda_{i,i} := ts_i^* \alpha_i \in A$ para tener

$$m_i = \lambda_{i,i} m_i'$$

y

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

□

Proposición 3.2.8. *Dado un anillo A, un subconjunto multiplicativamente cerrado $S \subset A$ y un A-módulo M se tiene*

$$S^{-1}A \otimes_A M \cong S^{-1}M.$$

Prueba. Definimos la aplicación

$$\begin{array}{rrcl} F: & S^{-1}A \times M & \longrightarrow & S^{-1}M \\ & (\frac{a}{s}, m) & \longmapsto & \frac{am}{s} \end{array}.$$

En primer lugar, veamos que F está bien definida. Sean $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ de forma que existe $s \in S$ tal que $s(s_2a_1 - s_1a_2) = 0_A$. Tenemos que

$$s(s_2a_1m - s_1a_2m) = 0_A \iff \frac{a_1m}{s_1} = \frac{a_2m}{s_2} \iff F\left(\frac{a_1}{s_1}, m\right) = F\left(\frac{a_2}{s_2}, m\right).$$

Por otro lado, es claro que F es A-bilineal. Así, tenemos que existe un único homomorfismo A-lineal $f : S^{-1}A \otimes_A M \longrightarrow S^{-1}M$ tal que $f(\frac{a}{s} \otimes m) = \frac{am}{s}$.

Comprobamos que f es inyectiva. Si $f(\frac{a}{s} \otimes m) = 0_M$, entonces $\frac{am}{s} = 0_{S^{-1}M}$, es decir, existe $t \in S$ tal que $tam = 0_M$. Así,

$$\frac{a}{s} \otimes m = \frac{ta}{ts} \otimes m = \frac{1_A}{ts} \otimes tam = 0_{S^{-1}A\otimes M}$$

La sobreyectividad es clara. Con todo f es un isomorfismo.]

De forma análoga, definimos la aplicación

$$\begin{array}{rccc} h: & S^{-1}M & \longrightarrow & S^{-1}A \otimes M \\ & \frac{m}{s} & \longmapsto & \frac{1_A}{s} \otimes m \end{array}.$$

De nuevo debemos comprobar que está bien definida. Dados $\frac{m_1}{s_1} = \frac{m_2}{s_2} \in S^{-1}M$ existe $s \in S$ tal que $s(s_2m_1 - s_1m_2) = 0_M$ o equivalentemente $ss_2m_1 = ss_1m_2$. Es por esto que

$$\begin{aligned} h\left(\frac{m_1}{s_1}\right) &= \frac{1_A}{s_1} \otimes m_1 = \frac{ss_2}{ss_2s_1} \otimes m_1 = \frac{1_A}{ss_2s_1} \otimes ss_2m_1 \\ &= \frac{1_A}{ss_2s_1} \otimes ss_1m_2 = \frac{ss_1}{ss_2s_1} \otimes m_2 = \frac{1_A}{s_2} \otimes m_2 = h\left(\frac{m_2}{s_2}\right). \end{aligned}$$

Por último, tenemos tanto que $h \circ f$ restringida a los elementos de la forma $\frac{a}{s} \otimes m \in S^{-1}A \otimes_A M$ como $f \circ h$ a los $\frac{m}{s} \in S^{-1}M$ resultan ser las respectivas identidades $\mathrm{Id}_{S^{-1}A\otimes_A M}$ y $\mathrm{Id}_{S^{-1}M}$; es decir, $f = h^{-1}$ y

$$S^{-1}A \otimes_A M \cong S^{-1}M.$$

□

Corolario 3.2.9. *El functor* $S^{-1} : \mathrm{Mod}_A \to \mathrm{Mod}_{S^{-1}A}$ *es exacto.*

Prueba. Dada la sucesión exacta $M' \xrightarrow{f} M \xrightarrow{g} M''$, tensorizando por el A-módulo plano $S^{-1}A$ resulta que

$$S^{-1}A \otimes_A M' \xrightarrow{\mathrm{Id}_{S^{-1}A} \otimes f} S^{-1}A \otimes_A M \xrightarrow{\mathrm{Id}_{S^{-1}A} \otimes g} S^{-1}A \otimes_A M''$$

también es exacta.

