Álgebra Conmutativa

Miguel González
mgonzalez.contacto@gmail.com
miguelgg.com

Mayo de 2022

$$\ker(f') \xrightarrow{i} \ker(f) \xrightarrow{p} \ker(f'') \xrightarrow{d} \operatorname{coker}(f') \xrightarrow{i'} \operatorname{coker}(f) \xrightarrow{p'} \operatorname{coker}(f'')$$

Revisado en 2022
Apuntes de la asignatura impartida por Rosario González
en la Universidad Autónoma de Madrid en Mayo de 2022.

Acerca de este documento

Estos apuntes son una versión revisada de los de la asignatura Álgebra Conmutativa del grado en matemáticas, tomados en Mayo de 2022 por Miguel González. La asignatura fue impartida por Rosario González. A los apuntes originales se les ha añadido esta página, una imagen de portada, y breves párrafos explicativos en las zonas menos completas. Asimismo se han revisado las erratas y completado los contenidos faltantes.

Este documento es:

- Una recopilación ordenada y directa de las definiciones y resultados más importantes del tema en cuestión, al nivel de los estudios de grado.
- Una colección de demostraciones completas de dichos resultados (salvo en los casos más básicos).
- Una *guía* para revisar de manera rápida las ideas que se han adquirido previamente, o para consultar enunciados puntuales que puedan no haberse comprendido en su totalidad.

Este documento NO es:

- Un libro de texto de la asignatura.
- Una colección de ejercicios para practicar los conceptos adquiridos.
- Un listado de ejemplos para ilustrar las ideas tratadas. A pesar de ello, en ocasiones se incluyen ejemplos puntuales que puedan ser de especial interés o curiosidad, pero se intentan reducir al mínimo en virtud del primer punto de la lista anterior.

Sobre Álgebra Conmutativa

Esta asignatura se centra en el estudio del álgebra de los anillos conmutativos con unidad, en su mayoría como herramienta de desarrollo de la geometría algebraica. De hecho, se hace una introducción a este último tema a través de las variedades afines y los esquemas afines. Se hace un repaso de la teoría de anillos, y se explora la teoría de módulos sobre anillos, localización, dependencia entera...

Requisitos previos

1. Conocimientos de álgebra (espacios vectoriales, grupos, anillos, extensiones de cuerpos).

Índice

1. Anillos conmutativos

Definición 1. Un **anillo** es una tripleta $(A, +, \cdot)$, donde A es un conjunto y $+, \cdot$ son operaciones binarias sobre A, tales que $(A, +)$ es un grupo abeliano (cuyo neutro se denotará 0_A o 0), $\cdot$ es asociativa y $\cdot$ es distributiva sobre $+$, esto es, $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$, para todos $a, b, c \in A$.

Como es habitual, en ocasiones se referirá simplemente al conjunto A como anillo, omitiendo las operaciones, por conveniencia. Asimismo, $a \cdot b$ se suele denotar simplemente ab.

Definición 2. El anillo A es **conmutativo** si la operación $\cdot$ lo es.

Definición 3. El anillo A tiene **elemento identidad** si $\exists 1_A \in A$ con $1_A \cdot a = a \cdot 1_A = a$ para todo $a \in A$.

Dicho elemento suele denotarse simplemente como 1 si no hay ambigüedad. **En adelante, todos los anillos se asumirán conmutativos y con elemento identidad.**

Proposición 1. *El elemento identidad de un anillo es único.*

Demostración. Dados los elementos identidad $1, \tilde{1} \in A$, se tiene de las propiedades del elemento identidad que $1 = 1 \cdot \tilde{1} = \tilde{1}$ □

Definición 4. Sea A un anillo y $S \subset A$ un conjunto que preserva las operaciones, es decir, que cumple $+(S \times S) \subset S$ y $\cdot(S \times S) \subset S$. Si además $(S, +) \leq (A, +)$ y $1_A \in S$, se dice que S es un **subanillo** de A.

En otras palabras, un subanillo es un subconjunto que tiene estructura de anillo (conmutativo y con identidad) cuando se restringen las operaciones a él.

Definición 5. Dados anillos A y B, se dice que $f : A \mapsto B$ es un **homomorfismo** si $f(a + a') = f(a) + f(a')$, $f(aa') = f(a)f(a')$ para todos $a, a' \in A$, y además $f(1_A) = 1_B$.

Es inmediato comprobar que la composición de homomorfismos es a su vez un homomorfismo.

Definición 6. Sea $f : A \mapsto B$ un homomorfismo. Se define su **núcleo** como $\ker(f) = f^{-1}(\{0\})$ y su **imagen** como $\mathrm{Im}(f) = f(A)$.

Observación 1. Se tiene, para cualquier homomorfismo $f : A \mapsto B$, que $\mathrm{Im}(f) \subset B$ es un subanillo. Sin embargo, en un anillo no trivial (en el que, por tanto, $1 \neq 0$), el conjunto $\ker(f)$ no es un subanillo porque $1 \notin \ker(f)$.

Definición 7. Si A es un anillo, se dice que $I \subset A$ es un **ideal** si $(I, +) \leq (A, +)$ y además $A \cdot I = I \cdot A = I$.

Por ejemplo, en cualquier homomorfismo de anillos, su núcleo es un ideal.

Definición 8. Si $I \subset A$ es un ideal, el grupo cociente A/I adquiere estructura de anillo con la operación $[a] \cdot [b] = [ab]$, y la aplicación $\pi : A \mapsto A/I$ es un homomorfismo sobreyectivo.

Observación 2. Existe una correspondencia biyectiva entre los ideales de A que contienen a I y los ideales de A/I, dada por asociar al ideal $J \subset A$ con $I \subset J$ el ideal $J/I = \pi(J)$, y al ideal $\bar{J} \subset A/I$ el ideal $\pi^{-1}(\bar{J})$. Esta correspondencia preserva las inclusiones.

Típicamente, se denota $x \equiv y \mod I$ si $\pi(x) = \pi(y)$, es decir, si $x - y \in I$.

Definición 9. Sea A un anillo. Se dice que $x \in A$ es un **divisor de cero** si $\exists y \in A$, $y \neq 0$ con $xy = 0$. Si A no tiene divisores de cero no nulos, se dice que es un **dominio entero o de integridad**. El conjunto de divisores de cero se denota por $Z(A)$.

Definición 10. Sea A un anillo. Se dice que $x \in A$ es **nilpotente** si $\exists n \in \mathbb{Z}_{>0}$ tal que $x^n = 0$. El mínimo tal n se denomina **orden de nilpotencia**. El conjunto de nilpotentes se denomina **nilradical** y se denota por $N(A)$.

Es inmediato ver que el nilradical $N(A)$ es un ideal.

Proposición 2. *Sea $N(A)$ el nilradical de A. Se tiene que $A/N(A)$ no tiene nilpotentes no nulos, es decir, que $N(A/N(A)) = (0)$.*

Demostración. Supongamos que $x \notin N(A)$ verifica que $\overline{x} \in A/N(A)$ es nilpotente. Esto quiere decir que $\overline{x}^n = 0$ luego $x^n \in N(A)$. Entonces, $(x^n)^m = 0_A$, en contradicción con que $x \notin N(A)$. □

Observación 3. Los elementos nilpotentes de un anillo son divisores de cero, es decir, $N(A) \subset Z(A)$. Por un lado, si $x = 0$, es automáticamente nilpotente y divisor de cero. Si $x \neq 0$ es nilpotente y $n > 1$ es su orden de nilpotencia, entonces $0 = x^n = x \cdot x^{n-1}$ con $x^{n-1} \neq 0$, luego es divisor de cero.

Definición 11. Sea A un anillo. Se dice que $x \in A$ es **unidad** si $\exists y \in A$ tal que $xy = 1$. El conjunto de todas las unidades de A se denota $\mathcal{U}(A)$ y tiene estructura de grupo con el producto de A.

Observando que si $x \in A$ es unidad, y además $y, y' \in A$ cumplen $xy = xy' = 1$, multiplicando por y a ambos lados sigue que $1y = 1y'$, luego $y = y'$. Es decir, tal elemento es único y se denota x^{-1}.

Definición 12. Un **ideal principal** de A es aquel de la forma $I = \{\lambda \cdot x : \lambda \in A\}$, donde x es un elemento prefijado de A. Se dice que I **está generado por** x y se denota $I = (x)$.

Definición 13. El anillo A es un **cuerpo** si es no nulo y se tiene que $\mathcal{U}(A) = A \setminus \{0\}$.

Proposición 3. *Si $x \in A$ es una unidad, no es divisor de cero. Por tanto, los cuerpos son dominios enteros.*

Demostración. Como $xx^{-1} = 1$, si fuese un divisor de cero, multiplicando a ambos lados por un $y \neq 0$ tal que $xy = 0$, sigue que $0 = y \cdot 1 = y$, una contradicción. □

El recíproco en general no es cierto ($\mathbb{Z}$ es un dominio que no es un cuerpo), aunque se cumple en anillos finitos.

Proposición 4. *Se tiene que A es un cuerpo $\iff$ los únicos ideales en A son $\{0\}$ y A $\iff$ todos los homomorfismos $f : A \mapsto B$ donde B es un anillo no nulo son inyectivos.*

Demostración. Demostramos las implicaciones *de izquierda a derecha* cíclicamente. Para la primera, si A es un cuerpo y $\{0\} \subsetneq I \subset A$ es un ideal, tomamos $x \in A$ no nulo y, como es unidad, se tiene que $x^{-1} \cdot x \in I$, es decir $1 \in I$ luego $I = A$. Para la segunda, cualquier homomorfismo $f : A \mapsto B$ cumple que $\ker(f) \subset A$ es un ideal, y no puede ser todo A porque $1 \mapsto 1$ y ninguno de ellos es el 0. Así, $\ker(f) = \{0\}$ luego es inyectivo. Para la última implicación, si A no fuera un cuerpo, habría una unidad no nula $x \in A$, en cuyo caso el ideal no nulo $I = (x) \subsetneq A$ permite construir el mapa $\pi : A \mapsto A/I$ que tiene núcleo I, no trivial. □

A continuación estudiaremos distintas operaciones con ideales.

Definición 14. Sean A un anillo, $\{I_m\}_{m \in M}$ una familia de ideales del mismo y $I, J \subset A$ dos ideales. Se definen:

1. La **suma de ideales** es el ideal $I + J = \{i + j : i \in I, j \in J\}$. Es el menor ideal que contiene a ambos. Asimismo, si M es infinita, puede definirse el ideal suma como $\sum_{m \in M} I_m = \{\sum_{m \in M} i_m : i_m \in I_m$, siendo los i_m no nulos una cantidad finita.$\}$.
2. Si M es finito, el **producto de ideales** es el ideal $\Pi_{m \in M} I_m = \{\sum \Pi_{m \in M} i_m : i_m \in I_m\}$. Es decir, es el ideal generado por los productos de elementos.

3. El **ideal intersección** está dado por la intersección de conjuntos $\bigcap_{m\in M} I_m$. Véase que, si M es finita, se tiene que $\Pi_{m\in M} I_m \subset \bigcap_{m\in M} I_m$.
4. El **conductor** de J en I es $(I : J) = \{x \in A : xJ \subset I\}$. Es inmediato comprobar que se trata de un ideal.
5. El **anulador** de I es $\mathrm{Ann}(I) = ((0) : I) = \{x \in A : xI = \{0\}\}$. Al ser un caso particular de conductor, es un ideal.
6. El **radical** de I es $\mathrm{rad}(I) = \sqrt{I} = \{x \in A : \exists n > 0, x^n \in I\}$. También es un ideal, como se verá en una proposición posterior.

Proposición 5. *Sea A un anillo, $I, J, L \subset A$ ideales y $\{I_m\}_{m\in M}$ una familia de ideales. Se tiene que:*

1. $I \subset (I : J)$.
2. $(I : J) \cdot J \subset I$.
3. $((I : J) : L) = ((I : L) : J) = (I : JL)$.
4. $(\bigcap_{m\in M} I_m : J) = \bigcap_{m\in M}(I_m : J)$.
5. $(I : \sum_{m\in M} I_m) = \bigcap_{m\in M}(I : I_m)$.

Demostración. 1 y 2 son evidentes de la definición. Para 3, veamos que $x \in ((I : J) : L) \iff xL \subset (I : J) \iff xLJ \subset I \iff x \in (I : JL)$. Para 4, se tiene que $x \in (\bigcap_{m\in M} I_m : J) \iff xJ \subset \bigcap_{m\in M} I_m \iff \forall m \in M,\ xJ \subset I_m \iff \forall m \in M,\ x \in (I_m : J)$. El punto 5 sigue del hecho de que $x \sum_{m\in M} I_m \subset I \iff \forall m \in M,\ xI_m \subset I$. □

Proposición 6. *Sea A un anillo, $I, J \subset A$ ideales. Se tiene que:*

1. $\mathrm{rad}(I)$ *es un ideal.*
2. $I \subset \mathrm{rad}(I)$.
3. $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$.
4. $\mathrm{rad}(IJ) = \mathrm{rad}(I \cap J) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$.
5. $\mathrm{rad}(I) = A \iff I = A$.
6. $\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$.

Demostración. El único aspecto no trivial de 1 es comprobar que si $a, b \in \mathrm{rad}(I)$, entonces $a + b \in \mathrm{rad}(I)$. Puesto que $a, b \in \mathrm{rad}(I)$ quiere decir que $a^r, b^s \in I$ para ciertos $r, s > 0$, consideramos ahora $(a+b)^{r+s} = \sum_{j=0}^{r+s} \binom{r+s}{j} a^j b^{r+s-j}$. Ahora, si $j \geq r$ entonces $a^j \in I$, y si $j < r$ entonces $r + s - j \geq s$ y por tanto $b^{r+s-j} \in I$. Por tanto, todos los sumandos pertenecen a I luego $(a + b)^{r+s} \in I$. Para 2, basta con ver que $x \in I$ puede leerse como $x^1 \in I$. Para 3, se tiene que $\supseteq$ sigue de 2, y si $x \in \mathrm{rad}(\mathrm{rad}(I))$ entonces $x^n \in \mathrm{rad}(I)$ luego $x^{nm} \in I$ así que $x \in \mathrm{rad}(I)$.

Para 4, por un lado, si $x \in \mathrm{rad}(IJ)$, entonces $x^n \in IJ \subset I \cap J$ luego $x \in \mathrm{rad}(I \cap J)$. Además, si $x \in \mathrm{rad}(I \cap J)$ entonces $x^n \in I \cap J$ luego $x^n \in I, J$ y por tanto $x \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$. Finalmente, si $x \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$, se tiene que $x^r \in I$, $x^s \in J$, de donde sigue que $x^{r+s} \in IJ$, luego $x \in \mathrm{rad}(IJ)$.

Para 5, como $I \subset \mathrm{rad}(I)$ se tiene $\Longleftarrow$. Para $\Longrightarrow$, dado $x \in A = \mathrm{rad}\, I$, sabemos que $x^n \in I$. En particular, $1^n = 1 \in I$ de tal modo que $A = (1) \subset I$.

Para 6, por un lado se tiene que $I + J \subset \mathrm{rad}(I) + \mathrm{rad}(J)$ luego $\mathrm{rad}(I + J) \subset \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$. Ahora, si $x \in \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$ es porque hay un $n > 0$ con $x^n = y + z$, que cumplen que hay $r, s > 0$ con $y^r \in I$, $z^s \in J$. Entonces, $(x^n)^{r+s} = (y + z)^{r+s} \in I + J$. □

Observación 4. Es posible definir el radical de un conjunto cualquiera $E \subset A$ como $\operatorname{rad}(E) = \{x \in A : x^n \in E\}$, aunque en este caso no es necesariamente un ideal. Con esta definición, se tiene evidentemente que $\operatorname{rad}(\bigcup_{i\in I} E_i) = \bigcup_{i\in I} \operatorname{rad}(E_i)$.

Proposición 7. *Sea A un anillo y $Z(A)$ sus divisores de cero. Entonces, $Z(A) = \bigcup_{x\neq 0} \operatorname{Ann}(x) = \operatorname{rad}(Z(A)) = \bigcup_{x\neq 0} \operatorname{rad}(\operatorname{Ann}(x))$.*

Demostración. Nótese que $Z(A)$ no es necesariamente un ideal al no ser cerrado por la suma. La única igualdad que no es inmediata es $Z(A) = \operatorname{rad}(Z(A))$. Si $x \in \operatorname{rad}(Z(A))$, entonces x^n es un divisor de cero, es decir, hay un $y \neq 0$ con $x^n y = 0$. Si x no fuese divisor de cero, entonces $x^{n-1}y = 0$, de donde $x^{n-1} \in Z(A)$, lo cual permite argumentar por descenso para concluir que $x \in Z(A)$. □

Observación 5 (Ejemplos en $\mathbb{Z}$). Si $A = \mathbb{Z}$, $I = (m)$, con $m = \Pi p^{m_p}$ la factorización en primos y $J = (n)$ con $n = \Pi p^{n_p}$, existen interpretaciones más sencilla para las operaciones de ideales, fácilmente verificables:

1. $I + J = (\gcd(m, n))$, por Bézout.
2. $I \cap J = (\operatorname{mcm}(m, n))$.
3. $IJ = (mn)$.
4. $(I : J) = (k)$, donde k contiene los primos que le faltan a n para ser múltiplo de m, es decir $k = \Pi p^{\max\{m_p - n_p, 0\}}$.
5. $\operatorname{rad}(I) = (\Pi p \cdot \chi(m_p > 0))$.

