Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

Anillos henselianos y morfismos étale

Autor: Juan Mardomingo Sanz
Tutor: Santiago Encinas Carrión
Curso 2023-2024

Resumen

Los anillos henselianos son anillos locales tales que cada álgebra finita sobre ellos es a su vez producto de anillos locales. Quedan caracterizados también por el lema de Hensel y son bastante importantes en Geometría Algebraica. Además, están íntimamente ligados a las álgebras étale, cuyas propiedades se estudiarán también. El trabajo concluye con una versión «afín» del conocido teorema principal de Zariski demostrada por Christian Peskine en 1966. De este resultado se deduce un teorema de estructura local para las álgebras étale: localmente todas tienen la misma forma, que se denomina estándar étale.

Palabras clave

Anillos henselianos, morfismos étale, álgebras quasifinitas, teorema principal de Zariski.

Abstract

Henselian rings are local rings such that every finite algebra over them is product of local rings itself. These rings are also characterised by Hensel's lemma and are quite relevant in Algebraic Geometry. Moreover, they are closely linked to the so-called étale algebras, whose propreties will be studied here as well. The text concludes with the proof of an 'affine' version of the well-known Zariski's main theorem proposed by Christian Peskine in 1966. From this result it follows a local structure theorem for étale algebras: locally they all show a very specific form, which is called standard étale.

Keywords

Henselian rings, étale morphisms, quasi-finite algebras, Zariski's main theorem.

Introducción

El objetivo de este trabajo es el estudio de dos objetos, los anillos henselianos y los morfismos étale, y la demostración de la versión del *teorema principal de Zariski* propuesta por Christian Peskine en 1966 ([7]). Para ello, nuestra referencia fundamental ha sido el libro de Michel Raynaud ([9]), que recoge estos tres temas en sus primeros capítulos.

Los *anillos henselianos* son anillos locales $(A, \mathfrak{m})$ tales que toda álgebra finita B sobre ellos es a su vez producto de anillos locales, esto es, *descomponible*. Su nombre proviene del resultado conocido como *lema de Hensel*, que sirve también para caracterizarlos: si K es el cuerpo residual de $(A, \mathfrak{m})$, y para un polinomio mónico $P \in A[X]$ se tiene una descomposición de su clase $\overline{P} \in K[X]$ en factores primos entre sí, entonces dicha descomposición «puede levantarse» (corresponde) a una de P en $A[X]$. Veremos además que, aunque el álgebra $B/\mathfrak{m}B$ es siempre isomorfa al producto de sus localizaciones en sus ideales maximales, dicha descomposición se levanta a una de B si y solo si A es henseliano. Después de estas caracterizaciones, se introducen los primeros ejemplos de anillos henselianos (cuerpos, anillos de espectro unipuntual, completados ádicos de anillos locales Hausdorff...) y se incluye una sección sobre sistemas inductivos donde se prueba que el límite inductivo de anillos locales y henselianos conserva estas dos propiedades.

Otra de las caracterizaciones presentadas al inicio relaciona la descomponibilidad de una álgebra con sus idempotentes: se prueba que B es descomponible si y solo si cada idempotente del cociente $B/\mathfrak{m}B$ puede levantarse a uno de B. Este resultado se vuelve a tratar en la última sección del primer capítulo, y se intenta reformular en términos de levantamientos de morfismos de álgebras, introduciendo así la noción de *álgebra étale*.

Si A es un anillo, B es una A-álgebra étale si es de presentación finita y además para cualquier otra A-álgebra C y J un ideal de C de cuadrado nulo, cada morfismo de A-álgebras $\bar{u} : B \longrightarrow C/J$ corresponde a un único morfismo $u : B \longrightarrow C$, es decir, solo existe una flecha u que hace el diagrama siguiente conmutativo

$$\begin{tikzcd} C \arrow[r] & C/J \\ & B. \arrow[ul, "u?"] \arrow[u, "\bar{u}"'] \end{tikzcd}$$

Esta familia de álgebras responde a la pregunta natural de cuándo se puede factorizar a través de $C \longrightarrow C/J$ un morfismo, y cuándo dicha factorización es única. Si solo se puede garantizar la unicidad, hablaremos de *álgebras no-ramificadas*, o *formalmente no ramificadas* si no se piden tampoco propiedades de finitud. En el segundo capítulo estudiamos cómo se comportan estas propiedades a través de morfismos, extensiones de escalares, localizaciones; y se introducirán algunos ejemplos entre los que destacarán las llamadas *álgebras estándar étale*: un cierto tipo de localizaciones de cocientes de $A[X]$ por un polinomio que revelarán su interés al final de esta memoria.

El tercer capítulo comienza introduciendo una noción un poco más débil que la finitud para álgebras, la *quasifinitud*, que nos permitirá enunciar el resultado principal del texto: *el teorema principal de Zariski*. La versión que presentamos (Peskine, 1966), llamada a veces versión «afín» por enunciarse en términos estrictamente algebraicos sin utilizar el lenguaje de la Geometría Algebraica, prueba a grandes rasgos que toda álgebra quasifinita es localmente isomorfa a una entera. De este resultado se deduce un teorema de estructura local para las álgebras étale (que enunciamos sin demostración por falta de tiempo): las álgebras étale son localmente isomorfas a álgebras estándar étale, y de ahí el interés de estas últimas.

La memoria acaba con un cuarto capítulo que contiene los conceptos y resultados de Álgebra Conmutativa que se utilizan en el resto del texto. El estudiante no ha cursado una asignatura de esta rama en la carrera y los conocimientos que presupone Raynaud en su libro han tenido que adquirirse de manera autónoma. Aunque figure como anexo para no perder el hilo del texto principal, consideramos que es parte fundamental del trabajo, pues ha sido el resultado de muchos meses de estudio, y habría sido imposible entender los conceptos y demostraciones del resto del TFG si antes no se hubiera ahondado en estos. En la sección de *Ideales* se introducen algunas correspondencias con ideales y los conceptos de nilradical y radical de Jacobson; en la de *Módulos* se definen las álgebras y las sucesiones exactas de módulos y se hace especial hincapié en las diferentes nociones de finitud que se tratarán constantemente en el texto. Después se presenta el concepto de *Localización* para anillos y módulos, seguido de nuevas *Condiciones de finitud* para módulos: los módulos noetherianos y artinianos y la longitud (nociones equivalentes en el caso de espacios vectoriales). Definimos y construimos también el *Producto tensorial* de módulos, y nos interesamos especialmente por sus propiedades de exactitud en la sección de *Platitud* y por la noción de *Extensión de escalares* de un módulo. La sección de *Dependencia entera* generaliza las extensiones algebraicas de cuerpos vistas en el Grado y en la de *Levantamiento de ideales primos* se introducirán más correspondencias entre ideales a través de morfismos de anillos. Se introduce la noción de *Límite inductivo* en el caso de módulos, y la de *Límite proyectivo* para la *Topología* $\mathfrak{a}$-*ádica*, que son los dos casos concretos que aparecerán en el trabajo, y se termina con una sección sobre la *Topología de Zariski* en el espectro.

Para la elaboración de este anexo se han consultado varios manuales de Álgebra Conmutativa, especialmente el de Bosch ([2]), el de Atiyah-Macdonald ([1]) y el Stacks Project ([10]), aunque como Raynaud refiere siempre a los textos de Bourbaki ([4] y [3]), se incluyen también varios resultados extraídos de estos.

Para terminar, quiero dejar constancia aquí de mi inmenso agradecimiento a Santiago por su dedicación, su paciencia y su tiempo. Sin su guía me habría sido imposible escribir esta memoria.

Índice general

Notación

Salvo que indique lo contrario, en todo este trabajo se supondrá que los anillos son conmutativos y con unidad. Los ideales primos y maximales serán ideales estrictos de los anillos correspondientes. Si A es un anillo, $A^\times$ denotará las unidades del anillo y A^* los elementos no nulos del mismo. Dado un anillo A y un cociente $A/\mathfrak{a}$ del mismo, diremos que un elemento $a \in A$ *levanta* a un elemento $\bar{z} \in A/\mathfrak{a}$ (o que a en *un levantamiento* de $\bar{z}$) si $a + \mathfrak{a} = \bar{z}$, es decir, si a es una preimagen de $\bar{z}$ por la aplicación de paso al cociente. Por extensión, diremos que un subconjunto $B \subseteq A$ levanta a un subconjunto $C \subseteq A/\mathfrak{a}$ si $B + \mathfrak{a} = C$.

Capítulo 1

Anillos locales henselianos

1.1. Descomposición de una álgebra finita en producto de anillos locales

En esta sección, el par $(A, \mathfrak{m})$ denotará un anillo local A de ideal maximal $\mathfrak{m}$. Su cuerpo de residuos $A/\mathfrak{m}$ se denotará por K y B será una A-álgebra finita de morfismo estructural $\varphi : A \longrightarrow B$. Su radical de Jacobson y su nilradical se denotarán por $\mathcal{J}(B)$ y $\mathcal{N}(B)$ respectivamente. Además, $\bar{B} = B/\mathfrak{m}B$, donde $\mathfrak{m}B$ es el ideal de B engendrado por $\varphi(\mathfrak{m})$. Diremos que un anillo es *descomponible* si es producto de anillos locales.

Observación 1.1.1. En las condiciones anteriores, $\mathfrak{m}B \subseteq \mathcal{J}(B)$ (esto es, todos los ideales maximales de B contienen al ideal $\mathfrak{m}B$). Basta notar que, por ser B finita sobre A, si $\mathfrak{n}$ es un ideal maximal de B, su imagen inversa por el morfismo estructural $\varphi : A \longrightarrow B$ debe ser un ideal maximal de A en virtud de la proposición 4.7.6. Como A es local, $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$ y se tiene la cadena de contenciones

$$\varphi(\mathfrak{m})B = \varphi(\varphi^{-1}(\mathfrak{n}))B \subseteq \mathfrak{n},$$

de donde se deduce el resultado, pues $\varphi(\mathfrak{m})B$ es otra notación para $\mathfrak{m}B$.

El siguiente lema nos muestra, utilizando el *teorema de estructura de anillos artinianos*, que $\bar{B}$ es semilocal y de hecho descomponible. Además, por la biyección entre los ideales maximales de $\bar{B}$ y los de B que contienen a $\mathfrak{m}B$ se deducirá también que B es semilocal aunque no necesariamente descomponible, de ahí el interés de los *anillos henselianos*, que definimos después.

Lema 1.1.2. *Sea $(A, \mathfrak{m})$ un anillo local de cuerpo residual K y B una A-álgebra finita de familia de ideales maximales $(\mathfrak{n}_i)_{i\in I}$. Entonces I es finito y B es semilocal. Además, la aplicación canónica de descomposición*

$$\bar{B} \longrightarrow \prod_{i\in I} \bar{B}_{\bar{\mathfrak{n}}_i} \tag{1.1.2.1}$$

es un isomorfismo. En particular, $\bar{B}$ es descomponible.

Demostración. El morfismo estructural de B como A-álgebra (finita) induce en $\bar{B}$ una estructura de álgebra finita sobre $K = A/\mathfrak{m}$. Por tanto $\bar{B}$ es un anillo de Artin en virtud de la proposición 4.4.15. Usando ahora el teorema de estructura (4.4.10), $\bar{B}$ es isomorfa al producto de sus localizaciones en sus ideales maximales, que son una cantidad finita. Como la biyección entre los ideales del anillo cociente $B/\mathfrak{m}B$ y los del anillo B que contienen a $\mathfrak{m}B$ preserva las contenciones, esta biyección también se da entre ideales maximales del cociente y maximales de B que contienen a $\mathfrak{m}B$. Sin embargo, en la observación anterior (1.1.1) hemos visto que $\mathfrak{m}B$ está contenido en todos los ideales maximales de B, luego los maximales del cociente son justamente las imágenes de los maximales de B, esto es, de la forma $\bar{\mathfrak{n}}_i = \mathfrak{n}_i + \mathfrak{m}B$. Por tanto, los ideales maximales de B son también una cantidad finita (B es semilocal).

$\square$

Definición 1.1.3. **[Anillo henseliano]** Un anillo local $(A, \mathfrak{m})$ se llama *henseliano* o *de Hensel* si toda A-álgebra finita B es *descomponible.*

Proposición 1.1.4. *Sean $(A, \mathfrak{m})$ un anillo henseliano y B una A-álgebra finita. Entonces B es un anillo semilocal cuyos ideales maximales son los ideales primos de B por encima de $\mathfrak{m}$.*

Demostración. Invocando en primer lugar el lema 1.1.2, sabemos que el álgebra B es semilocal simplemente por ser A un anillo local. Vamos ahora a utilizar la proposición 4.7.6 de la sección sobre levantamiento de ideales primos, y el lema 4.6.7 de la sección sobre enteros. El morfismo entre A y B que se considerará para aplicar dichos resultados no es otro que el estructural de B como A-álgebra.

Gracias al lema 4.6.7, sabemos que B es entera sobre A por ser una A-álgebra finita. Así que podemos aplicar la proposición 4.7.6 y concluir que los ideales maximales de B son justamente los ideales primos de B por encima de ideales maximales de A. Ahora bien, el único ideal maximal de A es $\mathfrak{m}$ por hipótesis, de modo que los ideales maximales de B serán sus ideales primos por encima de $\mathfrak{m}$.

$\square$

Hemos visto al inicio del capítulo (lema 1.1.2) que el álgebra $\bar{B}$ es producto de sus localizados en sus ideales maximales. El álgebra finita B, pese a ser semilocal también y ser sus ideales maximales levantamientos de los de $\bar{B}$, no es necesariamente descomponible. La siguiente proposición nos muestra que, cuando sí lo es, dicha descomposición es de hecho un levantamiento de la de $\bar{B}$. Necesitaremos también este lema previo.

Lema 1.1.5. *Sea $(A, \mathfrak{m})$ un anillo local y B una A-álgebra finita y descomponible. Sea $B \simeq \prod_{j \in J} B_j$ una descomposición de B en producto de los anillos locales $(B_j, \mathfrak{n}_j)$. Entonces $B_j \simeq B_{\mathfrak{n}_j}$ para todo $j \in J$.*

Demostración. Para cada $j \in J$, $(B_j)_{\mathfrak{m}_j} \simeq B_j$ pues $S = B_j \setminus \mathfrak{m}_j$ solo contiene unidades de B_j (ver el cuarto apartado del lema 4.3.7), así que basta probar que $B_{\mathfrak{n}_j} \simeq (B_j)_{\mathfrak{m}_j}$. Recordemos que

$$B_{\mathfrak{n}_j} = \{b/a \ : \ b = (b_j)_{j \in J} \in \prod_{j \in J} B_j \ , \ a = (a_j)_{j \in J} \in B \setminus \mathfrak{n}_j = (B_j \setminus \mathfrak{m}_j) \times \prod_{i \neq j; i \in J} B_i\} / \sim,$$

donde $\sim$ hace referencia a la relación de equivalencia siguiente:

$$b/a \sim c/d \ \Leftrightarrow \ \exists t \in B \setminus \mathfrak{n}_j \ : \ t(bd - ac) = 0 \Leftrightarrow b_j \text{ y } c_j \text{ son asociados}.$$

Veamos esta última equivalencia: como $S = B \setminus \mathfrak{n}_j = (B_j \setminus \mathfrak{m}_j) \times \prod_{i \neq j; i \in J} B_i$, podemos coger t con todas las componentes nulas salvo la j-ésima de modo que $t(bd - ac) = 0$ para cierto $t \in B \setminus \mathfrak{n}_j$ equivale a que $u(b_j d_j - a_j c_j) = 0$ para cierto $u \in B_j \setminus \mathfrak{m}_j = B_j^{\times}$. Como a_j y d_j son también unidades de B_j, concluimos que $b/a \sim c/d$ si y solo si $b_j = v c_j$ para $v \in B_j^{\times}$, esto es, b_j y c_j son asociados.

Definimos pues la aplicación $B_{\mathfrak{n}_j} \longrightarrow (B_j)_{\mathfrak{m}_j}$; $b/a \longmapsto b_j/a_j$, que está bien definida por el comentario anterior, es evidentemente sobreyectiva y también inyectiva: si $b_j/a_j = 0$ entonces $b_j = 0$, de modo que $b/a \sim 0$, o lo que es lo mismo, $b/a = 0$ en $B_{\mathfrak{n}_j}$.

$\square$

Proposición 1.1.6. *Dado* $(A, \mathfrak{m})$ *un anillo local y* B *una* A*-álgebra finita, las condiciones siguientes son equivalentes:*

1. B *es descomponible.*

2. B *es semilocal de ideales maximales* $(\mathfrak{n}_i)_{i \in I}$ *y el morfismo canónico* $B \longrightarrow \prod_{i \in I} B_{\mathfrak{n}_i}$ *es un isomorfismo.*

3. *La descomposición de* $\bar{B}$ *dada por 1.1.2.1 se levanta a una descomposición de* B*.*

Demostración. Para probar (1) $\implies$ (2) consideremos $B = \prod_{j \in J} B_j$, una descomposición de B en producto de anillos locales. Para cada $j \in J$, sea $\mathfrak{m}_j$ el ideal maximal de B_j. Entonces los ideales $\mathfrak{n}_j = \mathfrak{m}_j \times \prod_{i \in J,\, j \neq i} B_i$ para $j \in J$ son maximales. De la proposición 1.1.4 sabemos que B es semilocal por ser descomponible, de modo que J debe ser finito. Además, todos los ideales maximales de B son producto de ideales maximales de los B_j (o de los propios B_j, ver observación 4.1.5), de modo que los anteriores son de hecho todos los ideales maximales de B. Finalmente, como $B_j \simeq B_{\mathfrak{n}_j}$ para todo $j \in J$ (ver lema 1.1.5) se deduce el isomorfismo.

Las otras implicaciones son rápidas de probar: del isomorfismo $B \simeq \prod_{i \in I} B_{\mathfrak{n}_i}$ se deduce, tomando cocientes por el ideal $\mathfrak{m}B$, el de la ecuación (1.1.2.1) y así se tiene (2) $\implies$ (3); por otro lado, (3) $\implies$ (1) es clara porque (3) nos da una descomposición de B en producto de anillos locales por ser los ideales $\mathfrak{n}_i$ maximales.

□

Recordamos ahora que los *idempotentes* de un anillo cualquiera R son los elementos $e \in R$ tales que $e^2 = e$. Denotaremos dicho conjunto por $idemp(R)$. Antes de presentar un resultado que relaciona la «descomponibilidad» de un álgebra finita con sus idempotentes, los siguientes lemas nos muestran que los anillos locales no tienen idempotentes no triviales y el papel que estos juegan en la caracterización de los anillos producto.

Lema 1.1.7. *Un anillo* A *(unitario) es isomorfo a un producto de anillos* $A_1 \times A_2$ *si y solo si* A *presenta idempotentes no triviales (i.e. distintos de* $0, 1$*).*

Demostración. Si $e \in A$ es un idempotente distinto de 1, entonces $(1-e)^2 = 1 + e^2 - 2e = 1 - e$ también es un idempotente no trivial. Consideramos ahora los subanillos eA y $(1-e)A$ de A, dados por los productos ea y $(1-e)a$ respectivamente, donde a es un elemento de A. Entonces el homomorfismo de anillos siguiente es biyectivo

$$\psi : eA \times (1-e)A \longrightarrow A \; ; \; (x, y) \longmapsto x + y.$$

Basta notar que para cualquier $a \in A$ se tiene $\psi(ea, (1-e)a) = a$, luego el morfismo es sobreyectivo; y

$$\psi(ea, (1-e)b) = ea + (1-e)b = 0 \Leftrightarrow ea = (e-1)b \Leftrightarrow ea = e(ea) = e(e-1)b = (ee-e)b = 0,$$

pues e es idempotente. De ahí se tiene que $(e-1)b = 0$ también, y se concluye que la aplicación es inyectiva.

Recíprocamente, si $A \simeq A_1 \times A_2$, entonces $(1, 0)$ es un ejemplo de idempotente no trivial en A.

□

Lema 1.1.8. *Dado un anillo local* $(A, \mathfrak{m})$*, sus únicos idempotentes son el* 1 *y el* 0*. Por tanto, un anillo local no puede ser isomorfo a ningún producto de anillos no triviales.*

Demostración. Dado $e \in idemp(A)$, se tiene que $e^2 = e$ o lo que es lo mismo, $e(1-e) = 0$. Se dan dos posibilidades: si $e \in \mathfrak{m}$ entonces $(1-e) \in A^\times$ y $e = 0$; si $e \in A \setminus \mathfrak{m}$ entonces $e \in A^\times$ luego $1 - e = 0 (\Leftrightarrow e = 1)$.

□

Proposición 1.1.9. *Sea $(A, \mathfrak{m})$ un anillo local y B una A-álgebra finita. La aplicación*

$$idemp(B) \longrightarrow idemp(\bar{B}),$$

deducida del epimorfismo canónico $B \longrightarrow \bar{B}$, es inyectiva. Además, es biyectiva si y solamente si B es descomponible.

Demostración. En primer lugar, si $e \in idemp(B)$, entonces $e + \mathfrak{m}B \in idemp(\bar{B})$, de modo que la aplicación está bien definida. Veamos ahora que es inyectiva. Sean $e, e' \in idemp(B)$ tales que $e + \mathfrak{m}B = e' + \mathfrak{m}B$ (i.e. $x = e - e' \in \mathfrak{m}B$), probemos que $x = 0$. Calculemos x^3 teniendo en cuenta que e y e' son idempotentes:

$$x^3 = e^3 - (e')^3 - 3e^2e' + 3e(e')^2 = e - e' - 3ee' + 3ee' = x.$$

Por tanto, $x - x^3 = x(1 - x^2) = 0$. Como $x \in \mathfrak{m}B$ y $\mathfrak{m}B$ pertenece al radical de Jacobson de B, por el lema 4.1.7 se tiene que $1 - x^2$ es una unidad de B, así que $x = 0$ como queríamos.

Como ya tenemos la inyectividad asegurada, nos falta ver que la aplicación es sobreyectiva si y solo si B es descomponible.

Supongamos que B es descomponible, esto es, $B \simeq \prod_{i \in I} B_{\mathfrak{n}_i}$ y tomemos $e \in idemp(B)$. Como los anillos $B_{\mathfrak{n}_i}$ son locales, sus idempotentes son triviales según el lema 1.1.8, de modo que $e = (e_i)_{i \in I}$ con $e_i \in \{0, 1\}$ para cada $i \in I$. Y como $\bar{B} \simeq \prod_{i \in I} \bar{B}_{\bar{\mathfrak{n}}_i}$, sus idempotentes son de la misma forma. Así que la aplicación es suprayectiva puesto que la descomposición anterior se levanta a la descomposición de B indicada.

Pongamos ahora que la aplicación es una biyección y veamos que la descomposición $\bar{B} \simeq \prod_{i \in I} \bar{B}_{\bar{\mathfrak{n}}_i}$ se levanta en una descomposición en anillos locales de B. Para cada $i \in I$, tomamos el elemento $\bar{e}_i \in idemp(\bar{B})$ que tiene todas las componentes nulas salvo un 1 en la i-ésima. Por hipótesis, existe un idempotente $e_i \in idemp(B)$ que lo levanta, y por la biyección entre ambos conjuntos, e_i es también un idempotente no trivial de B. Así que e_iB es factor directo de B para cada $i \in I$ invocando el lema 1.1.7. La unicidad de ideales maximales en e_iB se deduce pasando al cociente, pues $\bar{e}_i\bar{B} \simeq \bar{B}_{\bar{\mathfrak{n}}_i}$, luego los anillos e_iB son locales y por tanto B es descomponible (de hecho, $e_iB \simeq B_{\mathfrak{n}_i}$ para cada i).

□

La última proposición de este capítulo nos da aún nuevas caracterizaciones de los anillos henselianos. Veremos que basta limitarse a estudiar que las A-álgebras del tipo $A[X]/(P)$ sean descomponibles (con $P \in A[X]$ mónico) y que ser henseliano equivale a una de las versiones del *lema de Hensel* (de ahí el nombre de estos anillos). En nuestra versión, un polinomio mónico con coeficientes en nuestro anillo local A verifica que de cada descomposición suya en producto de primos en el cuerpo residual K se puede obtener una descomposición en A levantando la primera.

Antes de presentar la proposición, introducimos dos lemas que se usarán en su demostración. Para el primero, aunque se supone en la hipótesis que el anillo A es local por estar trabajando en ese contexto, el resultado es válido con la condición de que el ideal maximal $\mathfrak{m}$ esté contenido en el radical de Jacobson de A.

Lema 1.1.10. *Sea $(A,\mathfrak{m})$ un anillo local de cuerpo residual K. Sea C una A-álgebra finita, tal que $\bar{C} = C/\mathfrak{m}C$ sea isomorfa a $K[X]/(\bar{Q})$, donde $\bar{Q}$ es un polinomio mónico de grado n. Sea $\bar{X}$ la clase de X en $\bar{C}$ y x un levantamiento de $\bar{X}$ en C (esto es, $x + \mathfrak{m}C = \bar{X}$). Entonces x engendra el A-álgebra C y es raíz de un polinomio mónico Q de $A[X]$ (de grado n) cuya clase en $K[X]$ es $\bar{Q}$.*

Demostración. Sea I el sub-A-módulo de C engendrado por $1, x, \ldots, x^{n-1}$. Como $\bar{C} \simeq K[X]/(\bar{Q})$, y el segundo miembro está engendrado por las potencias de $\bar{X}$ hasta grado $n-1$, se deduce que $\bar{C}$ debe estar engendrado por las de $x + \mathfrak{m}C$. Por tanto, $I + \mathfrak{m}C = C$, y como C es un A-módulo de tipo finito y $\mathfrak{m} = \mathcal{J}(A)$ por ser A local, del corolario 4.2.17 del lema de Nakayama se concluye que $I = C$, de modo que las potencias $1, x, x^2, \ldots, x^{n-1}$ engendran la A-álgebra C.

Por lo anterior, podemos escribir $x^n = a_{n-1}x^{n-1} + \cdots + a_0$ para ciertos coeficientes $a_i \in A$. Así, x es raíz del polinomio de grado n mónico $Q(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_0 \in A[X]$. Por tanto, su reducción en $K[X]$ es múltiplo de $\bar{Q}$, y como ambos son polinomios mónicos de grado n, coinciden. □

Lema 1.1.11. *Sea $(A,\mathfrak{m})$ un anillo local de cuerpo residual K. Sea $U(X) \in A[X]$ un polinomio mónico e irreducible y sea $P(X) = U(X)^s$ para un cierto $s \in \mathbb{N}$. En estas condiciones:*

1. *El anillo $K[X]/(P)$ solo admite un ideal primo, que es la imagen del ideal (U) de $K[X]$. En particular, es un anillo local.*
2. *El anillo $A[X]/(P)$ es local.*

Demostración. Comenzamos probando el primer punto, que se usará después en la demostración del segundo. Sea pues $\bar{J}$ un ideal primo de $K[X]/(P)$. Como los ideales primos de $K[X]/(P)$ están en biyección con los primos de $K[X]$ que contienen a (P) (ver observación 4.1.4) se deduce que existe un ideal primo $J \subseteq K[X]$ con $(P) \subseteq J$ y tal que $J + (P) = \bar{J}$. Al ser K un cuerpo, el anillo $K[X]$ es en particular un dominio de ideales principales, de manera que existe $T \in K[X]$ mónico con $J = (T) \supseteq (P) = (U^s)$. Así, $U^s \in (T)$, y como (T) es primo se tiene que $U \in (T)$, esto es, T divide a U. Pero U es irreducible y mónico, de modo que, o bien T es una unidad o bien $T = U$. Como lo primero no tiene sentido si $J = (T)$ es primo, deducimos que $J = (U)$. Acabamos de probar que el único ideal primo de $K[X]$ que contiene a P es este, y por tanto $\bar{J}$ es también el único ideal primo de $K[X]/(P)$.

Veamos ahora que el anillo $B \coloneqq A[X]/(P)$ es local. Como es una A-álgebra finita, en virtud de la observación 1.1.1 y del lema 1.1.2 sabemos que es semilocal y que sus ideales maximales contienen a $\mathfrak{m}B$. Además, estos ideales maximales están de hecho en biyección con los maximales de $B/\mathfrak{m}B$ y usando las proposiciones 4.5.14 y 4.5.31 se tienen los isomorfismos de A-álgebras siguientes:

$$B/\mathfrak{m}B \simeq B \otimes_A A/\mathfrak{m} = \frac{A[X]}{(P)} \otimes_A A/\mathfrak{m} \simeq \frac{A/\mathfrak{m}[X]}{(\overline{P})}.$$

Como $A/\mathfrak{m} = K$, el punto anterior nos garantiza que este anillo solo tiene un ideal maximal. Por la cadena de isomorfismos anteriores deducimos que el propio B tiene también un único ideal maximal, así que es local como queríamos. □

Proposición 1.1.12. *Dado $(A,\mathfrak{m})$ un anillo local de cuerpo de residuos K, las condiciones siguientes son equivalentes:*

1. *El anillo local A es henseliano.*
2. *Toda A-álgebra finita y libre es descomponible.*

3. Para todo polinomio mónico $P \in A[X]$, el álgebra $A[X]/(P)$ es descomponible.

*4. **[Lema de Hensel]** Sea $P \in A[X]$ un polinomio mónico cuya imagen $\bar{P}$ en $K[X]$ puede descomponerse como $\bar{P} = \bar{Q}\bar{R}$, donde $\bar{Q}$ y $\bar{R}$ son dos polinomios mónicos de $K[X]$, primos entre sí. Entonces P es de la forma $P = QR$, donde Q y R son polinomios mónicos de $A[X]$ que son además levantamientos de $\bar{Q}$ y $\bar{R}$ respectivamente.*

Demostración.
La implicación (1) $\implies$ (2) está clara por definición de anillo henseliano. Como el álgebra $A[X]/(P)$ es finita y libre (de dimensión dada por el grado de P), se deduce que (2) $\implies$ (3).