Sean $\varphi : S^{-1}A \otimes_A M' \longrightarrow S^{-1}M$ y $\psi : S^{-1}A \otimes_A M \longrightarrow S^{-1}M$ los isomorfismos que da la proposición anterior. Veamos que $\mathrm{Id}_{S^{-1}A} \otimes f = \psi^{-1} \circ S^{-1}f \circ \varphi$. Dado $\frac{a}{s} \otimes m \in S^{-1}A \otimes_A M'$, se tiene

$$\begin{aligned}
\psi^{-1} \circ S^{-1}f \circ \varphi\left(\frac{a}{s} \otimes m\right) &= \psi^{-1} \circ S^{-1}f\left(\frac{am}{s}\right) \\
&= \psi^{-1}\left(\frac{af(m)}{s}\right) \\
&= \frac{1_A}{s} \otimes af(m) = \frac{a}{s} \otimes f(m) = \mathrm{Id}_{S^{-1}A} \otimes f\left(\frac{a}{s} \otimes m\right).
\end{aligned}$$

Esto mismo se prueba para el homomorfismo $\mathrm{Id}_{S^{-1}A} \otimes g$ y los A-módulos M y M''.

De todo lo anterior se sigue que la sucesión

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

es exacta. □

Ejemplo 3.2.10. Sea A un anillo y $\mathfrak{p}_0 \in \mathrm{Spec}(A)$. Sea $S = A \setminus \mathfrak{p}_0$. S es multiplicativamente cerrado y definimos $A_{\mathfrak{p}_0} = S^{-1}A$. Existe una biyección, dada por la extensión-contracción, entre

$$\mathrm{Spec}(A_{\mathfrak{p}_0}) \longleftrightarrow \mathrm{Spec}(A) \backslash \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \cap (A \backslash \mathfrak{p}_0) = \varnothing\} = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \subset \mathfrak{p}_0\}$$

Esta relación es análoga a la que da el teorema de la correspondencia entre los ideales del cociente y los ideales del anillo que contienen al ideal por el que cocientamos.

Geométricamente, tomando $A \xrightarrow{\delta} A_{\mathfrak{p}_0}$, se considera $\delta^* : \mathrm{Spec}(A_{\mathfrak{p}_0}) \longrightarrow \mathrm{Spec}(A)$, siendo $\mathrm{im}(\delta^*) = \{\mathfrak{p} : \mathfrak{p} \subset \mathfrak{p}_0\}$. De esta forma, todo ideal primo de $A_{\mathfrak{p}_0}$ es el extendido de un ideal primo de A que está contenido en $\mathfrak{p}_0$. Es decir, todo ideal primo de $A_{\mathfrak{p}_0}$ está contenido en $\mathfrak{p}_0^e$.

$A_{\mathfrak{p}_0}$ es un anillo local. Su único ideal maximal es $\mathfrak{p}_0^e = \{\frac{x}{s} : x \in A, s \notin \mathfrak{p}_0\}$.

Definición 3.2.11. Sea $\mathfrak{p}$ un ideal primo de un anillo A. Un ideal $\mathfrak{q}$ se dice $\mathfrak{p}$-*primario* si $\mathfrak{q}$ es primario y $\sqrt{\mathfrak{q}} = \mathfrak{p}$.

Proposición 3.2.12. *Sea A un anillo, $\mathfrak{p}_0 \in \mathrm{Spec(A)}$, y $A_{\mathfrak{p}_0}$. Hay una biyección entre los ideales primos de A contenidos en $\mathfrak{p}_0$ y los ideales primos de $A_{\mathfrak{p}_0}$. Esta biyección conserva el ser $\mathfrak{p}_0$-primario.*

Prueba. Consideremos $\delta : A \longrightarrow A_{\mathfrak{p}_0}$. Supongamos $\mathfrak{q}$ $\mathfrak{p}_0$-primario. Veamos que $\mathfrak{q}^e$ es $A_{\mathfrak{p}_0}$-primario. Sean $\frac{x_1}{s_1}, \frac{x_2}{s_2} \in A_{\mathfrak{p}_0}$ tal que $\frac{x_1}{s_1}\frac{x_2}{s_2} \in \mathfrak{q}^e$. Supongamos que $\frac{x_1}{s_1} \notin \mathfrak{q}^e$. Se tiene $\frac{x_1}{s_1}\frac{x_2}{s_2} = \frac{q}{s}$, con $q \in \mathfrak{q}, s \notin \mathfrak{p}_0$. Esto es, existe $s' \notin \mathfrak{p}_0$ tal que $s'(sx_1x_2 - qs_1s_2) = 0_A$, luego $s'sx_1x_2 \in \mathfrak{q}$.