Definición 15. Un anillo A es **reducido** si $N(A) = (0)$.

Por tanto, los dominios de integridad (y, por consiguiente, los cuerpos) son reducidos.

Teorema 1 (Isomorfía)**.** *Si $f : A \mapsto B$ es un homomorfismo de anillos, induce otro morfismo $\bar{f} : A/\ker(f) \mapsto B$ inyectivo, tal que $\bar{f}(A/\ker(f)) = f(A)$ y $f = \bar{f} \circ \pi$. En particular, $A/\ker(f) \simeq f(A)$ (a través de $\bar{f}$).*

Demostración. Basta con tomar $\bar{f}([a]) := f(a)$. Es fácil comprobar que está bien definido, comparte imagen con f, tiene núcleo trivial y es homomorfismo de anillos. □

Observación 6. Esto es un caso particular de la propiedad universal de los conjuntos cocientes: si A es un anillo e $I \subset A$ un ideal, dado cualquier homomorfismo $f : A \mapsto B$ que cumpla $I \subset (\ker f)$, existe un único homomorfismo $\bar{f} : A/I \mapsto B$ tal que $\bar{f} \circ \pi = f$. Este se define como $\bar{f}(\bar{x}) := f(x)$, está bien definido, comparte imagen con f y cumple $\ker(\bar{f}) = \ker(f)/I$.

Definición 16. La **característica** de un anillo A es el menor entero positivo tal que $\forall x \in A$, $nx = 0$ (aquí nx es x sumado n veces), o bien 0 si no existe tal entero. Se denota por $\operatorname{char} A$. Equivalentemente basta con considerar los n con $n \cdot 1 = 0$, o bien mirar al único homomorfismo $f : \mathbb{Z} \mapsto A$, cuyo núcleo es de la forma $\operatorname{char} A \cdot \mathbb{Z}$.

Proposición 8. *En un dominio de integridad A, se cumple* $\operatorname{char} A = p$ *primo o bien* $\operatorname{char} A = 0$.

Demostración. Si la característica no es nula y es un número compuesto $n = ab$, entonces $ab \cdot 1 = 0$, es decir, $(a \cdot 1) \cdot (b \cdot 1) = 0$ lo que contradice que sea un dominio. También puede verse considerando el $f : \mathbb{Z} \mapsto A$, que cumple $\mathbb{Z}/\ker(f) \simeq f(A)$. Como $f(A)$ es un dominio, debe darse que $\ker(f) = a\mathbb{Z}$ con a primo o 0. □

Por distributividad, se tiene claramente que $I(J+L) = IJ+IL$. En ocasiones, además, la intersección conmuta con la suma. Por ejemplo, en los ideales de $\mathbb{Z}$ es así, o bien:

Proposición 9 (Ley modular)**.** *Si $I, J, L \subset A$ son ideales y $J \subset I$, entonces $I \cap (J + L) = I \cap J + I \cap L$.*

Demostración. Siempre se tiene $\supseteq$, dado que $x \in I \cap J + I \cap L$ implica que $x = j + l$ con $j \in J$, $l \in L$ y $j, l \in I$. Entonces, $x \in I$ y $x \in J + L$, como se quería. Para el recíproco, si $x \in I \cap (J + L)$, entonces $x = j + l$ con $j \in J \subset I$ y $l \in L$. Por tanto, $l = x - j \in I$ y entonces $j \in J \cap I$ y $l \in I \cap L$, como se quería. □

Proposición 10. *Se tiene que $(I \cap J)(I + J) \subset IJ$*

Demostración. $(I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subset JI + IJ = IJ$. □

En particular, si $I + J = A$ entonces $I \cap J = (I \cap J)(I + J) \subset IJ$, y como la otra inclusión vale siempre, se tiene que $I \cap J = IJ$.

Definición 17. Sea M un conjunto finito o numerable de índices (sin perder generalidad, $M = \mathbb{N}$ o $M = \{1, \dots, n\}$). Sea $\{A_m\}_{m \in M}$ una familia de anillos indexada por M. Se define la **suma directa** como:

$$\bigoplus_{m \in M} A_m = \{(a_1, \dots, a_i, \dots) : a_m \in A_m, \text{con solo una cantidad finita de elementos no nulos}\}.$$

Las operaciones se definen de la manera natural elemento a elemento. Si M es finito, tiene elemento unidad $(1, 1, \dots, 1)$ pero, si M es infinito, no tiene unidad.

Definición 18. Sea M un conjunto finito o numerable de índices (sin perder generalidad, $M = \mathbb{N}$ o $M = \{1, \dots, n\}$). Sea $\{A_m\}_{m \in M}$ una familia de anillos indexada por M. Se define el **producto directo** como:

$$\prod_{m \in M} A_m = \{(a_1, \dots, a_i, \dots) : a_m \in A_m\},$$

es decir, el producto cartesiano. Las operaciones se definen de la manera natural elemento a elemento. El elemento unidad es $(1, 1, 1, \dots)$.

Evidentemente, si M es finito, ambas nociones son iguales. Se tienen homomorfismos de anillos sobreyectivos naturales a la proyección sobre cada coordenada: $\bigoplus_{m \in M} A_m \mapsto A_i$, $\prod_{m \in M} A_m \mapsto A_i$, y aplicaciones inyectivas naturales de inclusión: $A_i \mapsto \bigoplus_{m \in M} A_m$, $A_i \mapsto \prod_{m \in M} A_m \mapsto A_i$, que son homomorfismos de grupos compatibles con el producto pero no envían el elemento unidad en el elemento unidad $(1 \mapsto (0, 0, \dots, 0, 1, 0, \dots))$.

Proposición 11 (Propiedad universal del producto)**.** *Sea $A = \prod_{m \in M} A_m$ el producto directo de los anillos $\{A_m\}_{m \in M}$. Supongamos que existen otro anillo B y homomorfismos $f_m : B \mapsto A_m$. Entonces, existe un único homomorfismo $f : B \mapsto A$ tal que $\pi_r \circ f = f_r$, donde $\pi_r : A \mapsto A_r$ es la proyección natural.*

Demostración. Puede construirse como $f(b) = (f_m(b))_{m \in M}$. Además, si hubiera otro $\tilde{f}$, como $\pi_r \circ f = f_r = \pi_r \circ \tilde{f}$, seguiría que todas las *coordenadas de f y $\tilde{f}$* coincidirían, con lo que $f \equiv \tilde{f}$. □

Proposición 12. *Sea A un anillo y $\{I_j\}_{j=1}^n$ una familia de ideales. Consideramos (a partir de la propiedad universal previa) el morfismo $\varphi : A \mapsto \prod_j A/I_j$. Entonces:*

1. *Si $I_i + I_j = A$ siempre que $i \neq j$, entonces $I_1 \dots I_n = I_1 \cap \dots \cap I_n$.*
2. *φ es sobreyectiva $\iff$ $I_i + I_j = A$ siempre que $i \neq j$.*
3. *φ es inyectiva $\iff$ $\bigcap_j I_j = (0)$.*

4. Si $I_i + I_j = A$ siempre que $i \neq j$, entonces $\prod A/I_j \simeq A/\bigcap_j I_j = A/\prod_j I_j$.

Demostración. El 1 se ha visto para 2 ideales, por lo que, inductivamente, basta con ver que se cumple que $I_1 \dots I_{n-1}$ y I_n son coprimos (es decir, su suma da A) y aplicar el caso $n = 2$. Sabemos que existen $x_i \in I_i$, $y_i \in I_n$ tales que $x_i + y_i = 1$. Por tanto, el elemento $\prod x_i = \prod(1 - y_i)$ está en $1 + I_n$. Por tanto, $1 \in \prod_{i=1}^{n-1} I_i + I_n$, como se quería.

Para 2, si φ es sobreyectiva, entonces existe un elemento $x \in A$ tal que $\varphi(x) = (0, \dots, 0, 1, 0, \dots, 0)$, con el 1 en la posición i-ésima. Este elemento, por tanto, cumple $x \in 1 + I_i$ y $x \in I_j$ para $j \neq i$. Entonces, $1 = (1 - x) + x \in I_i + I_j$, como se quería. Por otro lado, si se tiene la condición de coprimalidad dos a dos, dado un elemento $(0, \dots, x, \dots, 0)$ con x en la posición i y $x \notin I_i$, es posible obtener para $j \neq i$ elementos $x_j \in I_j$, $y_j \in I_i$ tales que $x_j + y_j = x$. Entonces, el $y = \prod x_j = \prod(x - y_j)$ verifica que $\pi_j(y) = 0$ si $j \neq 0$, y $\pi_i(y) = x$, luego $\varphi(y) = (0, \dots, x, \dots, 0)$. Esto ya basta para probar que φ es sobreyectiva, porque todos los elementos de la imagen pueden descomponerse como suma de estos.

Para 3, basta con darse cuenta de que $\ker(f) = \bigcap_j I_j$. Con esto, y el 2, sigue el 4 del teorema de isomorfía.

Definición 19. Un ideal $I \subsetneq A$ es **primo** si $\forall x, y \in A$ con $xy \in I$, se tiene $x \in I$ o $y \in I$. Equivalentemente, es primo si A/I es un dominio de integridad no nulo.

Definición 20. Un ideal $I \subsetneq A$ es **maximal** si no existe un ideal $J \subsetneq A$ con $I \subsetneq J$. Equivalentemente, es maximal si A/I es un cuerpo (recordemos que el anillo nulo no es un cuerpo).

Definición 21. Un ideal $I \subsetneq A$ es **primario** si $\forall x, y \in A$ tales que $xy \in I$, se tiene $x \in I$ o $y \in \mathrm{rad}(I)$, es decir, $x \in I$ o $y^n \in I$ para cierto $n > 0$. Equivalentemente, es primario si A/I es no nulo y cumple que todo divisor de cero suyo es nilpotente.

Vamos a comprobar la definición equivalente en este último caso. Si $\bar{y}$ es un divisor de cero del cociente, entonces $\bar{x}\bar{y} = 0$ en el cociente, con $\bar{x} \neq 0$. Entonces, al ser primario, se tiene $x \in I$ o $y^n \in I$. No puede ser $x \in I$ porque $\bar{x} \neq 0$, luego $y^n \in I$ de donde $\bar{y}^n = 0$, como se quería. Para el recíproco, si $xy \in I$ con $x \notin I$, entonces $\bar{y}$ es divisor de cero en el cociente, luego $\bar{y}^n = 0$, es decir, $y^n \in I$.

Definición 22. Sea A un anillo. Se define el **espectro primo** de A como $\mathrm{Spec}(A) = \{P \subset A,\ \text{P primo}\}$.

Proposición 13. *Sea $f : A \mapsto B$ un homomorfismo de anillos. Si $I \subset B$ es un ideal, entonces $f^{-1}(I) \subset A$ también. Además, $I \in \mathrm{Spec}(B) \implies f^{-1}(I) \in \mathrm{Spec}(A)$.*

Demostración. Es un ideal por ser el núcleo de $\pi \circ f : A \mapsto B \mapsto B/I$. Además, si I es primo y $xy \in f^{-1}(I)$, entonces $f(xy) \in I$, luego $f(x)f(y) \in I$. De aquí sigue que $f(x)$ o $f(y)$ está en I, luego x o y está en $f^{-1}(I)$. □

No se cumple, sin embargo, que la preimagen de un maximal sea maximal. Basta con considerar, por ejemplo, $i : \mathbb{Z} \mapsto \mathbb{Q}$ junto con el ideal (0).

Observación 7. Sean $M_1, M_2 \subset A$ ideales maximales distintos. Entonces $M_1 + M_2 = A$.

Esto es así porque, por un lado, no pueden ser nulos (porque si, por ejemplo, M_1 fuera nulo, se tendría $M_1 \subsetneq M_2$ y no sería maximal), pero entonces $M_1 \subsetneq M_1 + M_2$, luego ha de ser forzosamente $M_1 + M_2 = A$.

Lema 1 (Zorn)**.** *Sea $(S, \preceq)$ un conjunto parcialmente ordenado tal que toda cadena $T \subset S$ (recordemos que una cadena es un subconjunto totalmente ordenado) tiene una cota superior en S. Entonces, S admite un elemento maximal.*

Teorema 2. *Todo anillo A no nulo admite un ideal maximal.*

Demostración. Basta con tomar $S \neq \emptyset$ el conjunto de ideales propios de A, ordenado por inclusión. En tal caso, si $T = \{I_m\}_{m \in M}$ es una cadena, se cumple que $I = \bigcup_{m \in M} I_m$ es un ideal de A (aquí es esencial que los ideales formen una cadena, dado que, si no, podría no ser cerrado a la suma). Además, es propio porque $1 \neq I$. Entonces, I es una cota superior para T y por tanto S admite un elemento maximal. □

Observación 8. Si $I \subsetneq A$ es un ideal propio en A, existe un ideal maximal M con $I \subset M$. En particular, si $x \notin \mathcal{U}(A)$, entonces, al ser (x) propio, existe un ideal maximal que contiene a x.

Para demostrarlo, basta con considerar A/I y aplicar el teorema previo.

Definición 23. Sea A un anillo. Se dice que A es **local** si solo admite un único ideal maximal M. En ese caso, A/M se denomina **cuerpo de residuos de** M.

Por otro lado, se dice que A es **semilocal** si admite un número finito de ideales maximales.

Observemos que si A es local con maximal M y $x \notin U(A)$, por uno de los comentarios previos ha de darse que $x \in M$, luego $A \setminus M \subset \mathcal{U}(A)$. Esta condición es equivalente a la localidad:

Proposición 14. *Sea A un anillo con un ideal $M \subsetneq A$ tal que $A \setminus M \subset \mathcal{U}(A)$. Entonces A es local con maximal M.*

Demostración. Sea $I \subsetneq A$ un ideal propio. Por ser propio, $I \subset A \setminus \mathcal{U}(A)$, de tal modo que $I \subset M$ dado M contiene a todos los elementos que no son unidades. □

Proposición 15. *Sea A un anillo con un ideal maximal $M \subsetneq A$ que cumple que $\{1_A\} + M = \{1_A + m : m \in M\} \subset \mathcal{U}(A)$. Entonces A es local (luego su único maximal es M).*

Demostración. Sea $x \in A \setminus M$. Como M es maximal, debe darse que $(x) + M = A$ (porque $M \subsetneq (x) + M$). Por tanto, se tienen $a \in A$ y $m \in M$ con $ax + m = 1$, es decir, $ax = 1 - m \in 1_A + M \subset \mathcal{U}(A)$. Como ax es una unidad, ha de ser que x lo sea (porque $(tx) \subset (x)$), luego puede aplicarse la proposición previa. □

Proposición 16. *Se tiene que* $N(A) = \bigcap_{P \in \mathrm{Spec}(A)} P$.

Demostración. Sea $z \in N(A)$. Entonces, $0 = z^n \in P$ para cualquier ideal primo P, y, por ser primo, $z \in P$, lo que prueba una de las inclusiones. Por otro lado, si $z \notin N(A)$, podemos denotar $S = \{I \subset A : I \text{ ideal, y} \forall n > 0, z^n \notin I\}$. Este conjunto contiene al ideal (0) porque $z \notin N(A)$, luego $S \neq \emptyset$, y está ordenado por inclusión de tal manera que toda cadena tiene una cota superior (la unión de la cadena). Por el lema de Zorn, tiene un elemento maximal P. Por hipótesis, $z \notin P$, luego solo falta ver que P es primo. Si $x, y \notin P$, entonces $P + (x)$ y $P + (y)$ contienen estrictamente a P, luego, por maximalidad, existen r, s con $z^r \in P + (x), z^s \in P + (y)$. De aquí sigue que $z^{r+s} \in P + (xy)$, luego forzosamente ha de ser $xy \notin P$ o si no sería $P \notin S$. Por tanto, P es primo. □

Proposición 17. *Sea $I \subset A$ un ideal y $\pi : A \mapsto A/I$ el paso al cociente. Entonces, el ideal $\pi^{-1}(N(A/I))$ que corresponde a $N(A/I)$ es precisamente* $\mathrm{rad}(I)$. *En particular,* $\mathrm{rad}(I) = \bigcap_{P \in \mathrm{Spec}(A), I \in P} P$.

Demostración. $x \in \pi^{-1}(N(A/I)) \iff [x^n] = [0] \iff x^n \in I \iff x \in \mathrm{rad}(I)$. Para probar lo segundo basta con usar la proposición previa para $N(A/I)$, y tomar preimágenes. □

Estas caracterizaciones motivan la siguiente definición:

Definición 24. Sea A un anillo. El **radical de Jacobson** de A es el ideal $J(A) = \bigcap_{M \in \mathrm{Spm}(A)} M$, donde $\mathrm{Spm}(A)$ es el *espectro maximal*, es decir, el conjunto de ideales maximales.