(3) $\implies$ (4) Denotemos $B = A[X]/(P)$ y $\bar{B} = K[X]/(\bar{P})$. Como $\bar{Q}$ y $\bar{R}$ son primos entre sí, del teorema chino de los restos se deduce el isomorfismo

$$\bar{B} = K[X]/(\bar{P}) \simeq K[X]/(\bar{Q}) \times K[X]/(\bar{R}).$$

Como B es descomponible por hipótesis, sabemos de la proposición 1.1.6, que la descomposición anterior de $\bar{B}$ debe levantarse a una de B. Esto es, existen dos A-álgebras B_1 y B_2, levantamientos de $K[X]/(\bar{P})$ y $K[X]/(\bar{Q})$ respectivamente, tales que $B \simeq B_1 \times B_2$. Como B es una A-álgebra finita, en particular lo son B_1 y B_2, luego podemos aplicarles a cada una el lema 1.1.10. Por lo tanto, existen $x_1 \in B_1$ y $x_2 \in B_2$ levantamientos de las clases de X en $K[X]/(\bar{P})$ y $K[X]/(\bar{Q})$ respectivamente. Y existen polinomios mónicos Q y R de $A[X]$, levantamientos de $\bar{Q}$ y $\bar{R}$ y tales que x_1 es raíz de Q y x_2 lo es de R. Sea x el elemento de $A[X]/(P)$ correspondiente a (x_1, x_2) por la biyección $B \simeq B_1 \times B_2$. Entonces x es raíz de QR en B y, por tanto, QR es múltiplo de P. Pero como ambos son mónicos del mismo grado, entonces deben coincidir.

(4) $\implies$ (3) Sea $P \in A[X]$ un polinomio mónico. Veamos que el álgebra $A[X]/(P)$ es descomponible. Tomemos la clase $\bar{P}$ de P en $K[X]$ y sea $\bar{P} = \prod_{i\in I} \bar{P}_i$ la descomposición de $\bar{P}$ en potencias de irreducibles mónicos primos entre sí. Aplicando (4) por recurrencia, esta descomposición puede levantarse a una de P, del tipo

$$P = \prod_{i\in I} P_i,$$

donde cada factor P_i es mónico y su clase en $K[X]$ es $\bar{P}_i$, pero en general no son primos entre sí. Podemos tomar ahora el morfismo canónico

$$u : A[X]/(P) \longrightarrow \prod_{i\in I} A[X]/(P_i).$$

Como los $\bar{P}_i$ son primos entre sí, podemos aplicar el teorema chino de los restos al morfismo $\bar{u}$ siguiente

$$\bar{u} : K[X]/(\bar{P}) \longrightarrow \prod_{i\in I} K[X]/(\bar{P}_i),$$

que es por tanto un isomorfismo. En particular, es sobreyectivo, de manera que se puede aplicar la versión del lema de Nakayama dada en 4.2.18, tomando como ideal $\mathfrak{m} = \mathcal{J}(A)$ y como A-módulo finitamente generado $\prod_{i\in I} A[X]/(P_i)$. Se tiene pues que u es sobreyectiva también. Ahora bien, como $P = \prod_{i\in I} P_i$, entonces $deg(P) = \sum_{i\in I} deg(P_i)$, de modo que $A[X]/(P)$ y $\prod_{i\in I} A[X]/(P_i)$ son dos A-álgebras libres y finitas del mismo rango como A-módulos ($deg(P)$). Así que el morfismo, que es sobreyectivo, debe ser de hecho biyectivo. Ahora bien, como los polinomios P_i son potencia de irreducibles mónicos, los anillos $A[X]/(P_i)$ son locales en virtud del lema 1.1.11. Así que $A[X]/(P)$ es isomorfo a un producto de anillos locales, esto es, descomponible.

(3) $\implies$ (1) Sea B una A-álgebra finita. Por la proposición 1.1.9, B es descomponible si y solo si la aplicación $idemp(B) \longrightarrow idemp(\bar{B})$ es sobreyectiva, así que solo necesitamos ver que cualquier

idempotente de $\bar{B}$ puede levantarse a uno de B.

Sabemos que $\bar{B} \simeq \prod_{i \in I} \bar{B}_{\bar{\mathfrak{n}}_i}$, donde los $\bar{\mathfrak{n}}_i$ son los maximales de $\bar{B}$, que sabemos también (ver lema 1.1.2) que son las clases módulo $\mathfrak{m}B$ de los ideales maximales $\mathfrak{n}_i$ de B. Por tanto, cuando hablemos del idempotente $\bar{e}_i$ de $\bar{B}$ relativo a $\mathfrak{n}_i$ nos referiremos al relativo a $\bar{\mathfrak{n}}_i$, esto es, el que vale 0 en todas las componentes $\bar{B}_{\bar{\mathfrak{n}}_j}$ con $j \neq i$ y 1 en la restante. Como todos los idempotentes de $\bar{B}$ son de esta forma, basta mostrar que $\bar{e}_i$ se levanta a un idempotente de B.

Fijemos un $i \in I$ cualquiera y sea b un levantamiento de $\bar{e}_i$. Como B es una A-álgebra finita, en virtud del lema 4.6.7, B es entera sobre A, de modo que existe $P \in A[X]$ mónico tal que $P(b) = 0$. Consideremos ahora el A-morfismo $u : A[X]/(P) \longrightarrow B$ que envía la clase de X, $X + (P)$, al elemento $b \in B$, y el resto de elementos a los correspondientes para que sea homomorfismo. Así está bien definido porque recordemos que para definir un morfismo de A-módulos φ entre $A[X]$ y un A-módulo B basta definir la imagen de X y prolongar. Para pasar al cociente solo hace falta remarcar que en este caso $(P) \subseteq Ker(\varphi)$ pues P se anula en $b = \varphi(X)$.

Sea ahora $p \coloneqq u^{-1}(\mathfrak{n}_i)$, que es un ideal primo de $A[X]/(P)$ por ser imagen inversa de un ideal primo. No es necesariamente maximal, pero debe estar contenido en uno de los de $A[X]/(P)$. Esta álgebra es además descomponible por hipótesis. Sea $\{\mathfrak{s}_t\}_{t \in T}$ su familia (finita) de ideales maximales. Sabemos que se tiene el isomorfismo

$$A[X]/(P) \simeq \prod_{t \in T} (A[X]/(P))_{\mathfrak{s}_t},$$

luego podemos considerar el idempotente e relativo al ideal maximal $\mathfrak{s}_i$ que contiene a p. Por tanto, su imagen por u, $u(e)$ es un idempotente de B, y resulta que $u(e) + \mathfrak{m}B = \bar{e}_i$. Así que $\bar{e}_i$ se levanta a un idempotente de B, como queríamos.

$\square$

1.2. Ejemplos de anillos henselianos

Introducimos ahora los primeros ejemplos de anillos henselianos usando las caracterizaciones demostradas en la sección anterior.

Lema 1.2.1. *Cualquier cuerpo L es un anillo local henseliano.*

Demostración. Ya sabemos que los cuerpos son anillos locales pues su único maximal es el ideal $\{0\}$. Además, una L-álgebra finita es artiniana, y por tanto descomponible. Así que L es efectivamente henseliano.

$\square$

Lema 1.2.2. *Dado un anillo henseliano A, cualquier álgebra finita sobre él B es a su vez un anillo henseliano. En particular los cocientes no nulos de un anillo henseliano lo son.*

Demostración. Sea C una álgebra finita sobre B, por transitividad de la finitud (4.2.7), C es a su vez finita sobre A, luego descomponible. Si I es un ideal estricto de A, A/I es una A-álgebra finita (tiene por generador $1 + I$).

$\square$

Recordemos que un ideal I de un anillo A se llama *nilideal* si está contenido en el nilradical de A (ver definición 4.1.12). En particular se tiene el lema siguiente, cuya demostración se ha extraído de [8].

Lema 1.2.3. *Sea A un anillo e I un nilideal de A. Entonces la aplicación*

$$idemp(A) \longrightarrow idemp(A/I)$$

es una biyección.

Demostración. Veamos inyectividad y sobreyectividad por separado:

1. *Inyectividad.* Sean $e_1, e_2 \in idemp(A)$ tales que $e_1 + I = e_2 + I$. Entonces $x = e_1 - e_2 \in I \subseteq \mathcal{N}(A)$. Por tanto, x es nilpotente, luego existe $n \in \mathbb{N}$ tal que $x^m = 0$ para todo $m \geq n$. Sea $m \geq n$ impar, entonces se tiene

   $$0 = x^m = (e_1 - e_2)^m = \sum_{i=0}^{m} \binom{m}{i} (e_1)^i (-e_2)^{m-i} = e_1^m - m e_1^{m-1} e_2 + \cdots + m e_1 e_2^{m-1} + e_2^m = e_1 - e_2.$$

   Donde se ha usado que, al ser m impar, los coeficientes binomiales aparecen «por parejas», y todos los sumandos, salvo el primero y el último, se cancelan usando la idempotencia de e_1 y e_2.

2. *Sobreyectividad.* Sea $e + I \in idemp(A/I)$ cualquiera y sea $f := 1 - e$ para e un representante de $e + I$. Entonces

   $$ef + I = e(1 - e) + I = e - e^2 + I = 0 + I,$$

   pues $e + I$ es idempotente. Así que $ef \in I$ y, por tanto, existe un $n \in \mathbb{N}$ tal que $e^n f^n = 0$ (pues I es un nilideal de A). Tomamos ahora $x := 1 - e^n - f^n$. Usando de nuevo la idempotencia de $e + I$ se tiene que

   $$f^n + I = \sum_{i=0}^{n} \binom{n}{i} (-e)^i + I = 1 + e \sum_{i=1}^{n} \binom{n}{i} (-1)^i + I = 1 - e((1-1)^n - 1) + I = 1 - e + I = f + I.$$

Por tanto, $x + I = 1 - e - (1-e) + I = 0 + I$, así que $x \in I$, luego es nilpotente. Usando ahora el lema 4.1.11 deducimos que $1 + x$ es una unidad de A. Si definimos $u := (1-x)^{-1}$, se tiene

$$ue^n + uf^n = u(e^n + f^n) = u(1-x) = 1.$$

Como $e^n f^n = 0$, multiplicando ahora ambos miembros por ue^n tenemos

$$(ue^n)^2 = ue^n,$$

luego $ue^n \in idemp(A)$. Acabamos de ver que $u(1-x) = 1$, y como $x \in I$, $u + I = 1 + I$, de donde

$$ue^n + I = 1e^n + I = e + I.$$

Así que ue^n es un levantamiento de $e + I$.

□

De la observación 1.1.1, sabemos que, en el contexto en el que estamos trabajando en este capítulo, $\mathfrak{m}B \subseteq \mathcal{J}(B)$. En general, $\mathcal{N}(B) \subsetneq \mathcal{J}(B)$, luego $\mathfrak{m}B \nsubseteq \mathcal{N}(B)$ en principio y no se puede aplicar el lema anterior. En el ejemplo siguiente veremos un caso en el que sí puede utilizarse.

Proposición 1.2.4. *Un anillo local A es henseliano si y solo si su reducido $A_{red} = A/\mathcal{N}(A)$ es henseliano. En particular, si A solo tiene un ideal primo, entonces es henseliano.*

Demostración.
$\Longrightarrow$ Sea B' una álgebra finita sobre A_{red}, veamos que es descomponible. Notemos que A_{red} es una A-álgebra finita por ser cociente de A. Así, por transitividad de la finitud (proposición 4.2.7), B' debe ser finita sobre A, y por tanto descomponible.

$\Longleftarrow$ Supongamos ahora que A_{red} es henseliano y sea B una A-álgebra finita. En virtud de la proposición 1.1.9 basta ver que $idemp(B) \simeq idemp(\bar{B})$. Usaremos la notación $\mathcal{N}(A)$ para el nilradical de A y $\mathcal{N}(A)B$ será el ideal de B engendrado por las imágenes de los elementos de $\mathcal{N}(A)$ a través del morfismo estructural de B como A-álgebra. Por las propiedades de los morfismos de anillos, está claro que la imagen del nilradical de A a través del morfismo estructural estará contenido en el nilradical de B. Como este es un ideal, también el ideal engendrado por dicha imagen $\mathcal{N}(A)$ estará contenido en él, es decir, $\mathcal{N}(A)B \subseteq \mathcal{N}(B)$ (así que $\mathcal{N}(A)B$ es un nilideal de B).

Poniendo $B' = B/\mathcal{N}(A)B$, B' es una álgebra finita sobre A_{red}, por tanto descomponible. Aplicando de nuevo la proposición 1.1.9, $idemp(B') \simeq idemp(\bar{B}')$, donde $\bar{B}' = B'/\mathfrak{m}B = \bar{B}/\mathcal{N}(A)B$. Como $\mathcal{N}(A)B$ es un nilideal de B, aplicando el lema 1.2.3 se tiene el isomorfismo $idemp(B) \simeq idemp(B')$. Tomando la clase correspondiente, $\mathcal{N}(A)B$ es también un nilideal de $\bar{B}$ y podemos aplicar el mismo lema para obtener $idemp(\bar{B}') = idemp(\bar{B}/\mathcal{N}(A)B) \simeq idemp(\bar{B})$. El diagrama siguiente muestra todos los isomorfismos anteriores, que inducen el isomorfismo buscado entre $idemp(B)$ e $idemp(\bar{B})$.

$$\begin{tikzcd}
idemp(B) \arrow[r, "\sim"] \arrow[d] & idemp(B') \arrow[d, "\sim"] \\
idemp(\bar{B}) \arrow[r, "\sim"] & idemp(\bar{B}')
\end{tikzcd}$$

Este mismo argumento se podría haber utilizado para probar la otra implicación, ya que en ese caso se tiene isomorfismo a la izquierda del diagrama anterior en lugar de a la derecha y se razona idénticamente.

□

Corolario 1.2.5. *Si A es un anillo con un único ideal primo no trivial (distinto de 0), entonces es henseliano.*

Demostración. Si A solo tiene un ideal primo, entonces este debe ser también el único maximal, $\mathfrak{m}$. Por tanto A es un anillo local y $\mathcal{N}(A) = \mathfrak{m}$. Así, $A_{red} = A/\mathfrak{m}$, esto es, el cuerpo residual de A (que es un cuerpo por ser $\mathfrak{m} \neq 0$). Por el lema 1.2.1, A_{red} es henseliano, y por la proposición anterior (1.2.4), A debe serlo también.

□

Corolario 1.2.6. *Sea $(A, \mathfrak{m})$ un anillo local y sea $n \in \mathbb{N}$ cualquiera. Entonces el anillo $A/\mathfrak{m}^n$ es henseliano.*

Demostración. Vamos a ver que para cada $n \in \mathbb{N}$, el anillo $A/\mathfrak{m}^n$ solo tiene un ideal primo, que es de hecho la clase módulo $\mathfrak{m}^n$ de $\mathfrak{m}$. Por tanto, usando el corolario 1.2.5, $A/\mathfrak{m}^n$ debe ser henseliano. Por la observación 4.1.4, sabemos que los ideales primos de $A/\mathfrak{m}^n$ están en biyección con los primos de A que contienen a $\mathfrak{m}^n$. Sea pues $\mathfrak{q}$ un ideal primo de A con $\mathfrak{m}^n \subseteq \mathfrak{q}$. En particular, debe estar contenido en un ideal maximal de A, que tiene que ser forzosamente $\mathfrak{m}$ por ser A local. Veamos que dicha contención es de hecho una igualdad. Sea $m \in \mathfrak{m}$ cualquiera. Entonces $m^n \in \mathfrak{m}^n \subseteq \mathfrak{q}$, pero como $\mathfrak{q}$ es primo, $m \in \mathfrak{q}$. Por tanto el único ideal primo de A que contiene a $\mathfrak{m}^n$ es $\mathfrak{m}$, así que $A/\mathfrak{m}^n$ tiene un único ideal primo.

□

Proposición 1.2.7. *Un anillo noetheriano local $(A, \mathfrak{m})$ Hausdorff y completo para la topología $\mathfrak{m}$-ádica es henseliano. En particular, dado un anillo noetheriano local cualquiera $(A, \mathfrak{m})$ tal que $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$, su completado $\mathfrak{m}$-ádico $\hat{A} = \varprojlim A/\mathfrak{m}^n$ es henseliano.*

Demostración. Dada B una A-álgebra finita, queremos ver que es descomponible. Sabemos ya que, por ser finita, es semilocal (ver lema 1.1.2), así que denotamos por $\mathfrak{n}_i$ con $i = 1, \dots, r \leq \infty$ a sus ideales maximales. Vamos a dotar a B de la topología $\mathfrak{m}B$-ádica. Como el anillo A es Hausdorff para la topología $\mathfrak{m}$-ádica entonces $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$. Por tanto, $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n B = (\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n)B = 0$, así que B es Hausdorff también. Además, como A es completo también se tiene la completitud de B usando la proposición 4.9.12, de modo que $B = \varprojlim B/\mathfrak{m}^n B$.

Para cada $n \in \mathbb{N}$, $A/\mathfrak{m}^n$ es henseliano por el corolario 1.2.6. Por tanto, $B/\mathfrak{m}^n$, que es una álgebra finita sobre $A/\mathfrak{m}^n$ por serlo B sobre A, es descomponible. Teniendo en cuenta la biyección entre ideales maximales del cociente $\mathfrak{m}^n B$ e ideales maximales de B que contienen a $\mathfrak{m}^n B$, y que para todo n se tiene que $\mathfrak{m}^n B \subseteq \mathfrak{m}B \subseteq \mathcal{J}(B)$, entonces los ideales maximales de $B/\mathfrak{m}^n B$ son justamente las clases de los maximales de B, esto es, $\mathfrak{n}_i/\mathfrak{m}^n B$ para $i = 1, \dots, r$.

Utilizando ahora la proposición 1.1.9, como $B/\mathfrak{m}^n B$ es descomponible, debe ser isomorfo al producto de sus localizados en sus ideales maximales, esto es,

$$B/\mathfrak{m}^n B \simeq \prod_{i=1}^{r} (B/\mathfrak{m}^n B)_{\mathfrak{n}_i/\mathfrak{m}^n B} = \prod_{i=1}^{r} (B_{\mathfrak{n}_i}/\mathfrak{m}^n B_{\mathfrak{n}_i}),$$

donde se ha usado la conmutatividad de localizaciones y cocientes (4.3.21).
Finalmente, tomando límites proyectivos en la igualdad anterior, y teniendo en cuenta la completitud de B para la topología $\mathfrak{m}B$-ádica, la compatibilidad del límite proyectivo con el producto cartesiano y las localizaciones (4.9.11) se tiene el isomorfismo deseado.

$$B = \varprojlim B/\mathfrak{m}^n B = \prod_{i=1}^{r} \varprojlim (B/\mathfrak{m}^n B)_{\mathfrak{n}_i/\mathfrak{m}^n B} = \prod_{i=1}^{r} (\varprojlim (B/\mathfrak{m}^n B)_{\mathfrak{n}_i}) = \prod_{i=1}^{r} B_{\mathfrak{n}_i}.$$

□

Acabamos esta sección viendo el primer ejemplo de anillo local que no es henseliano.

Ejemplo 1.2.8. Sea $p \in \mathbb{Z}$ un primo. Tomemos como anillo A el localizado de $\mathbb{Z}$ en el ideal primo (p), esto es

$$\mathbb{Z}_{(p)} = \{m/n \ : \ m \in \mathbb{Z}, \ n \notin (p)\}.$$

El polinomio $X(X-1) + p \in A[X]$ puede factorizarse módulo $(p)\mathbb{Z}_{(p)}$ en producto de dos polinomios primos entre sí (las clases módulo p de X y $X-1$). Sin embargo, levantamientos de estas clases no dan lugar a una descomposición del polinomio original en $A[X]$. Por tanto, en virtud de la proposición 1.1.12, el anillo local A no es henseliano.

1.3. Propiedad de paso al límite inductivo

Nuestro objetivo aquí será probar que el límite inductivo de anillos locales sigue siendo local y si son henselianos preserva también dicha propiedad. Como consecuencia de este hecho veremos que los anillos henselianos pueden definirse también como aquellos tales que toda álgebra entera sobre ellos es descomponible, aunque parezca que esta propiedad es más fuerte (pues una álgebra finita es siempre entera, 4.6.7, pero el recíproco no es cierto en general).

Proposición 1.3.1. *Sean I un conjunto dirigido y $((A_i)_{i\in I}, \varphi_{ij})$ un sistema inductivo de anillos locales (con ideales maximales respectivos $\mathfrak{m}_i$) donde los morfismos de transición φ_{ij} son locales también (ver definición 4.3.3). Denotemos por A su límite inductivo,*

$$A := \varinjlim A_i,$$

sea $\varphi : \oplus_{i\in I} A_i \longrightarrow A$ el epimorfismo canónico y sean $\varphi_i : A_i \longrightarrow A$ sus restricciones a cada A_i. Entonces se tienen las propiedades siguientes:

1. *El límite inductivo A es local y para cada $i \in I$ los morfismos $\varphi_i : A_i \longrightarrow A$ son locales.*
2. *Si para todos los $i \in I$, los anillos A_i son henselianos, el límite A es henseliano.*

Demostración.

1. Veamos que el subconjunto de A dado por $\mathfrak{m} := \cup_{i\leq j}\varphi_j(\varphi_{ij}(\mathfrak{m}_i)) = \cup_{i\in I}\varphi_i(\mathfrak{m}_i)$ es un ideal del mismo:

   - $\mathfrak{m} \neq \emptyset$ ya que el 0 pertenece al conjunto.
   - Sean $x, y \in \mathfrak{m}$. Entonces existen índices $i, j \in I$, y elementos $m_i \in \mathfrak{m}_i$, $m_j \in \mathfrak{m}_j$ tales que $\varphi_i(m_i) = x$ y $\varphi_j(m_j) = y$. Como I es dirigido, existe un índice k mayor que i y j, y por la compatibilidad de los morfismos dada en 4.8.3, se tiene que $\varphi_i = \varphi_k \circ \varphi_{ik}$, y lo mismo para j. Además, como hemos supuesto que los morfismos de transición del sistema inductivo son locales, se tiene que $\varphi_{ik}(\mathfrak{m}_i) \subseteq \mathfrak{m}_k$ y $\varphi_{jk}(\mathfrak{m}_j) \subseteq \mathfrak{m}_k$. Uniendo esto a la compatibilidad anterior, concluimos que existen elementos $m_{ki}, m_{kj} \in \mathfrak{m}_k$ tales que

     $$\varphi_k(m_{ki}) = x,\ \varphi_k(m_{kj}) = y \implies x + y = \varphi_k(m_{ki} + m_{kj}).$$

     Como $\mathfrak{m}_k$ es estable para la suma de sus elementos concluimos que $x + y$ pertenece a su imagen por φ_k y por tanto a $\mathfrak{m}$.
   - Sean $a \in A$, $x \in \mathfrak{m}$. En virtud de la observación 4.8.4, existen $j \in I$ y $x_j \in A_j$ tales que $a = \varphi_j(x_j)$. Por definición de $\mathfrak{m}$, existen $i \in I$ y $m_i \in \mathfrak{m}_i$ tales que $\varphi_i(m_i) = x$. Razonamos ahora como antes: al ser I dirigido existe un $k \geq i, j$, y por la compatibilidad con los morfismos de transición se tiene que $a \in \varphi_k(A_k)$ y $x \in \varphi_k(\mathfrak{m}_k)$. Como $\mathfrak{m}_k$ es un ideal de A_k, se concluye que $ax \in \varphi_k(\mathfrak{m}_k) \subseteq \mathfrak{m}$.

   Ahora que sabemos que $\mathfrak{m}$ es un ideal, queremos aplicar la proposición 4.3.4 para ver que A es local y $\mathfrak{m}$ es su maximal. Usando dicho resultado basta ver que cualquier $x \in A \setminus \mathfrak{m}$ es una unidad. De nuevo por la observación 4.8.4 sabemos que existen $i \in I$ y $x_i \in A_i$ tales que $\varphi_i(x_i) = x$. Está claro que $x \notin \mathfrak{m}_i$, pues en caso contrario pertenecería a $\mathfrak{m}$ por definición. Así que x_i es un elemento invertible de A_i (usando que los $(A_i, \mathfrak{m}_i)$ son locales y de nuevo la caracterización 4.3.4), y en consecuencia x es invertible en A. Para acabar, notemos que por definición de $\mathfrak{m}$, este contiene todos los $\varphi_i(\mathfrak{m}_i)$, así que los morfismos φ_i son todos locales.

2. Si todos los anillos A_i son henselianos, veamos que su límite inductivo lo es también. Sea pues $P \in A[X]$ un polinomio mónico. Usando una vez más la observación 4.8.4, sabemos que cada coeficiente del polinomio es imagen de un elemento de un anillo A_i a través de φ_i. Usando recursivamente que el conjunto I es dirigido, se puede encontrar un índice común $i_0 \in I$ tal que todos los coeficientes del polinomio provengan de A_{i_0}. Así pues, P proviene de un $P_{i_0} \in A_{i_0}[X]$ mónico. Escojamos $i \geq i_0$ cualquiera y sean P_i la imagen (por $\varphi_{i_0 i}$) de P_{i_0} en $A_i[X]$ y $B_i := A_i[X]/(P_i)$. Usando la propiedad de extensión de escalares en anillos de polinomios (4.5.31 se tienen los isomofismos de A_{i_0}-álgebras siguientes:

$$B_i = A_i[X]/(P_i) \simeq B_{i_0} \otimes_{A_{i_0}} A_i = \frac{A_{i_0}[X]}{(P_{i_0})} \otimes_{A_{i_0}} A_i.$$

Si denotamos por B al límite inductivo de los anillos B_i, usando de nuevo la propiedad anterior y la conmutatividad del límite inductivo con el producto tensorial (4.8.10),

$$B = \varinjlim B_i \simeq B_{i_0} \otimes_{A_{i_0}} \varinjlim A_i = B_{i_0} \otimes_{A_{i_0}} A = \frac{A_{i_0}[X]}{(P_{i_0})} \otimes_{A_{i_0}} A \simeq \frac{A[X]}{(P)}.$$

Sea $\overline{P}_i$ la clase de P_i en $K_i[X]$, donde K_i denota el cuerpo residual de $(A_i, \mathfrak{m}_i)$. Para cada $i \geq i_0$ se tiene la sucesión exacta canónica de A_{i_0}-módulos

$$0 \longrightarrow \mathfrak{m}_i \longrightarrow A_i \longrightarrow A_i/\mathfrak{m}_i,$$

de modo que, usando la exactitud del límite inductivo (4.8.11), se deduce la sucesión exacta

$$0 \longrightarrow \mathfrak{m} = \varinjlim \mathfrak{m}_i \longrightarrow A = \varinjlim A_i \longrightarrow \varinjlim K_i,$$

de donde se tiene el isomorfismo de A_{i_0}-módulos $K = A/\mathfrak{m} \simeq \varinjlim K_i$. Es fácil comprobar que se trata también de un isomorfismo de álgebras (ver observación 4.8.12), y por tanto una descomposición de $\bar{P}$ en factores irreducibles en $K[X]$ proviene de una descomposición de $\bar{P}_i \in K_i[X]$ para i suficientemente grande. Como los A_i son henselianos, se verifica el lema de Hensel (1.1.12), pero esto implica que también se verifica para una descomposición de $\bar{P}$ en $K[X]$, así que A es también henseliano.

□

Como anunciamos al principio de la sección, podemos probar ahora que en un anillo henseliano todas las álgebras enteras sobre él son descomponibles también.

Proposición 1.3.2. *Sean $(A, \mathfrak{m})$ un anillo local henseliano y B una A-álgebra entera. Entonces se verifican las dos propiedades siguientes:*

1. *La aplicación idemp$(B) \longrightarrow$ idemp$(\overline{B})$ es biyectiva. Por tanto B es descomponible.*

2. *Para todo ideal maximal η de B, la localización B_η es entera sobre A y henseliana. En particular B es también henseliano.*

Demostración.

1. Usando la proposición 4.8.13, sabemos que B es límite inductivo de sus sub-A-álgebras finitas, en particular, si $(B_i)_{i\in I}$ son dichas subálgebras,

$$B = \varinjlim B_i = \bigcup_{i \in I} B_i.$$

Usando la proposición 4.5.31 y la conmutatividad del límite inductivo y el producto tensorial (4.8.10), se deduce la cadena de igualdades siguiente:

$$\overline{B} = B/\mathfrak{m}B = B \otimes_A A/\mathfrak{m} = (\varinjlim B_i) \otimes_A A/\mathfrak{m} = \varinjlim (B_i \otimes_A A/\mathfrak{m}) = \varinjlim \overline{B}_i.$$

Vamos a ver ahora que

$$idemp(B) = \varinjlim (idemp(B_i)).$$

En este caso el límite inductivo es de *conjuntos* y no de módulos como hemos introducido en la sección correspondiente del anexo. Para un tratamiento exhaustivo del límite inductivo en distintas categorías puede consultarse [2], pero solo necesitamos usar que en el caso de subconjuntos de un conjunto, su límite inductivo cuando están ordenados por la inclusión (como es el caso de los $idemp(B_i)$) es también su unión. Así pues la igualdad deseada se reduce a probar que $idemp(B)$ está en biyección con $\cup_{i\in I} idemp(B_i)$: las imágenes de idempotentes de B_i a través de los morfismos $\varphi_i : B_i \longrightarrow B$ son también idempotentes de B y, recíprocamente, dado un idempotente de B, existe un índice $i_0 \in I$ suficientemente grande para que provenga del correspondiente B_{i_0} por ser $B = \bigcup_{i\in I} B_i$.