Como $\frac{x_1}{s_1} \notin \mathfrak{q}^e, x_1 \notin \mathfrak{q}$, pues de estarlo podríamos escribir $\frac{x_1}{s_1} = \frac{x_1}{1}\frac{1}{s_1} \in \mathfrak{q}^e$. Entonces, por ser $\mathfrak{q}$ $\mathfrak{p}_0$-primario, $s'sx_2 \in \sqrt{\mathfrak{q}} = \mathfrak{p}_0$. Por ser $\mathfrak{p}_0$ primo y $ss' \notin \mathfrak{p}_0$, $x_2 \in \mathfrak{p}_0$. Por tanto, existe un $n \in \mathbb{N}$ tal que $x_2^n \in \mathfrak{q}^n$, luego $(\frac{x_2}{s_2})^n \in \mathfrak{q}^e$. Hemos visto que $\mathfrak{q}^e$ es primario y que su raíz es $\mathfrak{p}_0$, pues $\frac{x_2}{s_2} \in \mathfrak{p}_0^e$.

Recíprocamente, tomemos un ideal $\mathfrak{q}'$ que sea $\delta(\mathfrak{p}_0)A_{\mathfrak{p}_0}$-primario. Nótese que $\delta(\mathfrak{p}_0)A_{\mathfrak{p}_0} = \mathfrak{p}_0^e$. Supongamos $x_1, x_2 \in A$ tal que $x_1x_2 \in \mathfrak{q}'^c$ y $x_1 \notin \mathfrak{q}'^c$. Esto es, $\frac{x_1x_2}{1} \in \mathfrak{q}'$. Como $\frac{x_1}{1} \notin \mathfrak{q}'$, se tiene que $\frac{x_2}{1} \in \mathfrak{p}_0^e$, ya que $\mathfrak{q}'$ es p_0^e-primario. Es decir, $x_2 \in \mathfrak{p}_0^{ec} = \delta^{-1}(\mathfrak{p}_0^e)$. Como $\mathfrak{p}_0^{ec} = \mathfrak{p}_0$, $x_2 \in \mathfrak{p}_0$. □

Observación 3.2.13. Dado $\mathfrak{p}_0 \in \operatorname{Spec}(A)$, $\mathfrak{p}_0^n$ no es necesariamente $\mathfrak{p}_0$-primario. Sin embargo, hay algo que se le aproxima bastante.

Tomando $A \xrightarrow{\delta} A_{\mathfrak{p}_0}$, $\mathfrak{p}_0^e$ es maximal. En este caso, sí tenemos que $(\mathfrak{p}_0^e)^n$ tiene por raíz un maximal, a saber $\mathfrak{p}_0^e$, p_0^e-primario. Se tiene que $((\mathfrak{p}_0^e)^n)^e$ es $\mathfrak{p}_0$-primario.

A esto se le llama *potencias simbólicas* y se denota $\mathfrak{p}_0^n$.

Tenemos ya maquinaria suficiente para construir anillos locales.

Teorema 3.2.14 (de Cayley). *Sean A un anillo, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y $f : M \longrightarrow M$ una aplicación A-lineal tal que $f(M) \subset \mathfrak{a}M$. Entonces, existen $a_i \in \mathfrak{a}, n \in \mathbb{N}$ tal que*

$$f^{(n)} + a_1 s^{(n-1)} + \cdots + a_i I_M = 0_{Hom_A(M,M)}$$

donde cada $f^{(i)} = f \circ \overset{(i)}{\ldots} \circ f$

Prueba. □

Lema 3.2.15 (de Nakayama). *Se expresa en tres formulaciones equivalentes.*

1. *Sea A un anillo local, $\mathfrak{m}$ su único ideal maximal y M un A-módulo finitamente generado. Si $\mathfrak{m}M = M$, entonces $M = 0$.*

2. *Sea A un anillo local, $\mathfrak{m}$ su único ideal maximal y M un A-módulo finitamente generado. Si $N \subset M$ y $N + \mathfrak{m}M = M$, entonces $M = N$.*

3. *Sea A un anillo local maximal y sea M un A-módulo finitamente generado. Entonces, el menor número de generadores de M como A-módulo es la dimensión de $M/\mathfrak{m}M$ como $A/\mathfrak{m}$-espacio vectorial.*

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 $A \in \mathrm{Obj(Ann)}$, 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

$$^{N}\!\!\diagup_{\mathrm{im}(u)} = \{\, 0 \,\}\,.$$

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

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

¿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.