Los elementos del radical de Jacobson se pueden caracterizar de esta otra manera:

Proposición 18. *Se tiene que $x \in J(A) \iff \forall y \in A,\ 1 - xy \in \mathcal{U}(A)$.*

Demostración. Supongamos que $1 - xy \notin \mathcal{U}(A)$ para cierto y. Entonces, se tiene un ideal maximal M con $1 - xy \in M$. Si fuese $x \in M$, entonces se tendría $1 - xy + xy = 1 \in M$, lo cual no es posible. Por tanto, $x \notin J(A)$. Por otra parte, si $1 - xy \in \mathcal{U}(A)$ para cualquier $y \in A$, pero $x \notin M$ para cierto maximal M, entonces $A = M + (x)$, luego $1 = m + tx$ con $m \in M$, $t \in A$. Como $1 - tx$ es una unidad, sigue que $(m + tx) - tx = m$ es una unidad, contradiciendo que M sea maximal. □

Proposición 19. *Sea $I \subset A$ un ideal. Si* $\mathrm{rad}(I)$ *es maximal, entonces I es primario.*

Demostración. Recordemos que $\mathrm{rad}(I) = \bigcap_{P \in \mathrm{Spec}(A), I \subset P} P$. Como $\mathrm{rad}(I)$ es maximal, aparece en la intersección de la derecha, lo que implica que no hay más ideales primos que contengan a I (si hubiera otro primo P que contenga a I, tendría que ser $\mathrm{rad}(I) \subset P \cap \mathrm{Spec}(A)$, luego $\mathrm{Spec}(A) \subset P$, y por maximalidad $P = \mathrm{Spec}(A)$). De esta manera, pasando al cociente, A/I solo tiene un ideal primo y, por tanto, solo tiene un ideal maximal (que es $\mathrm{rad}(I)/I$). Esto implica que todos los elementos de A/I son unidades o están en $\mathrm{rad}(I)/I$, luego todos los divisores de cero son nilpotentes en A/I, lo que equivale a que I sea primario. □

La demostración previa también puede hacerse de manera elemental, sin invocar las proposiciones sobre radicales.

Proposición 20. *Sea A un anillo y $\{P_j\}_{j=1}^n$ una cantidad finita de ideales primos. Si $I \subset A$ es otro ideal, y $I \subset \bigcup_j P_j$, entonces $I \subset P_{j_0}$ para cierto j_0. Por otro lado, si $\{I_j\}_{j=1}^n$ son ideales y $P \subset A$ es un ideal primo con $\bigcap_j I_j \subset P$, entonces $I_{j_0} \subset P$ para cierto j_0.*

Demostración. Comenzamos demostrando la primera afirmación. Si $n = 1$ el resultado es evidente, así que procedemos ahora por inducción. Supongamos que $I \subset \bigcup_{i=1}^n P_j$ pero $I \nsubseteq P_j$ para todo j. Por hipótesis de inducción, ha de ser que $I \nsubseteq \bigcap_{j=1, j\neq i}^n P_j := U_i$ para todos los i. Sea $x_i \in I \setminus U_i$. Es necesario que $x_i \in P_i$, dado que, en caso contrario, se tendría que $x_i \notin U_i \cup P_i = \bigcup_{i=1}^n P_i$ y por tanto $x_i \notin I$. Denotamos $\hat{x}_i = \prod_{j=1, j\neq i}^n \hat{x}_i$. Sea $y = \sum_{i=1}^n \hat{x}_i$. Como $y \in I$, ha de ser $y \in \bigcup_{i=1}^n P_i$ y por tanto $y \in P_k$ para cierto k. Entonces, $\hat{x}_k = y - \sum_{i\neq k} \hat{x}_i \in P_k$ al estarlo todos los sumandos. Por primalidad de P_k, alguno de los factores de $\hat{x}_k$, digamos x_l con $l \neq k$, verifica $x_l \in P_k$. Entonces $x_l \in U_l$, cosa imposible porque x_l se eligió en $I \setminus U_l$.

Para la segunda afirmación, si un tal P cumpliese $I_j \subsetneq P$ para todo j, bastaría con tomar los $x_j \in I_j \setminus P$ y considerar $y = \prod_{j=1}^n x_j$. Este elemento cumple $y \in \bigcap_{j=1}^n I_j$, pero $y \notin P$ (porque si $y \in P$, por primalidad, alguno de sus factores estaría en P). □

Definición 25. Sea $f : A \mapsto B$ un homomorfismo. Sea $I \subset A$ un ideal. Se define la **extensión de I por f** como el ideal $I^e = \langle f(I) \rangle \subset B$. Sea $J \subset B$ un ideal. Se define la **contracción de J por f** como el ideal $J^c = f^{-1}(J)$.

Proposición 21. *Sea $f : A \mapsto B$ un homomorfismo. Sean $I \subset A$ y $J \subset B$ ideales. Entonces:*

1. $I \subset I^{ec}$.
2. $J^{ce} \subset J$.
3. $J \in \mathrm{Spec}(B) \implies J^c \in \mathrm{Spec}(A)$.
4. $I^{ece} = I^e$.
5. $J^{cec} = J^c$.
6. *Si $\mathcal{C}$ son los ideales $I \subset A$ con $I^{ec} = I$, y $\mathcal{D}$ son los ideales $J \subset B$ con $J^{ce} = J$, entonces existe una correspondencia biyectiva entre ambos conjuntos, dada por $\varphi : \mathcal{C} \mapsto \mathcal{D}$ con $\varphi(I) = I^e$, cuya inversa es $\varphi^{-1} : \mathcal{D} \mapsto \mathcal{C}$ dada por $\varphi^{-1}(J) = J^c$.*

Demostración. Para 1, se tiene que $I \subset f^{-1}(f(I)) \subset f^{-1}(I^e) = I^{ec}$. Para 2, se tiene que $f(J^c) = f(f^{-1}(J)) \subset J$, de modo que $J^{ce} = \langle f(J^c) \rangle \subset J$ al ser J un ideal. El 3 ya se probó en la proposición 13. El 4 sigue de que $I^{ece} \subset I^e$ por 2, pero también $I^e \subset I^{ece}$ dado que $I \subset I^{ec}$ por 1. El 5 sigue de que $J^c \subset J^{cec}$ por 1, pero como $J^{ce} \subset J$ por 2, tomando preimagen sigue $J^{cec} \subset J^c$. El 6 sigue de que esas aplicaciones están bien definidas por 4 y 5, y además evidentemente son inversas luego biyectivas. □

La extensión y contracción de ideales se relacionan con las operaciones de ideales como sigue:

Proposición 22. *Sean $I_1, I_2 \subset A$ y $J_1, J_2 \subset B$ ideales. Sea $f : A \mapsto B$ un homomorfismo. Entonces:*

1. $(I_1 + I_2)^e = I_1^e + I_2^e$.
2. $J_1^c + J_2^c \subset (J_1 + J_2)^c$.
3. $(I_1 \cap I_2)^e \subset I_1^e \cap I_2^e$.
4. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.
5. $(I_1 I_2)^e = I_1^e I_2^e$.
6. $J_1^c J_2^c \subset (J_1 J_2)^c$.
7. $\mathrm{rad}(I)^e \subset \mathrm{rad}(I^e)$.
8. $\mathrm{rad}(J)^c = \mathrm{rad}(J^c)$.

Todas ellas se verifican fácilmente de las propiedades de la preimagen e imagen, así como de las definiciones de las operaciones entre ideales.

Ahora completamos los teoremas de isomorfía:

Teorema 3. *Sea A un anillo, $S \subset A$ un subanillo y $I \subset A$ un ideal. Entonces, $(S + I)/I \simeq S/(I \cap S)$.*

Demostración. Basta con considerar $S \hookrightarrow S + I \mapsto (S + I)/I$ las aplicaciones naturales. Claramente la composición es sobreyectiva y su núcleo es $(S \cap I)$, luego puede aplicarse el primer teorema de isomorfía. □

Teorema 4. *Sea A un anillo y sean $I \subset J \subset A$ ideales. Entonces, $(A/I)/(J/I) \simeq A/J$.*

Demostración. Consideramos $A/I \mapsto A/J$ que envía $a + I$ en $a + J$. Está bien definida porque $I \subset J$ y es sobreyectiva. Su núcleo es J/I luego basta con aplicar el primer teorema de isomorfía. □

Proposición 23. *Sea A un anillo y $A[X]$ su anillo de polinomios. Sea $b \in A$. Entonces $A[X]/(x-b) \simeq A$.*

Demostración. Basta con considerar la aplicación $f_b : A[X] \mapsto A$ dada por *evaluar en b*, es decir, $\sum_{j=0}^n a_j X^j \mapsto \sum_{j=0}^n a_j b^j$. Evidentemente, es un homomorfismo y sobreyectivo (porque, de hecho, $f_b(A) = A$). Además, $\ker f_b = (x-b)$ (esto sigue de dividir euclídeamente un polinomio dado por $x-b$, que siempre es posible por ser el polinomio mónico), luego sigue el resultado del primer teorema de isomorfía. □

Proposición 24. *Sea A un anillo. Sea $I \subset A$ un ideal. Sea $P = A[X_1, \ldots, X_n]$. En este caso, se tiene $(I) = IP$ un ideal en P. Entonces, se verifica que $P/IP \simeq (A/I)[X_1, \ldots, X_n]$.*

Demostración. Basta con considerar $\pi : P \mapsto (A/I)[X_1, \ldots, X_n]$ dado por enviar los coeficientes del polinomio a sus clases en A/I. De nuevo, está claro que es un homomorfismo sobreyectivo, y $\ker \pi = IP$. □

Proposición 25. *Sea A un anillo, $P = A[X_1, \ldots, X_n]$. Sean $a_1, \ldots, a_m \in A$ con $m \leq n$. Sea $I = (X_1 - a_1, \ldots, X_m - a_m)$. Entonces $P/I \simeq A[X_{m+1}, \ldots, X_n]$.*

Demostración. Cabe observar en primer lugar que basta probarlo para $m = n$. En caso contrario, basta con observar que $P = (A[X_{m+1}, \ldots, X_n])[X_1, \ldots, X_m]$, que tiene m indeterminadas con coeficientes en $A[X_{m+1}, \ldots, X_n]$. Después, se aplica el resultado (dado que en este caso $m = n$), y entonces $P/I \simeq A[X_{m+1}, \ldots, X_n]$, el anillo de coeficientes, como se quería.

Para probar el caso $m = n$, se procede por inducción. El caso $n = 1$ ha sido demostrado en la proposición 23. Ahora, escribimos $P' = A[X_1, \ldots, X_{n-1}]$ e $I' = (X_1 - a_1, \ldots, X_{n-1} - a_{n-1})$. Por hipótesis

de inducción, se tiene que $P'/I' \simeq A$. Ahora, como $P = P'[X_n]$, por la proposición previa sigue que $P/(I'P) \simeq (P'/I')[X_n] \simeq A[x_n]$.

Ahora, observamos que $P/I \simeq (P/I'P)/(IP/I'P)$, por el segundo teorema de isomorfía, y que $I = I'P + (X_n - a_n)P$ (por definición de I' e I). De esta última expresión sigue que $I \cdot (P/I'P) = (X_n - a_n)(P/I'P)$, es decir, que módulo $I'P$, se tiene que $I \equiv (X_n - a_n)$. Por tanto, podemos concluir juntando todas las expresiones hasta ahora: $P/I \simeq (P/I'P)/(IP/I'P) \simeq A[X_n]/(X_n - a_n) \simeq A$, como se quería. □

2. Módulos

2.1. Definición y operaciones

El concepto de módulo es una generalización natural del de espacio vectorial:

Definición 26. Sea A un anillo. Un **A-módulo** M es un grupo abeliano $(M, +)$ dotado de una *operación producto por escalar*, $\cdot : A \times M \mapsto M$, que verifica:

1. $a(m + n) = am + an$ para todos $a \in A$, $m, n \in M$.
2. $(ab)m = a(bm)$ para todos $a, b \in A$, $m \in M$.
3. $1_A m = m$ para todo $m \in M$.

Si K es un cuerpo, los K-módulos son los K-espacios vectoriales. Asimismo, si G es un grupo abeliano, es de manera natural un $\mathbb{Z}$-módulo. También, si $I \subset A$ es un ideal, entonces I es un A-módulo.

Observación 9. Los A-módulos están en correspondencia con las representaciones de A en anillos de endomorfismos de grupos abelianos. Es decir, si $(M, +)$ es un grupo abeliano, consideramos el anillo (no conmutativo) $\mathrm{End}(M)$ de endomorfismos de grupos abelianos con la suma y la composición. Entonces, dado un homomorfismo de anillos $\mu : A \to \mathrm{End}(M)$, induce la estructura de módulo en M dada por $am := \mu(a)(m)$.

Por otro lado, si M es un A-módulo, la aplicación $\mu : A \to \mathrm{End}(M)$ dada por $\mu(a) = \mu_a$, con $\mu_a(m) = am$, es un homomorfismo de anillos.

Definición 27. Un subgrupo N de un A-módulo M se dice **A-submódulo** si el producto por escalar restringe a N dándole estructura de A-módulo.

Definición 28. Sean M, M' dos A-módulos. Un **homomorfismo de A-módulos** es un homomorfismo de grupos $f : M \to M'$ tal que, además, $f(am) = af(m)$, $\forall a \in A$, $m \in M$.

Un homomorfismo biyectivo se denomina **isomorfismo**.

Por ejemplo, si M es un A-módulo, la aplicación $M \to M$ dada por $m \mapsto am$, fijado el $a \in A$, es un homomorfismo. Asimismo, notando que A es en sí mismo un A-módulo, se tiene que, fijado $m \in M$, hay un homomorfismo $A \to M$ dado por $a \mapsto am$.

Como es habitual, la composición de homomorfismos de módulos es de nuevo un homomorfismo de módulos, y:

Definición 29. Sean M, N dos A-módulos. Se define $\hom_A(M, N)$ como el conjunto de homomorfismos de módulos entre M y N, que adquiere a su vez estructura de A módulo de manera natural.

Proposición 26. *Se tiene que* $M \simeq \hom_A(A, M)$.

Demostración. La aplicación que envía $f \in \hom_A(A, M)$ en $f(1_A) \in M$ es el isomorfismo buscado, con la inversa dada por enviar el $m \in M$ a la aplicación $f : A \to M$ que cumple $1_A \to m$. (Es decir, la aplicación *producto* por m mencionada anteriormente).

Definición 30. Sean $\{M_i\}_{i\in I}$ A-módulos. Se define la **suma directa** como:

$$\bigoplus_{i\in I} M_i = \{(m_1,\dots,m_i,\dots) : m_i \in M_i, \text{con solo una cantidad finita de elementos no nulos}\}.$$

Tiene estructura de A-módulo con las operaciones componente a componente.

Definición 31. Sean $\{M_i\}_{i\in I}$ A-módulos. Se define el **producto directo** como:

$$\prod_{i\in I} M_i = \{(m_1,\dots,m_i,\dots) : m_i \in M_i\}.$$

Tiene estructura de A-módulo con las operaciones componente a componente.

Introducimos asimismo la noción de A-álgebra, que es un A-módulo con producto interno, es decir, un anillo que a su vez es A-módulo. Esto equivale a la existencia de un homomorfismo de anillos entre A y el álgebra en cuestión, de modo que lo definimos así:

Definición 32. Sea A un anillo. Si $f : A \to B$ es un homomorfismo de anillos, se dice que B es un **A-álgebra** y se define el producto $ab := f(a)b$. En particular, es un A-módulo. La aplicación f se denomina **aplicación estructural**.

Definición 33. Sean B, C dos A-álgebras con aplicaciones estructurales f y g respectivamente. El homomorfismo de anillos $h : B \to C$ es un **homomorfismo de álgebras** si $h \circ f = g$, es decir, si es a su vez un homomorfismo de los A-módulos dados por f y g.

Teorema 5 (Propiedad universal del producto directo)**.** *Sean $\{M_i\}_i$ y N A-módulos. Supongamos que se tienen homomorfismos $f_i : N \to M_i$. Entonces, existe un único $f : N \to \prod_i M_i$ de modo que $f_{i_0} = \pi_{i_0} \circ f$ para todo índice i_0.*

Demostración. Análoga al caso de los anillos: basta con definir $f(n) = (f_i(n))_i$. □

Observación 10. De esta propiedad sigue directamente que $\hom_A(N, \prod M_i) \simeq \prod \hom_A(N, M_i)$.

Teorema 6 (Propiedad universal de la suma directa)**.** *Sean $\{M_i\}_i$ y N A-módulos. Supongamos que se tienen homomorfismos $f_i : M_i \to N$. Entonces, existe un único homomorfismo $f : \bigoplus M_i \to N$ tal que $f_{i_0} = f \circ j_{i_0}$ para todo índice i_0, donde $j_{i_0} : M_{i_0} \hookrightarrow \bigoplus M_i$.*

Demostración. Basta con definir $f((a_i)_{i\in I}) = \sum_{i\in I} f_i(a_i)$, que está bien definida porque solo hay una cantidad finita de sumandos. □

Observación 11. De esta propiedad sigue directamente que $\hom_A(\bigoplus M_i, N) \simeq \bigoplus \hom_A(M_i, N)$.

Definición 34. Dado un homomorfismo $f : M \to N$ de A-módulos, se definen $\ker(f) = f^{-1}(0)$, $Im(f) = f(M)$ y $\operatorname{coker}(f) = N/Im(f)$ el **núcleo, imagen y conúcleo de** f respectiamente.