En resumen, obtenemos las dos igualdades siguientes:

$$idemp(B) = \varinjlim (idemp(B_i)) \qquad idemp(\overline{B}) = \varinjlim (idemp(\overline{B}_i)).$$

Además, como A es henseliano y las B_i son A-álgebras finitas, estas son descomponibles, así que la proposición 1.1.9 nos garantiza que $idemp(B_i)$ está en biyección con $idemp(\overline{B}_i)$ para cada $i \in I$. Así que los límites inductivos de arriba deben coincidir y, por lo tanto, $idemp(B)$ está en biyección con $idemp(\overline{B})$, como queríamos demostrar. Invocando ahora la proposición 1.1.9 sabemos que B es descomponible.

2. Mantengamos las notaciones del apartado anterior. Sabemos por la proposición 4.3.22 que las sub-A-álgebras finitas de B_η son las localizaciones en dicho ideal de las subálgebras finitas de B, y por tanto

$$B_\eta = \varinjlim (B_i)_\eta = \bigcup_{i\in I} (B_i)_\eta.$$

Dado ahora un elemento $b \in B_\eta$ cualquiera, existirá $k \in I$ tal que $b \in (B_k)_\eta$, y como esta última es una A-álgebra finita, en particular es entera (4.6.7), de modo que b es entero sobre A y B_η también.

Como η es un ideal primo, la localización B_η es un anillo local (4.3.12) y para ver que es henseliano basta mostrar que todos los $(B_i)_\eta$ son henselianos por la proposición anterior (1.3.1). Sean pues $i \in I$ cualquiera y C_i una álgebra finita sobre $(B_i)_\eta$. Como esta segunda es finita sobre A, por transitividad (4.2.7), C_i también es una A-álgebra finita. Al ser A henseliano, se concluye que C_i es descomponible y por tanto $(B_i)_\eta$ es henseliano también. Finalmente, para ver que B es henseliano también basta replicar esta demostración obviando las localizaciones en cada paso.

□

1.4. Estudio de los idempotentes de una álgebra finita

Dado $(A, \mathfrak{m})$ un anillo local y B una álgebra finita sobre A, hemos visto que B es descomponible si y solo si podemos levantar cualquier idempotente de $\bar{B}$ en uno de B (proposición 1.1.9). En esta sección estudiaremos qué es lo que puede impedir la existencia de dicho levantamiento siguiendo la sección homónima de [9] y [8].

Por ahora, A designará un anillo (por descontado conmutativo y unitario) no necesariamente local, y B será una A-álgebra finita y libre (recordemos que, por la proposición 1.1.12, para que un anillo local sea henseliano, basta estudiar la descomponibilidad de sus álgebras finitas y libres). Sea $\{e_i\}_{i=1}^r$ una base de B como A-módulo. Dados dos índices $i, j \in \{1, \ldots, r\}$ cualesquiera, podemos escribir su producto en la misma base con ciertos coeficientes $\mu(i, j, k) \in A$,

$$e_i e_j = \sum_{k=1}^{r} \mu(i, j, k) e_k.$$

Sea $b = \sum_{i=1}^r a_i e_i$ un elemento de B. Utilizando las notaciones del párrafo anterior para $e_i e_j$ podemos escribir

$$b^2 = \sum_{i,j=1}^{r} a_i a_j e_i e_j = \sum_{i,j=1}^{r} a_i a_j \left(\sum_{k=1}^{r} \mu(i, j, k) e_k \right) = \sum_{k=1}^{r} \left(\sum_{i,j=1}^{r} a_i a_j \mu(i, j, k) \right) e_k.$$

Sabemos que b es idempotente si y solo si $b^2 = b$, y como $\{e_i\}_{i=1}^r$ es una base, esta condición puede traducirse a que se verifiquen las ecuaciones

$$\sum_{i,j=1}^{r} a_i a_j \mu(i, j, k) = a_k,$$

para cada $k = 1, \ldots, r$. Definimos ahora los polinomios $P_k(X_1, \ldots, X_r) \in A[X_1, \ldots, X_r]$ como

$$P_k(X_1, \ldots, X_r) = \sum_{i,j=1}^{r} \mu(i, j, k) X_i X_j - X_k,$$

para $k = 1, \ldots, r$. De esta manera $b = \sum_{i=1}^r a_i e_i \in B$ es idempotente si y solo si la r-upla de coeficientes $(a_1, \ldots, a_r)$ satisface las ecuaciones

$$P_k(a_1, \ldots, a_r) = 0,$$

para todo $k = 1, \ldots, r$. Sea ahora

$$E(B) = E := \frac{A[X_1, \ldots, X_r]}{< P_1, \ldots, P_r >} = A[x_1, \ldots, x_r],$$

donde x_i es la clase de X_i en el cociente. Entonces el razonamiento anterior prueba que los conjuntos siguientes están en biyección

$$Hom_{A-álg}(E, A) \Leftrightarrow idemp(B).$$

Esta última observación es fácil de comprobar puesto que cada morfismo de A-álgebras de E en A queda determinado por las imágenes de los elementos x_i, que serán ciertos $a_i \in A$. Así pues, cada morfismo puede asociarse a una r-upla de elementos de A, y por tanto a un elemento $b = \sum_{i=1}^r a_i e_i$ de B. Pero no un elemento cualquiera, pues los x_i verifican por construcción que $P_k(x_1, \ldots, x_r) = 0$ para todo $k = 1, \ldots, r$, y por ser los polinomios en A y el morfismo de A-álgebras, $P_k(a_1, \ldots, a_r)$

también, y el elemento b anterior es idempotente. Con argumentos similares podemos obtener también una biyección si tomamos las clases módulo $\mathfrak{m}$, un ideal de A:

$$Hom_{A-\acute{a}lg}(E, A/\mathfrak{m}) \Leftrightarrow idemp(B/\mathfrak{m}B).$$

Podemos generalizar este razonamiento para cualquier A-álgebra C y su producto tensorial con B, $B \otimes_A C$. Entonces tenemos que $\{e_1 \otimes 1, \ldots, e_r \otimes 1\}$ es una base de dicho producto tensorial visto como C-módulo. Sea $\beta = \sum_{i=1}^{r} e_i \otimes c_i \in B \otimes_A C$ cualquiera. Entonces

$$\beta^2 = \sum_{i,j=1}^{r} e_i e_j \otimes c_i c_j = \sum_{i,j=1}^{r} \left(\sum_{k=1}^{r} \mu(i,j,k) e_k \right) \otimes c_i c_j = \sum_{k=1}^{r} e_k \otimes \left(\sum_{i,j=1}^{r} \mu(i,j,k) c_i c_j \right).$$

Por tanto, β es idempotente si y solo si sus coeficientes $(c_1, \ldots, c_r)$ verifican las ecuaciones

$$P_k(c_1, \ldots, c_r) = 0,$$

para $k = 1, \ldots, r$. En tal caso la biyección anterior puede de hecho extenderse a

$$Hom_{A-\acute{a}lg}(E, C) \Leftrightarrow idemp(B \otimes_A C), \tag{1.4.0.1}$$

donde cada morfismo ϕ se envía en el elemento $\sum_{i=1}^{r} e_i \otimes \phi(x_i)$. De nuevo los $\phi(x_i)$ son elementos de C tales que los polinomios P_k se anulan en ellos, y por tanto la imagen indicada corresponde a un idempotente del producto tensorial.

En este nuevo marco, el problema de levantar un idempotente de $\overline{B}$ a uno de B se puede reescribir como la siguiente pregunta: ¿puede un homomorfismo de A-álgebras $\bar{u} : E \longrightarrow K = A/\mathfrak{m}$ levantarse en otro homomorfismo de A-álgebras $u : E \longrightarrow A$? ¿Puede encontrarse una «flecha u» que haga conmutativo el diagrama siguiente?

$$\begin{tikzcd} E \arrow[r, dashed, "u?"] \arrow[dr, "\bar{u}"'] & A \arrow[d, "\pi"] \\ & K \end{tikzcd}$$

Volvamos a suponer que $(A, \mathfrak{m})$ es un anillo local y sea $\mathfrak{q} \coloneqq Ker(\bar{u})$. Por ser $E = A[x_1, \ldots, x_n]$ y $\bar{u}$ un morfismo de A-álgebras, los elementos de A se envían a sus clases módulo $\mathfrak{m}$, así que es sobreyectivo. Por el primer teorema de isomorfía, $\bar{u}$ factoriza en un isomorfismo entre $E/\mathfrak{q}$ y $Im(\bar{u}) = K$. Así pues, $E/\mathfrak{q} \simeq K$, y como este es un cuerpo, $\mathfrak{q}$ tiene que ser un ideal maximal de E. Por otro lado, como $Ker(\bar{u}) = \mathfrak{q}$, $\bar{u}(E \setminus \mathfrak{q}) \subseteq K \setminus \{0\} = K^{\times}$. Así que podemos aplicar la propiedad universal de las localizaciones 4.3.13 para garantizar la existencia de un morfismo de A-álgebras $\bar{v} : E_{\mathfrak{q}} \longrightarrow K$ de manera que el diagrama siguiente sea conmutativo:

$$\begin{tikzcd} E \arrow[r, "\bar{u}"] \arrow[d, "\pi_{\mathfrak{q}}"] & K \\ E_{\mathfrak{q}}, \arrow[ur, "\bar{v}"'] & \end{tikzcd}$$

donde $\pi_{\mathfrak{q}}$ es el morfismo canónico de localización en $\mathfrak{q}$.

Una vez tenemos el $\bar{v}$ anterior, nuestro objetivo es ver que la existencia del levantamiento u que buscamos equivale a la existencia de un morfismo de A-álgebras $v : E_{\mathfrak{q}} \longrightarrow A$ que haga conmutativo el diagrama

$$\begin{tikzcd}
E_{\mathfrak{q}} \arrow[r, "v"] \arrow[d, "\bar{v}"] & A \arrow[dl, "\pi"] \\
K &
\end{tikzcd}$$

Para ver la equivalencia será útil observar el diagrama siguiente:

$$\begin{tikzcd}
E \arrow[rr, "\bar{u}"] \arrow[dr, "\pi_{\mathfrak{q}}"] \arrow[drr, bend right, "u?"'] & & K \\
& E_{\mathfrak{q}} \arrow[ur, "\bar{v}"] \arrow[r, "v?"] & A \arrow[u, "\pi"]
\end{tikzcd}$$

En efecto, observamos que, si existe el morfismo v de arriba tal que $\pi \circ v = \bar{v}$, entonces existe el levantamiento u que queremos, definiendo $u \coloneqq v \circ \pi_{\mathfrak{q}}$. Recíprocamente, si existe u tal que $\bar{u} = \pi \circ u$, dicho morfismo puede factorizarse a través de $\pi_{\mathfrak{q}}$ gracias a la propiedad universal de la localización: como $(\pi \circ u)(E \setminus \mathfrak{q}) = \bar{u}(E \setminus \mathfrak{q}) \subseteq K^{\times}$, entonces $u(E \setminus \mathfrak{q}) \subseteq A \setminus \mathfrak{m} = A^{\times}$ (donde para la última igualdad se ha usado la proposición 4.3.4). Y existe por tanto un morfismo de A-álgebras $v : E_{\mathfrak{q}} \longrightarrow A$ tal que $u = v \circ \pi_{\mathfrak{q}}$, que es el que buscamos.

Por tanto, nuestro problema inicial es equivalente a la pregunta siguiente: dado $\bar{v} : E_{\mathfrak{q}} \longrightarrow K$, ¿existe $v : E_{\mathfrak{q}} \longrightarrow A$ tal que $\pi \circ v = \bar{v}$? De manera intuitiva, en [9] Raynaud dice que la «distancia» entre A y $E_{\mathfrak{q}}$ puede interpretarse como una medida de la obstrucción a la existencia de un levantamiento en B de un idempotente $\bar{e} \in \overline{B}$.

Es el momento de estudiar la álgebra E anterior. Ya sabemos por construcción que es una A-álgebra de *presentación finita*, pero además verifica la siguiente propiedad: *para cada A-álgebra C y todo ideal J de C de cuadrado nulo, cualquier morfismo de A-álgebras $\bar{w} : E \longrightarrow C/J$ puede levantarse de manera única a un morfismo de A-álgebras $w : E \longrightarrow C$*. Para probarlo volvamos en primer lugar a la biyección 1.4.0.1 para C y C/J, así podemos reducir nuestro problema a ver que cada idempotente de $idemp(B \otimes_A (C/J))$ puede levantarse a uno de $idemp(B \otimes_A C)$. Recordemos también el lema 1.2.3, que prueba que los idempotentes de un cociente de un anillo por un nilideal están en biyección con los idempotentes del anillo original. Como los elementos de J son de cuadrado nulo, en particular J es un nilideal, así que veamos que $B \otimes_A (C/J)$ es isomorfo como A-álgebra a $(B \otimes_A C)/\mathcal{J}$, donde $\mathcal{J}$ es el ideal del producto tensorial engendrado por elementos $b \otimes j$ (con $b \in B$ y $j \in J$). En efecto, si definimos la aplicación

$$\varphi : B \times C \longrightarrow B \otimes_A (C/J)$$

que envía un par (b, c) en el tensor $b \otimes (c + J)$, es inmediato comprobar que es A-bilineal, así que podemos aplicar la propiedad universal del producto tensorial para garantizar la existencia de un morfismo de A-álgebras

$$\tilde{\varphi} : B \otimes_A C \longrightarrow B \otimes_A (C/J); \quad b \otimes c \longmapsto b \otimes (c + J).$$

Con esta definición, está claro que $\mathcal{J} \subseteq Ker(\tilde{\varphi})$, de modo que se tiene una aplicación inyectiva de $(B \otimes_A C)/\mathcal{J}$ en $B \otimes_A (C/J)$ en virtud del primer teorema de isomorfía. Es inmediato comprobar que la vuelta está bien definida y es un A-homomorfismo y por tanto se tiene el isomorfismo de A-álgebras deseado.

Las álgebras que verifican las dos propiedades de E se denominan *álgebras étale*, y serán estudiadas en el capítulo siguiente. Por razones técnicas, veremos también una noción más débil: las *álgebras no-ramificadas*. Además de este papel crucial en el estudio de los anillos henselianos, estas álgebras aparecen de manera recurrente en Geometría Algebraica, aunque no llegaremos a tratar estas aplicaciones.

Capítulo 2

Álgebras étale y no-ramificadas

Como prometimos al final del capítulo anterior, introducimos ahora las nociones de álgebras *étale* y *no-ramificadas*, junto a una noción áun más débil: las álgebras *formalmente no-ramificadas*, donde se elimina la condición de finitud que pedimos en general a las no-ramificadas. Aunque definimos las nociones para álgebras sobre un anillo A, sabemos por la observación 4.2.3 que hay una correspondencia biunívoca entre estas y los morfismos de anillos con salida de A. Así, por ejemplo, será equivalente decir que el morfismo de anillos $A \longrightarrow B$ es étale a decir que B es una A-álgebra étale.

Definición 2.0.1. [**Álgebra étale**] Dado un anillo A, decimos que una A-álgebra B es *étale* [1] si verifica las dos propiedades siguientes:

1. B es una A-álgebra de presentación finita.
2. Para toda A-álgebra C y para todo ideal J de C de cuadrado nulo ($J^2 = 0$), la aplicación canónica
$$Hom_{A-alg}(B, C) \longrightarrow Hom_{A-alg}(B, C/J)$$
es una biyección.

Definición 2.0.2. [**Álgebra formalmente no-ramificada**] Dado un anillo A, una A-álgebra B se llama *formalmente no-ramificada o formalmente neta* [2] si para toda A-álgebra C y todo ideal J de C de cuadrado nulo ($J^2 = 0$), la aplicación canónica

$$Hom_{A-alg}(B, C) \longrightarrow Hom_{A-alg}(B, C/J)$$

es inyectiva.

Definición 2.0.3. [**Álgebra no-ramificada**] Dado un anillo A, una A-álgebra B se llama *no-ramificada* o *neta* si B es formalmente no-ramificada sobre A y además de tipo finito sobre A.

Observación 2.0.4. Obviando por un momento las condiciones de finitud, comentemos qué quieren decir las definiciones anteriores. Sean A un anillo, B y C álgebras sobre A y J un ideal de C de cuadrado nulo. Podemos considerar siempre los morfismos estructurales de B y C como A-álgebras y el paso al cociente de C a C/J.

[1] Del francés *étaler*, «desplegar, extender».

[2] La denominación preferida actualmente es la inglesa *unramified*, «sin ramificaciones». Decidimos adaptarla al castellano por *no-ramificada*. La palabra *neta* es un calco del francés *nette*, «nítido, claro».

$$\begin{tikzcd} C \arrow[r, "\pi"] & C/J \\ A \arrow[u] \arrow[r] & B \arrow[ul, "u"] \arrow[u, "\bar{u}"'] \end{tikzcd}$$

Dado un morfismo $u \in Hom_{A-alg}(B, C)$, siempre podemos a partir de él definir otro de B a C/J componiendo el primero con el paso al cociente $\pi : C \longrightarrow C/J$, $\bar{u} = \pi \circ u$. Diremos en este caso que *u es un levantamiento de $\bar{u}$*. Sin embargo, no sabemos en principio si existen morfismos de $Hom_{A-alg}(B, C/J)$ que no se obtengan así (es decir, que no puedan factorizarse a través de C) o si uno de ellos puede «levantarse» en diferentes morfismos $B \longrightarrow C$ (hay varias factorizaciones posibles). La idea es que un morfismo de B con llegada en C/J nos «aporta menos información» que uno con llegada en C, pues en el cociente hemos «pegado» elementos distintos de C en la misma clase. Introducimos por eso una familia de álgebras donde esta pérdida de información no es tal: si B es étale, la correspondencia entre morfismos con llegada en C y C/J es biunívoca, y si es no-ramificada un morfismo $B \longrightarrow C/J$ no tiene por qué provenir de otro $B \longrightarrow C$, pero en caso de que sí, dicha factorización es única.

2.1. Propiedades de los morfismos étale y no-ramificados

Comenzamos esta sección con las primeras propiedades de las álgebras étale y no-ramificadas que acabamos de introducir. En particular, veremos que estas propiedades son transitivas, estables por cambio de base, producto tensorial o localizaciones, etc. Para no perder el hilo de las demostraciones, probamos las propiedades relativas a la finitud en lemas previos a la proposición correspondiente.

Lema 2.1.1. *Dado A un anillo, si B una A-álgebra de tipo finito (resp. de presentación finita), y C una B-álgebra de tipo finito (resp. de presentación finita), entonces C es de tipo finito (resp. de presentación finita) como A-álgebra.*

Demostración. Las dos pruebas consisten esencialmente en «construir» el morfismo apropiado de un anillo de polinomios sobre A y con llegada en C, utilizando los morfismos que tenemos por hipótesis.

Tipo finito Sean $\varphi : A[X_1, \ldots, X_n] \longrightarrow B$ y $B[Y_1, \ldots, Y_m] \longrightarrow C$ los epimorfismos que dan a B y C sus estructuras de álgebra de tipo finito. Definimos el morfismo de A-álgebras $\tilde{\varphi} : A[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \longrightarrow B[Y_1, \ldots, Y_m]$ como prolongación de φ dejando fijas las variables Y_j. Este es claramente sobreyectivo por definición, así que el morfismo

$$\rho := \psi \circ \tilde{\varphi} : A[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \longrightarrow C$$

será también sobreyectivo. Por tanto, C es de tipo finito sobre A.

Presentación finita Consideremos los mismos morfismos de la parte anterior, teniendo en cuenta que ahora existen elementos $f_1, \ldots, f_k \in A[X_1, \ldots, X_n]$ y $g_1, \ldots, g_t \in B[Y_1, \ldots, Y_m]$ tales $Ker(\varphi) =< f_1, \ldots, f_k >$ y $Ker(\psi) =< g_1, \ldots, g_t >$. Notemos que $Ker(\tilde{\varphi})$ está también engendrado por los elementos f_i con $i = 1, \ldots, k$ pero como ideal de $A[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Veamos que, definiendo ρ como antes, $Ker(\rho)$ es el ideal de $A[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ engendrado por todos los f_i y por las $\tilde{\varphi}$-preimágenes de los g_j. Por la definición de ρ, es evidente que este ideal generado por dichos elementos está contenido en su núcleo. Dado ahora un elemento η cualquiera del núcleo, se tiene que

$$0=\rho(\eta)=\rho(\sum_{finita} a_{\underline{(\alpha,\beta)}}X_1^{\alpha_1}\cdots X_n^{\alpha_n}Y_1^{\beta_1}\cdots Y_m^{\beta_m})=\psi(\sum_{finita}\varphi(a_{\underline{(\alpha,\beta)}}X_1^{\alpha_1}\cdots X_n^{\alpha_n})Y_1^{\beta_1}\cdots Y_m^{\beta_m})\Longleftrightarrow$$

$$\Longleftrightarrow \sum_{finita}\varphi(a_{\underline{(\alpha,\beta)}}X_1^{\alpha_1}\cdots X_n^{\alpha_n})Y_1^{\beta_1}\cdots Y_m^{\beta_m}\in Ker(\psi) \Longleftrightarrow$$

$$\Longleftrightarrow \quad \forall j=1,\ldots,t \;\; \exists b_j\in B[Y_1,\ldots,Y_m] \;\; : \;\; \sum_{finita}\varphi(a_{\underline{(\alpha,\beta)}}X_1^{\alpha_1}\cdots X_n^{\alpha_n})Y_1^{\beta_1}\cdots Y_m^{\beta_m}=\sum_{j=1}^{t} b_j g_j.$$

Ahora bien, como $\tilde{\varphi}$ es sobreyectiva, existen $\tilde{b}_j,\tilde{g}_j\in A[X_1,\ldots,X_n,Y_1,\ldots,Y_m]$ tales que $\tilde{\varphi}(\tilde{b}_j)=b_j$ y $\tilde{\varphi}(\tilde{g}_j)=g_j$ para cada j de 1 a t. Si denotamos $\tilde{\eta}\coloneqq\sum_{j=1}^{t}\tilde{b}_j\tilde{g}_j$, entonces $\tilde{\varphi}(\eta-\tilde{\eta})=0$, esto es, $\eta-\tilde{\eta}\in Ker(\tilde{\varphi})$, de modo que existen $a_i\in A[X_1,\ldots,X_n,Y_1,\ldots,Y_m]$ tales que

$$\sum_{finita} a_{\underline{(\alpha,\beta)}}X_1^{\alpha_1}\cdots X_n^{\alpha_n}Y_1^{\beta_1}\cdots Y_m^{\beta_m}-\sum_{j=1}^{t}\tilde{b}_j\tilde{g}_j=\sum_{i=1}^{k}a_i f_i.$$

Así vemos que cualquier elemento del núcleo de ρ está engendrado por los f_i y $\tilde{g}_j$. En particular, C es de presentación finita como A-álgebra.

$\square$

Proposición 2.1.2. *Sean A un anillo, B una A-álgebra de morfismo estructural $f: A\longrightarrow B$ y C una B-álgebra de morfismo estructural $g: B\longrightarrow C$. Si B es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A y C formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre B, entonces C es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A.*

Demostración. Ser de presentación finita o de tipo finito son propiedades transitivas en virtud del lema 2.1.1, así que solo probamos las propiedades «formales».

-Caso no-ramificada. Sea D una A-álgebra, J un ideal de D de cuadrado nulo, $\pi: D\longrightarrow D/J$ el epimorfismo canónico y $\bar{u}: C\longrightarrow D/J$ un morfismo de A-álgebras. Queremos entonces probar que si u y v son dos morfismos de A-álgebras tales que $\bar{u}=\pi\circ u=\pi\circ v$ entonces $u=v$. Considerando la estructura de A-álgebra de B, el morfismo g se puede ver como morfismo de A-álgebras, y por tanto, también lo será la composición $\bar{u}'\coloneqq\bar{u}\circ g: B\longrightarrow D/J$. Resulta que $u\circ g$ y $v\circ g$ son levantamientos de $\bar{u}'$ y como B es no-ramificada sobre A por hipótesis, $u\circ g=v\circ g$. Dotemos ahora a $C, D, D/J$ de sus estructuras de B-álgebras a través de g, $u\circ g$ (ó $v\circ g$) y $\bar{u}\circ g$ respectivamente. Entonces, $u, v, \bar{u}$ son morfismos de B-álgebras:

$$\begin{tikzcd} D \arrow[r, "\pi"] & D/J \\ C \arrow[u, shift left, "u"'] \arrow[u, shift right, "v"] \arrow[ur, "\bar{u}"'] & \end{tikzcd}$$

Así, como C es no-ramificada sobre B por hipótesis, concluimos que $u=v$ y por tanto C es no-ramificada sobre A.

-Caso étale. Sea de nuevo D una A-álgebra, J un ideal suyo de cuadrado nulo y π el epimorfismo canónico. Como la inyectividad acabamos de verla en el caso anterior, basta probar la sobreyectividad, esto es, para cada $\bar{u}\in Hom_{A-alg}(C,D/J)$ podemos encontrar un levantamiento ($u\in Hom_{A-alg}(C,D)$ tal que $\pi\circ u=\bar{u}$). Consideramos el morfismo de B-álgebras

$\bar{u}' := \bar{u} \circ g : B \longrightarrow D/J$. Como B es étale sobre A, existe un (único) morfismo de A-álgebras $u' : B \longrightarrow D$ tal que $\bar{u}' = \pi \circ u'$. Dotemos ahora a $D, D/J, C$ de sus estructuras de B-álgebras via $u', \bar{u}', g$ respectivamente. Entonces $\bar{u}$ puede verse como un morfismo de B-álgebras y, como C es étale sobre B, $\bar{u}$ se levanta en un morfismo de B-álgebras $u : C \longrightarrow D$, que puede verse también como morfismo de A-álgebras via f. Así que C es étale sobre A.

□

Lema 2.1.3. *Dado un anillo A. Si B y C son dos A-álgebras de tipo finito (resp. de presentación finita), entonces el producto tensorial $B \otimes_A C$ es también una B- (ó C-) álgebra de tipo finito (resp. de presentación finita). Además, usando la transitividad anterior también es una A-álgebra de tipo finito (resp. de presentación finita).*

Demostración. Si B es de tipo finito como A-álgebra, entonces existe un isomorfismo

$$\frac{A[X_1, \ldots, X_n]}{I} \simeq B,$$

para ciertos $n \in \mathbb{N}$ e I ideal de $A[X_1, \ldots, X_n]$. Por tanto, $B \otimes_A C \simeq A[X_1, \ldots, X_n]/I \otimes_A C$, y usando el corolario 4.5.12,

$$B \otimes_A C \simeq \frac{C[X_1, \ldots, X_n]}{\mathcal{I}},$$

donde $\mathcal{I} = IC[X_1, \ldots, X_n]$. Así vemos que $B \otimes_A C$ es efectivamente de tipo finito como C-álgebra (un razonamiento análogo nos permite verla como B-álgebra de tipo finito). Si B fuera de presentación finita, entonces el ideal I sería finitamente generado, y por extensión $\mathcal{I}$, de modo que $B \otimes_A C$ sería de presentación finita como C-álgebra.
Finalmente, usando la transitividad mostrada en la proposición 2.1.1, deducimos que $B \otimes_A C$ es una A-álgebra de tipo finito (resp. de presentación finita).

□

Proposición 2.1.4. *Sean A un anillo, A' y B dos A-álgebras. Entonces si B es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A, $B' = B \otimes_A A'$ es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A'.*

Demostración. Las propiedades de finitud ya las hemos probado en el lema 2.1.3. Para las propiedades formales vamos a recurrir a la propiedad universal de la extensión de escalares para álgebras (4.5.30). Sea C una A'-álgebra con J un ideal de cuadrado nulo. Si denotamos por $C|_A$ la restricción de escalares de C a A, también tenemos que $(C/J)|_A = C|_A \,/\, J|_A$, así que usando la propiedad universal se tienen los isomorfismos siguientes:

$$Hom_{A'-\acute{a}lg}(B \otimes_A A', C) \simeq Hom_{A-\acute{a}lg}(B, C|_A),$$
$$Hom_{A'-\acute{a}lg}(B \otimes_A A', C/J) \simeq Hom_{A-\acute{a}lg}(B, (C/J)|_A).$$

Por tanto, la inyectividad o biyectividad (caso no-ramificado o caso étale respectivamente) entre los grupos de homomorfismos pasan de la A-álgebra B a la A'-álgebra $B \otimes_A A'$ via los isomorfismos anteriores.

□

Proposición 2.1.5. *Sean A un anillo, B y C dos A-álgebras. Si B y C son formalmente no-ramificadas (resp. no-ramificadas, resp. étale) sobre A, entonces $B \otimes_A C$ es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A.*

Demostración. Las propiedades de finitud vienen dadas por la proposición 2.1.3. Para las propiedades formales basta notar que, al ser B formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A, de la proposición anterior (2.1.5), $B \otimes_A C$ verifica esa misma propiedad sobre C. Como C es a su vez formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A, por la propiedad de transtividad dada en la proposición 2.1.2, se deduce que $B \otimes_A C$ es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A, como queríamos.