Se tiene que $\ker(f)$ es un A-submódulo de M e $Im(f)$ de N. Por otro lado, $\operatorname{coker}(f)$ es un ejemplo de módulo cociente: a priori, se tiene la estructura de grupo cociente pero se puede extender de modo natural:

Definición 35. Si M es un A-módulo y $N \subset M$ es un A-submódulo, se define el **módulo cociente** M/N como el grupo cociente dotado del producto natural por elementos de A.

Teorema 7 (Propiedad universal del cociente)**.** *Sea M un A-módulo y $L \subset M$ un A-submódulo, y sea $f : M \to M'$ un homomorfismo de A-módulos tal que $L \subset \ker(f)$. Entonces, existe un único $g : M/L \to M'$ tal que $f = g \circ \pi$.*

Demostración. Al igual que en anillos, basta con definir $g(\bar{x}) = f(x)$.

Del mismo modo que en anillos, esta propiedad universal da lugar a:

Teorema 8 (Isomorfía)**.** *Sea $f : M \to N$ un homomorfismo de A-módulos. Entonces, $M/\ker(f) \simeq Im(f)$.*

Teorema 9 (Propiedad universal del conúcleo)**.** *Sea $f : M \to N$ un homomorfismo de A-módulos. Supongamos que $g : N \to P$ es un homomorfismo con $g \circ f = 0$, es decir, $Im(f) \subset \ker(g)$. Entonces, existe un único homomorfismo $h : \operatorname{coker}(f) \to P$ de modo que $g = h \circ \pi$.*

Demostración. Es un caso particular de la propiedad universal del cociente para $Im(f) \subset N$ y la aplicación $g : N \to P$. □

Asimismo, se tiene el teorema de correspondencia habitual entre submódulos del cociente y del espacio de partida:

Teorema 10. *Sea $N \subset M$ un A-submódulo. Sea $\pi : M \to M/N$. Existe una correspondencia biyectiva entre los submódulos de M/N y los submódulos de M que contienen a M, dada por enviar $\bar{P} \subset M/N$ en $\pi^{-1}(\bar{P})$.*

Demostración. Es análoga al caso de anillos. □

Definición 36. Sea M un A-módulo y $\{M_i\}_{i\in I}$ una familia de A-submódulos. Se define la **suma** como el menor A-submódulo que contiene a todos los M_i. Explícitamente, $\sum_i M_i = \{\sum_i m_i : m_i \in M_i,$ solo una cantidad finita de m_i no nulos$\}$.

Si se tiene $M_i \cap M_j = \{0\}$ cuando $i \neq j$, se dice que la suma es **directa** y se denota $\bigoplus_i M_i$.

Observación 12. La suma directa definida de esta forma (de manera *interna* con submódulos) se denomina y se denota igual que la suma directa de módulos (*externa*) dado que si $\{M_i\}_i \subset M$ es una familia de submódulos tal que su suma es directa, entonces $\sum_i M_i \simeq \bigoplus_i M_i$, siendo la última suma directa la *externa*, por medio de enviar el elemento $\sum_i m_i$ al elemento $(m_i)_i$.

Teorema 11 (Segundo de isomorfía)**.** *Sean M_1, M_2 dos A-submódulos del A-módulo M. Entonces, $\frac{M_1+M_2}{M_1} \simeq \frac{M_2}{M_1\cap M_2}$.*

Demostración. Basta con aplicar el primer teorema de isomorfía a la flecha $M_2 \hookrightarrow M_1 + M_2 \to (M_1 + M_2)/M_1$, que es sobreyectiva de núcleo $M_1 \cap M_2$. □

Teorema 12 (Tercero de isomorfía)**.** *Sea $L \subset N \subset M$ una cadena de A-submódulos. Entonces, $(M/L)/(N/L) \simeq M/N$.*

Demostración. Consideramos $\pi : M \to M/N$. Como $L \subset \ker(\pi) = N$, se tiene por la propiedad universal un $\tilde{\pi} : M/L \to M/N$ sobreyectivo. Su núcleo es precisamente N/L, de modo que basta con aplicar el primer teorema de isomorfía. □

Definición 37. Sea $I \subset A$ un ideal y M un A-módulo. Se define el submódulo $I \cdot M = \{\sum_{i=1}^n a_i m_i : a_i \in I, m_i \in M\}$.

Definición 38. Dados M_1, M_2 dos A-submódulos de M, se define el **conductor** $(M_1 : M_2) = \{a \in A : aM_2 \subset M_1\}$, que es un ideal de A.

Si $M_1 = 0$, entonces $(0 : M_2)$ se denomina **anulador** de M_2 y se denota $\operatorname{Ann}(M_2)$. Si es el ideal nulo, se dice que M_2 es **fiel**.

Proposición 27. *Sea M un A-módulo e $I \subset A$ un ideal tal que $I \subset \operatorname{Ann}(M)$. Entonces, es posible definir en M una estructura de A/I-módulo mediante el producto $[x]m := xm$. Además, M es fiel como A/I-módulo.*

Demostración. Basta con ver que si $x - y \in I$, entonces $xm = ym$. Pero esto sigue de que $xm - ym = (x - y)m = 0$, dado que $x - y \in I \subset \operatorname{Ann}(M)$. □

2.2. Independencia, generadores y módulos libres

Definición 39. Sea M un A-módulo. Dado un conjunto $\{m_i\}_{i\in I} \subset M$, se define el **$A$-submódulo generado por** $\{m_i\}$ como:

$$\langle\{m_i\}_{i\in I}\rangle = \left\{\sum_{i\in I} a_i m_i : a_i \in A, \text{ una cantidad finita de } a_i \text{ no nulos}\right\}.$$

Si $M = \langle\{m_i\}_i\rangle$, se dice que $\{m_i\}_i$ es un **conjunto de generadores de** M. Si, además, $|\{m_i\}_i| < \infty$, se dice que M es **finitamente generado**.

Definición 40. Sea M un A-módulo. Se dice que un conjunto de elementos $\{m_i\} \subset M$ es **linealmente independiente** si $\sum_i a_i m_i = 0$ (donde solo una cantidad finita de los a_i son no nulos) implica que $a_i = 0$ para todo i.

Si además el conjunto genera M, se denomina **base**.

Definición 41. Denotamos, para un conjunto I, $M^I = \bigoplus_{i\in I} M$, es decir, la suma directa de $|I|$ copias de M.

Definición 42. Un A-módulo M se dice **libre** si $M \simeq A^I$ para cierto I. Si $|I| < \infty$, entonces $|I|$ se suele denominar **dimensión** de M y todas las bases de M tienen ese tamaño.

Proposición 28 (Propiedad universal de los módulos libres)**.** *Sea I un conjunto de índices no vacío. Sea A^I el A-módulo libre correspondiente. Sea M otro A-módulo, y elegimos $m_i \in M$ para cada $i \in I$. Entonces, existe un único homomorfismo $f : A^I \to M$ con $f((a_i)_{i\in I}) = \sum_{i\in I} m_i$.*

Demostración. Lo único que hay que ver es que la función así definida es un homomorfismo. Basta con considerar los generadores de A^I, que son $e_i = (\delta_{ij})_j = \iota_i(1)$. Como cada aplicación $f_i : A \to M$ dada por $1 \mapsto m_i$ es un homomorfismo de A-módulos, entonces la propiedad universal de la suma directa garantiza que $f : A^I \to M$ dada por $e_i \mapsto m_i$ es un homomorfismo, pero esta es precisamente la aplicación buscada. □

Proposición 29. *Sea M un A-módulo. M es finitamente generado $\iff$ $M \simeq A^n/N$, con $N \subset A^n$ un submódulo y n el tamaño del conjunto de generadores.*

Demostración. Para $\implies$, basta con considerar el conjunto de generadores $\{x_i\}_{i=1}^n$ y la aplicación $f : A^n \to M$ dada por $e_i \to x_i$ que es un homomorfismo por la propiedad universal. Es sobreyectiva por ser los x_i generadores, de modo que $M \simeq A^n/\ker(f)$. Para $\impliedby$, si $e_1, \ldots, e_n$ son los generadores de A^n, entonces $[e_1], \ldots, [e_n]$ generan A^n/N. □

Proposición 30. *Sea M un A-modulo finitamente generado con un conjunto de generadores de tamaño n. Sea $I \subset A$ un ideal $\varphi \in \mathrm{End}(M)$. Si $\varphi(M) \subset I \cdot M$, entonces existen $a_i \in I$ tales que $\varphi^n + a_1\varphi^{n-1} + \cdots + a_n \cdot Id = 0 \in \mathrm{End}(M)$.*

Demostración. Sea $\{x_i\}_{i=1}^n$ un conjunto de generadores. Sabemos que $\varphi(x_i) \in I \cdot M$, de modo que podemos escribir $\varphi(x_i) = \sum_j a_{ij}x_j$ con los $a_{ij} \in I$. Es decir, $\sum_j(\delta_{ij}\varphi - a_{ij})x_j = 0$ para todo $i \in \{1, \ldots, n\}$. Es decir, si $B_{ij} = (\delta_{ij}\varphi - a_{ij})_{ij}$, entonces $\mathrm{adj}(B_{ij}) \cdot B_{ij} \cdot (x_j)_j = 0$, pero eso es lo mismo que $\det(B_{ij}) \cdot (x_j)_j = 0$. Como $\det(B_{ij})$ se anula en todos los generadores de M, sigue que es nulo, lo cual da la expresión deseada. □

Observación 13. Como corolario, puede tomarse $\varphi = Id_M$. Es decir, si M es un A-módulo finitamente generado e $I \subset A$ es un ideal tal que $M \subset I \cdot M$, sigue que existe un $x \in A$, con $x \equiv 1 \mod I$ y tal que $xM = 0$.

Basta con observar que $0 = (1 + a_1 + \cdots + a_n) \cdot Id \in \mathrm{End}(M)$ por la proposición previa, y tomar $x = 1 + a_1 + \cdots + a_n \in A$. Claramente $x \equiv 1 \mod I$ (porque $a_1 + \cdots + a_n \in I$) y, además, si $m \in M$ se tiene que $xm = (1 + a_1 + \cdots + a_n) \cdot Id(m) = 0$. □

Proposición 31 (Lema de Nakayama)**.** *Sea M un A-módulo finitamente generado. Sea $I \subset A$ un ideal con $I \subset J_A$, es decir, contenido en el radical de Jacobson. Si $IM = M$, entonces $M = 0$.*

Demostración. Usando la observación previa, obtenemos $x \in I$ con $x \equiv 1 \mod I$ y $xM = 0$. Como $1 - x \in I \subset J_A$, sabemos que $1 - (1 - x) = x \in \mathcal{U}(A)$. Entonces, $M = x^{-1}0 = 0$. □

Proposición 32. *Sea M un A-módulo finitamente generado, $I \subset J_A$ un ideal contenido en el radical de Jacobson y $N \subset M$ un submódulo tal que $M = IM + N$. Entonces $N = M$.*

Demostración. Basta con aplicar el lema de Nakayama al módulo M/N, observando que $I \cdot M/N \simeq (IM + N)/N$. □

Proposición 33. *Sea A un anillo local con maximal $\mathfrak{m} \subset A$ y $k = A/\mathfrak{m}$ su cuerpo residual. Sea M un A-módulo finitamente generado. Si $\{x_1, \ldots, x_n\}$ son elementos de M que son base de $M/\mathfrak{m}M$ como k-espacio vectorial (recordemos que, como $\mathfrak{m} \subset \mathrm{Ann}(M/\mathfrak{m}M)$, entonces puede verse como un $A/\mathfrak{m}$-módulo), entonces $\langle \{x_i\} \rangle = M$.*

Demostración. Sea $N = \langle \{x_i\}_i \rangle$. Sabemos que N pasado al cociente lo genera, es decir, que: $N/\mathfrak{m}\mathfrak{M} = M/\mathfrak{m}\mathfrak{M}$, o, en notación aditiva, $M = M + \mathfrak{m}M = N + \mathfrak{m}M$. De la proposición previa sigue $N = M$. □

2.3. Producto tensorial

Definición 43. Sean M, N, P tres A-módulos. Se dice que $f : M \times N \to P$ es **A-bilineal** si para todo $m \in M$ se tiene que $f(m, \cdot) : N \to P$ es un homomorfismo, y para todo $n \in N$ se tiene que $f(\cdot, n) : M \to P$ también lo es.

Definición 44. Sean M, N dos A-módulos. Se define su **producto tensorial** como sigue: consideramos el módulo libre $C = A^{(M \times N)}$, es decir, asignaciones de coeficientes a cada elemento de $(M \times N)$ con solo una cantidad finita de ellos no nulos:

$$C = A^{(M \times N)} = \left\{ \sum_{i=1}^{n} a_i(x_i, y_i) : a_i \in A, x_i \in M, y_i \in N \right\}.$$

Ahora, consideramos $D \subset C$ el submódulo generado por todos los elementos de la forma $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$, $(ax, y) - a(x, y)$ o $(x, ay) - a(x, y)$, con $x, x' \in M$, $y, y' \in N$, $a \in A$. Entonces, el producto tensorial es el módulo $M \otimes N := C/D$. Evidentemente, está generado por las clases de elementos de $M \times N$, $[(x, y)]$, que se denotan típicamente $x \otimes y$.

Proposición 34 (Propiedad universal del producto tensorial)**.** *Sean M, N dos A-módulos. Consideramos la aplicación $g : M \times N \to M \otimes N$ dada por $(x, y) \mapsto x \otimes y$. Entonces, dado cualquier A-módulo P y aplicación bilineal $f : M \times N \to P$, existe una única aplicación lineal $\bar{f} : M \otimes N \to P$ tal que $f = \bar{f} \circ g$.*

Demostración. Basta con definirla en los generadores como sigue: $\bar{f}(x \otimes y) := f(x, y)$. Puede comprobarse con las propiedades que caracterizan al producto tensorial que está bien definida y es un homomorfismo de módulos. □

Definición 45. Dadas $f : M \to M'$, $g : N \to N'$ dos homomorfismos entre A-módulos, se define $f \otimes g : M \otimes N \to M' \otimes N'$ como el levantamiento (según la propiedad universal) de $h : M \times N \to M' \otimes N'$ dada por $(x, y) \mapsto f(x) \otimes g(y)$.

Nótese que si $f : M \to M'$, $g : N \to N'$, $f' : M' \to M''$, $g' : N' \to N''$, entonces $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$, siendo ambas la dada por $x \otimes y \mapsto f'(f(x)) \otimes g'(g(y))$.

Observación 14. En lugar de considerar aplicaciones 2-lineales, se puede considerar aplicaciones k-lineales y hacer el análogo para definir el producto tensorial de k A-módulos.

Observación 15. Supongamos que M, N son A-módulos y $M' \subset M$, $N' \subset N$ submódulos. A la hora de considerar $M' \otimes N'$, tanto el módulo libre $C_{M',N'}$ como el submódulo de relaciones $D_{M',N'}$ son más pequeños, de modo que no está clara la relación entre $M \otimes N$ y $M' \otimes N'$. De hecho, por ejemplo, en $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, el elemento $2 \otimes [1] = 1 \otimes [2]$ es nulo, pero en el producto de submódulos $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ el $2 \otimes [1]$ no lo es.

Proposición 35. *Sean M, N dos A-módulos. Supongamos que $\{x_i\}_{i=1}^r \subset M$ y $\{y_i\}_{i=1}^r \subset N$ son tales que $\sum x_i \otimes y_i = 0$. Entonces, existen submódulos $M_0 \subset M$, $N_0 \subset N$, finitamente generados, y tales que $\sum x_i \otimes y_i = 0$ como elemento de $M_0 \otimes N_0$.*

Demostración. $\sum(x_i, y_i) \in D_{M,N}$, de modo que es suma de ciertos elementos *relación* que generan $D_{M,N}$. Sea M_0 el módulo generado por los x_i junto con las primeras componentes que aparecen en esos generadores de $D_{M,N}$, y N_0 el generado por los y_i junto con las segundas componentes. Entonces, son finitamente generados, y por construcción $\sum(x_i, y_i) \in C_{M_0,N_0}$ y $\sum(x_i, y_i) \in D_{M_0,N_0}$. □

Proposición 36. *Se tienen estos isomorfismos naturales (y únicos):*

1. $M \otimes N \simeq N \otimes M$.
2. $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P) \simeq M \otimes N \otimes P$.
3. $(M \oplus N) \otimes P \simeq (M \otimes P) \oplus (N \otimes P)$.
4. $A \otimes M \simeq M$.

Demostración. En 1, basta con considerar $x \otimes y \mapsto y \otimes x$. Para 2, consideramos primero $f_z : M \times N \to M \otimes N \otimes P$ dado por $(x, y) \mapsto x \otimes y \otimes z$, que es bilineal, de modo que $\tilde{f}_z : M \otimes N \to M \otimes N \otimes P$ dado por $x \otimes y \mapsto x \otimes y \otimes z$ está bien definido y es lineal. Esto garantiza a su vez que $f : (M \otimes N)xP \to M \otimes N \otimes P$ dada por $(x \otimes y, z) \mapsto x \otimes y \otimes z$ sea bilineal, de modo que $\tilde{f} : (M \otimes N) \otimes P \to M \otimes N \otimes P$ dada por $(x \otimes y) \otimes z \mapsto x \otimes y \otimes z$ está bien definida y es lineal. Un argumento similar define la inversa $x \otimes y \otimes z \mapsto (x \otimes y) \otimes z$ y se tiene el isomorfismo deseado (análogo con la otra configuración de paréntesis).

Para 3, se argumenta del mismo modo para construir el isomorfismo $(x, y) \otimes p \mapsto (x \otimes p, y \otimes p)$. Finalmente, 4 sigue del morfismo $a \otimes m \mapsto am$. □

2.4. Extensión y restricción de escalares

Definición 46 (Extensión de escalares)**.** Sea $f : A \to B$ un homomorfismo de anillos. Recordemos que B tiene estructura de A-módulo vía f. Dado M otro A-módulo, se define la **extensión de escalares a B vía f** como el B-módulo $M \otimes_A B$ dotado del producto por escalar $b \cdot (m \otimes b') := m \otimes bb'$.

Definición 47 (Restricción de escalares)**.** Sea $f : A \to B$ un homomorfismo de anillos y N un B-módulo. Se define la **restricción de escalares a A vía f** como el A-módulo N_A dotado de la operación $a \cdot n := f(a)n$.

Proposición 37. *Sea $f : A \to B$ homomorfismo de anillos. Sea N un B-módulo finitamente generado. Si B también es finitamente generado (como A-módulo), entonces la restricción de escalares N_A es finitamente generada.*

Demostración. Sean $\{x_i\}$ y $\{y_j\}$ A-generadores de B y B-generadores de N respectivamente. Dado $n \in N$, se tiene $n = \sum_j b_j y_j = \sum_j \sum_i a_i x_i y_j$, luego los $\{x_i y_j\}$ generan N_A. □

Proposición 38. *Sea $f : A \to B$ homomorfismo de anillos. Si M es un A-módulo finitamente generado, entonces la extensión de escalares M_B también lo es.*

Demostración. Si $\{x_i\}_i$ son A-generadores de M, entonces $\{x_i \otimes 1\}_i$ son B-generadores de M_B, dado que $m \otimes b = \sum_j a_j x_j \otimes b = \sum_j (a_j x_j \otimes b_j) = \sum_j (x_j \otimes f(a_j)b_j) = \sum_j f(a_j)b_j \cdot (x_j \otimes 1)$. □

2.5. Sucesiones exactas

Definición 48. Sea $f : M \to N$ un homomorfismo de A-módulos y P otro A-módulo. Se tiene el morfismo $f_* \equiv \hom_A(P, f) : \hom_A(P, M) \to \hom_A(P, N)$ dado por $h \mapsto f \circ h$. Asimismo, se tiene el morfismo $f^* \equiv \hom_A(f, P) : \hom_A(N, P) \mapsto \hom_A(M, P)$ dado por $h \mapsto h \circ f$.

De hecho, $\hom_A(P, -)$ es un functor covariante y $\hom_A(-, P)$ contravariante, de modo que se verifican ciertas propiedades básicas como $(Id_M)_* = Id_{\hom_A(P,M)}$, $(f \circ g)_* = f_* \circ g_*$, $(af + a'g)_* = af_* + a'f_*$, $(Id_M)^* = Id_{\hom_A(M,P)}$, $(f \circ g)^* = g^* \circ f^*$ y $(af + a'g)^* = af^* + a'g^*$.

Definición 49. Una sucesión de homomorfismos

$$\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \dots$$

es **exacta** en M_n si $\mathrm{Im}(f_n) = \ker(f_{n+1})$, y es **exacta** si lo es en todo M_n.

Observación 16.
- $0 \to M' \xrightarrow{f} M$ es exacta $\iff$ f es inyectiva.
- $M \xrightarrow{g} M'' \to 0$ es exacta $\iff$ g es sobreyectiva.
- $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es exacta $\iff$ f es inyectiva, g es sobreyectiva, y $\ker(g) = \mathrm{Im}(f)$.

Las sucesiones del último punto de la observación se denominan **exactas cortas**. Véase que en una sucesión exacta corta, se tiene que $\mathrm{coker}(f) = M/\mathrm{Im}(f) = M/\ker(g) \simeq \mathrm{Im}(g) = M''$.

Proposición 39. *Si $\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \dots$ es una sucesión exacta, da lugar a sucesiones exactas cortas en cada paso, de la forma:*

$$0 \to \ker(f_{n+1}) \hookrightarrow M_n \xrightarrow{f_{n+1}} \mathrm{Im}(f_{n+1}) \to 0.$$

Demostración. Claramente la segunda flecha es inyectiva y la tercera sobreyectiva. Además, la imagen de la primera flecha es $\ker(f_{n+1})$ por definición. □

Teorema 13. *Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una sucesión exacta corta. Son equivalentes:*

- *Existe una sección de p, es decir, $s : M'' \to M$ tal que $p \circ s = Id_{M''}$.*
- *Existe un retracto de i, es decir, $r : M' \to M$ tal que $r \circ i = Id_{M'}$.*

Demostración. Para $1 \implies 2$, definimos la función $\pi \circ i : M' \to M \to M/\mathrm{Im}(s)$. Veamos que es un isomorfismo. Para ver que es inyectiva, supongamos que $\pi(i(m')) = 0$. Esto quiere decir que $i(m') = s(m'')$ y, componiendo ahora con p, sigue que $0 = p(i(m')) = p(s(m'')) = m''$, luego $i(m') = s(0) = 0$ y, como i es inyectiva, sigue $m' = 0$. Para ver que es sobreyectiva, sea $[m] \in M/\mathrm{Im}(s)$. Como $[m] = [m - s(p(m))]$, y además $m - s(p(m)) \in \ker(p) = \mathrm{Im}(i)$, se tiene lo que se quería. Una vez visto que es un isomorfismo, basta con definir $r : M \to M/\mathrm{Im}(s) \simeq M'$, y se comprueba de inmediato que es un retracto.

Para $2 \implies 1$, la estrategia es similar pero con la función $p \circ j : \ker(r) \to M \to M''$. Es inyectiva porque, si $m \in \ker(r)$ y además $p(j(m)) = 0$, como $\ker p = \mathrm{Im}\, i$, sigue que $j(m) = i(m')$. Ahora, componiendo con r, se tiene que $0 = m'$ luego, por inyectividad de j, sigue que $m = 0$. Es sobreyectiva porque si $m'' \in M''$, entonces $m'' = p(m) = p(m - i \circ r(m))$, con $m - i \circ r(m) \in \ker(r)$. Ahora, basta con definir $s : M'' \simeq \ker(r) \hookrightarrow M$ y se comprueba de inmediato que es una sección. □

Definición 50. Si una sucesión exacta corta cumple alguna de las condiciones del teorema previo, se dice que **escinde** y se tiene que $M \simeq M' \oplus M''$.

Esto último es así porque como $m - i(r(m)) \in \ker(r)$, se tiene que $M = \mathrm{Im}(i) + \ker(r)$, y además tienen intersección nula porque si $i(m)$ está en ambos, $0 = r(i(m)) = m$. Así, $M = \mathrm{Im}(i) \oplus \ker(r)$, pero por ser i inyectiva sigue que $\mathrm{Im}(i) \simeq M'$, y sabemos de la demostración del teorema previo que $\ker(r) \simeq M''$.

Teorema 14. *Sean M, M', M'' A-módulos. Se tienen:*

- $M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ *es exacta* $\iff 0 \to \hom_A(M'', N) \xrightarrow{p^*} \hom_A(M, N) \xrightarrow{i^*} \hom_A(M', N)$ *es exacta para todo A-módulo N.*
- $0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$ *es exacta* $\iff 0 \to \hom_A(N, M') \xrightarrow{i_*} \hom_A(N, M) \xrightarrow{p_*} \hom_A(N, M'')$ *es exacta para todo A-módulo n.*

Demostración. Veremos la del punto 2. Para $\implies$, veamos que i_* es inyectiva: si $i_*(g_1) = i_*(g_2)$, tenemos en todo $n \in N$ que $i(g_1(n)) = i(g_2(n))$ que, por inyectividad de i, garantiza que $g_1(n) = g_2(n)$ luego $g_1 = g_2$. Ahora, veremos que $\ker(p_*) = \mathrm{Im}(i_*)$. Por un lado, $p_*(i_*) = (p \circ i)_* = 0_* = 0$, luego $\mathrm{Im}(i_*) \subset \ker(p_*)$. Ahora, dado $\gamma \in \ker(p_*)$, se tiene que $p \circ \gamma = 0$ luego $\mathrm{Im}(\gamma) \subset \ker(p) = \mathrm{Im}(i)$. Por tanto, podemos definir un $\alpha : N \to M'$ tal que $\alpha(n) = m'$, donde m' es tal que $f(m') = \gamma(n)$. Es decir, $f \circ \alpha = \gamma$, como se quería.

Para $\impliedby$, basta con usar la identificación $M \simeq \hom_A(A, M)$ que asocia i_* con i y p_* con p. □

Proposición 40. *Toda sucesión exacta corta de A-módulos $0 \to M' \to M \xrightarrow{g} L \to 0$, con L libre, escinde.*

Demostración. Basta con tomar una base $\{e_i\}_i \subset L$ y definir la sección $s(e_i) = m_i$, donde m_i es aquel tal que $g(m_i) = e_i$. □

Teorema 15. *Sea $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta. Si N es un A-módulo, entonces la tensorización*

$$M' \otimes N \xrightarrow{f \otimes Id} M \otimes N \xrightarrow{g \otimes Id} M'' \otimes N \to 0$$

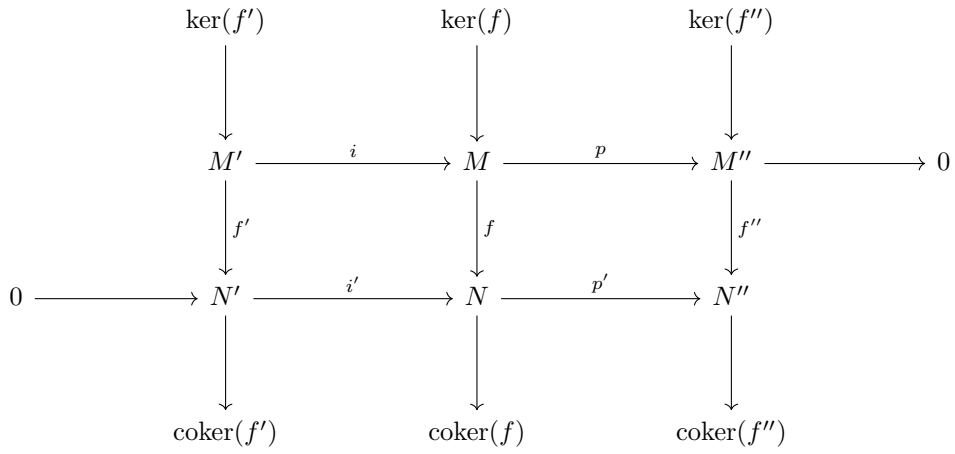
es exacta.

Demostración. Basta con observar que si P es otro A-módulo, entonces $\hom_A(M \otimes N, P) \simeq \hom_A(M, \hom_A(N, P))$, mediante enviar $f : M \otimes N \to P$ en el $\overline{f}$ definido como $\overline{f}(m)(n) = f(m \otimes n)$. Entonces, puede usarse el criterio del teorema sobre sucesiones exactas y homomorfismos. En otras palabras, $\hom_A(M', \hom_A(N, P)) \to \hom_A(M, \hom_A(N, P)) \to \hom_A(M'', \hom_A(N, P)) \to 0$ es exacta para todo P, de modo que $\hom_A(M' \otimes N, P) \to \hom_A(M \otimes N, P) \to \hom_A(M'' \otimes N, P) \to 0$ también, así que se tiene lo que se quería. □

Definición 51. Si N es un A-módulo tal que la tensorización de toda sucesión exacta corta sigue siendo exacta corta, se dice que N es **plano**. Es decir, si toda vez que $f : M' \to M$ es un homomorfismo de módulos inyectivo, se tiene que $f \otimes Id_N : M' \otimes N \to M \otimes N$ lo es.

Proposición 41. *Si P es un A-módulo plano y $f : A \to B$ es homomorfismo de anillos, entonces la extensión de escalares $P_B = P \otimes_A B$ es plana.*

Lema 2 (Serpiente)**.** *Sea el diagrama conmutativo*



un diagrama exacto en las filas. Entonces, se tiene una sucesión exacta:

$$\ker(f') \xrightarrow{i} \ker(f) \xrightarrow{p} \ker(f'') \xrightarrow{d} \operatorname{coker}(f') \xrightarrow{i'} \operatorname{coker}(f) \xrightarrow{p'} \operatorname{coker}(f''),$$

donde i, p, i', p' representan los morfismos inducidos de manera natural entre esos espacios. Si además se añaden módulos nulos para que las filas del diagrama original sean dos sucesiones exactas cortas, entonces pueden añadirse en la secuencia resultante módulos nulos en los extremos.

Demostración. Puede comprobarse que i, p restringen correctamente a los núcleos, y i', p' están bien definidas entre los conúcleos. Vamos a ver como definir $d : \ker(f'') \to \operatorname{coker}(f)$. Sea $x'' \in \ker(f'')$. Como p es sobreyectiva, $\exists x \in M$ con $p(x) = x''$. Entonces, $p'(f(x)) = f''(p(x)) = 0$, de modo que $f(x) \in \ker(p') = \Im(i')$. Por tanto, $f(x) = i'(x')$ para cierto x'. Entonces, definimos $d(x'') := [x']$. Puede comprobarse que está bien definida sin depender de las elecciones realizadas. Del mismo modo, las demostraciones de exactitud en cada punto pueden comprobarse una vez conocidas las definiciones de cada una de las funciones. □

Concluimos la sección con algunas terminologías:

Definición 52. Un A-módulo M es **de presentación finita** o **finitamente presentado** si existe una sucesión exacta $A^m \xrightarrow{i} A^n \to M \to 0$, es decir $M \simeq A^n/i(A^n)$. En particular M es finitamente generado.

Definición 53. Sean A, B anillos. Se dice que N es un (A, B)**-bimódulo** si es un módulo para ambos anillos, y además $a(nb) = (an)b$, es decir, ambas estructuras son compatibles.

Observación 17. Si N es un (A, B)-bimódulo, M es un A-módulo y P un B-módulo, entonces $M \otimes_A N$ y $(N \otimes_B P)$ tienen estructura de (A, B)-bimódulo (multiplicando siempre en el factor N) y además resulta que $(M \otimes_A N) \otimes_B P \simeq M \otimes_A (N \otimes_B P)$.

Definición 54. Dadas dos A-álgebras B y C, se puede dotar a $B \otimes C$ de estructura de A-álgebra mediante $(b \otimes c)(b' \otimes c') := (bb' \otimes cc')$.

3. Localización

Definición 55. Sea A un anillo conmutativo con unidad y $S \subset A$ un subconjunto. Se dice que es **multiplicativamente cerrado** si $1 \in S$ y $a, b \in S \implies ab \in S$.

Por ejemplo, si $P \subset A$ es un ideal primo, entonces $A \setminus P$ es multiplicativamente cerrado (mientras que P no, porque $1 \notin P$).

Definición 56. Dado A un anillo y $S \subset A$ un conjunto multiplicativamente cerrado, definimos el **anillo de fracciones o anillo localizado de** A **en** S como $S^{-1}A := (A \times S)/\sim$, donde $(a,s) \sim (b,t) \iff au = bv$, $su = tv$ para ciertos $u, v \in S$. La clase del elemento (a,s) suele denotarse $\frac{a}{s}$.

Las operaciones de anillo en el localizado se definen como $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ y $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$. Nótese que st sigue estando en S por ser multiplicativamente cerrado, luego están bien definidas (y además no dependen del representante). El neutro es $\frac{0}{1}$ y la identidad $\frac{1}{1}$. El opuesto de $\frac{a}{s}$ es $\frac{-a}{s}$.

Por ejemplo, como es razonable, $\frac{a}{s} = \frac{at}{st}$ si $t \in S$, tomando $u = 1$ y $v = t$ en la definición de la relación de equivalencia.

Observación 18. Una condición equivalente para que $\frac{a}{s} = \frac{b}{t}$ es que $\exists \omega \in S$ con $\omega(at - bs) = 0$. Esto es así tomando $\omega = uv$ con la notación usada para definir $\sim$ y, recíprocamente, si se tiene el ω, pueden tomarse $u = t\omega$, $v = s\omega$ para verificar la equivalencia.

Como corolario sigue que si A es un dominio entero y $0 \notin S$, entonces $\frac{a}{s} = \frac{b}{t} \iff at = bs$ como es habitual.

Definición 57. Si A es un dominio entero y se toma $S = A \setminus \{0\}$, entonces el localizado $S^{-1}A$ se denomina **cuerpo de fracciones de** A y el elemento $\frac{a}{s} \neq \frac{0}{1}$ tiene el inverso $\frac{s}{a}$.

Definición 58. Si A es un anillo y $S \subset A$ un conjunto multiplicativamente cerrado, se define el **homomorfismo de localización** $\gamma : A \to S^{-1}A$ dado por $a \mapsto \frac{a}{1}$.

Si A es un dominio entero y $0 \notin S$, γ es inyectivo pues si $\frac{0}{1} = \gamma(a) = \frac{a}{1}$, entonces $1 \cdot a - 0 = 0$ es decir $a = 0$.