□

Lema 2.1.6. *Sean A un anillo, A' una A-álgebra fielmente plana, B una A-álgebra y $B' := B \otimes_A A'$. Entonces si B' es de tipo finito (resp. de presentación finita) sobre A', B es de tipo finito (resp. de presentación finita) sobre A.*

Demostración. Sean $(B_i)_{i\in I}$ las sub-A-álgebras de tipo finito de B. Como los A-morfismos de inclusión $\mu_i : B_i \longrightarrow B$ para $i \in I$ son inyectivos y A' es un A-módulo plano, los morfismos tensorizados $\mu_i \otimes id_{A'} : B'_i \longrightarrow B'$ siguen siendo inyectivos.

1. En el primer caso, como B' es de tipo finito como A'-álgebra, tiene un número finito n de generadores $b'_k \in B' = B \otimes_A A'$ con $k = 1, \dots, n$, que son por tanto sumas finitas de tensores (ver proposición 4.5.6):
$$b'_k = \sum_{j=1}^{m_k} b_j^k \otimes a_j^k.$$
En particular, podemos considerar la subálgebra de tipo finito de B que tiene por generadores los elementos $(b_j^k)_{jk}$. Esta álgebra será una de las B_i anteriores, pues en esa familia estaban todas las subálgebras de tipo finito de B, de manera que $B'_i = B'$.

   Consideramos la sucesión exacta canónica
$$0 \longrightarrow B_i \longrightarrow B \longrightarrow B/B_i \longrightarrow 0$$
y consideramos su extensión de escalares a A', que sigue siendo exacta,
$$0 \longrightarrow B'_i \longrightarrow B' \longrightarrow B'/B'_i \longrightarrow 0.$$
Observamos que la segunda flecha de esta segunda sucesión es un isomorfismo, pero como A' es fielemente plana sobre A, dicho isomorfismo se mantiene en la sucesión original, esto es, $B \simeq B_i$. Así que B es de tipo finito sobre A como queríamos demostrar.

2. Supongamos ahora que B' es de presentación finita sobre A'. Como en particular es de tipo finito, por el punto anterior sabemos que B es también de tipo finito sobre A. Así pues, para cierto anillo de polinomios $A[X_1, \dots, X_n]$ y cierto ideal suyo I, se tiene que
$$B \simeq A[X_1, \dots, X_n]/I.$$
En particular, como A' es fielmente plana, el isomorfismo anterior es equivalente
$$B' \simeq A'[X_1, \dots, X_n]/I',$$
donde $I' := I \otimes_A A'$.

   Como B' es de presentación finita como A'-álgebra, el ideal I' es de tipo finito como A'-álgebra. Usando ahora los A-ideales de tipo finito de I', $(I'_i)_{i\in I}$ se concluye como en el caso 1 que I es de tipo finito como A-álgebra, y por tanto B es de presentación finita sobre A.

$\square$

La siguiente proposición da un recíproco a la 2.1.4, únicamente cuando realizamos la extensión de escalares a una álgebra fielmente plana.

Proposición 2.1.7. *Sean A un anillo, B una A-álgebra, A' una A-álgebra fielmente plana sobre A y $B' = B \otimes_A A'$. Entonces, si B' es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A', B es formalmente no-ramificada (resp. no-ramificada, resp. étale) sobre A.*

Demostración. Las propiedades de finitud ya han sido probadas en el lema 2.1.6, así que nos limitamos a las propiedades formales una vez más.

1. *Caso (formalmente) no-ramificada:* Sean C una A-álgebra, J un ideal de cuadrado nulo de C, $\overline{C} = C/J$, $C' = C \otimes_A A'$, $J' = J \otimes_A A'$ las extensión de escalares de C y J a A', $\overline{C}' = \overline{C} \otimes_A A' = C'/J'$ la extensión de $\overline{C}$. Sean $\bar{u} \in Hom_{A-\acute{a}lg}(B, \overline{C})$ y u y v dos levantamientos de $\bar{u}$, que queremos ver que coinciden. Tensorizamos ahora $\bar{u}$ con A' sobre A y consideramos el morfismo resultante, $\bar{u}' := \bar{u} \otimes id_{A'}$ como homomorfismo de A'-álgebras (este proceso se conoce como *cambio de base* o *cambio de anillo*). Entonces $\bar{u}' \in Hom_{A'-alg}(B', \overline{C}')$, y con el cambio de base podemos obtener dos levantamientos u' y v' de $\bar{u}'$ a partir de los levantamientos de $\bar{u}$. Ahora bien, como B' es (formalmente) no-ramificada sobre A', $u' = v'$, y como A' es fielmente plano sobre A, el cambio de base es biyectivo (apartado 2 de la caracterización de módulos fielmente planos, proposición 4.5.26), luego $u = v$ también.

2. *Caso étale:* Tomemos C una A-álgebra, y guardemos las mismas notaciones que en el caso anterior. Habiendo probado ya la inyectividad, basta ver que todo homomorfismo de A-álgebras $\bar{u} : B \longrightarrow \overline{C}$ admite un levantamiento $u : B \longrightarrow C$ (también morfismo de A-álgebras). Por cambio de anillo de A a A', obtenemos un morfismo $\bar{u}' := \bar{u} \otimes id_{A'} : B' \longrightarrow \overline{C}'$, que se levanta en un A-morfismo $u' : B' \longrightarrow C'$ ya que B' es étale sobre A' por hipótesis. Como A' es fielmente plana, consideremos los morfismos de A-álgebras del lema 4.5.32

$$i_1 : A' \longrightarrow A''; \; a \longmapsto a \otimes 1,$$

$$i_1 : A' \longrightarrow A''; \; a \longmapsto 1 \otimes a,$$

donde $A'' = A' \otimes_A A'$. Se utilizará también la notación $B'' := B' \otimes_A A'$ (análoga con C'') y consideremos los morfismos $u''_t := u' \otimes i_t : B'' \longrightarrow C''$ con $t = 1, 2$. Como B' es étale sobre A' por hipótesis, en particular B' es no-ramificada sobre A' y, usando la parte anterior, B también lo es sobre A. En virtud de la proposición 2.1.4, B'' es no-ramificada sobre A'', y como u''_1 y u''_2 son dos morfismos de A-álgebras que levantan $\bar{u}'' := \bar{u}' \otimes id_{A'}$, deben ser iguales, $u''_1 = u''_2 = u''$.

Invocando el lema 4.5.32 una vez más, tenemos el diagrama conmutativo con filas exactas siguiente:

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "\phi_1"] \arrow[d, "u?"] & B' \arrow[r, "\phi_2"] \arrow[d, "u'"] & B'' \arrow[d, "u''"] \\
0 \arrow[r] & C \arrow[r, "\psi_1"] & C' \arrow[r, "\psi_2"] & C''.
\end{tikzcd} \tag{2.1.7.1}$$

Nuestro objetivo es construir el morfismo u anterior mediante «caza de diagramas» de modo que el diagrama anterior sea conmutativo. Sea entonces un elemento $b \in B$ cualquiera. Si $b' = \phi_1(b)$ y $c' = u'(b')$ veamos que existe una única preimagen de c' por ψ_1, que será nuestro $u(b)$. Como la primera fila es exacta, $Ker(\phi_2) = Im(\phi_1)$, luego $\phi_2(b') = 0$. Además, $\psi_2 \circ u' = u'' \circ \phi_2$, de donde $0 = u''(0) = \psi_2(c')$. Por tanto $c' \in Ker(\psi_2)$, pero este coincide con $Im(\phi_1)$ por la exactitud de la segunda fila. Así pues, existe $c \in C$ tal que $\psi_1(c) = c'$; y por el cero al inicio de la segunda fila, ψ_1 es inyectiva y este c, único. Por construcción, este u hace el diagrama entero conmutativo y solo nos falta remarcar por qué levanta $\bar{u}$. Denotamos por π y π' los epimorfismos de C y C' en sus cocientes c/J y C/J' respectivamente, y por $\xi_1 : C/J \longrightarrow C'/J'$ la aplicación que envía una clase $c + J$ en $c \otimes 1 + J'$. De esta manera, se tiene el diagrama siguiente

$$\begin{tikzcd}
B \arrow[r, "\phi_1"] \arrow[d, "u"] \arrow[dd, bend right=60, "\bar{u}"'] & B' \arrow[d, "u'"] \arrow[dd, bend left=60, "\bar{u}'"] \\
C \arrow[r, "\psi_1"] \arrow[d, "\pi"] & C' \arrow[d, "\pi'"] \\
C/J \arrow[r, "\xi_1"] & C'/J',
\end{tikzcd} \tag{2.1.7.2}$$

donde los morfismos de los dos cuadrados y el bucle de la derecha son conmutativos, y además $\xi_1 \circ \bar{u} = \bar{u}' \circ \phi_1$, ya que $\bar{u}' = \bar{u} \otimes id_{A'}$. Usando de nuevo el lema 4.5.32 sabemos que el morfismo de extensión de escalares ξ_1 es inyectivo por ser A' fielmente plano, así que para ver que $\bar{u} = \pi \circ u$ basta también ver que sus imágenes por ξ_1 coinciden. Pero, como $\xi_1 \circ \bar{u} = \bar{u}' \circ \phi_1$, y el centro y la derecha del diagrama conmutan, se deduce que

$$\xi_1 \circ (\pi \circ u) = \bar{u}' \circ \phi_1 = \xi_1 \circ \bar{u}.$$

□

Antes de comentar cómo se relacionan los morfismos étale y no-ramificados con las localizaciones, introducimos un lema sobre nilideales que utilizaremos en la demostración.

Lema 2.1.8. *Sean C un anillo, $\mathfrak{n}$ un nilideal de C y $\overline{C} = C/\mathfrak{n}$. Sea $a \in C$ y $\bar{a}$ su clase en $\overline{C}$. Entonces a es invertible si y solo si $\bar{a}$ lo es.*

Demostración. Si a es invertible, existe $b \in C$ tal que $ab = 1$ y por tanto, $\bar{a}\bar{b} = \bar{1}$ y $\bar{a}$ es invertible en $C/\mathfrak{n}$. Por otro lado, si $\bar{a}$ es invertible en $C/\mathfrak{n}$, sea $b \in C$ un levantamiento de la clase del inverso de $\bar{a}$. Entonces $ab = 1 + n$ para cierto $n \in \mathfrak{n}$, y como $\mathfrak{n}$ está contenido en el nilradical de C, sus elementos son nilpotentes. Como n es nilpotente, el lema 4.1.11 nos garantiza que $1 + n$ es invertible, y por tanto a es invertible (su inverso es b multiplicado por el inverso de $1 + n$).

□

Proposición 2.1.9. *Sean A un anillo, B una A-álgebra y S un subconjunto multiplicativamente cerrado de B.*

1. *Si B es formalmente no-ramificada sobre A, la localización $S^{-1}B$ es formalmente no-ramificada sobre A.*

2. *Si además S está engendrado por un elemento (existe $f \in A$ tal que $S = \{1, f, f^2, \dots\}$) y B es no-ramificada (resp. étale) sobre A, entonces $S^{-1}B$ es no-ramificada (resp. étale) sobre A.*

Demostración. Sean C una A-álgebra, $\overline{C} = C/J$, y $\bar{u} : S^{-1}B \longrightarrow C$ un homomorfismo de A-álgebras, y designemos por $\pi : B \longrightarrow S^{-1}B$ el morfismo canónico. Demostremos ahora cada apartado por separado:

1. Sean u y v dos levantamientos de $\bar{u}$. Si definimos $\bar{u}' := \bar{u} \circ \pi$, entonces $u \circ \pi$ y $v \circ \pi$ son dos levantamientos de $\bar{u}'$. Ahora bien, como B es formalmente no-ramificada sobre A por hipótesis, $u \circ \pi = v \circ \pi$, y como π es es un epimorfismo, $u = v$, y por tanto $S^{-1}B$ es formalmente no-ramificada sobre A.

2. Si ahora tomamos el conjunto $S = \{f^i\}_{i=0}^{+\infty}$, utilizando el lema 4.3.16, tenemos el isomorfismo de álgebras
$$B_f \simeq B[X]/(1 - fX).$$
De manera que B_f es una B-álgebra de presentación finita (en particular de tipo finito). Como B es también de presentación finita (resp. tipo finito) sobre A, la transitividad de estas propiedades dada en 2.1.1 nos garantiza que B_f es de presentación finita (resp. tipo finito) sobre A.

   Queda por ver la parte formal del caso étale: usando las notaciones de esta demostración, si $\bar{u} : B_f \longrightarrow \overline{C}$ es un homomorfismo de A-álgebras, queremos encontrar un levantamiento $u \in Hom_{A-alg}(B_f, C)$ de $\bar{u}$. Como B es étale sobre A por hipótesis, $\bar{u} \circ \pi \in Hom_{A-álg}(B, C/J)$ se levanta a un A-homomorfismo $v : B \longrightarrow C$. Gracias a la propiedad universal de las localizaciones (proposición 4.3.13), el morfismo v se factoriza a través de B_f si y solo si $v(S) \subseteq C^{\times}$, lo que equivale a que $v(f)$ sea una unidad de C (pues el resto de elementos de S son potencias de f y v es homomorfismo de anillos). Usando el lema anterior (2.1.8), $v(f)$ es invertible en C si y solo si su clase en $\overline{C}$ es invertible. Pero $v(f) + J$ es efectivamente invertible en $\overline{C}$, ya que $v(f) + J = \bar{u} \circ \pi(f)$, y $\pi(f)$ es una unidad de B_f (su inverso es $1/f$), así que $\bar{u}$ debe enviarla en una unidad de $\overline{C}$ (puesto que es un morfismo de anillos). Así, existe $u : B_f \longrightarrow C$ morfismo de A-álgebras tal que $v = u \circ \pi$. Si escribimos con $\pi_J : C \longrightarrow \overline{C}$ el epimorfismo canónico, por ser v un levantamiento de $\bar{u} \circ \pi$, tenemos que $\pi_J \circ u \circ \pi = \pi_J \circ v = \bar{u} \circ \pi$, y como π es sobreyectivo se tiene que $\pi_J \circ u = \bar{u}$. Hemos encontrado un levantamiento de $\bar{u}$ como queríamos, así que B_f es efectivamente étale sobre A.

□

Proposición 2.1.10. *Sean A un anillo, B una A-álgebra y supongamos que para cada $\mathfrak{q} \in Spec(B)$, existe un elemento $f \notin \mathfrak{q}$ tal que B_f es no-ramificada (resp. étale) sobre A. Entonces B es no-ramificada (resp. étale) sobre A. En otras palabras, para $A \longrightarrow B$, la propiedad de ser no-ramificada (resp. étale) es local sobre $Spec(B)$.*

Demostración. La demostración de esta proposición puede consultarse en el capítulo 2 del libro de Raynaud ([9]) , y la omitimos por requerir de técnicas de Geometría Algebraica.

□

Proposición 2.1.11. *Sea $\varphi : A \longrightarrow B$ un epimorfismo de anillos. Entonces B es formalmente no-ramificada sobre A. En particular, si S es un subconjunto multiplicativamente cerrado de A, $S^{-1}A$ es formalmente no-ramificada sobre A, y para todo ideal $\mathfrak{a}$ de A y $A/\mathfrak{a}$ es no-ramificada sobre A.*

Demostración. Sean como siempre C una A-álgebra, J un ideal de C de cuadrado nulo y $\overline{C} = C/J$. Dado $\bar{u} \in Hom_{A-álg}(B, C/J)$, sean u y v dos levantamientos suyos. Como $u, v \in Hom_{A-álg}(B, C)$ y φ también puede entenderse como morfismo de A-álgebras (pues en B se considera la estructura de A-álgebra de morfismo estructural φ), entonces se tiene que $u \circ \varphi = v \circ \varphi$. En efecto, para cada $a \in A$,
$$(u \circ \varphi)(a) = a(u \circ \varphi)(1) = a = a(v \circ \varphi)(1) = (v \circ \varphi)(a),$$

donde se ha usado que son todos morfismos de anillos y A-lineales. Así, como φ es sobreyectiva, $u = v$ y se deduce que B es formalmente no-ramificada sobre A.

Para los casos particulares basta considerar el epimorfismo canónico correspondiente y en el caso del ideal recordar que los cocientes de un anillo por un ideal son obviamente álgebras de tipo finito (el anillo $A[X_1, \ldots, X_n]$ es en este caso el propio A, esto es, $n = 0$), así que no-ramificada sobre A.

□

2.2. Álgebras estándar étale

La siguiente proposición nos sirve para introducir un tipo especial de álgebras étale, las *álgebras estándar étale*, que no son un ejemplo anecdótico: veremos que las álgebras étale con cierta propiedad son de hecho localmente isomorfas a álgebras estándar étale. Veamos antes un lema previo que se deduce del binomio de Newton.

Lema 2.2.1. ***[Fórmula de Taylor para anillos de polinomios]*** *Sea A un anillo conmutativo y $f(X) \in A[X]$ un polinomio de grado n. Si $a, b \in A$, entonces*

$$f(a+b) = \sum_{k=0}^{n} \frac{f^{k)}(a)}{k!} b^k.$$

Demostración. Basta demostrar la fórmula para un monomio x^n cualquiera y por linealidad se tiene para cualquier polinomio. Sea pues $f(x) = x^n$ y apliquemos el binomio de Newton por ser el anillo conmutativo:

$$f(a+b) = (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} n \cdot (n-1) \cdots (n-k+1) a^{n-k} \frac{b^k}{k!} = \sum_{k=0}^{n} \frac{f^{k)}(a)}{k!} b^k.$$

□

Proposición 2.2.2. *Dados A un anillo, $f(X) \in A[X]$, $f'(X)$ su polinomio derivada, $B = A[X]/(f)$ y $g(X) \in A[X]$ también. Si la imagen en B_g de f' es invertible, entonces B_g es una A-álgebra étale.*

Demostración. Sean C una A-álgebra, J un ideal suyo de cuadrado nulo, $\overline{C} = C/J$, $i : B \longrightarrow B_g$ el morfismo canónico de localización y $\bar{u} \in Hom_{A-alg}(B_g, \overline{C})$. Queremos ver que existe un levantamiento único de $\bar{u}$. Sea x la clase de la variable X en B (esto es, $X + (f)$), de manera que $B = A[x]$. Denotemos por $p : C \longrightarrow C/J$ el epimorfismo canónico. Tenemos entonces el diagrama siguiente:

$$\begin{tikzcd} A[x] = B \arrow[r, "i"] & B_g \arrow[dr, "\bar{u}"] & C \arrow[d, "p"] \\ & & C/J. \end{tikzcd}$$

Sea $\bar{c} := (\bar{u} \circ i)(x)$. Como $\bar{u} \circ i$ es un morfismo de A-álgebras sobre $B = A[x]$, queda determinado por la imagen de x, esto es $\bar{c}$. Por tanto, para encontrar un levantamiento u de $\bar{u}$, necesitamos un elemento $\gamma \in C$ tal que $u(i(x)) = \gamma$, el cual determina unívocamente u. Este γ debe verificar además las condiciones siguientes:

1. $p(\gamma) = \bar{c}$, pues $p \circ u = \bar{u}$ y $p \circ u(\gamma) = p \circ u(i(x)) = \bar{u}(i(x)) = \bar{c}$.

2. $f(\gamma) = 0$, ya que $f \in A[X]$, $f(x) = 0$ y $u \circ i$ es un morfismo de A-álgebras ($f(\gamma) = f(u(i(x))) = (u \circ i)(f(x)) = 0$).

Sea ahora c un levantamiento cualquiera de $\bar{c}$ en C, esto es, $p(c) = \bar{c}$. Como $f(x) = 0$,

$$\overline{f(c)} = f(\bar{c}) = f((\bar{u} \circ i)(x)) = (\bar{u} \circ i)(f(x)) = 0,$$

pues de nuevo $\bar{u} \circ i$ es un morfismo de A-álgebras y f un polinomio en A. Por tanto, $\overline{f(c)} = 0 \implies f(c) \in J$. Invocando ahora la fórmula de Taylor 2.2.1, para cada $j \in J$ tenemos

$$f(c+j) = f(c) + jf'(c) + P(j),$$

donde $P(j)$ es un polinomio en j sin términos de grado 0 o 1 (puede ser en principio nulo). Por tanto $P(j) = j^2Q(j)$ para cierto polinomio Q, pero como $j \in J$, que es de cuadrado nulo, $P(j) = 0$ y se tiene la ecuación siguiente

$$f(c + j) = f(c) + jf'(c). \tag{2.2.2.1}$$

Por otro lado, usando de nuevo que f' es un polinomio en A y $\bar{u} \circ i$ un morfismo de A-álgebras,

$$\overline{f'(c)} = f'(\bar{c}) = f'((\bar{u} \circ i)(x)) = (\bar{u} \circ i)(f'(x)).$$

Como $(i \circ f')(x)$ es la clase de $f'(x)$ en B_g, es invertible por hipótesis, y por lo tanto $\overline{f'(c)}$ lo es en C/J. Invocando ahora el lema 2.1.8, como J es un nilideal (todos sus elementos al cuadrado son nulos, así que en particular son nilpotentes), la invertibilidad de $\overline{f'(c)}$ en $\bar{C}$ implica la que $f'(c)$ en C.

Así las cosas, por la ecuación 2.2.2.1, se tiene la equivalencia siguiente para cualquier $j \in J$:

$$f(c + j) = 0 \iff j = -\frac{f(c)}{f'(c)}.$$

Como $f(c) \in J$ y este es un ideal de C, $-f(c)(f'(c))^{-1} \in J$, de modo que existe un único valor de $j \in J$ para que $f(c + j) = 0$. En particular existe un único elemento de C, $c - f(c)(f'(c))^{-1}$, al cual llamaremos γ, tal que $f(\gamma) = 0$.

Definamos ahora $v : B \longrightarrow C$ como el morfismo de A-álgebras tal que $v(x) = \gamma$ (recordemos que como $B = A[x]$ y pedimos que v sea morfismo de A-álgebras basta indicar la imagen de x). Entonces $(p \circ v)(x) = p(\gamma) = \bar{c} = (\bar{u} \circ i)(x)$, y como ambos son morfismos de A-álgebras sobre $B = A[x]$, deben coincidir:

$$p \circ v = \bar{u} \circ i. \tag{2.2.2.2}$$

De nuevo, como $g \in A[X]$ y las aplicaciones son morfismos de A-álgebras, puede permutar con ellas en la ecuación anterior:

$$g(p \circ v) = g(\bar{u} \circ i) \quad \Longrightarrow \quad (p \circ v)(g(x)) = \bar{u} \circ (i \circ g)(x).$$

Y como $(i \circ g)(x)$ es invertible en B_g, entonces $(\bar{u} \circ i \circ g)(x) = p(v(g(x)))$ es invertible en $\overline{C} = C/J$. De nuevo por el lema 2.1.8, esto implica que $(v \circ g)(x)$ es invertible en C. Como $B = A[x]$, de lo anterior se deduce que toda la imagen $(v \circ g)(B)$ está compuesta por unidades de C. Así, usando la propiedad universal de las localizaciones (la versión para álgebras de 4.3.13), sabemos que existe un único morfismo de A-álgebras $u : B_g \longrightarrow C$ tal que $v = u \circ i$, es decir, tal que el diagrama siguiente es conmutativo

$$\begin{tikzcd} B \arrow[r, "v"] \arrow[d, "i"'] & C \\ B_g. \arrow[ur, dashed, "u"'] & \end{tikzcd} \tag{2.2.2.3}$$

Entonces $p \circ (u \circ i) = p \circ v$, y de la ecuación 2.2.2.2, tenemos también que

$$p \circ (u \circ i) = p \circ v = \bar{u} \circ i.$$

Como además i es un epimorfismo, $p \circ u = \bar{u}$, así que u es un levantamiento de $\bar{u}$ que, como ya hemos dicho, es único por la unicidad de γ.

□

Observación 2.2.3. .

1. En particular podemos elegir como g la clase de f' en B, en cuyo caso $B_{f'}$ es obviamente étale sobre A, ya que f' pertenece al sistema multiplicativamente cerrado de la localización, y por tanto su inverso $1/f'$ está en $B_{f'}$.

2. Usando la proposición 2.1.11 anterior todo cociente de B_g por un ideal es no-ramificado sobre la propia B_g, y si B_g es no-ramificada sobre el anillo A, la transitividad dada en 2.1.2 nos garantiza que todo cociente de B_g es no-ramificado sobre A también.

3. En la proposición anterior y en la definición siguiente, g es un polinomio con coeficientes en A; así que cuando se escribe la localización B_g nos estamos refiriendo en realidad a $B_{\bar{g}}$, donde $\bar{g}$ es la clase de g en B.

Definición 2.2.4. [**Álgebra estándar étale**] Dados un anillo A, un polinomio mónico $f(X) \in A[X]$, su derivada $f'(X)$, $B = A[X]/(f)$ y $g(X) \in A[X]$ otro polinomio no necesariamente mónico. Si f' es invertible en B_g, el álgebra B_g es étale sobre A y se denominará *álgebra estándar étale* sobre A.

Capítulo 3

Morfismos quasifinitos. Teorema principal de Zariski

En la primera sección de este capítulo se presenta la noción de *álgebra quasifinita*, una familia de álgebras de tipo finito que, sin llegar a ser finitas, tienen propiedades interesantes que nos permitirán después enunciar el resultado principal de esta memoria: el *teorema principal de Zariski*. En la última sección se demostrarán un par de corolarios del mismo y se enunciará una de sus consecuencias fundamentales, un teorema de estructura local para álgebras étale.

3.1. Álgebras quasifinitas

Consideramos como siempre un anillo A y una A-álgebra de tipo finito B y comenzamos el capítulo estudiando las fibras $B \otimes_A K(\mathfrak{p})$, donde $\mathfrak{p}$ es un ideal primo de A y $K(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, el cuerpo de residuos correspondiente.

Proposición 3.1.1. *Sean A un anillo y B una A-álgebra de tipo finito. Las siguientes condiciones son equivalentes:*

1. *B es no-ramificada sobre A.*
2. *Para todo ideal primo $\mathfrak{p}$ de A, la fibra $B \otimes_A K(\mathfrak{p})$ es no-ramificada sobre $K(\mathfrak{p})$.*

Demostración. La prueba de la implicación directa es inmediata aplicando la proposición 2.1.4, ya que $K(\mathfrak{p})$ y B son dos A-álgebras y la segunda es no-ramificada sobre A. La implicación recíproca puede consultarse en el capítulo 3 del libro de Raynaud ([9]).

□

La demostración del siguiente lema, que en algunos textos se llama *lema de Zariski*, puede consultarse en el capítulo 5 del manual de Álgebra Conmutativa de Bourbaki ([3]) o, de manera más compacta, en los apuntes de Milne ([6]).

Lema 3.1.2. ***[Lema de Zariski]*** *Sea $K \subseteq L$ una extensión de cuerpos. Si L es finitamente generado como K-álgebra (esto es, de tipo finito), entonces el algebraico sobre K (por tanto una álgebra finita sobre K).*

Proposición 3.1.3. *Sean K un cuerpo, B una K-álgebra de tipo finito y $\mathfrak{q}$ un ideal primo de B. Las siguientes condiciones son entonces equivalentes:*

1. *$\mathfrak{q}$ es un punto aislado de $Spec(B)$.*

2. $B_{\mathfrak{q}}$ es finita sobre K.

Demostración.
(1) $\Longrightarrow$ (2) Supongamos que $\mathfrak{q}$ es aislado en $Spec(B)$. Entonces $\{\mathfrak{q}\}$ es un abierto de $Spec(B)$ para la topología de Zariski. Por tanto, como los abiertos principales son una base para dicha topología, existe $f \in B$ tal que

$$D(f) = \{\mathfrak{p} \in Spec(B) \ : \ f \notin \mathfrak{p}\} \subseteq \{\mathfrak{q}\}.$$

Pero como $\{\mathfrak{q}\}$ está reducido a un ideal, $\{\mathfrak{q}\} = D(f)$ para cierto $f \in B$. Usando el corolario 4.10.11 de la sección sobre topología de Zariski, sabemos que $Spec(B_f)$ es homeomorfo a $D(f)$ y por tanto a $\{\mathfrak{q}\}$, de modo que $Spec(B_f) = \{\mathfrak{q}B_f\}$.

Veamos ahora que B_f es noetheriano. En primer lugar, B es isomorfo a un cociente de un anillo de polinomios $K[X_1, \ldots, X_n]$ por un ideal, de modo que es noetheriano en virtud del teorema de la base de Hilbert (4.4.6). Además, cualquier localización de un anillo noetheriano mantiene esta propiedad (proposición 4.4.5), de modo que B_f es efectivamente noetheriano.

Por otro lado, como $Spec(B_f) = \{\mathfrak{q}B_f\}$, en particular B_f solo tiene un ideal maximal, así que es local. Y por ser noetheriano y tener un único ideal primo (dimensión de Krull nula), el teorema 4.4.17 nos garantiza que B_f es de hecho un anillo artiniano. Por la proposición 4.4.15, al ser una K-álgebra artiniana, B_f es de hecho una K-álgebra finita.