Proposición 42 (Propiedad universal de la localización)**.** *Sea $\gamma : A \to S^{-1}A$ el homomorfismo de localización y $f : A \to B$ un homomorfismo tal que $f(s) \in \mathcal{U}(B)$ toda vez que $s \in S$. Entonces, existe un único homomorfismo $\Phi : S^{-1}A \to B$ tal que $f = \Phi \circ \gamma$.*

Demostración. Basta con definir $\Phi(\frac{a}{s}) = f(a)f(s)^{-1}$. Puede verificarse que está bien definido y es homomorfismo. □

Proposición 43. *Si $f : A \to B$ es homomorfismo de anillos, $S \subset A$ y $T \subset B$ son multiplicativamente cerrados y $f(S) \subset T$, entonces se tiene una (única) $\phi : S^{-1}A \to S^{-1}B$ tal que $\phi \circ \gamma_S = \gamma_T \circ f$.*

Demostración. Basta con aplicar la propiedad universal a $\gamma_T \circ f$. □

Como corolario, si $S \subset T \subset A$ son multiplicativamente cerrados en el anillo A, entonces puede tomarse $f = Id_A$ en la proposición previa y se tiene una aplicación $S^{-1}A \to T^{-1}A$.

Proposición 44. *Sea $\gamma : A \to S^{-1}A$ es el homomorfismo de localización, entonces:*

1. *Si $s \in S$, $\gamma(s)$ es una unidad.*
2. *Si $\gamma(a) = 0$, entonces $as = 0$ para cierto $s \in S$.*
3. *Todo elemento de $S^{-1}A$ es de la forma $\gamma(a)\gamma(s)^{-1}$.*

Además, si $f : A \to B$ es un homomorfismo que cumple todas esas propiedades (con B en lugar de $S^{-1}A$), entonces $B \simeq S^{-1}A$.

Demostración. El inverso de $\gamma(s) = \frac{s}{1}$ es $\frac{1}{s}$. Si $\frac{a}{1} = \frac{0}{1}$, entonces sabemos que $\exists s \in S$ con $s(a \cdot 1 - 0 \cdot 1) = 0$, que es lo que se quería. Finalmente, el $\frac{a}{s}$ es de la forma $\gamma(a)\gamma(s)^{-1} = \frac{a}{1}\frac{1}{s}$. El último comentario es consecuencia directa de la propiedad universal: el punto 1 permite construir Φ, el punto 2 establece que Φ es inyectiva y el punto 3 que es sobreyectiva. □

Proposición 45. *Existe una correspondencia biyectiva entre* $\mathrm{Spec}(S^{-1}A)$ *y* $\mathcal{C} = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$*, dada por la contracción y la extensión a través de* γ*.*

Demostración. Dado $\mathfrak{q} \in \mathrm{Spec}(S^{-1}A)$, sabemos que su contracción $\gamma^{-1}(\mathfrak{q})$ es primo. Veamos que no interseca con S: si fuera $s \in \gamma^{-1}(\mathfrak{q}) \cap s$, entonces, $\gamma(s) \in \mathfrak{q}$, pero $\gamma(s)$ es una unidad, contradiciendo la primalidad de q. Ahora veremos que la extensión de un $\mathfrak{p} \in \mathrm{Spec}(A)$ que no corta con S es primo. Supongamos que $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}^e$. Entonces, puede ponerse $\frac{ab}{st} = \frac{p}{t}$ con $p \in \mathfrak{p}$. Esto quiere decir que $\omega(abr - pst) = 0$ para cierto $\omega \in S$ y, por tanto, $(\omega r)(ab) = pst \in \mathfrak{p}$. Como $\omega r \notin \mathfrak{p}$ al estar en S, ha de ser que $ab \in \mathfrak{p}$ luego $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, de donde $\frac{a}{s} \in \mathfrak{p}^e$ o $\frac{b}{t} \in \mathfrak{p}$.

Finalmente, hay que ver que la correspondencia es biyectiva, es decir, que $\mathfrak{p}^{ec} = \mathfrak{p}$, lo que se traduce en ver que si $\frac{a}{1} = \frac{q}{s}$ con $q \in \mathfrak{p}$, entonces $a \in \mathfrak{p}$. Esto se comprueba con un argumento idéntico al anterior. □

Definición 59. Si $\mathfrak{p} \in \mathrm{Spec}(A)$, sabemos que $S = A \setminus \mathfrak{p}$ es multiplicativamente cerrado. Denotamos $A_{\mathfrak{p}} := A_S = S^{-1}A$. Asimismo, dado $f \in A$, se denota $A_f = T^{-1}A$, siendo $T = \{f^0, f^1, f^2, \ldots\}$. Se denota por $(f)_0$ a los ideales primos de A que contienen a f.

Entonces, como corolario de la correspondencia previa, se tiene que $\mathrm{Spec}(A_f)$ está en biyección con $\mathrm{Spec}(A) \setminus (f)_0$.

Proposición 46. *Sea* A *un anillo,* S *multiplicativamente cerrado y* $I \subset A$ *un ideal con* $I \cap S = \emptyset$*. Sea* Σ *el conjunto de ideales* $J \subset A$ *con* $I \subset J$ *e* $I \cap S = \emptyset$*. Entonces,* Σ *contiene un elemento maximal con respecto de la inclusión,* $\mathfrak{p} \in \Sigma$*, que además es un ideal primo (*$\mathfrak{p} \in \mathrm{Spec}(A)$*).*

Demostración. Como $I \in \Sigma$ y toda cadena creciente en Σ tiene su unión como cota superior, el lema de Zorn garantiza la existencia de elemento maximal. Ahora veamos que tales maximales de Σ son ideales primos. Dados $x, y \notin \mathfrak{p}$, consideramos $\mathfrak{p} + (x), \mathfrak{p} + (y)$, que contienen estrictamente a $\mathfrak{p}$. Por maximalidad, deben cortar con S, así que $p_1 + t_1 x, p_2 + t_2 y \in S$ para ciertos $p_1, p_2 \in \mathfrak{p}$, $t_1, t_2 \in A$. Entonces, por ser S cerrado multiplicativamente, se tiene que $(p_1 + t_1 x)(p_2 + t_2 y) = p_1 p_2 + p_1 t_2 y + p_2 t_1 x + t_1 t_2 xy \in S$. Pero ese elemento también está en $\mathfrak{p} + (xy)$, luego ha de ser que $xy \notin \mathfrak{p}$, como se quería. □

Definición 60. Sea M un A-módulo y $S \subset A$ un conjunto multiplicativamente cerrado. Se define el **módulo de fracciones o localización de** M **en** S como el módulo $S^{-1}M = (M \times S)/\sim$, con $(m, s) \sim (n, t) \iff mu = nv, su = tv$ para ciertos $u, v \in S \iff \omega(mt - ns) = 0$ para cierto $\omega \in S$. Tiene estructura de $S^{-1}A$-módulo mediante la suma $\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$ y el producto $\frac{a}{s}\frac{m}{t} = \frac{am}{st}$.

Nótese que $S^{-1}M$ también tiene estructura de A-módulo con la operación $a\frac{m}{s} := \frac{am}{s}$.

Definición 61. Se define el homomorfismo de localización como $\gamma : M \to S^{-1}M$ dado por $m \to \frac{m}{1}$. Es un homomorfismo de A-módulos.

Proposición 47 (Propiedad universal)**.** *Sea* M *un* A*-módulo y* N *un* $S^{-1}A$ *módulo. Sea* $f : M \to N$ *un homomorfismo* A*-lineal. Entonces,* $\exists! \phi : S^{-1}M \to N$ *tal que* $f = \phi \circ \gamma$*.*

Demostración. Basta con definir $\phi(\frac{m}{s}) = \frac{1}{s} \cdot f(m)$. □

Definición 62. El **soporte** del A-módulo M se define como $\mathrm{sop}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) : M_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}M \neq 0\}$.

Definición 63. El **submódulo de torsión** de un A-módulo M se define por $T(M) = \{m \in M : \exists a \in A, a \neq 0, am = 0\}$. Si $T(M) = 0$ se dice que M es **libre de torsión**. Si $T(M) = M$ se dice que M es un **módulo de torsión**.

Por ejemplo, si $S = A \setminus \{0\}$ y $\gamma : M \to S^{-1}M$ es la localización, es inmediato ver que $\ker(\gamma) = T(M)$.

Proposición 48. *Sea $S \subset A$ multiplicativamente cerrado y $f : M \to N$ un homomorfismo de A-módulos. Se tiene una única $f_S : S^{-1}M \to S^{-1}N$ que cumple $\gamma_N \circ f = f_S \circ \gamma_M$. También se suele denotar $f_S \equiv S^{-1}f$.*

Demostración. Basta con aplicar la propiedad universal a $\gamma_N \circ f$. □

Proposición 49. *Sea $f : M \to N$ un homomorfismo de A-módulos. Entonces $S^{-1}\ker(f) = \ker(S^{-1}f)$ y $S^{-1}\operatorname{Im}(f) = \operatorname{Im}(S^{-1}f)$.*

Demostración. Como $i : \ker(f) \hookrightarrow M$, se tiene una aplicación $S^{-1}i : S^{-1}\ker(f) \to S^{-1}M$. Puede comprobarse rutinariamente que de hecho va sobre $\ker(S^{-1}f)$ y es un isomorfismo. De modo análogo con la imagen. □

Teorema 16. *Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ exacta. Entonces $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ también es exacta. En particular, las aplicaciones inyectivas son transformadas en inyectivas y las sobreyectivas en sobreyectivas.*

Demostración. $\operatorname{Im}(S^{-1}f) = S^{-1}\operatorname{Im}(f) = S^{-1}\ker(g) = \ker(S^{-1}g)$. □

Pueden comprobarse las siguientes propiedades:

Proposición 50. *Si N, P son A-submódulos de M, se tienen:*

1. $S^{-1}(M + N) = S^{-1}M + S^{-1}N$.
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$.
3. $S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N$.
4. $S^{-1}(M/N) = S^{-1}M/S^{-1}N$.

Proposición 51. *Se tiene que $S^{-1}A \otimes_A M \simeq S^{-1}M$. Por tanto $S^{-1}A$ es plano.*

Demostración. La aplicación bilineal $S^{-1}A \times M \to S^{-1}M$ dada por $(\frac{a}{s}, m) \to \frac{am}{s}$ levanta a un isomorfismo. El segundo comentario sigue de que, como tensorizar por $S^{-1}A$ es equivalente a localizar por S, y localizar es exacto, $S^{-1}A$ es plano. □

Observación 19. Si M, N son A-módulos, entonces $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq S^{-1}(M \otimes_A N)$. La correspondencia es $\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$, y puede verse convirtiendo las localizaciones en productos tensoriales por $S^{-1}A$ y usando las propiedades del producto tensorial.

3.1. Propiedades locales

A continuación veremos una serie de propiedades que pueden estudiarse localmente.

Proposición 52. *Sea M un A-módulo. Se tiene que $M = 0 \iff M_{\mathfrak{p}} = 0$ para todo $\mathfrak{p} \in \operatorname{Spec}(A) \iff M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \in \operatorname{Spm}(A)$.*

Demostración. Las dos implicaciones hacia la derecha son evidentes, así que probamos que la última afirmación implica la primera. Supongamos que $M \neq 0$ y sea $x \in M$, $x \neq 0$. Sea $I = \operatorname{Ann}(x)$. Como $1 \notin I$, entonces $I \subsetneq A$ de modo que hay un maximal $\mathfrak{m}$ con $I \subset \mathfrak{m}$. Se afirma que entonces $M_{\mathfrak{m}} \neq 0$, dado que $\frac{x}{1} = 0 \iff \omega x = 0$ con $\omega \in A \setminus \mathfrak{m}$, lo cual no es posible porque $\operatorname{Ann}(x) \subset \mathfrak{m}$. □

Proposición 53. *Sea $f : M \to N$ un homomorfismo de A-módulos. Se tiene que f es inyectiva $\iff f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ es inyectiva para todo $\mathfrak{p} \in \operatorname{Spec}(A) \iff f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ es inyectiva para todo $\mathfrak{m} \in \operatorname{Spm}(A)$.*

Demostración. El primer $\implies$ ya está visto por exactitud de la localización y el segundo $\implies$ es obvio. Ahora, si $f_{\mathfrak{m}}$ es inyectiva para todo $\mathfrak{m} \in \operatorname{Spm}(A)$, entonces $0 = \ker(f_{\mathfrak{m}}) = (\ker f)_{\mathfrak{m}}$ lo que, por la proposición previa, implica $\ker f = 0$. □

Proposición 54. *Sea $f : M \to N$ un homomorfismo de A-módulos. Se tiene que f es sobreyectiva $\iff$ $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ es sobreyectiva para todo $\mathfrak{p} \in \operatorname{Spec}(A)$ $\iff$ $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ es sobreyectiva para todo $\mathfrak{m} \in \operatorname{Spm}(A)$.*

Demostración. Igual que antes pero considerando el $\operatorname{coker} f$. □

Proposición 55. *Sea M un A-módulo. Se tiene que M es plano $\iff$ $M_{\mathfrak{p}}$ es plano $\forall \mathfrak{p} \in \operatorname{Spec}(A)$ $\iff$ $M_{\mathfrak{m}}$ es plano $\forall \mathfrak{m} \in \operatorname{Spm}(A)$.*

Demostración. De nuevo, los dos $\implies$ son sencillos. Ahora, para demostrar que la tercera afirmación implica la primera, sea $f : N \to P$ inyectiva. Entonces, si $\mathfrak{m} \in \operatorname{Spm}(A)$, se tiene que $f_{\mathfrak{m}} : N_{\mathfrak{m}} \to P_{\mathfrak{m}}$ es inyectiva. Como $M_{\mathfrak{m}}$ es plano, se tiene que $f'_{\mathfrak{m}} : M_{\mathfrak{m}} \otimes N_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes P_{\mathfrak{m}} \simeq (M \otimes N)_{\mathfrak{m}} \to (M \otimes P)_{\mathfrak{m}}$ es inyectiva. Como esto sucede para todo $\mathfrak{m} \in \operatorname{Spm}(A)$, sigue que $f' : M \otimes N \to M \otimes P$ es inyectiva, luego M es plano. □

3.2. Extensión y contracción en localizados

Enunciamos ahora algunas propiedades que se tienen cuando A es un anillo, S es un sistema cerrado multiplicativamente y $\gamma : A \to S^{-1}A$ es la localización.

Proposición 56. *Se tienen:*

1. *Todo ideal de $S^{-1}A$ es extendido de γ, dado que si $I \in S^{-1}A$, entonces $I^{ce} = I$.*
2. *Si $I \subset A$ es un ideal, entonces $I^{ec} = \bigcup_{s \in S}(I : s)$. Además, $I^e = S^{-1}A \iff I \cap S \neq \emptyset$.*
3. *$I \subset A$ es contraído por $\gamma \iff$ ningún elemento de S es divisor de cero en A/I.*
4. *$S^{-1}(I + J) = S^{-1}I + S^{-1}J$, $S^{-1}(IJ) = S^{-1}IS^{-1}J$, $\operatorname{rad}(S^{-1}I) = S^{-1}\operatorname{rad}(I)$, $S^{-1}N_A = N_{S^{-1}A}$.*
5. *Si M es finitamente generado, entonces $S^{-1}\operatorname{Ann}(M) = \operatorname{Ann}(S^{-1}M)$.*

Proposición 57. *Sea A un anillo y S un sistema multiplicativamente cerrado. Sea $T' \subset S^{-1}A$ un sistema multiplicativamente cerrado tal que $S \subset \gamma^{-1}(T')$, siendo γ la localización de A por S. Entonces $(T')^{-1}(S^{-1}A) = T^{-1}A$.*

Demostración. Vamos a ver que $(T')^{-1}(S^{-1}A)$ cumple la propiedad universal de $T^{-1}A$ para el homomorfismo $\gamma : A \to (T')^{-1}(S^{-1}A)$ dado por localizar en S y luego en T', es decir, $\gamma = \gamma_{T'} \circ \gamma_S$. Por unicidad, entonces, deberá ser $T^{-1}A = (T')^{-1}(S^{-1}A)$. Sea $g : A \to C$ tal que $g(T) \subset \mathcal{U}(C)$. Como $S \subset T$, entonces $g(S) \subset g(T) \subset \mathcal{U}(C)$, luego $\exists g_S : S^{-1}A \to C$ con $g = g_S \circ \gamma_S$. Ahora, dado $r = \frac{x}{s} \in T'$, se tiene que $x \in T$ (dado que $\frac{x}{1} = \frac{s}{1}r \in T'$ porque $S \subset T$ así que $\frac{s}{1} \in T'$), de modo que $g_S(r) = g_S(\frac{x}{1})g_S(\frac{1}{s}) = g(x)g_S(\frac{1}{s}) \in \mathcal{U}(C)$. Entonces, $\exists g_{T'} : (T')^{-1}S^{-1}A \to C$ con $g_S = g_{T'} \circ \gamma_{T'}$. Ahora, componiendo a ambos lados con γ_S sigue que $g = g_{T'} \circ \gamma$ como se quería. □

Observación 20. Como corolario, si A es un anillo y $p, q \in \operatorname{Spec}(A)$ con $p \subset q$, se tiene que $T = A \setminus p$ y $S = A \setminus q$ cumplen $S \subset T$. Además, $pA_{(q)}$ es primo en $A_{(q)}$ porque $p \cap (A \setminus q) = \emptyset$. Entonces, $T' = A_{(q)} \setminus pA_{(q)}$ es otro sistema multiplicativo y, por la proposición previa, sigue que $A_{(p)} = (A(q))_{(pA_{(q)})}$.

Proposición 58. *Sea $f : A \to B$ y $p \in \operatorname{Spec}(A)$. Entonces $p = q^c$ para cierto $q \in \operatorname{Spec}(B) \iff p^{ec} = p$.*

Demostración. $\implies$ es obvia. Para $\impliedby$, definimos $S = f(A \setminus p)$, que es un sistema multiplicativamente cerrado (inmediato de comprobar). Además, $p^e \cap S = \emptyset$ al ser S la imagen de todo salvo p. Por tanto, $S^{-1}p^e \subsetneq S^{-1}B$, así que $S^{-1}p^e \subset m$ con m maximal. Definiendo $q = \gamma_S^{-1}(m)$, se tiene que q es primo (es la contracción de un maximal), $p^e \subset q$ y $q \cap S = \emptyset$, de modo que $q^c = p$. □

4. Anillos Noetherianos.

Proposición 59. *Sea $(\Sigma, \leq)$ un conjunto parcialmente ordenado. Son equivalentes:*

1. ***Condición de cadena ascendente.*** *Para toda sucesión ascendente $x_1 \leq x_2 \leq \dots$, existe un $N \in \mathbb{N}$ tal que $x_N = x_{N+t}$ para todo $t \in \mathbb{N}$.*
2. *Todo subconjunto no vacío de Σ tiene un elemento maximal.*

De manera análoga, son equivalentes:

1. ***Condición de cadena descendente.*** *Para toda sucesión descendente $x_1 \geq x_2 \geq \dots$, existe un $N \in \mathbb{N}$ tal que $x_N = x_{N+t}$ para todo $t \in \mathbb{N}$.*
2. *Todo subconjunto no vacío de Σ tiene un elemento minimal.*

Demostración. Demostramos el caso ascendente siendo el otro idéntico. Para $1 \implies 2$, si $S \subset \Sigma$ es no vacío pero no hay elemento maximal, es posible construir una sucesión estrictamente creciente, dado que todo elemento tiene otro distinto por encima. Para $2 \implies 1$, se toma como subconjunto no vacío $\{x_n\}_{n\in\mathbb{N}}$ y ha de estabilizar en el maximal. □

Definición 64. Un A-módulo M es **noetheriano** si el conjunto de submódulos ordenado por inclusión satisface la condición de cadena ascendente, y **artiniano** si satisface la condición de cadena descendente.

Considerando A como A-módulo, cuyos submódulos son los ideales, es posible hablar de anillos noetherianos y artinianos.

Observación 21. Cualquier dominio de ideales principales es noetheriano, dado que si $(x_1) \subset (x_2) \subset \dots$ es una cadena, escribiendo $(x) = \bigcup_i (x_i)$, la cadena estabiliza a partir del primer (x_i) que contenga a x. Los cuerpos son artinianos y noetherianos, al solo tener dos ideales. Un subanillo de un noehteriano no tiene por qué ser noetheriano: por ejemplo $K[X_1, X_2, \dots]$ no es noetheriano pero, al ser un dominio, es subanillo de su cuerpo de fracciones. El caso de artinianos es lo mismo: $\mathbb{Z} \subset \mathbb{Q}$, pero $\mathbb{Z}$ no es artiniano: $(2) \supset (4) \supset (8) \supset \dots$.

Proposición 60. *El anillo M es noetheriano $\iff$ todo $N \subset M$ submódulo es finitamente generado.*

Demostración. Para $\implies$, si hubiera un submódulo N no finitamente generado, es posible tomar $x_1 \in N$ no nulo, e iterativamente tomar $x_k \in N \setminus (x_1, \dots, x_{k-1})$, que siempre será no vacío. Entonces la cadena $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$ es ascendente y nunca estabiliza. Para $\impliedby$, sea $M_1 \subset M_2 \subset \dots$ una cadena de submódulos. Como $N = \bigcup M_i \subset M$ es un submódulo (al ser una cadena), es finitamente generado: $N = \langle m_1, \dots, m_r \rangle$. El primer submódulo de la cadena que contenga a todos los $m_1, \dots, m_r$ es el punto donde estabiliza. □

Proposición 61. *Si $0 \to M' \to M \to M'' \to 0$ es una sucesión exacta corta, M es noetheriano (resp. artiniano) $\iff$ M' y M'' son noetherianos (resp. artinianos).*

Observación 22. Como corolario, se tiene que si $\{M_i\}_i$ son noetherianos (resp. artinianos), entonces $\bigoplus_i M_i$ es noetheriano (resp. artiniano). Basta con considerar $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ y aplicar inducción.

Observación 23. Otro corolario es que si M es un A-módulo finitamente generado, con A noetheriano (resp. artiniano), entonces M es noetheriano (resp. artiniano). Esto es así porque sabemos que $M \simeq A^k/N$, y basta con considerar $0 \to N \to A^k \to A^k/N \to 0$.

Teorema 17 (Base de Hilbert)**.** *Si A es un anillo noetheriano, entonces $A[X]$ (y $A[[X]]$) lo es.*

Demostración. Sea $\mathfrak{a} \subset A[X]$ un ideal e I el ideal generado por los coeficientes principales de polinomios de $\mathfrak{a}$. Como A es Noetheriano, $I = \langle a_1, \ldots, a_n \rangle$. Sea $f_i \in \mathfrak{a}$ con coeficiente principal a_i. Sea $r_i = \deg f_i$ y $r = \max_i\{r_i\}$. Sea $\mathfrak{a}' = \langle f_i \rangle \subset \mathfrak{a}$. Ahora, dado $f \in \mathfrak{a}$ con $\deg f = m$ y coeficiente principal a, si $m \geq r$, como $a \in I$ podemos escribir $a = \sum u_i a_i$ con cada $u_i \in A$. Entonces es posible restar un polinomio de $\mathfrak{a}'$: $f - \sum u_i f_i x^{m-r_i} \in \mathfrak{a}$ para conseguir grado estrictamente menor que m. Es decir, podemos continuar hasta obtener g con $\deg g < r$ y tal que $f - g \in \mathfrak{a}'$. En otras palabras, si $M = \langle 1, x, \ldots, x^{r-1} \rangle$ es el A-submódulo de $A[X]$ de polinomios de grado menor que r, hemos probado que $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Pero como A es noetheriano y M finitamente generado, M es noetheriano y $\mathfrak{a} \cap M$ finitamente generado, de modo que ambos sumandos son finitamente generados y por tanto $\mathfrak{a}$ también. □

Proposición 62. *Si S es un conjunto multiplicativamente cerrado del anillo A y A es noetheriano (resp. artiniano) entonces $S^{-1}A$ es noetheriano (resp. artiniano).*

Demostración. Sigue directamente de la correspondencia entre ideales de $S^{-1}A$ e ideales de A que preserva inclusiones por medio de la localización γ. □

Proposición 63. *Sea A artiniano y $\mathfrak{p} \in \operatorname{Spec}(A)$. Entonces $\mathfrak{p}$ es maximal. En particular, $N_A = J_A$.*

Demostración. Sabemos que $B = A/\mathfrak{p}$ es un dominio artiniano. Dado $x \in B$, $x \neq 0$, consideramos $(x) \supset (x^2) \supset (x^3) \supset \ldots$. Sabemos que hay un $n \in \mathbb{N}$ con $(x^n) = (x^{n+1})$, luego existe $y \in B$ con $x^n = x^{n+1}y$. Como B es un dominio, esto implica que $1 = xy$, de modo que B es un cuerpo y $\mathfrak{p}$ es maximal. □

Proposición 64. *Si A es artiniano, es semilocal.*

Definición 65. Sea A un anillo, $I \subset A$ un ideal. Una **descomposición primaria** de I es una expresión $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$, con cada $\mathfrak{q}_i$ un ideal $\mathfrak{p}_i$-primario. Cada $\mathfrak{p}_i$ se denomina **ideal primo asociado a** I. Si $\mathfrak{p}_i$ es minimal, se denomina **primo minimal de** I, mientras que en caso contrario se denomina **primo sumergido en** I. Si los $\mathfrak{p}_i$ son distintos entre sí y no es posible eliminar ningún $\mathfrak{q}_i$, se dice que la descomposción es **reducida**.

La descomposición no tiene por qué existir. Sin embargo:

Teorema 18. *Si A es noetheriano, todo ideal $I \subset A$ admite descomposición primaria.*

Tampoco está garantizada la unidad: por ejemplo, si K es un cuerpo y consideramos $I = (x^2, xy) \subset K[x, y]$, se tiene que $I = (x) \cap (y, x^2) = (x) \cap (y, x)^2$. Sin embargo los primos asociados coinciden: (x) y (x, y). En este caso, (x) es minimal y (x, y) sumergido.

5. Topología de Zariski

Definición 66. En un anillo A, definimos la función $V : \mathcal{P}(A) \to \mathcal{P}(\operatorname{Spec}(A))$ dada por $V(E) = \{\mathfrak{p} \in \operatorname{Spec}(A) : E \subset p\}$. Nótese que la función también puede definirse restringida a los ideales de A sin perder imagen, dado que $V(E) = V(\langle E \rangle)$.

Utilizaremos esta función para definir la topología de Zariski en $\operatorname{Spec}(A)$.

Proposición 65. *La función v satisface:*

1. $E \subset E' \implies V(E') \subset V(E)$.
2. $V(0) = \operatorname{Spec}(A)$.
3. $V(1) = \emptyset$.

4. $V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$.

5. $V(A \cap B) = V(A) \cup V(B)$, *y también coincide con* $V(AB)$ *en caso de que* A, B *sean ideales.*

Demostración. Del 1 al 4 son obvias. Ahora, $\mathfrak{p} \in V(A \cap B) \implies A \cap B \subset \mathfrak{p} \implies A \subset \mathfrak{p}$ o $B \subset \mathfrak{p}$ al ser $\mathfrak{p}$ primo. La otra inclusión es evidente. □

Definición 67. Sea $X = \operatorname{Spec}(A)$ y $\tau = \{\operatorname{Spec} A \setminus V(E) : E \subset A\}$. El espacio topológico (X, τ) se conoce como **topología de Zariski**.

Es una topología que se define por los cerrados, que son los conjuntos $V(E)$. Estos satisfacen los axiomas de cerrados de una topología por la proposición previa.

Definición 68. El anillo $A/\langle E\rangle$ se denomina **anillo de coordenadas** de $V(\langle E\rangle)$. Los elementos de A se suelen denominar **funciones** y los de $\operatorname{Spec}(A)$ **puntos**, en el contexto de topología de Zariski. Los puntos $x \in \operatorname{Spec}(A)$ se denotan también $\mathfrak{p}_x$ cuando es conveniente interpretarlos como ideales. Diremos que una función $f \in A$ **se anula en** $x \in \operatorname{Spec}(A)$ si $f \in \mathfrak{p}_x$, es decir, si $f = 0$ en coordenadas $A/\mathfrak{p}_x$.

La siguiente proposición es útil para calcular espectros primos a través de homomorfismos:

Proposición 66. *Sea* $g : A \to B$ *un homomorfismo de anillos y* $g^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ *la dada por contracción. Si* $x \in \operatorname{Spec}(A)$, *se tiene que* $(g^*)^{-1}(x) = \operatorname{Spec}(B_x/\mathfrak{p}_x B_x)$, *donde* B_x *es la localización en* $S = g(A \setminus \mathfrak{p}_x)$.

Demostración. Los primos $y \in \operatorname{Spec}(B)$ con $g^*(y) = x$ son precisamente aquellos tales que $\mathfrak{p}_y^c = \mathfrak{p}_x$. Esto impone dos condiciones: $\mathfrak{p}_y^c \subset \mathfrak{p}_x$, es decir, $\mathfrak{p}_y$ no corta a S y por tanto la localización de $\mathfrak{p}_y$ es un ideal en B_x y, por otro lado, $\mathfrak{p}_x \subset \mathfrak{p}_y^c$, es decir, $\mathfrak{p}_y$ es un ideal que contiene a $\mathfrak{p}_x B_x$ luego es un ideal en el cociente. La primalidad se preserva en todo momento. □

Obsérvese que en la topología de Zariski los cerrados $V(E)$ son precisamente los puntos anulados por un conjunto de funciones E.

Proposición 67. *Definimos* $D(f) = \operatorname{Spec}(A) \setminus V(f)$ *como el abierto de los primos no anulados por* f. *Entonces* $\{D(f) : f \in A\}$ *es una base de la topología.*

Demostración. Cualquier abierto $U = \operatorname{Spec}(A) \setminus V(E)$ son los puntos no anulados por E, es decir, los puntos no anulados por algún elemento de E. En otras palabras: $U = \operatorname{Spec}(A) \setminus V(E) = \operatorname{Spec}(A) \setminus V(\bigcup_{f\in E}\{f\}) = \operatorname{Spec}(A) \setminus \bigcap_{f\in E} V(\{f\}) = \bigcup_{f\in E} D(f)$. □

Observación 24. Si $S = \{1, f, f^2, \ldots\}$, entonces la localización de $S^{-1}A = A_f$ cumple que sus ideales primos son los ideales primos de A que no contienen a f, es decir, $\operatorname{Spec}(A_f) = D(f)$.

Definición 69. Un **esquema afín** $(A, \operatorname{Spec}(A))$ consiste en un anillo A y su espectro con la topología de Zariski.

Proposición 68. *Sea* $x \in \operatorname{Spec}(A)$. *Se tiene que* $\overline{\{x\}} = V(\mathfrak{p}_x)$. *Por tanto,* $y \in \overline{x} \iff \mathfrak{p}_x \subset \mathfrak{p}_y$. *De este modo,* x *es cerrado* $\iff V(\mathfrak{p}_x) = x \iff p_x$ *es maximal. Así,* $\operatorname{Spec}(A)$ *no tiene por qué ser* T_1 *pero siempre es* T_0.

Demostración. En primer lugar, como $x \in V(\mathfrak{p}_x)$, entonces $\overline{\{x\}} \subset V(\mathfrak{p}_x)$. Ahora, si escribimos $\overline{\{x\}} = V(E)$, entonces, como $x \in \overline{\{x\}} = V(E)$ sigue $E \subset \mathfrak{p}_x$, de donde $V(\mathfrak{p}_x) \subset V(E) = \overline{\{x\}}$, como se quería. Entonces, $y \in \overline{\{x\}} \iff y \in V(\mathfrak{p}_x) \iff \mathfrak{p}_x \subset \mathfrak{p}_y$. Si $x \neq y$, es porque $\mathfrak{p}_x \not\subseteq \mathfrak{p}_y$ (sin perder generalidad) y entonces sigue que $y \notin \overline{\{x\}}$, luego $\operatorname{Spec}(A) \setminus \overline{\{x\}}$ es un entorno de y que no contiene a x, así que la topología es T_0. □

Definición 70. Un espacio topológico X es **irreducible** si no puede escribirse $X = C_1 \cup C_2$, donde cada $C_i \subsetneq X$ es un cerrado. Las **componentes irreducibles** de X son sus subespacios irreducibles maximales.

Obsérvese que si $C \subset X$ es irreducible, entonces $\overline{C}$ es irreducible, dado que si pudiera ser $\overline{C} = C_1 \cup C_2$, con cada C_j cerrado en $\overline{C}$ (equivalentemente, en X al ser $\overline{C}$ cerrado) tendríamos que $C = (C_1 \cap C) \cup (C_2 \cap C)$, que son dos cerrados de C, luego $C = (C_1 \cap C)$ sin perder generalidad y, por tanto, $C \subset C_1$. Pero entonces $\overline{C} \subset \overline{C_1} = C_1$, lo que completa el argumento. Se deduce también de aquí que las componentes irreducibles son cerradas.

Lema 3. *Los cerrados irreducibles de* $\mathrm{Spec}(A)$ *son clausuras de puntos. Las componentes irreducibles son las clausuras de primos minimales.*

Demostración. Sea C un cerrado irreducible, $C = V(E) = V(\langle E \rangle) = V(I)$, donde I es el ideal generado por los elementos que se anulan en C y por tanto es un ideal radical. Ahora veamos que I es primo y por tanto $V(I) = \overline{I}$. Si $fg \in I$, entonces $C \subset V(fg)$ luego $C = C \cap V(fg) = C \cap (V(f) \cup V(g)) = (C \cap V(f)) \cup (C \cap V(g))$. Por irreducibilidad, sin perder generalidad, $C = C \cap V(f)$ así que $f \in I$. □

La misma demostración sirve para ver que si I es un ideal radical, $V(I)$ irreducible implica I primo.

Proposición 69. *Si X es irreducible, entonces es conexo.*

Demostración. Si no fuese conexo, es decir, $X = A \cup B$ con A, B abiertos disjuntos, entonces sus complementarios darían una descomposición de X en cerrados no triviales. □

Proposición 70. *Existe una correspondencia entre los subconjuntos $U \subset X = \mathrm{Spec}(A)$ que son simultáneamente abiertos y cerrados, y los elementos idempotentes de A ($e \in A$ con $e^2 = e$).*

Demostración. Si e es idempotente no nulo, entonces se le asocia el $V(e) := V((e))$. Para ver que es abierto y cerrado, comprobaremos que $X \setminus v(e) = V(1-e)$. Por un lado, son disjuntos, dado que si fuese $e, 1-e \in \mathfrak{p}$ entonces $1 \in \mathfrak{p}$ y no sería primo. Por otro lado, si $\mathfrak{p} \notin V(e)$, entonces debe ser que $\mathfrak{p} \in V(1-e)$ dado que, si no, se tendría $e, 1-e \notin \mathfrak{p}$ pero $e(1-e) = 0 \in \mathfrak{p}$ contradiciendo la primalidad. Estas dos observaciones implican que $X \setminus V(e) = V(1-e)$.