Si denotamos $S_f \coloneqq \{f^i \ : \ i = 0, 1, 2, \ldots\}$ y $S_{\mathfrak{q}} \coloneqq B \setminus \mathfrak{q}$ y aplicamos la conmutatividad de las localizaciones (proposición 4.3.15) obtenemos el isomorfismo de álgebras $(B_f)_{\mathfrak{q}} \simeq (S_f S_{\mathfrak{q}})^{-1}B$. Sin embargo, como $f \notin \mathfrak{q}$, todas las potencias de f están en $S_{\mathfrak{q}}$ así que $(S_f S_{\mathfrak{q}}) = S_{\mathfrak{q}} = B \setminus \mathfrak{q}$, luego $B_{\mathfrak{q}} \simeq (B_f)_{\mathfrak{q}}$. Ahora bien, como B_f es local, usando el corolario 4.3.14, es isomorfo a su localizado en su ideal maximal, esto es $B_f \simeq (B_f)_{\mathfrak{q}}$, de donde $B_f \simeq B_{\mathfrak{q}}$. Y como B_f era finita sobre K, también lo es $B_{\mathfrak{q}}$, como queríamos.

(2) $\Longrightarrow$ (1) Supongamos ahora que $B_{\mathfrak{q}}$ es finita sobre K y consideremos una sucesión exacta de B-módulos:

$$0 \longrightarrow M \longrightarrow B \longrightarrow B_{\mathfrak{q}} \longrightarrow N \longrightarrow 0.$$

Como la localización es exacta (ver proposición 4.3.20), si tomamos $S = B \setminus \mathfrak{q}$, la sucesión

$$0 \longrightarrow M_{\mathfrak{q}} \longrightarrow B_{\mathfrak{q}} \longrightarrow (B_{\mathfrak{q}})_{\mathfrak{q}} \longrightarrow N_{\mathfrak{q}} \longrightarrow 0$$

sigue siendo exacta. Usando el corolario 4.3.14, deducimos que $(B_{\mathfrak{q}})_{\mathfrak{q}}$ es isomorfo a $B_{\mathfrak{q}}$, de modo que la flecha central de la nueva sucesión exacta es un isomorfismo. El lema 4.2.23 nos permite entonces concluir que $N_{\mathfrak{q}} = M_{\mathfrak{q}} = 0$.

Ahora bien, como $M \hookrightarrow B$ es un submódulo de B y este es noetheriano, entonces M es finitamente generado. Como $M_{\mathfrak{q}} = 0$ y M es finitamente generado, gracias a la proposición 4.3.18, sabemos que existe un elemento $f' \in S = B \setminus \mathfrak{q}$ tal que $f'M = 0$. Y usando la misma proposición en sentido inverso deducimos que $M_{f'} = 0$. Por otro lado, como $B_{\mathfrak{q}}$ es una K-álgebra finita por hipótesis y en la sucesión exacta inicial veíamos que $B_{\mathfrak{q}} \twoheadrightarrow N$, entonces N es finito como K-módulo. Como B es una K-álgebra, en particular N es finito como B-módulo también, y razonando igual que con M, existe un $f'' \in B \setminus \mathfrak{q}$ tal que $N_{f''} = 0$.

Si tomamos ahora $f \coloneqq f'f'' \in B \setminus \mathfrak{q}$, entonces $N_f = M_f = 0$. Por tanto, si localizamos en f la sucesión exacta inicial, obtenemos la sucesión exacta

$$0 \longrightarrow M_f = 0 \longrightarrow B_f \longrightarrow (B_{\mathfrak{q}})_f \longrightarrow N_f = 0 \longrightarrow 0,$$

de donde se deduce que la flecha central debe ser un isomorfismo, así que $(B_\mathfrak{q})_f \simeq B_f$. Pero como $f \in B \setminus \mathfrak{q}$, razonando como en la implicación anterior obtenemos que $B_f \simeq (B_\mathfrak{q})_f \simeq B_\mathfrak{q}$, y en particular $Spec(B_f) = Spec(B_\mathfrak{q})$. Por otro lado, al ser $B_\mathfrak{q}$ finita sobre K, $B_\mathfrak{q}$ es artiniana (ver proposición 4.4.15). Por la proposición 4.4.9, todos sus ideales primos son también maximales, pero como de hecho es local, el único ideal primo es $\mathfrak{q}B_\mathfrak{q}$ (el único elemento de $Spec(B_\mathfrak{q})$). Usando de nuevo el corolario 4.10.11 se tiene el homemorfismo $D(f) \simeq Spec(B_f)$ y de ahí $D(f) \simeq \{\mathfrak{q}B_\mathfrak{q}\}$. Así que $\{\mathfrak{q}\}$ es homeomorfo al abierto $D(f)$ de $Spec(B)$, y por tanto $\mathfrak{q}$ es aislado.

□

Veamos ahora cómo extender la proposición anterior a álgebras sobre un anillo cualquiera (no necesariamente un cuerpo).

Proposición 3.1.4. *Sean A un anillo, B una A-álgebra de tipo finito, $\mathfrak{q}$ un ideal primo de B y $\mathfrak{p}$ su preimagen en A por el morfismo estructural de B como A-álgebra (es decir, su contracción). Entonces son equivalentes las condiciones siguientes:*

1. *$\mathfrak{q}$ es un punto aislado en su fibra: $Spec(B \otimes_A K(\mathfrak{p}))$.*
2. *$B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q}$ es finita sobre $K(\mathfrak{p})$.*

Demostración. En primer lugar, usando el corolario 4.3.21, sabemos que cocientes y localizaciones conmutan y por tanto

$$B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q} \simeq (B/\mathfrak{p}B)_{\mathfrak{q}/\mathfrak{p}},$$

donde $\mathfrak{q}/\mathfrak{p}$ hace referencia al ideal del anillo cociente $B/\mathfrak{p}B$ correspondiente a $\mathfrak{q}$. Por otro lado, de la proposición 4.5.14, se tiene el isomorfismo de A-álgebras

$$B/\mathfrak{p}B \simeq B \otimes_A A/\mathfrak{p}.$$

Definimos ahora la parte multiplicativamente cerrada de $B \otimes_A A/\mathfrak{p}$ formada por los tensores de la forma $1 \otimes \bar{a}$, con $a \in A \setminus \mathfrak{p}$. Usando la propiedad universal de las localizaciones y la del producto tensorial se puede comprobar - de manera un poco laboriosa de escribir - el isomorfismo de A-álgebras siguiente

$$S^{-1}(B \otimes_A A/\mathfrak{p}) \simeq B \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

Además, teniendo en cuenta la observación 4.3.19 sobre la conmutatividad de las localizaciones sucesivas se puede ver también que

$$(S^{-1}(B \otimes_A A/\mathfrak{p}))_{\mathfrak{q}/\mathfrak{p}} \simeq (B \otimes_A A/\mathfrak{p})_{\mathfrak{q}/\mathfrak{p}}.$$

Recapitulando, se tiene la cadena de isomorfismos de A-álgebras siguiente:

$$B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q} \simeq (B/\mathfrak{p}B)_{\mathfrak{q}/\mathfrak{p}} \simeq (B \otimes_A A/\mathfrak{p})_{\mathfrak{q}/\mathfrak{p}} \simeq (B \otimes_A K(\mathfrak{p}))_{\mathfrak{q}/\mathfrak{p}}.$$

Así las cosas, podemos aplicar el caso anterior (proposición 3.1.3) a la $K(\mathfrak{p})$-álgebra $B \otimes_A K(\mathfrak{p})$ para probar la equivalencia deseada.

□

Definición 3.1.5. [**Álgebra quasifinita**] Dado un anillo A, una B-álgebra de tipo finito y un ideal primo $\mathfrak{q}$ de B, si las condiciones equivalentes de la proposición 3.1.4 se verifican, se dice que B es *quasifinita sobre A en $\mathfrak{q}$*. Si B es quasifinita sobre todo punto $\mathfrak{q}$ de $Spec(B)$, decimos simplemente que B es *quasifinita sobre A*.

Observación 3.1.6. Vamos a darle otra vuelta de tuerca a la quasifinitud estudiando qué significa que el ideal $\mathfrak{q}$ sea aislado en su fibra.

Recordemos en primer lugar que los ideales primos de $B/\mathfrak{p}B \simeq B \otimes_A A/\mathfrak{p}$ corresponden a los primos de B que contienen a $\mathfrak{p}B$ (cf. observación 4.1.4), esto es,

$$Spec(B/\mathfrak{p}B) \Leftrightarrow \{\mathfrak{r} \in Spec(B) \ : \ \mathfrak{p} \subseteq \mathfrak{r} \cap A\}.$$

Por otro lado, ya comentamos en la proposición 3.1.4 que había un isomorfismo entre $S^{-1}(B \otimes_A A/\mathfrak{p})$ y $B \otimes_A K(\mathfrak{p})$, donde la parte S estaba formada por los tensores de la forma $1 \otimes \bar{a}$ con $a \in A \setminus \mathfrak{p}$. Además, por el corolario 4.3.11, sabemos que los primos de $B \otimes_A K(\mathfrak{p})$ corresponden a los de $B/\mathfrak{p}B$ que no cortan a S, esto es, tales que su contracción a A está contenida en $\mathfrak{p}$. Pero acabamos de ver que los ideales del cociente $B/\mathfrak{p}B$ corresponden a los de B cuya contracción a A contiene a $\mathfrak{p}$, así que uniendo ambas tenemos la correspondencia siguiente:

$$Spec(B \otimes_A K(\mathfrak{p})) \Leftrightarrow \{\mathfrak{r} \in Spec(B) \ : \ \mathfrak{r} \cap A = \mathfrak{p}\}.$$

Volviendo ahora a nuestro problema inicial, B es quasifinita sobre A en $\mathfrak{q}$ si y solo si el punto $\mathfrak{q}$ es aislado en $Spec(B \otimes_A K(\mathfrak{p}))$, es decir, que es abierto y cerrado en el espectro:

1. Por la proposición 4.10.7, sabemos que los puntos cerrados para la topología de Zariski corresponden a ideales maximales en $Spec(B \otimes_A K(\mathfrak{p})$, y por lo anterior, será en particular maximal entre los ideales primos por encima de $\mathfrak{p}$.

2. Como $\mathfrak{q}$ es abierto, en particular el espectro $Spec((B \otimes_A K(\mathfrak{p}))_{\mathfrak{q})}$ será unipuntual (véase la demostración de la proposición 3.1.3). Por otro lado, razonando como arriba,

   $$Spec((B\otimes_A K(\mathfrak{p}))_{\mathfrak{q}/\mathfrak{p}}) \Leftrightarrow \{\mathfrak{r} \in Spec(B\otimes_A K(\mathfrak{p})) \ : \ \mathfrak{r} \subseteq \mathfrak{q}/\mathfrak{p}\} \Leftrightarrow \{\mathfrak{d} \in Spec(B) \ : \ \mathfrak{d} \cap A = \mathfrak{p} \ y \ \mathfrak{d} \subseteq \mathfrak{q}\}.$$

   Acabamos de ver que este conjunto se reduce al ideal $\mathfrak{q}$, y por tanto ningún primo de B por encima de $\mathfrak{p}$ está contenido en él, esto es, es minimal entre ellos.

Concluimos por tanto que B es quasifinita sobre A en $\mathfrak{q}$ si y solo si el ideal $\mathfrak{q}$ es maximal y minimal entre los primos por encima de $\mathfrak{p}$.

Lema 3.1.7. *Sea, K un cuerpo y B una K-álgebra de tipo finito. El espacio topológico $Spec(B)$ es finito y discreto (para la topología de Zariski) si y solo si B es una K-álgebra finita.*

Demostración.
$\Longrightarrow$ Si B es finita sobre K, por la proposición 4.4.15, es artiniana, así que usando el teorema de estructura de anillos artinianos (4.4.10), B es producto de sus localizaciones en sus ideales maximales (que son una cantidad finita, digamos $\{\mathfrak{m}_i\}_{i=1}^n$):

$$B = \prod_{i=1}^{n} B_{\mathfrak{m}_i}.$$

Utilizando la proposición 4.10.12, de esta descomposición se deduce una de $Spec(B)$ en unión disjunta de abiertos,

$$Spec(B) = \bigsqcup_{i=1}^{n} Spec(B_{\mathfrak{m}_i}) = \bigsqcup_{i=1}^{n} \{\mathfrak{m}_i\},$$

donde la última igualdad se deduce de que cada anillo $B_{\mathfrak{m}_i}$ tiene un único ideal primo, que es $\mathfrak{m}_i B_{\mathfrak{m}_i}$ en este caso. Esto se debe a que los primos de la localización están en biyección con los primos de B que no cortan a la parte multiplicativamente cerrada donde se localiza (4.3.10), esto es, están contenidos en $\mathfrak{m}_i$. Pero es que todos los primos de B son maximales por ser este artiniano, así que no hay ideales primos allí contenidos. Así concluimos que $Spec(B)$ es un espacio discreto y finito.

$\Longleftarrow$ Supongamos ahora que $Spec(B)$ es discreto y finito. Como los abiertos principales son una base, $Spec(B)$ se puede expresar como unión suya, pero como además los puntos son abiertos en este espacio, en particular podemos coger abiertos principales unipuntuales, esto es, $Spec(B_{f_i}) \simeq D(f_i) = \{\mathfrak{q}_i\}$ (4.10.11), para $f_i \in B$ e $i = 1, \ldots, n$. Así pues

$$Spec(B) = \bigsqcup_{i=1}^{n} Spec(B_{f_i}),$$

y de la proposición 4.10.12 se tiene que $B = \prod_{i=1}^{n} B_{f_i}$. Como los B_{f_i} son locales de ideal maximal $\mathfrak{q}_i B_{f_i}$, por el corolario 4.3.14, son isomorfos a su localizado en su ideal maximal. Siendo además las localizaciones sucesivas conmutativas en virtud de 4.3.15, se tienen los isomorfismos siguientes:

$$B_{f_i} \simeq (B_{f_i})_{\mathfrak{q}_i} \simeq (B_{\mathfrak{q}_i})_{f_i} \simeq B_{\mathfrak{q}_i},$$

donde el último se deduce de que el conjunto multiplicativamente cerrado formado por productos de un elemento de $(B \setminus \mathfrak{q}_i)$ y otro de $\{f_i^k\}_{k \geq 0}$ coincide con el primero al ser $f_i \notin \mathfrak{q}_i$. Como los ideales $\mathfrak{q}_i$ son aislados en $Spec(B)$ por hipótesis, la proposición 3.1.3 concluye que las $B_{\mathfrak{q}_i}$ son K-álgebras finitas, y por tanto B es también K-álgebra finita por ser producto de las anteriores.

□

Proposición 3.1.8. *Sean A un anillo, B una A-álgebra de tipo finito. Las propiedades siguientes son equivalentes:*

1. *B es quasifinita sobre A.*
2. *Para todo punto $\mathfrak{p}$ en $Spec(A)$, la fibra $B \otimes_A K(\mathfrak{p})$ es finita sobre $K(\mathfrak{p})$.*

En particular, de la proposición 3.1.1 se deduce que si B es no-ramificada sobre A, entonces B es quasifinita sobre A.

Demostración. Al ser B una A-álgebra de tipo finito, por la proposición 2.1.3, $B \otimes_A K(\mathfrak{p})$ es una $K(\mathfrak{p})$-álgebra de tipo finito para cada ideal primo $\mathfrak{p}$ de A. Así pues, basta aplicar el lema anterior 3.1.7: $B \otimes_A K(\mathfrak{p})$ será finita sobre $K(\mathfrak{p})$ si y solo si el espectro $Spec(B \otimes_A K(\mathfrak{p}))$ es discreto para la topología de Zariski. Esto último equivale a que todos los puntos $\mathfrak{q}$ del mismo sean aislados, y por tanto B quasifinita sobre A en $\mathfrak{q}$ para todo punto.

□

Observación 3.1.9. «*La quasifinitud se preserva por cocientes y localizaciones*».

Sean S es una parte multiplicativamente cerrada de un anillo A, B un A-álgebra de tipo finito, $\mathfrak{q}$ un ideal primo de B y $\mathfrak{p}$ su contracción a A. Sea además $\mathfrak{n}$ es un ideal de B cuya contracción a A se denota por $\mathfrak{m}$ y supongamos que B es quasifinita sobre A en $\mathfrak{q}$. Entonces:

1. $S^{-1}B$ es quasifinita sobre $S^{-1}A$ en $\mathfrak{q}S^{-1}B$.
2. $B/\mathfrak{n}$ es quasifinita sobre $A/\mathfrak{m}$ en $\mathfrak{q}/\mathfrak{n}$.

Las demostraciones de estos resultados son sencillas pero la notación es muy pesada de escribir, así que nos limitamos a comentar la primera prueba. Partamos de que $B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$ es finita sobre $K(\mathfrak{p})$.

Entonces, al localizar en S se mantiene la finitud (ver corolario 4.3.22), y por la conmutatividad del cociente y las localizaciones (4.3.21) y la de las localizaciones sucesivas (4.3.15) se tiene que

$$\frac{(S^{-1}B)_{\mathfrak{q}}}{\mathfrak{p}(S^{-1}B)_{\mathfrak{q}}}$$

es finita sobre

$$S^{-1}K(\mathfrak{p}) \simeq \frac{(S^{-1}A)_{\mathfrak{p}}}{\mathfrak{p}(S^{-1}A)_{\mathfrak{p}}},$$

donde se ha usado la observación 4.3.17 para simplificar la notación.

Ejemplo 3.1.10. [Ejemplos de álgebras quasifinitas]

1. Las álgebras no-ramificadas son quasifinitas.
2. Si B es una A-álgebra finita, en particular B es quasifinita sobre A.
3. Si C es una A-álgebra finita y B es una C álgebra de tipo finito tal que $Spec(B) \longrightarrow Spec(C)$ es una inmersión abierta, entonces B es quasifinita sobre A. En particular, uno de los corolarios del teorema principal de Zariski (3.3.2) nos dirá que de hecho todas las A-álgebras quasifinitas son de esta forma.

Demostración.

1. Ya se ha comentado en la proposición 3.1.8.
2. Si B es una A-álgebra finita (de generadores $b_1, \dots, b_n \in B$), entonces para cada ideal primo $\mathfrak{p}$, $B \otimes_A K(\mathfrak{p})$ es una $K(\mathfrak{p})$-álgebra finita (de generadores $b_1 \otimes 1, \dots, b_n \otimes 1$). Así que B es quasifinita sobre A usando la proposición 3.1.8.
3. Razonando como antes, al ser C finita sobre A, se tiene que $C \otimes_A K(\mathfrak{p})$ es finita sobre $K(\mathfrak{p})$ para todo primo $\mathfrak{p}$ de A. Usando de nuevo 3.1.8, C es quasifinita sobre A. Pero además, por 3.1.7, se tiene que $Spec(C \otimes_A K(\mathfrak{p}))$ es discreto para todo $\mathfrak{p}$. Como $Spec(B) \hookrightarrow Spec(C)$ es una inyección abierta, también lo es $Spec(B \otimes_A K(\mathfrak{p})) \hookrightarrow Spec(C \otimes_A K(\mathfrak{p}))$, y se deduce que $Spec(B \otimes_A K(\mathfrak{p}))$ es un subespacio de $Spec(C \otimes_A K(\mathfrak{p}))$ y por tanto discreto. Usando de nuevo el lema 3.1.7, se tiene que B es quasifinita sobre A.

□

Terminamos esta sección con un par de lemas sobre álgebras quasifinitas que serán usados en la demostración del *teorema principal de Zariski* a continuación.

Lema 3.1.11. *Sean $A \longrightarrow C \longrightarrow B$ homomorfismos de anillos tales que su composición $A \longrightarrow B$ es de tipo finito, y sea $\mathfrak{q}$ un ideal primo de B. Si B es quasifinita sobre A en $\mathfrak{q}$, entonces es quasifinita sobre C en $\mathfrak{q}$.*

Demostración. Sean $\mathfrak{p}_A$ y $\mathfrak{p}_C$ las imágenes inversas de $\mathfrak{q}$ en A y C respectivamente. Veamos que entonces $Spec(B \otimes_C K(\mathfrak{p}_C))$ es un subespacio de $Spec(B \otimes_A K(\mathfrak{p}_A))$.

De los morfismos de anillos $A \hookrightarrow C \hookrightarrow B$ se deducen los morfismos recíprocos sobre los espectros correspondientes:

$$\begin{array}{ccccc} Spec(B) & \xrightarrow{\alpha} & Spec(C) & \xrightarrow{\beta} & Spec(A) \\ \mathfrak{q} & \longmapsto & \mathfrak{p}_C & \longmapsto & \mathfrak{p}_A. \end{array} \tag{3.1.11.1}$$

Consideremos los conjuntos de $Spec(B)$ siguientes:

$$\begin{aligned}\mathcal{C}_1 &:= (\beta\circ\alpha)^{-1}(\mathfrak{p}_A) = \{\mathfrak{r}\in Spec(B)\ :\ (\beta\circ\alpha)(\mathfrak{r}) = \mathfrak{r}\cap A = \mathfrak{p}_A\},\\ \mathcal{C}_2 &:= \alpha^{-1}(\mathfrak{p}_C) = \{\mathfrak{r}\in Spec(B)\ :\ \alpha(\mathfrak{r}) = \mathfrak{r}\cap C = \mathfrak{p}_C\}.\end{aligned}$$

Dado $\mathfrak{r}\in\mathcal{C}_2$ se tiene que $\beta\circ\alpha(\mathfrak{r}) = \mathfrak{p}_A$, así que $\mathfrak{r}\in\mathcal{C}_1$ y por tanto $\mathcal{C}_2\subseteq\mathcal{C}_1$. Por esta contención, si probamos que $\mathcal{C}_1\simeq Spec(B\otimes_A K(\mathfrak{p}_A))$ y $\mathcal{C}_2\simeq Spec(B\otimes_C K(\mathfrak{p}_C))$ veremos que el segundo es un subespacio del primero, como queríamos. Como el razonamiento es el mismo, vamos a restringirnos a probarlo para $\mathcal{C}_1$.

En primer lugar recordemos que $B/\mathfrak{p}_A B$ es isomorfo como A-álgebra a $B\otimes_A (A/\mathfrak{p}_A)$ en virtud de la proposición 4.5.14. Consideremos ahora la parte multiplicativamente cerrada de A dada por $S = A\setminus\mathfrak{p}_A$. Como el isomorfismo anterior manda elementos $\bar{a}$ en tensores $a\otimes\bar{1}$, la parte multiplicativa S en el producto tensorial corresponde a $\{a\otimes\bar{1} = 1\otimes\bar{a}\ :\ a\in A\setminus\mathfrak{p}_A\}$. Utilizando ahora la proposición 4.10.10, se tiene el homeomorfismo

$$Spec(S^{-1}(B/\mathfrak{p}_A B)) \Leftrightarrow \{\mathfrak{r}\in Spec(B/\mathfrak{p}_A B)\ :\ \mathfrak{r}\cap A\subseteq\mathfrak{p}_A\}.$$

Por la observación 4.1.4, los ideales del cociente corresponden a los de B cuya contracción a A contiene a $\mathfrak{p}_A$, esto es,

$$\{\mathfrak{r}\in Spec(B)\ :\ \mathfrak{r}\cap A\subseteq\mathfrak{p}_A,\ \ \mathfrak{r}\cap A\supseteq\mathfrak{p}_A\},$$

que coincide con $\mathcal{C}_1$. Además, usando las propiedades universales del producto tensorial y la localización se puede comprobar el isomorfismo de A-álgebras siguiente:

$$S^{-1}(B\otimes_A A/\mathfrak{p}_A)\simeq B\otimes_A K(\mathfrak{p}_A),$$

y uniendo esto a lo anterior se tiene que $\mathcal{C}_1\simeq Spec(B\otimes_A K(\mathfrak{p}_A))$ como queríamos.

Una vez sabemos que $Spec(B\otimes_C K(\mathfrak{p}_C))$ es un subespacio de $Spec(B\otimes_A K(\mathfrak{p}_A))$, está claro que un punto aislado en el segundo lo será también en el primero, y se tiene el resultado.

□

Lema 3.1.12. *Sea $L|K$ una extensión algebraica de cuerpos, y sea M un anillo tal que $K\subseteq M\subseteq L$. Entonces M es un cuerpo.*

Demostración. Basta ver que cada elemento $a\in M\setminus\{0\}$ tiene inverso en M. Sea $K[a]$ el anillo de polinomios en a con coeficientes en K. Como es el mínimo anillo que contiene a K y a a, entonces $K[a]\subseteq M$. Además, al estar $a\in L$ y ser la extensión $L|K$ algebraica, en particular a es algebraico sobre K, luego $K[a] = K(a)$, esto es, el cuerpo de cocientes. Pero esto implica que $K(a)\subseteq M$, y por tanto que $a^{-1}\in M$.

□

Lema 3.1.13. *Sean $A\subseteq C\subseteq B$ anillos. Sea $\mathfrak{q}$ un ideal primo de B y sean $\mathfrak{r} = \mathfrak{q}\cap C$ y $\mathfrak{p} = \mathfrak{q}\cap A$.*

1. *Si $\mathfrak{q}$ es minimal para la contención entre los ideales primos de B por encima de $\mathfrak{p}$, entonces existe $u\in C\setminus\mathfrak{q}$ tal que $C_u = B_u$, y $\mathfrak{r}$ es minimal entre los ideales primos de C por encima de $\mathfrak{p}$.*

2. *Si B es entera sobre una A-subálgebra de tipo finito suya B_0 y $\mathfrak{q}$ es maximal entre los ideales primos de B por encima de $\mathfrak{p}$, entonces $\mathfrak{r}$ es maximal entre los ideales primos de C por encima de $\mathfrak{p}$.*

3. *Supongamos que B es entera sobre una sub-A-álgebra de tipo finito B_0 y que existe un $u \in C \setminus \mathfrak{q}$ tal que $C_u = B_u$. Si B es quasifinita sobre A en $\mathfrak{q}$, entonces C es quasifinita sobre A en $\mathfrak{r}$.*

Demostración.

1. Supongamos, por reducción al absurdo, que existe un ideal primo de C por encima de $\mathfrak{p}$, $\mathfrak{r}'$, estrictamente contenido en $\mathfrak{r}$. Si extendemos $\mathfrak{r}'$ a $C_u = B_u$, el ideal resultante sigue siendo primo puesto el inicial no corta al conjunto $\{u^i\}_{i \geq 0}$: $u \in C \setminus \mathfrak{q}$ y $\mathfrak{r}' \subsetneq \mathfrak{r} = \mathfrak{q} \cap C$. Contraemos ahora el resultado a B, y este sigue siendo un ideal primo $\mathfrak{q}'$. Como las contenciones se mantienen por los morfismos de espectros, $\mathfrak{q}'$ es un ideal primo de B por encima de $\mathfrak{p}$ y estrictamente contenido en $\mathfrak{q}$, lo que contradice la minimalidad de $\mathfrak{q}$.

2. En primer lugar, notemos que pueden sustituirse A, B y C por sus localizaciones en $\mathfrak{p}$, pues las contenciones de anillos e ideales se mantienen por la exactitud de la localización (4.3.20), las propiedades de finitud gracias al corolario 4.3.22 y las de integridad por la proposición 4.7.8. Podemos por tanto asumir que A es local de ideal maximal $\mathfrak{p}$. Consideramos ahora las contenciones
$$A/\mathfrak{p} \subseteq C/\mathfrak{r} \subseteq B/\mathfrak{q}; \quad A/\mathfrak{p} \subseteq B_0/\mathfrak{r}' \subseteq B/\mathfrak{q},$$
donde $\mathfrak{r}' = \mathfrak{q} \cap B_0$. Como $\mathfrak{q}$ es maximal entre los ideales primos por encima de $\mathfrak{p}$, en particular es un ideal maximal y $B/\mathfrak{q}$ es un cuerpo. Al ser $\mathfrak{r}'$ primo por ser contracción de un primo, $B_0/\mathfrak{r}'$ es un dominio de integridad. Como B es entera sobre B_0 por hipótesis, la proposición 4.7.8 nos garantiza que el cociente $B/\mathfrak{q}$ es entero sobre $B_0/\mathfrak{r}'$. Se verifican por tanto las hipótesis del lema 4.7.5, así que $B_0/\mathfrak{r}'$ es un cuerpo. Además, como B_0 era finitamente generado como A-álgebra (es decir, de tipo finito), $B_0/\mathfrak{r}'$ lo será como $A/\mathfrak{p}$-álgebra, y el lema de Zariski (3.1.2) nos garantiza que $B_0/\mathfrak{r}'$ es una extensión algebraica finita de $A/\mathfrak{p}$. Por transitividad (cf. asignatura *Ecuaciones Algebraicas*), $B/\mathfrak{q}$ es algebraico sobre $A/\mathfrak{p}$. Usando el lema anterior (3.1.12), se tiene que $C/\mathfrak{r}$ es un cuerpo, así que $\mathfrak{r}$ es maximal entre los ideales primos en C que por encima de $\mathfrak{p}$.

3. En este caso se cumplen las hipótesis de los dos apartados anteriores, así que $\mathfrak{r}$ es maximal y minimal entre los primos por encima de $\mathfrak{p}$. Usando la observación 3.1.6, se concluye que C es quasifinita sobre A en $\mathfrak{r}$ como queríamos.