Ahora, sea U abierto y cerrado en X. Como U es un cerrado de X que es cuasicompacto (es decir, compacto en el sentido topológico usual: es fácil ver que X lo es para cualquier anillo), sigue que U también es cuasicompacto y por tanto puede escribirse $U = \bigcup_{i=1}^{n} D(f_i)$. Análogamente $X \setminus U = \bigcup_{j=1}^{m} D(g_j)$. Además por ser disjuntos, $\emptyset = D(f_i) \cap D(g_j) = D(f_i g_j)$, lo que implica (verificable fácilmente) que $f_i g_j$ es nilpotente. De este modo, si $I = (f_1, \ldots, f_n)$ y $J = (g_1, \ldots, g_m)$, entonces existe un entero N con $(IJ)^N = 0$. Además, por construcción de I y J sigue que $U \subset V(J)$ y $X \setminus U \subset V(I)$, lo que permite escribir la unión disjunta: $X = V(I) \cup V(J)$, en otras palabras, $I + J = A$. Entonces, $I^N + J^N = A$ así que existe $x \in I^N$, $y \in J^N$ con $x + y = 1$ y, además, $xy = 0$ porque $(IJ)^N = 0$. En otras palabras, $x(1-x) = 0$ así que x es idempotente. Ahora es fácil verificar que $U = D(x)$ y $X \setminus U = D(1-x)$. □

5.1. Espacios afines

Definición 71. Sea k un cuerpo infinito y sea $A = k[x_1, \ldots, x_n]$ el anillo de polinomios en n indeterminadas. Definimos el **espacio afín n-dimensional sobre k** $\mathbb{A}_k^n = \{(a_1, \ldots, a_n) : a_j \in k\}$. Para $J \subset A$, definimos $V(J) = \{p \in \mathbb{A}_k^n : \forall p \in J,\ f(p) = 0\}$. Los conjuntos de esta forma se denominan **conjuntos algebraicos afines**. Asimismo, para $S \subset \mathbb{A}_k^n$, definimos $I(S) = \{f \in A : \forall p \in S,\ f(p) = 0\}$.

Observación 25. Se tienen:

1. $V(0) = \mathbb{A}_k^n$ y $V(A) = \emptyset$.
2. $I(\emptyset) = A$ y $I(\mathbb{A}_k^n) = 0$.
3. $J \subset J' \implies V(J') \subset V(J)$.
4. $S \subset S' \implies I(S') \subset I(S)$.

5. $S \subset V(I(S))$.
6. $J \subset I(V(J))$.
7. $I(S) = I(V(I(S)))$.
8. $V(J) = V(I(V(J)))$.
9. $\bigcap V(J_i) = V(\bigcup_i J_i)$.
10. $V(J) \cup V(J') = V(J \cap J')$.

Proposición 71. *Sea $S \subset \mathbb{A}_k^n$. Entonces $\overline{S} = V(I(S))$.*

Demostración. Por un lado, $S \subset V(I(S))$. Ahora, si $W = V(E)$ es otro cerrado con $S \subset W$, se tiene que $E \subset I(W) \subset I(S)$, con lo cual $V(I(S)) \subset V(E) = W$, lo que prueba que $V(I(S))$ es el menor cerrado que contiene a S. □

Observación 26. Por ejemplo, como $k[x_1]$ es un dominio de ideales principales, los conjuntos algebraicos de $\mathbb{A}_k^1$ son $V(f)$ y, por tanto, los cerrados son precisamente los conjuntos finitos y el total (es decir, la topología de Zariski es la cofinita).

Definición 72. Un conjunto algebraico afín $S \subset \mathbb{A}_k^n$ es **irreducible** si toda vez que $S = S_1 \cup S_2$, con S_1, S_2 cerrados (conjuntos algebraicos afines), se tiene $S = S_1$ o $S = S_2$.

Definición 73. Un conjunto algebraico afín irreducible se denomina **variedad algebraica afín**.

Definición 74. Sea $E \subset \mathbb{A}_k^n$ un conjunto algebraico afín. Se define el **anillo de coordenadas** o **anillo de polinomios** de E como $A(E) = k[x_1, \ldots, x_n]/I(E)$, es decir, los polinomios en n variables con $f \sim g \iff f - g \in I(E) \iff f - g = 0$ en $E \iff f = g$ en E.

Definición 75. Una **hipersuperficie algebraica** en $\mathbb{A}_k^n$ es un conjunto algebraico afín de la forma $V(f)$ con $f \in k[x_1, \ldots, x_n]$ no constante.

Observación 27. Si $V(E)$ es algebraico afín, entonces podemos escribir $V(E) = V(\langle E \rangle)$. Ahora, como $\langle E \rangle \subset k[x_1, \ldots, x_n]$ es un ideal en un anillo noetheriano, podemos poner $\langle E \rangle = (f_1, \ldots, f_m)$, de modo que los conjuntos algebraicos son ceros de una cantidad finita de polinomios, y $V(E) = V((f_1, \ldots, f_m)) = \bigcap_{i=1}^m V(f_i)$, es decir, todo conjunto algebraico se puede poner como intersección de hipersuperficies.

Definición 76. Un espacio topológico es **noetheriano** si sus cerrados cumplen la condición de cadena descendente, es decir, toda cadena de cerrados descendente $C_1 \supseteq C_2 \supseteq C_3 \supseteq \ldots$ es estacionaria.

Proposición 72. *El espacio $\mathbb{A}_k^n$ con la topología de Zariski es noetheriano.*

Demostración. Sea $V(E_1) \supseteq V(E_2) \supseteq \ldots$ una cadena de cerrados. Entonces $I(V(E_1)) \subseteq I(V(E_2)) \subseteq \ldots$ es una cadena ascendente de ideales en $k[x_1, \ldots, x_n]$ así que es estacionaria. Por tanto, la cadena $V(I(V(E_1))) \supseteq V(I(V(E_2))) \supseteq \ldots$ es estacionaria, pero esta es la cadena de partida. □

Proposición 73. *Todo conjunto algebraico afín no vacío $X = V(E)$ tiene una expresión única $X = X_1 \ldots X_r$ con cada X_j irreducible y $X_i \subsetneq X_j$ con $i \neq j$. Se denominan **componentes irreducibles de** X.*

Demostración. Mostramos que existe la descomposición: si X no es irreducible, puede separarse en dos cerrados $X = X_1 \cup X_2$. Ahora se continúa el proceso con cada uno de estos, y no puede durar indefinidamente (es decir, en algún momento se encuentran factores irreducibles) o, de lo contrario, $\mathbb{A}_k^n$ no sería noetheriano. □

Los siguientes resultados arrojan luz sobre la correspondencia entre I y V en el caso de cuerpos algebraicamente cerrados.

Teorema 19 (Ceros de Hilbert / Nullstellensatz)**.** *Sea k un cuerpo algebraicamente cerrado y $\mathfrak{a} \subset k[x_1, \ldots, x_n]$ un ideal. Entonces $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.*

Proposición 74. *Si k es algebraicamente cerrado, I y V establecen una correspondencia biunívoca entre ideales radicales de $k[x_1, \ldots, x_n]$ y conjuntos algebraicos (es decir, cerrados) de $\mathbb{A}_k^n$. Además, las variedades se corresponden con ideales primos y los puntos con ideales maximales.*

Demostración. Si $\mathfrak{a}$ es un ideal radical, $V(\mathfrak{a})$ es algebraico. Si $V(E) = V(\mathfrak{a})$ es un conjunto algebraico, entonces $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$, que es un ideal radical. Para ver que es biyectiva, si $\mathfrak{a}$ es radical entonces $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a}) = \mathfrak{a}$. Por otro lado, si $V(E)$ es cerrado entonces $V(I(V(E))) = V(E)$. □

Definición 77. Sean $W_1 \subset \mathbb{A}_k^n$, $W_2 \subset \mathbb{A}_k^m$ dos conjuntos algebraicos. Se dice que $f : W_1 \to W_2$ es **polinómica** si $f(p) = (F_1(p), \ldots, F_m(p))$ para todo $p \in W_1$, siendo cada $F_j \in k[x_1, \ldots, x_m]$.

Proposición 75. *Si $f : \mathbb{A}_k^n \to \mathbb{A}_k^m$ es polinómica, entonces es continua y, por tanto, la imagen de un conjunto irreducible es irreducible.*

Demostración. Sea $Z \subset A_k^m$ un cerrado. Entonces podemos poner $Z = Z(f_1, \ldots, f_l)$. Pero entonces $f^{-1}(Z) = Z(f_1 \circ f, \ldots, f_k \circ f)$, luego es cerrado. La segunda parte es inmediata sabiendo que f es continua (es análoga a la demostración de que la imagen de un conexo es conexo). □

Al igual que en el caso de conjuntos conexos, la preimagen no satisface esa propiedad. Por ejemplo, si $f(x, y) = xy$ es una aplicación polinómica entre $\mathbb{A}_k^2$ y $\mathbb{A}_k^1$, se tiene que $f^{-1}(0) = \{x = 0\} \cup \{y = 0\}$.

Definición 78. Sea Z un conjunto afín de $\mathbb{A}_k^n$. El anillo $A(Z) = k[x_1, \ldots, x_n]/I(Z)$ se denomina **anillo de coordenadas afín**. Si Z es variedad, es un dominio entero.

6. Dependencia entera

Definición 79. Sean $A \subset B$ anillos. Se dice que $b \in B$ es **algebraico** sobre A si $\exists p(X) \in A[X]$ con $p(b) = 0$ y **trascendente** en caso contrario. Si, además, el p puede tomarse mónico (con coeficiente principal 1) entonces se dice que b es **entero** sobre A.

Si todo $b \in B$ es entero sobre A, se dice que la extensión B es **entera** sobre A.

Proposición 76. *Sean $A \subset B$ anillos. Son equivalentes:*

1. *$x \in B$ es entero sobre A.*
2. *El A-módulo $A[x]$ es finitamente generado.*
3. *El A-módulo $A[x]$ está contenido en un subanillo $C \subset B$ tal que C es finitamente generado como A-módulo.*
4. *Existe un $A[x]$-módulo M fiel, finitamente generado como A-módulo.*

Demostración. Para $1 \implies 2$, supongamos que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Entonces, para todo $r \geq 0$, se tiene $x^{n+r} = a_{n-1}x^{n-1+r} + \cdots + a_0 x^r$. Por inducción en r, sigue que toda potencia de x puede ponerse como A-combinación lineal de $\{1, \ldots, x^{n-1}\}$, de donde $A[x] = \langle 1, \ldots, x^{n-1} \rangle_A$. Para $2 \implies 3$ basta con tomar $C = A[x]$. Para $3 \implies 4$ basta con tomar $M = C$. Este es fiel porque $1 \in C$ al ser subanillo, de modo que $yC = 0 \implies y \cdot 1 = 0 \implies y = 0$. Finalmente, para $4 \implies 1$ es consecuencia de la Proposición 30 con φ la multiplicación por x ($xM \subset M$ porque M es $A[x]$-módulo). □

Como corolarios:

Observación 28. Si $x_1, \ldots, x_n$ son elementos de B enteros sobre A, entonces $A[x_1, \ldots, x_n]$ es finitamente generado como A-módulo. Esto sigue sencillamente de aplicar inducción.

Además, el conjunto C de elementos de B enteros sobre A forma un subanillo, porque, por ejemplo, si $x, y \in C$ entonces $A[x, y]$ es finitamente generado, luego, como $A[x + y] \subset A[x, y]$, se tiene que $x + y \in C$. Este C se denomina **clausura entera de A en B**. Si $C = A$, se dice que A es **integramente/enteramente cerrado**.

Definición 80. Un anillo A que es enteramente cerrado sobre su cuerpo de fracciones se denomina simplemente **enteramente cerrado** o **normal**. La clausura entera de un anillo sobre su cuerpo de fracciones también se denomina **normalización**.

Proposición 77. *Si $A \subset B \subset C$ son extensiones con B entera sobre A y C entera sobre B, se tiene que C es entera sobre A.*

Demostración. Sea $x \in C$. Escribimos $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. Sabemos que $B' = A[b_1, \ldots, b_n] \subset B$ es finitamente generado como A-módulo por ser B entera sobre A. Además $B'[x]$ es finitamente generado como B'-módulo, porque x es entero sobre B'. Entonces $B'[x]$ es finitamente generado como A módulo, de donde x es entero sobre A. □

Como corolario: la clausura entera es íntegramente cerrada, dado que si $A \subset B$ y C es la clausura entera de A en B, entonces cualquier entero de B sobre C, por transitividad (C es entera sobre A) será entero sobre A, luego está en C.

Proposición 78. *Sea $A \subset B$ una extensión entera de anillos. Sea $\mathfrak{b} \subset B$ un ideal. Consideramos $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b} \cap A$ el ideal contraído por la inclusión. En este caso la aplicación $A \to B/\mathfrak{b}$ tiene como núcleo precisamente $\mathfrak{a}$, luego se tiene la inclusión $A/\mathfrak{a} \to B/\mathfrak{b}$. Esta extensión es entera.*

Asimismo, si S es multiplicativamente cerrado de A (y por tanto de B), sigue que la inclusión $S^{-1}A \to S^{-1}B$ (recordemos que localizar es exacto) es entera.

Demostración. La primera parte sigue de que si $x \in B$, sabemos que $p(x) = 0$ para cierto $p \in A[X]$. Ahora, tomando clases módulo $\mathfrak{b}$, sigue que, $\bar{p}(\bar{x}) = 0$. La segunda parte sigue de tomar $\frac{x}{s} \in S^{-1}B$. Ahora, si se tiene que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, entonces, localizando y multiplicando por $\frac{1}{s^n}$ sigue que $(\frac{x}{s})^n + (\frac{a_{n-1}}{s})(\frac{x}{s})^{n-1} + \cdots + \frac{a_1}{s^{n-1}}\frac{x}{s} + \frac{a_0}{s^n} = 0$. □

Proposición 79. *Sean $A \subset B$ dominios de integridad, con B entero en A. Entonces A es cuerpo $\iff$ B es cuerpo.*

Demostración. Si A es un cuerpo y $x \in B$ es no nulo con $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ de grado mínimo, ha de ser que $a_0 \neq 0$ dado que, de otro modo, al ser dominios, se podría cancelar x y reducir el grado. Entonces, el elemento $-a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in B$ invierte a x.

Por otro lado, si B es un cuerpo y $x \in B$ es no nulo, como $y := x^{-1} \in B$, puede ponerse $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$. Pero entonces, puede multiplicarse por x^{n-1} a ambos lados, obteniendo $y = -(a_{n-1} + a_{n-2}x + \cdots + a_0 x^{n-1}) \in A$. □

Como corolario:

Observación 29. Si $A \subset B$ es entera y $\mathfrak{q} \subset B$ es primo, y denotamos $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$ a su contracción (que también es prima), se tiene que $\mathfrak{q}$ es maximal $\iff$ $\mathfrak{p}$ es maximal.

Para verlo, basta con pasar al cociente, que también es una extensión entera, y usar el resultado previo.

Teorema 20. *Sea $A \subset B$ una extensión entera y $\mathfrak{p} \subset A$ un primo. Entonces, existe un primo $\mathfrak{q} \subset B$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$. Por tanto, además, si $\mathfrak{a} \subset B$ es un ideal tal que $\mathfrak{a} \cap A \subset \mathfrak{p} = \mathfrak{q} \cap A$, entonces $\mathfrak{a} \subset \mathfrak{q}$.*

Definición 81. Sean A, B anillos locales con maximales $\mathfrak{m}_A$ y $\mathfrak{m}_B$ respectivamente. Un **homomorfismo local** $f : A \to B$ es un homomorfismo de anillos tal que $f(\mathfrak{m}_A) \subset \mathfrak{m}_B$.

Teorema 21 (Ascenso)**.** *Sea $A \subset B$ una extensión entera y $\mathfrak{p}_1 \subset \dots \mathfrak{p}_n$ una cadena de primos en A. Si se tiene una cadena parcial $\mathfrak{q}_1 \subset \dots \mathfrak{q}_m$, $m \leq n$ tal que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, entonces puede completarse a una cadena $\mathfrak{q}_m \subset \dots \mathfrak{q}_n$ que mantiene la propiedad $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.*

Teorema 22 (Descenso)**.** *El mismo resultado que el teorema del ascenso se cumple para cadenas descendentes si, además, A, B son dominios enteros y A es íntegramente cerrado (sobre su cuerpo de fracciones).*

Proposición 80. *Se tiene que A es integramente cerrado $\iff$ $A_\mathfrak{p}$ es integramente cerrado en todo primo $\mathfrak{p}$ $\iff$ $A_\mathfrak{m}$ es integramente cerrado en todo maximal $\mathfrak{m}$.*