$\square$

3.2. El teorema principal de Zariski

Esta segunda sección del capítulo está dedicada enteramente a demostrar el resultado fundamental de este trabajo: el *teorema principal de Zariski.* Su enunciado, *grosso modo*, muestra que las álgebras quasifinitas sobre un cierto ideal primo son isomorfas localmente (en un entorno de dicho ideal) a abiertos de un álgebra entera sobre el anillo inicial. Para probar esta versión del teorema, seguiremos esencialmente el texto de Raynaud [9], y los apuntes de J.S.Milne [6] que, aunque siguen la misma estrategia de demostración que Raynaud, son más legibles y añaden resultados auxiliares para facilitar la demostración. Después del teorema se incluyen dos corolarios del mismo, aunque el resultado más importante que se deduce de él será esbozado brevemente en la sección siguiente.

Teorema 3.2.1. ***[Main Theorem]*** *Sean A un anillo, B una A-álgebra de tipo finito, A' la clausura íntegra de A en B y $\mathfrak{q} \in Spec(B)$. Si B es quasifinita sobre A en $\mathfrak{q}$, entonces existe un elemento $f \in A' \setminus \mathfrak{q}$ tal que $A'_f \simeq B_f$. Esto es, en un entorno de $\{\mathfrak{q}\}$, B es isomorfa a un abierto de una álgebra entera sobre A.*

La versión que presentamos del teorema principal de Zariski es una consecuencia de la proposición siguiente, que es un resultado aún más fuerte. A su vez, para demostrar esta proposición, se utilizarán cuatro lemas que son casos particulares del teorema principal y que se apoyan unos sobre otros.

Proposición 3.2.2. *Sean $A \subseteq B \subseteq C$ tres anillos. Supongamos que C es de tipo finito sobre A, B es finito sobre C y A es íntegramente cerrado en B. Sean además $\mathfrak{q}$ un ideal primo de B y $\mathfrak{p} = \mathfrak{q} \cap A$ tales que B es quasifinita sobre A en $\mathfrak{q}$. Entonces se tiene el isomorfismo de álgebras $B_\mathfrak{p} \simeq A_\mathfrak{p}$.*

Demostración. Vamos a probar ahora el teorema principal de Zariski utilizando esta proposición, que demostraremos al final de este capítulo con la ayuda de cuatro lemas previos. Apliquemos pues esta proposición 3.2.2 a los anillos $A' \subseteq B = B$ que aparecen en el enunciado del teorema principal (B es una A-álgebra de tipo finito, A' es la clausura íntegra de A en B). Sea además $\mathfrak{q}$ un ideal primo de B tal que B es quasifinita sobre A en él. Comprobamos que las hipótesis de esta proposición se cumplen efectivamente para estos anillos: A' es íntegramente cerrado en B por ser la clausura íntegra de A allí, B es de tipo finito sobre A' por serlo sobre A y B es finita sobre sí misma.

Aplicamos ahora el lema 3.1.11 a los homomorfismos $A \longrightarrow A' \longrightarrow B$, pues $A \longrightarrow B$ es de tipo finito por hipótesis. Así pues, como hemos supuesto que B es quasifinita sobre A en $\mathfrak{q}$, del lema se deduce que B es quasifinita sobre A' en $\mathfrak{q}$. Usando ahora la proposición 3.2.2, se tiene el isomorfismo de álgebras

$$A'_{\mathfrak{p}'} \simeq B_{\mathfrak{p}'},$$

donde $\mathfrak{p}' := \mathfrak{q} \cap A'$.

Como B es de tipo finito como A'-álgebra, sean $b_1, \ldots, b_n$ sus generadores y denotemos por b'_i sus imágenes respectivas en la localización $B_{\mathfrak{p}'} \simeq A'_{\mathfrak{p}'}$. Entonces $b'_i = a_i/f_i$, con $f_i \in A' \setminus \mathfrak{p}'$ para todo $i \in \{1, \ldots, n\}$. Como son un número finito, podemos coger $f := \prod_{i=1}^n f_i \in A' \setminus \mathfrak{p}'$ y escribir cada b'_i de la forma

$$b'_i := \frac{a_i \prod_{j \neq i} f_j}{f} \sim \frac{a_i}{f_i}.$$

Así, los b'_i están en la imagen de la aplicación $A'_f \longrightarrow B_f$, que es por tanto sobreyectiva. Pero es que además es inyectiva porque $A' \subseteq B$ y la localización preserva la inyectividad (4.3.20). Por tanto $A'_f \simeq B_f$ y queda probado el teorema.

$\square$

Usaremos la siguiente observación sobre espectros de anillos de polinomios para probar el primero de los lemas.

Observación 3.2.3. Si K es un cuerpo, y $K[X]$ un anillo de polinomios con coeficientes en K, entonces $Spec(K[X])$ no tiene puntos aislados.

Demostración. Como K es un cuerpo, $K[X]$ es un dominio de ideales principales, luego cada punto de $Spec(K[X])$ es de la forma (P) para cierto $P \in K[X]$, que además debe ser irreducible para que el ideal sea primo. Para que sea un punto aislado, debe ser abierto, es decir, debe existir un $F \in K[X]$ tal que $P \in D(F) \subseteq \{(P)\}$, donde

$$D(F) = \{\mathfrak{q} \in Spec(K[X]) \ : \ F \notin \mathfrak{q}\}.$$

Pero esto supone que $D(F) = \{(P)\}$, esto es, que existe cierto F para el cual P es el único irreducible de $K[X]$ que no lo divide. Esto es absurdo, pues F es producto de irreducibles de $K[X]$ (o irreducible él mismo) y existen infinitos irreducibles en dicho anillo, luego alguno de estos no dividirá a F. Por tanto, no hay abiertos $D(F)$ unipuntuales, y ningún punto puede ser aislado.

$\square$

Lema 3.2.4. ***[Lema 1]*** *Sean A y B dos anillos tales que existe $x \in B$ de manera que $B = A[x]$. Supongamos además que A es íntegramente cerrado en B. Si B es quasifinita sobre A en el ideal primo $\mathfrak{q}$, entonces $B_\mathfrak{p} = A_\mathfrak{p}$ con $\mathfrak{p} = \mathfrak{q} \cap A$.*

Demostración. Comencemos viendo que las hipótesis siguen siendo ciertas si sustituimos los anillos por sus localizaciones en $\mathfrak{p}$: como la localización es exacta (4.3.20) se mantienen las contenciones del enunciado; por 4.7.9, $A_\mathfrak{p}$ sigue siendo íntegramente cerrado en $B_\mathfrak{p}$; y la quasifinitud también se mantiene por localizaciones en virtud de la observación 3.1.9. Podemos suponer por tanto que A es local de ideal maximal $\mathfrak{p}$ y entonces $A_\mathfrak{p} \simeq A$ por el corolario 4.3.14. Es fácil comprobar que

$$B = A[x] \simeq A_\mathfrak{p}[\bar{x}] \simeq (A[x])_\mathfrak{p} = B_\mathfrak{p},$$

de modo que ahora nos reducimos a probar que $A \simeq B$.

Como $B = A[x]$ y A es íntegramente cerrado en B, basta comprobar que x es entero sobre A. Sea $K = A/\mathfrak{p}$ el cuerpo de residuos y consideremos la K-álgebra siguiente:

$$K[\bar{x}] \coloneqq A[x] \otimes_A K = B \otimes_A K(\mathfrak{p}),$$

donde la última igualdad se deduce de que $(A, \mathfrak{p})$ es local usando el corolario 4.3.14.

Por hipótesis, $\mathfrak{q}$ es un punto aislado en $Spec(B \otimes_A K(\mathfrak{p})) = Spec(K[\bar{x}])$, de modo que $\bar{x}$ debe ser algebraico sobre K, pues en caso contrario $K[\bar{x}]$ sería un anillo de polinomios en K y su espectro no tendría puntos aislados en virtud de la observación 3.2.3. Así pues, existe un polinomio $F \in A[X]$ (cuya clase en $K[X]$ no es una constante), tal que $\overline{F(x)} = 0$ o, de manera equivalente, $F(x) \in \mathfrak{p}A[x]$. El polinomio $P(X) \coloneqq F(X) - F(x)$ de $A[X]$ se anula en x y tiene al menos un coeficiente fuera de $\mathfrak{p}$ (pues hemos cogido F con imagen no constante en $K[X]$). Sea $H \in A[X]$

de grado mínimo entre los polinomios que se anulan en x y con al menos un coeficiente fuera de $\mathfrak{p}$. Supongamos que es de la forma

$$H(X) = a_m X^m + \cdots + a_0,$$

para ciertos $a_i \in A$. La ecuación $a^{m-1}H(x) = 0$ puede escribirse como

$$(a_m x)^m + a_{m-1}(a_m x)^{m-1} + \cdots + a_0 a_m^{m-1} = 0,$$

que es una ecuación de dependencia entera para $a_m x$ sobre A. Pero como A es íntegramente cerrado, esto implica que $a_m x \in A$. Por tanto podemos considerar el siguiente polinomio de $A[X]$,

$$(a_m x + a_{m-1})X^{m-1} + \cdots + a_0,$$

que se anula en x. Como tiene grado menor que m, por la elección de H sabemos que todos sus coeficientes deben estar en $\mathfrak{p}$. En particular, $a_m x + a_{m-1} \in \mathfrak{p}$. Para concluir que x es entero sobre A separemos en dos casos:

1. Si $a_{m-1} \in \mathfrak{p}$, entonces $a_m x \in \mathfrak{p}$ por ser este un ideal. Como además es primo, o bien $x \in \mathfrak{p} \subseteq A$ o bien $a_m \in \mathfrak{p}$. Pero el segundo caso no se puede dar, pues hemos supuesto que alguno de los coeficientes de H no está en $\mathfrak{p}$.

2. Si $a_{m-1} \notin \mathfrak{p}$, entonces $a_m \notin \mathfrak{p}$ tampoco (pues $a_m x + a_{m-1} \in \mathfrak{p}$ y $\mathfrak{p}$ es un ideal). Pero, como $(A, \mathfrak{p})$ es un anillo local, por la caracterización 4.3.4, a_m es una unidad de dicho anillo. Sabíamos además que $a_m x$ es entero sobre A, así que x es de hecho entero sobre A como queríamos, pues $A[x]$ es isomorfa a $A[a_m x]$ como A-álgebra.

□

El siguiente lema es el único cuya demostración no detallamos: aunque es sencilla, requiere de los teoremas de ascenso y descenso («going-up» y «going-down»), que no hemos desarrollado en los prerrequisitos. Puede consultarse en [9] o [6].

Lema 3.2.5. ***[Lema 2]*** *Sea B un dominio de integridad que contiene un anillo de polinomios $A[X]$ como subanillo y que es entero sobre él. Entonces B no es quasifinita sobre A en ningún ideal primo.*

Lema 3.2.6. ***[Lema 3]*** *Sean $A \subseteq A[x] \subseteq B$ anillos tales que B es entero sobre $A[x]$ y A es íntegramente cerrado en B. Si existe un polinomio mónico $F \in A[X]$ tal que $F(x)B \subseteq A[x]$, entonces $A[x] = B$.*

Demostración. Para ver la contención que falta, sea $b \in B$ arbitrario. Por hipótesis $F(x)b \in A[x]$ y en consecuencia existe un cierto polinomio $G \in A[X]$ tal que $F(x)b = G(x)$. Como F es mónico podemos hacer la división de G entre él:

$$G = QF + R \quad degR < degF \quad Q, R \in A[X].$$

Si tomamos $c := b - Q(x)$ y evaluamos la ecuación anterior en x, obtenemos

$$F(x)b = G(x) = Q(x)F(x) + R(x),$$

de donde,

$$F(x)c = R(x). \tag{3.2.6.1}$$

Para ver que $b \in A[x]$, basta ver que $c \in A[x]$ y, en particular, si vemos que $c \in A$ también se tiene el resultado. Como A coincide con su clausura íntegra en B por hipótesis, basta probar que c es entero sobre A para concluir. Sea pues A' la imagen de A en la localización B_c. La ecuación 3.2.6.1 puede considerarse en A'_c y en tal caso, reorganizando términos, tenemos la relación siguiente para $x/1 \in B_c$:

$$F\left(\frac{x}{1}\right) - \frac{R(x/1)}{c} = 0.$$

Como $degR < degF$ el polinomio $F - R/c \in A'_c[X]$ anterior es mónico por serlo F, de tal manera que la de arriba es una ecuación de dependencia entera para $x/1$ en A'_c.

Ahora bien, como B es entero sobre $A[x]$ por hipótesis y esta propiedad se mantiene por localizaciones (4.7.8), B_c lo es sobre $(A[x])_c$. A su vez, este anillo es entero sobre A'_c, pues acabamos de ver que $x/1$ es entero sobre A'_c. Usando la transitividad de la integridad 4.6.8, concluimos que B_c es entero sobre A'_c y en particular $c/1 \in B_c$ lo es. Satisface por tanto una ecuación de dependencia entera con coeficientes en A'_c (esto es, de la forma a/c^i, donde $a \in A$ y i un natural positivo). Multiplicando los numeradores por las cantidades adecuadas, se puede obtener dicha ecuación con un denominador común c^N:

$$\left(\frac{c}{1}\right)^n + \left(\frac{a_{n-1}}{c^N}\right)\left(\frac{c}{1}\right)^{n-1} + \cdots + \frac{a_0}{c^N} = 0,$$

con los $a_i \in A$. Esta ecuación está considerada en B_c (o bien $A'_c \subseteq B_c$), por tanto podemos multiplicar todo por c^N para obtener el elemento de B siguiente

$$\tilde{b} := c^{n+N} + a_{n-1}c^{n-1} + \cdots + a_0,$$

cuya imagen en B_c es cero. Por la definición de la relación de equivalencia de la localización, esto equivale a que exista un elemento t en el conjunto multiplicativamente cerrado correspondiente (en este caso $t = c^j$ para cierto $j > 0$) tal que $t\tilde{b} = 0$. Este producto da lugar a una ecuación de dependencia entera para c en A:

$$c^{n+j+N} + a_{n-1}c^{n+j-1} + \cdots + a_0c^j = 0;$$

de modo que c es efectivamente entero sobre A, como queríamos.

□

Antes del último lema debemos introducir el concepto de *conductor* de una álgebra y algunas propiedades inmediatas de este objeto.

Definición 3.2.7. [Conductor] Sean A un anillo y B una A-álgebra. El *conductor* de B en A es el conjunto

$$\mathfrak{f}(B/A) := \{a \in A \ : \ aB \subseteq A\}.$$

Observación 3.2.8.

1. El conductor $\mathfrak{f}(B/A)$ es un ideal de A y de B. De hecho, es el más grande de los ideales de A que también lo son de B.

2. Si S es un subconjunto multiplicativamente cerrado de A, entonces

$$S^{-1}\mathfrak{f}(B/A) \subseteq \mathfrak{f}(S^{-1}B/S^{-1}A),$$

y la inclusión es una igualdad si B es una A-álgebra finita.

Demostración.

1. En cualquier caso el conductor no es vacío (el cero está)y es estable para la suma pues si $x, y \in \mathfrak{f}(B/A)$, $xb, yb \in A$ para todo $b \in B$, luego $(x+y)b = xb+yb \in A$ también. Falta ahora ver que cumple la propiedad multiplicativa de los ideales para A y para B, por similitud de los argumentos veamos por ejemplo que para todos $a \in A$ y $x \in \mathfrak{f}(B/A)$, $ax \in \mathfrak{f}(B/A)$. Basta notar que si b es un elemento de B, entonces $xb \in A$ por ser x un elemento del conductor, y entonces $axb \in A$.
   Para la maximalidad, sea I un ideal de A que también lo es de B. Entonces para cada $x \in I$, $xB \subseteq I$ por ser I un ideal de B, y $I \subseteq A$ por serlo de A. Uniendo ambas $xB \subseteq A$, de modo que $x \in \mathfrak{f}(B/A)$ y el ideal está contenido en el conductor como queríamos demostrar.

2. Escribamos explícitamente los dos conjuntos a comparar:

$$C_1 := S^{-1}\mathfrak{f}(B/A) = \{a/s \ : \ a \in A, \ aB \subseteq A, \ s \in S\},$$

$$C_2 := \mathfrak{f}(S^{-1}B/S^{-1}A) = \{a/s \in S^{-1}A \ : \ (a/s)S^{-1}B \subseteq S^{-1}A\}.$$

   Dado $a/s \in C_1$, sea $b/s' \in S^{-1}B$ cualquiera: queremos probar que su producto $(ab)/(ss')$ está en $S^{-1}A$. No hace falta más que remarcar que $ab \in A$ por definición de C_1 y $ss' \in S$ por ser este estable por multiplicación de sus elementos.
   Supongamos ahora que B es finita sobre A y veamos que se da la otra contención. Dado $a/s \in C_2$ queremos ver que $a'B \subseteq A$ (o lo que es lo mismo, que $a' \in \mathfrak{f}(B/A)$) para cierto representante a'/s' de la clase de a/s. En particular, los elementos de la forma $a\tilde{s}/s\tilde{s}$ son representantes de dicha clase, por lo que basta ver que para nuestro a existe un $\tilde{s} \in S$ tal que $a\tilde{s} \in \mathfrak{f}(B/A)$. Como B es A-finita, sean $b_1, \ldots, b_n$ sus generadores como A-módulo. Para cada b_i de ellos se tiene que

$$\frac{a}{s}\frac{b_i}{1} \in S^{-1}A,$$

   por estar $a/s \in C_2$. Así pues, existen $a_i \in A$ y $s_i \in S$ tales que $ab_i/s = a_i/s_i$, esto es, existe un $t_i \in S$ tal que

$$(at_is_i)b_i = a_ist_i \in A.$$

   Si ahora tomamos $\tilde{s} := \prod_{i=1}^n t_is_i$, tenemos que $a\tilde{s}b_i \in A$ para todo $i = 1, \ldots, n$. Como todo elemento de B es combinación A-lineal finita de estos generadores, se tiene que $a\tilde{s} \in \mathfrak{f}(B/A)$, como queríamos.

□

Lema 3.2.9. ***[Lema 4]*** *Sean $A \subseteq A[x] \subseteq B$ anillos tales que B es de tipo finito sobre $A[x]$ y A es íntegramente cerrado en B. Si B es quasifinito sobre A en un ideal primo $\mathfrak{q}$, entonces $B_\mathfrak{p} = A_\mathfrak{p}$ con $\mathfrak{p} = \mathfrak{q} \cap A$.*

Demostración. Denotemos en esta demostración

$$\mathfrak{f} := \mathfrak{f}(B/A[x]) = \{\alpha \in A[x] \ : \ \alpha B \subseteq A[x]\}.$$

Vamos a probar primero el resultado en el caso en que $\mathfrak{f} \not\subseteq \mathfrak{q}$ y luego veremos que el otro caso no se puede dar por reducción al absurdo.

1. Empecemos con el caso en que $\mathfrak{f} \not\subseteq \mathfrak{q}$, sea $\mathfrak{r} := \mathfrak{q} \cap A[x]$ y sea $u \in \mathfrak{f} \setminus \mathfrak{q}$ cualquiera. Como $A[x]$ está contenido en B y la localización es exacta, la aplicación resultante $A[x]_u \longrightarrow B_u$ seguirá siendo inyectiva. Además, por pertenecer u al conductor, sabemos que $uB \subseteq A[x]$. En particular, dado un $b \in B$ cualquiera, existe un polinomio $P \in A[X]$ tal que $ub = P(x)$. Si consideramos ahora $b/1 \in B_u$, su clase en la localización será por tanto la misma que la de $P(x)/u$, que es un elemento de $A[x]_u$. Más en general, un elemento b/u^i cualquiera de

B_u coincidirá con $P(x)/u^{i+1}$, de modo que la aplicación anterior es también sobreyectiva y se tiene que

$$A[x]_u \simeq B_u.$$

A continuación vamos a utilizar el tercer apartado del lema 3.1.13 para los anillos $A \subseteq A[x] \subseteq B$, esto es, el anillo C del enunciado será $A[x]$ aquí. Como B es entero sobre A, $\exists u \in \mathfrak{f} \setminus \mathfrak{q} \subseteq A[x] \setminus \mathfrak{q}$ tal que $A[x]_u \simeq B_u$ y B es quasifinito sobre A en $\mathfrak{q}$ por hipótesis, se verifican todas las hipótesis del lema, así que $A[x]$ es quasfinito sobre A en $\mathfrak{r}$. Utilizando esto y que A es íntegramente cerrada en $A[x]$ por serlo en $B \supseteq A[x]$, el lema 1 (3.2.4) nos permite concluir que

$$A[x] \simeq A_{\mathfrak{p}},$$

para $\mathfrak{p} = \mathfrak{r} \cap A = \mathfrak{q} \cap A$.

Además de todo lo anterior, como B es finita sobre $A[x]$, $B_{\mathfrak{p}}$ es finita sobre $A[x]_{\mathfrak{p}} = A_{\mathfrak{p}}$ (ver lema 4.3.22). Y, por el corolario 4.7.9, como A es íntegramente cerrado en B, $A_{\mathfrak{p}}$ lo es en $B_{\mathfrak{p}}$. Siendo $B_{\mathfrak{p}}$ finita sobre $A_{\mathfrak{p}}$, en particular es entera sobre él, pero como $A_{\mathfrak{p}}$ es íntegramente cerrada en $B_{\mathfrak{p}}$, se concluye que

$$A_{\mathfrak{p}} \simeq B_{\mathfrak{p}}.$$

2. Supongamos $\mathfrak{f} \subseteq \mathfrak{q}$ e intentemos llegar a un absurdo. Sea $\mathfrak{n} \subseteq \mathfrak{q}$ un ideal primo de B minimal para la inclusión entre los que contienen a $\mathfrak{f}$. Sea t la clase de x en $B/\mathfrak{n}$ y $\mathfrak{m} = \mathfrak{n} \cap A$. Se tiene entonces que

$$A/\mathfrak{m} \subseteq (A/\mathfrak{m})[t] \subseteq B/\mathfrak{n}$$

y sabemos que $B/\mathfrak{n}$ es entero sobre $(A/\mathfrak{m})[t]$ en virtud de la proposición 4.7.8. Además, al ser B quasifinita sobre A en $\mathfrak{q}$, $B/\mathfrak{n}$ lo es sobre $A/\mathfrak{m}$ en $\mathfrak{q}/\mathfrak{n}$ por la observación 3.1.9.

Como $B/\mathfrak{n}$ es entero sobre $(A/\mathfrak{m})[t]$, si este último fuera un anillo de polinomios (esto es, si t fuera trascendente), el *lema 2* (3.2.5) prueba que $B/\mathfrak{n}$ no es finita sobre $A/\mathfrak{m}$ en ningún ideal primo, contradiciendo lo anterior. Así pues, t debe ser algebraico sobre $A/\mathfrak{m}$.

Veamos que todas las propiedades que estamos utilizando se mantienen si hacemos la extensión de escalares $A \longrightarrow A_{\mathfrak{m}}$: por exactitud de la localización (4.3.20), se tiene que $A_{\mathfrak{p}} \subseteq A_{\mathfrak{p}}[\bar{x}] \subseteq B_{\mathfrak{p}}$; por 4.3.22, $B_{\mathfrak{p}}$ sigue siendo finita sobre $A_{\mathfrak{p}}$; por 4.7.9, $A_{\mathfrak{p}}$ sigue siendo íntegramente cerrado en $B_{\mathfrak{p}}$; y la quasifinitud se deduce de 3.1.9. Por tanto, basta probar el resultado para el caso en que $(A, \mathfrak{m})$ es un anillo local. Denotemos ahora $\mathfrak{n}' := \mathfrak{n} \cap A[x]$, que es un ideal primo de $A[x]$ por ser contracción de un ideal primo de B, y por tanto $A[x]/\mathfrak{n}'$ es un dominio de integridad.

Como además t es algebraico sobre el cuerpo $A/\mathfrak{m}$, existe un polinomio $\overline{P} \in (A/\mathfrak{m})[X]$ tal que $\overline{P}(t) = 0$. Por tanto $P(x) \in \mathfrak{n}'$, y cada «polinomio» en x del dominio $A[x]/\mathfrak{n}'$ tiene un representante módulo $\mathfrak{n}'$ de «grado» menor que el de P. Así que $A[x]/\mathfrak{n}'$ es una $A/\mathfrak{m}$-álgebra finita. Utilizando ahora el lema 4.3.22, $A[x]/\mathfrak{n}'$ es de hecho un cuerpo. En consecuencia, $\mathfrak{n}'$ es maximal en $A[x]$, y como B es entero sobre $A[x]$, por la proposición 4.7.6, el ideal $\mathfrak{n}$ de B debe ser maximal, y $B/\mathfrak{n}$ es por tanto un cuerpo. Al ser t algebraico sobre $A/\mathfrak{m}$, existe un polinomio mónico $F \in A[X]$ cuya clase módulo $\mathfrak{m}$ se anula en t. Equivalentemente, $F(x) \in \mathfrak{n}$, pues t es la clase de x módulo $\mathfrak{n}$.

Habiendo escogido $\mathfrak{n}$ minimal entre todos los ideales primos de B que contienen a $\mathfrak{f}$, por la exactitud de las localizaciones (4.3.20) se mantienen las contenciones y $\mathfrak{n}B_{\mathfrak{n}}$ es minimal entre los primos de $B_\mathfrak{n}$ que contienen a $\mathfrak{f}_\mathfrak{n}$. De hecho, si $\mathfrak{w}$ es otro ideal primo de $B_\mathfrak{n}$ que contiene a $\mathfrak{f}_\mathfrak{n}$, debe provenir de un ideal primo de B que contiene a $\mathfrak{f}$. Pero esto es absurdo pues los ideales primos de la localización están en biyección con los ideales primos del anillo que no cortan a la parte $S = B \setminus \mathfrak{n}$, y este ideal tiene una parte (al menos $\mathfrak{f}$) dentro de $\mathfrak{n}$, y si fuera distinto, tendría otra parte en S. De modo que $\mathfrak{n}B_\mathfrak{n}$ es el único ideal primo de $B_\mathfrak{n}$ que contiene a $\mathfrak{f}_\mathfrak{n}$, esto es, su radical:

$$\mathcal{N}(\mathfrak{f}_\mathfrak{n}) = \mathfrak{n}B_\mathfrak{n}.$$

Por tanto, para cada elemento de $\mathfrak{n}B_\mathfrak{n}$ existe un natural positivo tal que, al elevarlos a dicha potencia, pertenecen a $\mathfrak{f}_\mathfrak{n}$. En particular, hemos visto antes que $F(x) \in \mathfrak{n}$, por tanto su clase $F(x)/1$ en la localización en $\mathfrak{n}$ pertenecerá a $\mathfrak{n}B_\mathfrak{n}$, así que existe $r > 0$ tal que $(F(x)/1)^r \in \mathfrak{f}_\mathfrak{n}$. Volviendo desde la localización al anillo B original, existe $y \in B \setminus \mathfrak{n}$ tal que $yF(x)^r \in \mathfrak{f} \subseteq A[x]$ (donde la última contención se deduce de la definición de $\mathfrak{f}$. Aplicando el *lema 3* (3.2.6) con $A \subseteq A[x] \subseteq B'$, donde $B' := A[x][yB]$ y $F' := F^r$ (que sigue siendo mónico por serlo F), deducimos que $B' = A[x]$, de manera que $yB \subseteq A[x]$. Por definición del conductor, $y \in \mathfrak{f} \subseteq \mathfrak{n}$, ¡pero esto contradice la definición de y! Hemos llegado a un absurdo que nos muestra que este segundo caso no es posible y que por tanto el lema siempre se verifica.

□

Antes de probar el teorema principal necesitamos el siguiente resultado auxiliar sobre subálgebras finitas y de tipo finito.

Lema 3.2.10. *Sean R un anillo, S una parte multiplicativamente cerrada del mismo, y A y B dos R-álgebras tales que B es de tipo finito sobre R y se tiene el isomorfismo de R-álgebras $S^{-1}A \simeq S^{-1}B$. Entonces existe una R-subálgebra finita de A, A_i, tal que*

$$S^{-1}B \simeq S^{-1}A_i.$$

Demostración. Como B es de tipo finito sobre R, existen ciertos $b_i \in B$, con $i = 1, \ldots, n$ tales que $B \simeq R[b_1, \ldots, b_n]$. Entonces

$$S^{-1}R[b_1/1, \ldots, b_n/1] \simeq S^{-1}B \simeq S^{-1}A.$$

Utilizando la proposición 4.8.13, sabemos que $S^{-1}A$ puede escribirse como unión de sus $S^{-1}R$-subálgebras de tipo finito, que son las localizaciones en S de las R-subálgebras de tipo finito de A, $(A_i)_{i\in I}$, en virtud de 4.3.22. Así pues,

$$S^{-1}B \simeq S^{-1}A = \bigcup_{i\in I} S^{-1}A_i.$$

Pero es que, para cada $k = 1, \ldots, n$ existe una subálgebra finita tal que $b_k/1 \in S^{-1}A_k$. El R-módulo engendrado por la unión de estas será todavía de tipo finito y por tanto una de las $S^{-1}A_i$. Así pues, existe un índice $z \in I$ tal que $S^{-1}B \simeq S^{-1}A_z$, pues la contención de las $S^{-1}A_z$ en $S^{-1}B$ se da siempre al ser subálgebras suyas, y para los índices mencionados antes se tiene la otra.

□

Como hemos venido anunciando, probamos ahora la **proposición 3.2.2** utilizando los lemas anteriores.

Demostración. Usaremos inducción sobre el número n de generadores de C como A-álgebra (que son una cantidad finita por ser C de tipo finito sobre A).

- Si $n = 0$, entonces $C = A$ y como B es finita sobre $C = A$, por el lema 4.6.7, B es entera sobre A. Y como A es íntegramente cerrada sobre B, se deduce que $B = A$ y en particular $B_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ para cualquier ideal primo $\mathfrak{p}$.

- Tomemos $n > 0$ y supongamos que la proposición ha sido probada para el caso en que C está generada por $n-1$ elementos. Escribamos $C \coloneqq A[x_1, \ldots, x_n]$ y sea A' la clausura íntegra de $R \coloneqq A[x_1, \ldots, x_{n-1}]$ en B. Se tiene entonces que

$$A' \subseteq A'[x_n] \subseteq B$$

y, como $C \longrightarrow B$ es finita y $C \subseteq A'[x_n]$, entonces B es finita sobre $A'[x_n]$.

Como B es finita sobre $A'[x_n]$ y quasifinita sobre A en $\mathfrak{q}$, por hipótesis, podemos aplicar el lema 3.1.11 y concluir que B es quasifinita sobre A' en $\mathfrak{q}$. Recapitulando, sabemos que B es finito sobre $A'[x_n]$, A' es íntegramente cerrado en B y B es quasifinito sobre A' en $\mathfrak{q}$, que son justamente las hipótesis del *lema 4* (3.2.9), y por tanto

$$B_{\mathfrak{p}'} \simeq A'_{\mathfrak{p}'},$$

donde $\mathfrak{p}' = \mathfrak{q} \cap A'$.

Denotemos por $(A'_i)_{i \in I}$ a las subálgebras de A' finitas sobre $R = A[x_1, \ldots, x_{n-1}]$. Utilizando el corolario 4.3.22 sabemos que las subálgebras de $A'_{\mathfrak{p}'}$ finitas sobre $R_{\mathfrak{p}'}$ serán justamente las localizaciones de estas, es decir $(A'_i)_{\mathfrak{p}'}$. Si denotamos $\mathfrak{p}'_i \coloneqq \mathfrak{q} \cap A'_i = \mathfrak{p}' \cap A_i$, de la observación 4.3.17 se tiene que $(A'_i)_{\mathfrak{p}'} \simeq (A'_i)_{\mathfrak{p}_i{}'}$ e invocando la proposición 4.8.13,

$$A'_{\mathfrak{p}'} = \bigcup_{i \in I} (A'_i)_{\mathfrak{p}'_i}.$$

Al ser B finita sobre C y C de tipo finito sobre A, B es de tipo finito sobre $A[x_1, \ldots, x_{n-1}] \supseteq A$. Al ser A' subanillo de B, también lo son las A'_i y, por exactitud de la localización, se mantiene esta inyectividad. Como B es de tipo finito sobre R, en virtud del lema 3.2.10, el homomorfismo

$$(A'_i)_{\mathfrak{p}'_i} \longrightarrow B_{\mathfrak{p}'_i} = B_{\mathfrak{q}} \tag{3.2.10.1}$$

es un isomorfismo para i «suficientemente grande».

Por otro lado, como B es quasifinita sobre A en $\mathfrak{q}$ por hipótesis, de la definición se deduce que $B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$ es finita sobre $K(\mathfrak{p})$, y del isomorfismo anterior se tiene que $(A'_i)_{\mathfrak{p}'_i}/\mathfrak{p}(A'_i)_{\mathfrak{p}'_i}$ es finita sobre $K(\mathfrak{p})$ también, de donde A'_i es quasifinita sobre A en $\mathfrak{p}'_i$.

Como $A'_i \subseteq A'$ para todo $i \in I$ y A' es la clausura íntegra de A en B, entonces A es íntegramente cerrado en A'_i. Además, $A[x_1, \ldots, x_{n-1}]$ es de tipo finito sobre A con $n-1$ generadores y A'_i es finita sobre $A[x_1, \ldots, x_{n-1}]$ por definición de las A'_i. Todas estas son las hipótesis del teorema para el caso de $n-1$ generadores, de modo que aplicando la hipótesis de inducción se concluye que $A_{\mathfrak{p}} \simeq (A'_i)_{\mathfrak{p}} \simeq (A'_i)_{\mathfrak{p}'_i}$, donde se ha hecho uso de la observación 4.3.17. Este isomorfismo, unido al de la ecuación 3.2.10.1, nos da el isomorfismo que queríamos

$$A_{\mathfrak{p}} \simeq B_{\mathfrak{p}},$$

usando que $B_{\mathfrak{p}} \simeq B_{\mathfrak{q}}$ gracias de nuevo a la observación 4.3.17.

□

3.3. Consecuencias del teorema principal

El resultado que acabamos de ver tiene implicaciones fundamentales en Álgebra Conmutativa, la más relevante es el *teorema de estructura local para álgebras étale y no-ramificadas*, que enunciamos a continuación sin poder dar su demostración por falta de tiempo. La tesis de este es que toda álgebra étale es localmente isomorfa a un álgebra estándar étale y, en el caso de las álgebras no-ramificadas, isomorfa aun cociente de una álgebra estándar étale. Incluimos también en esta sección dos corolarios del teorema, el segundo de los cuales también recibe a veces el nombre de *teorema principal de Zariski*.

Corolario 3.3.1. *Sean A un anillo, B una A-álgebra de tipo finito, el conjunto de puntos de $Spec(B)$ donde B es quasifinita sobre A es un abierto de $Spec(B)$.*

Demostración. Sea $\mathfrak{q}$ un ideal primo de B tal que B es quasifinito sobre A en él, y denotemos por A' la clausura íntegra de A en B. El teorema principal nos garantiza que existe un elemento $f \in A' \setminus \mathfrak{q}$ tal que $A'_f \simeq B_f$. Usando la proposición 4.8.13, podemos escribir

$$A' = \bigcup_{i \in I} A_i,$$

donde las A_i son A-subálgebras de A' de tipo finito que contienen a f. Notemos que, aunque se pierden álgebras al restringirnos a las que tienen a f de elemento, la igualdad sigue siendo válida, pues cada elemento de A' pertenece a una de sus A-subálgebras de tipo finito, y podemos considerar la subálgebra obtenida al añadirle f a esta, que por tanto está entre las A_i y contiene al elemento.

Sin embargo, como A' es entera sobre A, el lema 4.6.7 nos garantiza que las subálgebras de tipo finito A_i son de hecho finitas. Usando que las subálgebras de tipo finito de la localización en f son de hecho las localizaciones en f de las subálgebras de tipo finito (4.3.22), se tiene que

$$B_f \simeq A'_f = \bigcup_{i \in I} (A_i)_f.$$

Siendo B de tipo finito sobre A, su localización B_f lo es sobre A_f, y el lema 3.2.10 concluye que $B_f \simeq (A_i)_f$ para A_i suficientemente grande. Como las A_i son finitas sobre A y $f \in B$, usando el ejemplo 3.1.10, B_f es quasifinita sobre A. Se ha elegido f fuera de $\mathfrak{q}$, de modo que $\mathfrak{q} \in D(f) \simeq Spec(B_f)$ Así que $Spec(B_f)$ es un entorno abierto de $\mathfrak{q}$, y como B_f es quasifinita sobre A podemos decir que los puntos de dicho entorno «son quasifinitos».

□

Corolario 3.3.2. *Sean A un anillo, B una A-álgebra de tipo finito y quasifinita sobre A, y sea A' la clausura íntegra de A en B. Entonces:*

1. *$Spec(B) \longrightarrow Spec(A')$ es una inmersión abierta.*

2. *Existe una sub-A-álgebra A'' de A', finita sobre A, tal que $Spec(B) \longrightarrow Spec(A'')$ sea una inmersión abierta.*

Demostración.

1. Por ser B quasifinita sobre A en todos los puntos $\{\mathfrak{p}_i\}_{i \in I} = Spec(B)$, el teorema principal implica que, existen elementos $f_i \in A' \setminus \mathfrak{p}_i$ tales que $A'_{f_i} \simeq B_{f_i}$ y además $\mathfrak{p}_i \in D(f_i)$

por definición de los abiertos principales. Además, usando el corolario 4.10.11, $D(f_i) \simeq Spec(B_{f_i})$, de modo que

$$\{\mathfrak{p}_i\}_{i\in I} = Spec(B) = \bigcup_{i\in I} Spec(B_{f_i}).$$

Sin embargo, $Spec(B)$ es casicompacto (4.10.6), así que de este recubrimiento por abiertos se puede extraer un subrecubrimiento finito. Usando que $A'_{f_i} \simeq B_{f_i}$ en particular se tiene que $Spec(B_{f_i}) \simeq Spec(A'_{f_i})$ para todo i, así que la aplicación es abierta, y además es una inmersión puesto que

$$Spec(B) = \bigcup_{i=1}^{n} Spec(B_{f_i}) = \bigcup_{i=1}^{n} Spec(A'_{f_i}) = \bigcup_{i=1}^{n} D(f_i) \hookrightarrow Spec(A').$$

2. Acabamos de ver en la parte anterior que $Spec(B) = \cup_{1\leq i\leq n} Spec(B_{f_i})$ para ciertos elementos f_i de A' tales que $A'_{f_i} \simeq B_{f_i}$. El mismo argumento que hemos usado en el corolario anterior sobre subálgebras finitas de A' (basado en el lema 3.2.10) nos garantiza la existencia de una A-subálgebra de A', que denotaremos A'', tal que $f_1, \ldots, f_n$ pertenecen a A'' y además $B_{f_i} \simeq A''_{f_i}$ para cada i. Para concluir basta razonar como en el apartado 1 de este mismo corolario.

□

Definición 3.3.3. [**Álgebra étale/no-ramificada en un entorno de un ideal primo**] Sean A un anillo, B una A-álgebra y $\mathfrak{q}$ un ideal primo de B. Diremos que B es *no-ramificada (resp. étale) sobre A en un entorno de* $\mathfrak{q}$ si existe $f \in B\backslash\mathfrak{q}$ tal que B_f sea no-ramificada (resp. étale) sobre A.

Teorema 3.3.4. ***[Teorema de estructura local de álgebras étale y no-ramificadas]*** *Sean B una A-álgebra y $\mathfrak{q}$ un ideal primo de B por encima de un ideal primo de A, $\mathfrak{p}$. Se tienen las equivalencias siguientes para los casos étale y no-ramificado:*

1. ***Teorema de estructura para álgebras étale****. Son equivalentes las condiciones siguientes:*
   - *B es étale sobre A en un entorno de $\mathfrak{q}$.*
   - *Existen $f \in B \setminus \mathfrak{q}$ y $h \in A \setminus \mathfrak{p}$ tales que B_f es isomorfa como A-álgebra a una A_h-álgebra estándar étale, esto es, de la forma $C = (A_h[X]/P)_g$.*
2. ***Teorema de estructura para álgebras no-ramificadas****. Son equivalentes las condiciones siguientes:*
   - *B es no-ramificada sobre A en un entorno de $\mathfrak{q}$.*
   - *Existen $f \in B \setminus \mathfrak{q}$, $h \in A \setminus \mathfrak{p}$, una A_h-álgebra estándar étale C, y un morfismo sobreyectivo de A-álgebras $u : C \longrightarrow B_f$. Se tiene además que el morfismo*

     $$u \otimes_A id_{K(\mathfrak{p})} : C \otimes_A K(\mathfrak{p}) \longrightarrow B_f \otimes_A K(\mathfrak{p})$$

     es un isomorfismo de A-álgebras.

De otra forma, localmente sobre los espectros $Spec(B)$ y $Spec(A)$, una A-álgebra étale (resp. no-ramificada) B es estándar étale (resp. cociente de una álgebra estándar étale).

Capítulo 4

Anexo: Álgebra Conmutativa

Este anexo contiene los resultados de Álgebra Conmutativa que se han necesitado para el resto de la memoria. Las principales referencias son los manuales de Bosch y Atiyah-Macdonald ([2] y [1]), aunque hemos procurado en cada sección indicar los textos que se han seguido.

4.1. Ideales

Introduciremos en esta sección algunos resultados interesantes sobre ideales: qué forma tienen en productos y cocientes, cómo se transforman a través de morfismos de anillos, etc. Se definirán también dos ideales fundamentales de un anillo, su radical de Jacobson y su nilradial, que se obtendrán por intersección de todos los ideales maximales o primos del mismo. La principal referencia aquí ha sido [2].

Comenzamos con un teorema atribuido a Krull que, utilizando el lema de Zorn, nos garantiza la existencia de ideales maximales en un anillo no nulo.

Proposición 4.1.1. ***[Teorema de Krull]*** *Dado $A \neq 0$ un anillo, existe siempre un ideal maximal. En particular:*

1. *Para cada ideal propio $\mathfrak{a} \subset A$, existe un ideal maximal que lo contiene.*
2. *Para cada elemento x no unidad de A, existe un ideal maximal que lo contiene.*

Demostración. Sea Σ el conjunto de todos los ideales propios de A ordenado por inclusión. Σ es no vacío pues $0 \in \Sigma$. Dada una cadena $(\mathfrak{a}_t)_{t\in T}$ de ideales de Σ veamos que tiene un elemento maximal. Definimos $\mathfrak{a} := \bigcup_{t\in T} \mathfrak{a}_t$, que es un ideal de Σ por ser unión de una cadena de ideales y además $1 \notin \mathfrak{a}$ porque todos los ideales de Σ son propios. Así, $\mathfrak{a} \in \Sigma$ es una cota superior de la cadena. Invocando el lema de Zorn, Σ tiene un elemento maximal.

Para el enunciado (1) basta aplicar lo anterior al anillo $A/\mathfrak{a}$, de donde obtenemos un ideal $\mathfrak{m} + \mathfrak{a}$ maximal en el cociente. Como los ideales del cociente están en biyección con los de A que contienen a $\mathfrak{a}$ y la maximalidad se mantiene a través del isomorfismo, deducimos el ideal que queríamos. Finalmente para (2) no hay más que considerar el ideal $(x) \subsetneq A$.

□

Definición 4.1.2. [Espectro primo/espectro maximal] Dado A un anillo, se llama *espectro primo* (resp. *espectro maximal*) de A, al conjunto de sus ideales primos (resp. maximales). Se denota por $Spec(A)$ (resp. $Spm(A)$).

Observación 4.1.3. Dado un morfismo de anillos $\varphi : A \longrightarrow A'$, este induce una aplicación entre los espectros primos de ambos anillos de la manera siguiente:

$$Spec(\varphi) : Spec(A') \longrightarrow Spec(A), \ \ \mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p}).$$

Esto es, la imagen inversa por un morfismo de anillos de un ideal primo es un ideal primo. Esto no es cierto en general si se trata de ideales maximales en lugar de primos.

Demostración. Para un ideal primo $\mathfrak{p} \subset A'$ cualquiera, el morfismo φ induce un monomorfismo $\overline{\varphi} : A/\varphi^{-1}(\mathfrak{p}) \hookrightarrow A'/\mathfrak{p}$. Como $A'/\mathfrak{p}$ es un dominio por ser el ideal primo y $A/\varphi^{-1}(\mathfrak{p})$ puede considerarse subanillo vía $\overline{\varphi}$, este es también dominio, luego $\varphi^{-1}(\mathfrak{p})$ es un ideal primo de A. □

Observación 4.1.4. Sea A un anillo y $\mathfrak{a}$ un ideal del mismo. Es bien sabido que hay una biyección

$$\{ideales\ de\ A/\mathfrak{a}\} \longleftrightarrow \{ideales\ de\ A\ que\ contienen\ \mathfrak{a}\}, \tag{4.1.4.1}$$

y que dicha biyección preserva las contenciones. Este es un caso especial de la observación anterior, donde el morfismo de anillos es $\pi : A \longrightarrow A/\mathfrak{a}$. En esta situación, los ideales maximales (resp. primos) del cociente están en biyección con los ideales maximales (resp. primos) de A que contienen a $\mathfrak{a}$.

Demostración.

1. *Ideales primos.* Ya hemos probado en la observación anterior (4.1.3) que las imágenes inversas de ideales primos por cualquier morfismo de anillos son ideales primos también, y por la biyección (4.1.4.1), dicho ideal debe contener a $\mathfrak{a}$. Tomando ahora $\mathfrak{b} \in Spec(A)$ con $\mathfrak{a} \subseteq \mathfrak{b}$ veamos que $\pi(\mathfrak{b})$ es primo. Sean $c_1, c_2 \in A$ cualesquiera tales que $c_1c_2 + \mathfrak{a} \in \pi(\mathfrak{b})$. Entonces $c_1c_2 \in \mathfrak{b}$, que es primo, luego existe un $i \in \{1, 2\}$ tal que $c_i \in \mathfrak{b}$, de modo que $c_i + \mathfrak{a} \in \pi(\mathfrak{b})$.
2. *Ideales maximales.* Sea $\mathfrak{m}$ un ideal maximal de A que contiene a $\mathfrak{a}$. Entonces su imagen por π es un ideal de $A/\mathfrak{a}$ que debe ser maximal porque si no existiría otro ideal de $A/\mathfrak{a}$ que lo contiene. Y como la biyección de (4.1.4.1) preserva las contenciones, la imagen inversa de dicho ideal contendría estrictamente a $\mathfrak{m}$. El recíproco se razona igual.

□

Observación 4.1.5. Dada una familia finita de anillos $(A_i)_{i=1}^n$, es bien sabido que los ideales de un anillo producto $\prod_{i=1}^n A_i$ son de la forma $\prod_{i=1}^n \mathfrak{a}_i$ donde cada $\mathfrak{a}_i$ es ideal de A_i. En particular, es fácil deducir que los ideales primos (resp. maximales) de dicho anillo producto son también producto de ideales primos (resp. maximales) de los anillos correspondientes, con la salvedad de que algunos de ellos pueden coincidir con el anillo total A_i correspondiente y seguimos obteniendo un ideal primo (resp. maximal).

Definición 4.1.6. [Radical de Jacobson] Sea A un anillo. El *radical de Jacobson*, $\mathcal{J}(A)$, de A es el ideal resultante de la intersección de todos sus ideales maximales.

Lema 4.1.7. *Dado un anillo A, para $a \in A$ son equivalentes:*

1. $a \in \mathcal{J}(A)$.
2. $1 - ab$ *es una unidad de A para cada $b \in A$.*

Demostración.
(1) $\implies$ (2) Si $1 - ab$ no es una unidad, por el teorema de Krull sabemos que está contenido en un ideal maximal de A, $\mathfrak{m} \subset \mathcal{J}(A)$. Pero como $ab \in \mathfrak{m}$, esto supone también que $1 \in \mathfrak{m}$, lo que es absurdo.
(2) $\implies$ (1) Si a no está en el radical de Jacobson de A, existe $\mathfrak{m}$ ideal maximal tal que $a \notin \mathfrak{m}$, y como $\mathfrak{m} \subset < \mathfrak{m} \cup \{a\} >$, este segundo ideal debe ser el total. Así que deben existir $m \in \mathfrak{m}$, $b \in A$ tales que $ab + m = 1$, de donde $1 - ab \in \mathfrak{m}$, y en consecuencia no es una unidad.

□

Definición 4.1.8. [**Nilradical**] Sea A un anillo. El *nilradical*, $\mathcal{N}(A)$, de A es el ideal resultante de la intersección de todos sus ideales primos. Si $\mathcal{N}(A) = 0$, el anillo se llama *reducido*. En particular, el anillo $A_{red} = A/\mathcal{N}(A)$ se llama *anillo reducido de A*.

Veamos ahora que también podemos caracterizar el nilradical como el ideal de A dado por todos los elementos nilpotentes del anillo. Hemos dado la definición como intersección de ideales primos para deducir de inmediato que $\mathcal{N}(A)$ es un ideal. Si hubiéramos dado esta caracterización como definición habría tocado ver que efectivamente los elementos nilpotentes de un anillo son un ideal, mientras que ahora vendrá «de regalo» al probar la igualdad de conjuntos.

Proposición 4.1.9. *Sea A un anillo. Su nilradical $\mathcal{N}(A)$ es también el subconjunto formado por todos los elementos nilpotentes de A.*

Demostración. Dado un elemento $f \in A$ nilpotente, existe $n \in \mathbb{N}$ tal que $f^n = 0$ y si $\mathfrak{p}$ un ideal primo, entonces $f^n = 0 \in \mathfrak{p}$ implica que $f \in \mathfrak{p}$, luego un elemento nilpotente pertenece a cualquier ideal primo de A. Recíprocamente, si f no es nilpotente, sea Σ el conjunto de ideales $\mathfrak{a}$ de A con $f^n \notin \mathfrak{a}$ para todo $n \in \mathbb{N}$. Entonces $\Sigma \neq \emptyset$ porque $0 \in \Sigma$, luego se puede aplicar el lema de Zorn al conjunto Σ ordenado por la inclusión, de donde deducimos la existencia de un elemento maximal $\mathfrak{p}$. Queremos ver que dicho ideal es primo, pues entonces, por definición de Σ, $f \notin \mathfrak{p}$ y por tanto no está en la intersección de todos los ideales primos de A. Dados $x, y \notin \mathfrak{p}$, los ideales $\mathfrak{p} + (x)$ y $\mathfrak{p} + (y)$ contienen a $\mathfrak{p}$ estrictamente, y por maximalidad de este no pueden pertenecer a Σ. De modo que existen $m, n \in \mathbb{N}$ tales que

$$f^m \in \mathfrak{p} + (x), \quad f^n \in \mathfrak{p} + (y).$$

De modo que $f^{m+n} \in \mathfrak{p} + (xy)$, esto es, $\mathfrak{p} + (xy)$ no está en Σ, y por tanto $xy \notin \mathfrak{p}$, de donde se deduce que $\mathfrak{p}$ es un ideal primo como queríamos.

□

Como cada ideal maximal es en particular primo, es inmediato el siguiente corolario.

Corolario 4.1.10. *Dado un anillo A, su nilradical está contenido en su radical de Jacobson,*

$$\mathcal{N}(A) \subseteq \mathcal{J}(A).$$

Lema 4.1.11. *Sea A un anillo y $x \in A$ un elemento nilpotente de A. Entonces $1 + x$ es una unidad de A.*

Demostración. Como x es nilpotente, existe un $n \in \mathbb{N}$ tal que $x^n = 0$. Así, se tiene la igualdad

$$1 = 1 + x^n = (1 + x)(1 - x + \cdots + x^{n-1}),$$

de donde se deduce que $(1 + x)$ tiene inverso.

□

Definición 4.1.12. **[Nilideal]** Dado A un anillo, decimos que un ideal I de A es un *nilideal* de A si está formado por elementos nilpotentes, es decir, $I \subseteq \mathcal{N}(A)$. En particular, el nilradical de A es un nilideal de A. En la literatura inglesa se suele denominar *ideal localmente nilpotente.*

Fijado un ideal $\mathfrak{a}$ de un anillo A, podemos hablar también de su radical de Jacobson (resp. nilradical) como la intersección de todos los ideales maximales (resp. primos) de A que lo contienen. En este caso, el nilradical de $\mathfrak{a}$ se suele denotar por $\sqrt{\mathfrak{a}}$ en lugar de $\mathcal{N}(\mathfrak{a})$. Por otro lado, a causa de la relación biunívoca entre ideales de un anillo que contienen a un ideal dado, e ideales del anillo cociente por dicho ideal, estos radicales pueden entenderse como los del anillo cociente $A/\mathfrak{a}$. Concretamos esta idea en el lema siguiente.

Lema 4.1.13. *Dado A un anillo y $\mathfrak{a} \subset A$ un ideal. Sea $\pi : A \longrightarrow A/\mathfrak{a}$ el paso el cociente. Entonces:*

1. $\mathcal{J}(\mathfrak{a}) = \pi^{-1}(\mathcal{J}(A/\mathfrak{a}))$.
2. $\mathcal{N}(\mathfrak{a}) = \pi^{-1}(\mathcal{N}(A/\mathfrak{a}))$.

Demostración. Basta recordar que π define una biyección entre los ideales de $A/\mathfrak{a}$ y los de A que contienen a $\mathfrak{a}$, y que dicha biyección preserva la relación de contención. De aquí se deduce que dicha biyección se puede restringir a una entre los ideales maximales (resp. primos) de $A/\mathfrak{a}$ y los ideales maximales (resp. primos) de A que contienen $\mathfrak{a}$.

$\square$

Observación 4.1.14. Utilizando el lema anterior y la caracterización del nilradical de $A/\mathfrak{a}$ como el conjunto de sus elementos nilpotentes, se deduce fácilmente la siguiente igualdad:

$$\mathcal{N}(\mathfrak{a}) = \{a \in A \,:\, a^n \in \mathfrak{a} \, \textit{para cierto} \, n \in \mathbb{N}\}.$$

El ideal $\mathfrak{a}$ se llamará *reducido* si $\mathcal{N}(\mathfrak{a}) = \mathfrak{a}$.

Terminamos esta sección con dos lemas técnicos sobre ideales primos.

Lema 4.1.15. *Sea A un anillo, $\mathfrak{a} \subset A$ un ideal y $\mathfrak{p}_1, ..., \mathfrak{p}_n \subset A$ ideales primos tales que $\mathfrak{a} \subset \bigcup_{j=1}^n \mathfrak{p}_j$. Entonces existe un índice $i \in \{1, ..., n\}$ tal que $\mathfrak{a} \subset \mathfrak{p}_i$.*

Demostración. Razonamos por inducción sobre n. El caso $n = 1$ es trivial. Si $n > 1$, supongamos por reducción al absurdo que tenemos la contención $\mathfrak{a} \subset \bigcup_{j=1}^n \mathfrak{p}_j$ pero $\mathfrak{a} \not\subset \mathfrak{p}_i$ para todo $i = 1, ..., n$. Por hipótesis de inducción tenemos que $\mathfrak{a} \not\subset \bigcup_{j \neq i} \mathfrak{p}_j$ para todo $i = 1, ..., n$, pues si para algún i se diera la contención anterior se debería dar también una de las que hemos supuesto que no se dan por la hipótesis de inducción. En consecuencia, para cada i existe un elemento

$$a_i \in \mathfrak{a} \setminus \bigcup_{j \neq i} \mathfrak{p}_j \subset \mathfrak{p}_i.$$

Definimos así los elementos

$$b_i := \prod_{j \neq i} a_j \in \prod_{j \neq i} \mathfrak{p}_j, \quad i = 1, ..., n,$$

de manera que b_i pertenece a $\mathfrak{a}$ y para $j \neq i$ también a $\mathfrak{p}_j$, pero no a $\mathfrak{p}_i$ pues en ese caso, por ser este un ideal primo, algún a_j debería estar en él, y hemos elegido los a_j para que esto no pase si $j \neq i$. Por tanto,

$$b := \sum_{j=1}^n b_j$$

es un elemento de $\mathfrak{a}$ que no puede pertenecer a ninguno de los $\mathfrak{p}_i$ para $i = 1, ..., n$. Pero entonces $\mathfrak{a} \not\subset \bigcup_{j=1}^{n} \mathfrak{p}_j$, contradiciendo la hipótesis.

□

Lema 4.1.16. *Sea A un anillo, $\mathfrak{a}_1, ..., \mathfrak{a}_n \subset A$ ideales, y $\mathfrak{p} \subset A$ un ideal primo tal que $\bigcap_{j=1}^{n} \mathfrak{a}_j \subset \mathfrak{p}$. Entonces existe un índice $i \in \{1, ..., n\}$ tal que $\mathfrak{a}_i \subset \mathfrak{p}$. Si de hecho se tiene $\bigcap_{j=1}^{n} \mathfrak{a}_j = \mathfrak{p}$, entonces $\mathfrak{a}_i = \mathfrak{p}$ para el índice i anterior.*

Demostración. Razonando por reducción al absurdo, supongamos que $\bigcap_{j=1}^{n} \mathfrak{a}_j \subset \mathfrak{p}$ pero $\mathfrak{a}_j \not\subset \mathfrak{p}$ para $j = 1, ..., n$. Entonces para cada j podemos escoger $a_j \in \mathfrak{a}_j \setminus \mathfrak{p}$, y usando que $\mathfrak{p}$ es un ideal primo, $a_1 \cdots a_n \in (\bigcap_{j=1}^{n} \mathfrak{a}_j) \setminus \mathfrak{p}$, lo que contradice la inclusión $\bigcap_{j=1}^{n} \mathfrak{a}_j \subset \mathfrak{p}$.

□

4.2. Módulos

En esta sección se revisan algunos conceptos y resultados relacionados con los módulos. Estos, que son generalizaciones de los espacios vectoriales donde el cuerpo de escalares es sustituido por un anillo, ya han sido tratados por el alumno en una asignatura del grado, así que se presentan aquí solo los resultados nuevos. Se evita por ejemplo introducir formalmente la definición de los mismos, de módulo libre, o de sus submódulos, cocientes y morfismos. Sí que presentamos la noción de álgebra, que va un paso más allá que la de módulo y pide que el conjunto tenga además una estructura de anillo que sea compatible con la de módulo. Se hará especial hincapié en la diferencia entre álgebras finitas, de tipo finito y de presentación finita, que será fundamental en el trabajo. Terminaremos con una subsección sobre sucesiones exactas, una herramienta del Álgebra Homológica muy utilizada en Álgebra Conmutativa y en particular en esta memoria.

Definición 4.2.1. [**Álgebra**] Dado un anillo A, llamamos *A-álgebra (asociativa, conmutativa y unitaria)* a un anillo B que presenta estructura de A-módulo y tal que, para todos $x, y \in B$, $a \in A$ se da la regla de compatibilidad $a * (x \cdot y) = (a * x) \cdot y = x \cdot (a * y)$, donde $*$ denota el producto por escalares como A-módulo y $\cdot$ el producto del anillo. De ahora en adelante denotaremos ambos productos de la misma manera (con un pequeño espacio o con el punto $\cdot$) salvo que se requiera distinguirlos.

Definición 4.2.2. [**Morfismo de álgebras**] Dado un anillo A y dos A-álgebras B y C, un *homomorfismo de A-álgebras* es una aplicación $B \longrightarrow C$ que es homomorfismo con respecto a las estructuras de anillo y de módulo. Esto es, un homomorfismo de anillos ϕ tal que, si $a \in A, b \in B$, $\phi(ab) = a\,\phi(b)$.

Observación 4.2.3. Dado un homomorfismo de anillos $f : A \longrightarrow B$, B puede entenderse como una A-álgebra sin más que considerar el producto $a * x := f(a) \cdot x$ para $a \in A$ y $x \in B$. Recíprocamente, para cualquier A-álgebra B, la aplicación

$$f : A \longrightarrow B, \;\; a \longmapsto a \cdot 1_B,$$

define un homomorfismo de anillos tal que la estructura de A-álgebra de B coincide con la inducida por f. De hecho, para equipar a un anillo B con la estructura de A-álgebra basta indicar un homomorfismo de anillos $A \longrightarrow B$ que se llamará *estructural*. Así, se podrá hablar indistintamente de «el álgebra $A \longrightarrow B$» o «el A-álgebra B».

De hecho, visto así, un homomorfismo φ entre dos A-álgebras B y C es un homomorfismo de anillos $B \longrightarrow C$ compatible con los homomorfismos estructurales respectivos, es decir, que permite que el diagrama siguiente sea conmutativo.

$$\begin{tikzcd} A \arrow[r] \arrow[d] & C \\ B \arrow[ur, "\varphi"] & \end{tikzcd} \tag{4.2.3.1}$$

Ejemplo 4.2.4. Algunos ejemplos de módulos y álgebras:

- Si dado un anillo A consideramos su estructura de A-módulo, entonces sus submódulos no son otros que los ideales del anillo.
- Si B es un subanillo de un anillo A, entonces A es una álgebra sobre B.

4.2.1. Finitud para módulos y álgebras

Los conceptos que se introducen en este epígrafe serán utilizados constantemente en el resto del trabajo. Se comienza revisitando la suma, el producto y la suma directa de módulos, así como el producto de un módulo por un ideal de su anillo de escalares. Estaremos entonces en condiciones de definir las tres nociones de finitud para álgebras (finitas, de tipo finito y de presentación finita), y terminaremos probando el famoso lema de Nakayama en distintas versiones. En esta sección M denotará un módulo sobre un anillo A.

Definición 4.2.5. **[Suma de módulos]** Dada una familia $(N_i)_{i\in I}$ de submódulos de M, el conjunto

$$N \coloneqq \sum_{i\in I} N_i = \Big\{\sum_{i\in I} x_i \,:\, x_i \in N,\, x_i = 0 \text{ } \textit{para casi todo } \text{ } i \in I\Big\}$$

es un submódulo de M al que se llama *suma* de los submódulos N_i.
En particular, si consideramos una familia $(x_i)_{i\in I}$ de elementos de M, la suma de los A-módulos libres $(Ax_i)_{i\in I}$,

$$\sum_{i\in I} Ax_i = \{\sum_{i\in I} a_i x_i \;\; : a_i \in A,\, a_i = 0 \text{ } \textit{para casi todo } \text{ } i \in I\},$$

se llama *submódulo generado por los* x_i, $i \in I$ y resulta ser además el menor submódulo de M que contiene a todos los x_i.

Definición 4.2.6. **[Módulo finitamente generado/Álgebra finita]** Un A-módulo se dice que es *finitamente generado* o *de tipo finito* si puede expresarse como módulo generado por una cantidad finita de elementos. Una A-álgebra B se llama *finita* si, como A-módulo, es de tipo finito. También, si $\varphi : A \longrightarrow B$ es el morfismo estructural de B como A-álgebra, decimos que φ es un morfismo *finito* si B es finita como A-álgebra.

Proposición 4.2.7. *Dado un anillo A, y $N \subset M$ dos A-módulos, si M es de finitamente generado sobre N y este lo es sobre A, entonces M es finitamente generado sobre A.*

Demostración. Si los $y_1, ..., y_n$ generan M sobre N y $x_1, ..., x_m$ generan N sobre A, entonces los productos $x_i y_j$ con $i = 1, ..., n$ y $j = 1, ..., m$ generan M sobre A.

□

No debe confundirse una álgebra finita (que, como hemos dicho antes, es aquella que como módulo sobre el anillo correspondiente es de tipo finito) con una álgebra de tipo finito, que introducimos en la definición siguiente.

Definición 4.2.8. **[Álgebra de tipo finito/presentación finita]** Sean A un anillo y B una A-álgebra.

1. Decimos que B es *tipo finito sobre A* si existen un $n \in \mathbb{N}$ y un epimorfismo $\varphi : A[X_1, \ldots, X_n] \longrightarrow B$. Usando el primer teorema de isomorfía, esto equivale a que exista un ideal I de $A[X_1, \ldots, X_n]$ tal que
$$B \simeq A[X_1, \ldots, X_n]/I.$$

2. Decimos que B es *de presentación finita sobre* A si el núcleo del epimorfismo anterior es un ideal finitamente generado, esto es, si existe un $m \in \mathbb{N}$ y elementos $f_1, \dots, f_m \in A[X_1, \dots, X_n]$ tales que
$$B \simeq A[X_1, \dots, X_n]/ < f_1, \dots, f_m > .$$

Lema 4.2.9. *Dado un anillo A, una A-álgebra B es de tipo finito si y solo si existe un número finito de elementos $x_1, \dots x_n \in B$ tales que todo $b \in B$ se escribe como polinomio en las variables x_i $(i = 1, \dots, n)$ con coeficientes en A. Es decir, para cada $b \in B$ existe un subconjunto $S_b \subset \mathbb{N}^n$ finito y para cada $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in S_b$ existe un $a_{\underline{\alpha}} \in A$ de manera que*

$$b = \sum_{\underline{\alpha} \in S_b} a_{\underline{\alpha}} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Demostración. Usando las notaciones del enunciado, si suponemos que B tiene generadores $x_1, \dots, x_n$ como arriba, basta definir coger este n como el número de variables del anillo de polinomios y definir como imagen de cada variable X_i uno de los generadores x_i. Prolongando la definición para que sea un morfismo de anillos resulta en particular ser sobreyectivo por ser cada $b \in B$ un polinomio en las variables x_i, $i = 1, \dots, n$. Recíprocamente, si existe dicho morfismo sobreyectivo, todos los elementos de B podrán escribirse como un polinomio en las imágenes de las variables X_i y con coeficientes en A.

$\square$

Este lema nos permite entender por qué para álgebras tenemos la necesidad de distinguir entre finito y de tipo finito: en el primer caso, los elementos del álgebra son combinaciones A-lineales de una cantidad finita de elementos, mientras que en el segundo son polinomios en dichos elementos como variables y con coeficientes en A. Está claro que en particular una álgebra finita es de tipo finito, pues una combinación A-lineal es un caso concreto de polinomio con coeficientes en A. Observamos también que el segundo concepto no tiene siquiera sentido en un módulo general, pues la multiplicación de sus elementos no tiene por qué estar definida.

Comentamos ahora el producto de módulos con vistas a introducir el concepto de suma directa y algunas observaciones relevantes sobre esta.

Definición 4.2.10. [Producto de módulos] Dada una familia $(M_i)_{i \in I}$ de A-módulos, el producto cartesiano
$$\prod_{i \in I} M_i$$
es un A-módulo si se consideran la suma y el producto escalar componente a componente. Se llama *producto de los* M_i.

Es de especial interés el submódulo del producto constituido por los elementos $(x_i)_{i \in I}$ de soporte finito, esto es, tales que existe un subconjunto finito $J \subseteq I$ tal que $x_i = 0$ si $i \in I \setminus J$. Este submódulo se llama *suma directa* de los $(M_i)_{i \in I}$ y se denotará por

$$\bigoplus_{i \in I} M_i.$$

Observación 4.2.11. Si los $(M_i)_{i \in I}$ son submódulos de un mismo A-módulo M, cada I-upla $(m_i)_{i \in I} \in \oplus_{i \in I} M_i$ puede asociarse con el elemento $\sum_{i \in I} m_i \in M$ correspondiente (notación que tiene sentido, pues, al ser un elemento de la suma directa, todas las componentes salvo un número finito son nulas y por tanto la suma será de un número finito de términos.) Esta aplicación es biyectiva si y solo si cada elemento de M puede escribir de manera única como suma de elementos de los submódulos $(M_i)_{i\in I}$. Por tanto, *la suma directa de submódulos no es en general un submódulo ella misma.*

Proposición 4.2.12. ***[Propiedad universal de la suma directa]*** *Sea $(M_i)_{i\in I}$ una familia de A-módulos. Su suma directa $\oplus_{i\in I} M_i$ verifica la propiedad universal siguiente:*

«Para todo A-módulo N y para toda familia de morfismos de A-módulos $\beta_i : M_i \longrightarrow N$ existe un único morfismo de A-módulos $\beta : \oplus_{i\in I} M_i \longrightarrow N$ verificando que $\beta_i = \beta \circ \pi_i$ para todo $i \in I$ (donde $\pi_i : M_i \hookrightarrow \oplus_{i\in I} M_i$ es la inclusión canónica).»

Demostración. Nuestro objetivo es encontrar la única aplicación β que hace conmutativos los diagramas

$$\begin{tikzcd} M_i \arrow[r, "\pi_i"] \arrow[rr, bend left, "\beta_i"] & \bigoplus_{i\in I} M_i \arrow[r, dashed, "\beta"] & N \end{tikzcd} \tag{4.2.12.1}$$

para todo $i \in I$.

Para cada $\sum_{i\in I} m_i \in \oplus_{i\in I} M_i$ definimos $\beta(\sum_{i\in I} m_i) := \sum_{i\in I} \beta_i(m_i)$. Por definición de suma directa, sus elementos tienen todas las componentes nulas salvo una cantidad finita, luego β está bien definida, y por ser los β_i morfismos de A-módulos, es fácil comprobar que β también lo es. Como se tiene también la compatibilidad $\beta_i = \beta \circ \pi_i$ para todo $i \in I$, se deduce que β es de hecho el único morfismo de A-módulos con esta propiedad. Cualquier otro morfismo que la verifique coincidirá con β sobre los módulos M_i y, por ser un morfismo de A-módulos, coincidirá también con ella sobre la suma directa.

$\square$

Terminamos con algunos resultados sobre módulos de tipo finito extraídos del libro de Atiyah ([1]), del de Matsumura ([5]) y del Stacks Project ([10]), que nos permiten demostrar el utilísimo lema de Nakayama y algunos de sus corolarios. Estos se enuncian en toda generalidad para un ideal contenido en el radical de Jacobson del anillo de trabajo, pero en la práctica casi siempre estaremos en el caso particular del ideal maximal de un anillo local.

Definición 4.2.13. [Producto de un ideal por un módulo] Dado un ideal de A,

$$\mathfrak{a}M = \{sumas\ finitas\ de\ productos\ a\cdot m,\ con\ a\in\mathfrak{a},\ m\in M\}$$

es el submódulo de M generado por los productos am con $a \in \mathfrak{a}$ y $m \in M$.

Proposición 4.2.14. *Sea M un A-módulo finitamente generado, $\mathfrak{a}$ un ideal de A y φ un endomorfismo de A-módulos de M tal que $\varphi(M) \subset \mathfrak{a}M$. Entonces φ satisface una ecuación de la forma*

$$\varphi^n + a_{n-1}\varphi^{n-1} + ... + a_0 = 0,$$

con n natural y $a_i \in \mathfrak{a}$.

Demostración. Sea $\{x_1, ..., x_n\}$ un conjunto de generadores de M. Por hipótesis $\varphi(x_i) \in \mathfrak{a}M$ para cada i, de manera que podemos escribir $\varphi(x_i) = \sum_{j=1}^n a_{ij}x_j$ para ciertos $a_{ij} \in A$. De otra manera, para cada $1 \le i \le n$ se tiene

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})x_j = 0,$$

donde δ_{ij} es la delta de Kronecker. Premultiplicando por la adjunta de la matriz $(\delta_{ij}\varphi - a_{ij})$ se sigue que el determinante de dicha matriz, considerado como endomorfismo de M, anula cada x_i. Como los x_i son generadores de M, entonces el determinante debe ser el endomorfismo nulo. Y al desarrollarlo nos va a quedar una ecuación polinómica mónica de grado n en φ con coeficientes en $\mathfrak{a}$ como la requerida en el enunciado.

$\square$

Corolario 4.2.15. *Sea M un A-módulo finitamente generado y sea $\mathfrak{a}$ un ideal de A tal que $\mathfrak{a}M = M$. Entonces existe $x \equiv 1\,(mod\,\mathfrak{a})$ tal que $xM = 0$.*

Demostración. Tomando la identidad como endomorfismo en la proposición anterior, en particular $Id(M) \subset \mathfrak{a}M = M$, y se tiene debe verificar una ecuación (de endomorfismos)

$$Id + a_{n-1} + ... + a_0 = 0,$$

para ciertos $a_i \in \mathfrak{a}$, $i = 0, ..., n-1$. Si ponemos $x \coloneqq 1 + a_{n-1} + ... + a_0$ se tienen las condiciones pedidas.

$\square$

Corolario 4.2.16. ***[Lema de Nakayama]*** *Sea M un A-módulo finitamente generado y $\mathfrak{a}$ un ideal de A contenido en su radical de Jacobson, $\mathcal{J}(A)$. Si $\mathfrak{a}M = M$, entonces $M = 0$.*

Demostración. Invocando el corolario anterior, existe un $x \equiv 1(mod\,\mathcal{J}(A))$ tal que $xM = 0$. Como $1 - x \in \mathcal{J}(A)$, utilizando 4.1.7, x es una unidad de A, así que es invertible y se tiene $M = x^{-1}(xM) = x^{-1}0 = 0$.

$\square$

Corolario 4.2.17. *Sean M un A-módulo finitamente generado, N un submódulo de M y $\mathfrak{a} \subset \mathcal{J}(A)$ un ideal. Si $M = \mathfrak{a}M + N$, entonces $M = N$.*

Demostración. De la igualdad de la hipótesis, tomando módulos obtenemos $M/N = (\mathfrak{a}M+N)/N$. Si probamos que el segundo término coincide con $\mathfrak{a}(M/N)$, podemos aplicar el *lema de Nakayama* al A-módulo M/N (que es finitamente generado por serlo M) y concluir que $M/N = 0$, es decir, $M = N$. La igualdad deseada se deduce de que los elementos de $\mathfrak{a}(M/N)$ son de la forma $am + N$ con $a \in \mathfrak{a}$, $m \in M$, los cuales están en $(\mathfrak{a}M + N)/N$. Y los elementos de este último también son $am + n + N = am + N$ con $a \in \mathfrak{a}$, $m \in M, n \in N$. Luego se dan las dos contenciones.

$\square$

Corolario 4.2.18. *Sea A un anillo y $\mathfrak{a}$ un ideal de A contenido en su radical de Jacobson, $\mathcal{J}(A)$. Si $f : N \longrightarrow M$ es un morfismo de A-módulos tal que el morfismo inducido $\tilde{f} : N/\mathfrak{a}N \longrightarrow M/\mathfrak{a}M$ es sobreyectivo y M es finitamente generado, entonces también f es sobreyectivo.*

Demostración. Basta aplicar el corolario anterior, pues al ser $\tilde{f}$ sobreyectivo se deduce que $f(N) + \mathfrak{a}M = M$ pues el morfismo $\tilde{f}$ se define como $\tilde{f}(n + \mathfrak{a}N) = f(n) + \mathfrak{a}M$ para cada $n + \mathfrak{a}N \in N/\mathfrak{a}N$. Por tanto, como M es de tipo finito y $\mathfrak{a} \subseteq \mathcal{J}(A)$, se deduce que $f(N) = M$, y por tanto f es sobre.

$\square$

Proposición 4.2.19. *Sea A un anillo local, $\mathfrak{m}$ su ideal maximal, $k = A/\mathfrak{m}$ su cuerpo de residuos. Sea M un A-módulo finitamente generado. Entonces $M/\mathfrak{m}M$ puede considerarse un k-módulo, es decir, un k-espacio vectorial, y además es de dimensión finita. Más aún, si tomamos $\{x_i\}_{i=1,...,n} \subset M$ cuyas clases en $M/\mathfrak{m}M$ son generadores de dicho espacio, entonces las x_i generan M como A-módulo.*

Demostración. La dimensión finita se deduce de ser M finitamente generado, ya que estos generadores inducen una base del k-espacio vectorial. Tomando N como el submódulo de M engendrado por los x_i, podemos considerar $N/\mathfrak{m}M \subset M/\mathfrak{m}M$ a través de la aplicación $N \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$. Como las clases de los x_i módulo $\mathfrak{m}M$ son generadores de $M/\mathfrak{m}M$ entonces $M/\mathfrak{m}M = N/\mathfrak{m}M$, luego $M = N + \mathfrak{m}M$, y usando el corolario anterior, $M = N$, de modo que las x_i son generadoras de M.

□

4.2.2. Sucesiones exactas

Definición 4.2.20. [Sucesión exacta] Una sucesión de A-módulos y A-morfismos

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \tag{4.2.20.1}$$

se dice *exacta en* M_i si $Im(f_i) = Ker(f_{i+1})$. La sucesión es *exacta* si es exacta en cada M_i.

Observación 4.2.21.

1. $0 \longrightarrow M' \xrightarrow{f} M$ es exacta $\Leftrightarrow$ f es inyectiva.
2. $M \xrightarrow{g} M'' \longrightarrow 0$ es exacta $\Leftrightarrow$ g es suprayectiva.
3. $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ es exacta $\Leftrightarrow$ f es inyectiva, g es suprayectiva y $Ker(g) = Im(f)$. Las sucesiones de este tipo se llaman *sucesiones exactas cortas.*

   En este marco, M' puede verse como submódulo de M via f, y como $Im(f) = Ker(g)$, del primer teorema de isomorfía se tiene que $Coker(f) \simeq M/M' \simeq M''$. Recíprocamente, dado N un submódulo de M, se tiene la sucesión exacta corta canónica

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

Lema 4.2.22. *Cada sucesión exacta puede escindirse en sucesiones exactas cortas.*

Demostración. Usando la notación de 4.2.20.1, si tomamos $N_i = Im(f_i) = Ker(f_{i+1})$ se tienen las sucesiones exactas cortas $0 \longrightarrow N_i \longrightarrow M_i \longrightarrow N_{i+1} \longrightarrow 0$ para cada i.

□

Lema 4.2.23. *Sea*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} \tilde{N} \xrightarrow{h} T \longrightarrow 0$$

una sucesión exacta donde g es un isomorfismo. Entonces $M = T = 0$.

Demostración. Por ser la sucesión exacta sabemos que f es inyectiva, g es sobreyectiva, $Ker(g) = Im(f)$ y que $Im(g) = Ker(h)$. Pero como g es un isomorfismo $Ker(g) = 0$ y $Im(g) = \tilde{N}$, de modo que $Im(f) = Ker(f) = 0$ (luego $M = 0$) y $Ker(h) = \tilde{N}$ (luego $h = 0$ y al ser sobre se tiene que $T = 0$).

□

4.3. Localización

En esta sección se introducen y caracterizan los anillos locales, que son aquellos que tienen un único ideal maximal. Después se presenta un proceso para construir nuevos anillos a partir de uno dado llamado localización, el cual permitirá en algunos casos obtener anillos locales. Nos interesará especialmente estudiar cómo se relacionan los ideales de un anillo con los de sus localizaciones. Finalmente, veremos que este proceso puede generalizarse a módulos cualesquiera y veremos, entre otras propiedades, que preserva la exactitud de una sucesión. La referencia principal vuelve a ser [2], pero se incluyen resultados de [10] y [1].

Definición 4.3.1. [Anillo local. Cuerpo residual] Decimos que un anillo A es *local* (resp. *semilocal*) cuando contiene un único ideal maximal $\mathfrak{m}$ (resp. una cantidad finita de ideales maximales). Si A es local, al cuerpo $A/\mathfrak{m}$ se le llama *cuerpo residual o de residuos* del anillo local A.

Lema 4.3.2. *Un anillo A es local si y solo si su radical de Jacobson es un ideal maximal.*

Demostración. Si A es local, por definición solo tiene un ideal maximal, que por tanto coincide con su radical de Jacobson. Recíprocamente, si $\mathcal{J}(A)$ es un ideal maximal, no puede haber ningún otro pues contendría al radical de Jacobson por construcción, contradiciendo el hecho de que este sea maximal.

$\square$

Definición 4.3.3. [Morfismo local de anillos] Un *homomorfismo local de anillos locales* es un morfismo de anillos $\varphi : A \longrightarrow B$ tal que A y B son locales y la imagen por φ del ideal maximal de A está contenida en el ideal maximal de B. Por simplicidad se suelen denominar *morfismos (de anillos) locales.*

Proposición 4.3.4. *Dado A un anillo y $\mathfrak{m} \subsetneq A$ un ideal maximal de A, las condiciones siguientes son equivalentes:*

1. *A es local y su ideal maximal es $\mathfrak{m}$.*
2. *Los elementos de $A \setminus \mathfrak{m}$ son unidades en A.*
3. *El ideal $\mathfrak{m}$ es maximal y los elementos $1 + m$ con $m \in \mathfrak{m}$ son unidades en A.*

Demostración. Empecemos viendo que las condiciones *(1) y (2)* son equivalentes. Si *(1)* se da, y $a \in A$ no es una unidad, el teorema de Krull nos garantiza la existencia de un ideal maximal $\mathfrak{n} \subset A$ con $a \in \mathfrak{n}$. Por ser A local, $\mathfrak{n} = \mathfrak{m}$ necesariamente. Por tanto los elementos de $A \setminus \mathfrak{m}$ deben ser las unidades del anillo. Si suponemos ahora que *(2)* es cierta, cualquier ideal estricto de A estará contenido en $\mathfrak{m}$ pues no contiene a ninguna unidad, luego $\mathfrak{m}$ es el único ideal maximal de A.

Ahora, podemos utilizar conjuntamente las dos primeras afirmaciones para probar la tercera. Sabemos que $\mathfrak{m}$ es un ideal maximal y si m es un elemento suyo, $1 + m$ no puede serlo puesto que $1 \notin \mathfrak{m}$. Así que, por *(2)*, $1 + m$ debe ser una unidad de A. Recíprocamente, si suponemos *(3)* y tomamos $x \in A \setminus \mathfrak{m}$, el ideal engendrado por x y $\mathfrak{m}$ debe ser todo A por ser $\mathfrak{m}$ maximal. Por tanto, deben existir $m \in \mathfrak{m}$ y $a \in A$ tales que

$$1 = ax - m,$$

de modo que $ax = 1 + m$ es una unidad por *(3)* y también lo es x, de donde se deduce *(2)*.

$\square$

Observación 4.3.5. Podemos construir anillos locales a partir de un anillo A mediante el proceso de *localización*:

- Comenzamos cogiendo un *subconjunto multiplicativamente cerrado* de A, esto es, un subconjunto $S \subset A$ tal que $1 \in S$ y si $s, s' \in S$ entonces $ss' \in S$.
- Ahora definimos una relación de equivalencia $\sim$ en el producto $A \times S$ de la siguiente manera: dados $(a, s), (a', s') \in A \times S$,
$$(a, s) \sim (a', s') \iff \exists\, t \in S \;:\; (as' - a's)t = 0. \tag{4.3.5.1}$$
- De esta manera, el conjunto cociente $(A \times S)/\sim$ es un anillo cuando se considera la aritmética de fracciones usual.

Definición 4.3.6. **[Localización]** En las condiciones de la observación anterior, el anillo $(A \times S)/\sim$ se llama *localización de A en S* o *anillo de fracciones de A con respecto de S* y se denotará por $S^{-1}A$.

Lema 4.3.7. *Sea S un subconjunto multiplicativamente cerrado de un anillo A y sea $\pi : A \longrightarrow S^{-1}A$ el homomorfismo canónico ($\pi(a) = a/1$). Se verifican las propiedades siguientes:*

1. *$Ker(\pi) = \{a \in A : at = 0$ para algún $t \in S\}$.*
2. *Dado $s \in S$, $\pi(s) = s/1$ es una unidad de $S^{-1}A$.*
3. *$S^{-1}A = 0 \iff 0 \in S$.*
4. *En general, π no es inyectiva, así que no se tiene la inclusión $A \hookrightarrow S^{-1}A$. Sin embargo, si los elementos de S son unidades de A, entonces es biyectiva.*

Demostración. Para probar *(1)* basta tener en cuenta la relación 4.3.5.1. Dado $s \in S$ cualquiera, $1/s$ es el inverso de $s/1$ en el anillo de fracciones, de donde se deduce *(2)*. Para la equivalencia de *(3)*, recordemos que el anillo $S^{-1}A$ es el nulo si y solo si $1/1 = 0/1$, esto es, si y solo si existe un elemento $s \in S$ tal que $s = (1 \cdot 1 - 0 \cdot 1)s = 0$. Finalmente, si S solo contiene unidades del anillo, de la parte *(1)* deducimos que $Ker(\pi) = 0$ y, además, para cada $a/s \in S^{-1}A$ se tiene $a/s = as^{-1}/1 = \pi(as^{-1})$, así que π es también sobreyectiva.

□

Ejemplo 4.3.8. Algunos ejemplos de localizaciones de anillos:

(I) Dado un dominio de integridad A y el subconjunto $S := A \setminus \{0\}$, entonces $S^{-1}A$ coincide con $Fr(A)$, el cuerpo de fracciones del dominio. En este caso π es inyectiva, así que se puede considerar $A \subset S^{-1}A$.

(II) Dado un anillo A y un ideal primo $\mathfrak{p} \subset A$, entonces $S := A \setminus \mathfrak{p}$ es un sistema multiplicativo en A, y llamamos a $S^{-1}A$ la *localización de A en $\mathfrak{p}$*. Se suele denotar por $A_{\mathfrak{p}}$ y veremos que es un anillo local.

(III) Dado $a \in A$, el conjunto $S = \{a^i : i \in \mathbb{N}_0\}$ es un sistema multiplicativo en A. La localización $S^{-1}A$ en este caso se denota por A_a o $A[a^{-1}]$.

Observación 4.3.9. Dado un ideal $\mathfrak{a}$ de A, podemos considerar su *extensión en $S^{-1}A$*, $\mathfrak{a}S^{-1}A$, es decir, el ideal de $S^{-1}A$ engendrado por $\pi(\mathfrak{a})$. Se deduce además la igualdad siguiente:
$$\mathfrak{a}S^{-1}A = \left\{ \frac{a}{s} \;:\; a \in \mathfrak{a},\, s \in S \right\}. \tag{4.3.9.1}$$
También podemos considerar la *restricción* de un ideal $\mathfrak{b} \subset S^{-1}A$ en A, $\mathfrak{b} \cap A = \pi^{-1}(\mathfrak{b})$.

Proposición 4.3.10. *Sea $S^{-1}A$ la localización del anillo A por el sistema multiplicativo $S \subset A$. Entonces:*

1. *La extensión $\mathfrak{a}S^{-1}A$ de un ideal $\mathfrak{a} \subset A$ es un ideal propio de $S^{-1}A$ si y solo si $S \cap \mathfrak{a} = \emptyset$.*
2. *Para cualquier ideal $\mathfrak{b} \subset S^{-1}A$, su restricción $\mathfrak{a} = \mathfrak{b} \cap A$ verifica $\mathfrak{a}S^{-1}A = \mathfrak{b}$ (la extensión de su restricción coincide con él).*
3. *Si $\mathfrak{p} \subset A$ es un ideal primo tal que $S \cap \mathfrak{p} = \emptyset$ entonces su extensión $\mathfrak{p}S^{-1}A$ es también un ideal primo en $S^{-1}A$ y satisface $\mathfrak{p}S^{-1}A \cap A = \mathfrak{p}$.*
4. *Dado $\mathfrak{q} \subset S^{-1}A$ ideal primo, su restricción $\mathfrak{p} = \mathfrak{q} \cap A$ es un ideal primo en A y satisface $\mathfrak{p}S^{-1}A = \mathfrak{q}$. En particular, $\mathfrak{p} \cap S = \emptyset$ en virtud de la parte (1).*

Demostración.

1. Sea $\mathfrak{a} \subset A$ un ideal que contiene a un cierto elemento $s \in S$. Entonces su extensión $\mathfrak{a}S^{-1}A$ contiene a $s/1$, que es una unidad de $S^{-1}A$, de modo que la extensión no puede ser un ideal estricto. Recíprocamente, si $\mathfrak{a}S^{-1}A = S^{-1}A$ para un cierto ideal $\mathfrak{a}$, entonces existen elementos $a \in \mathfrak{a}$ y $s \in S$ tales que $a/s = 1/1$. Así, debe existir $t \in S$ tal que $(a-s)t = 0$, pero entonces $st = at \in \mathfrak{a}$, así que $\mathfrak{a} \cap S \neq \emptyset$.
2. Sea $a/s \in \mathfrak{b}$ cualquiera. Como $a/1 = s/1 \cdot a/s$, $s/1 \in S^{-1}A$ y $\mathfrak{b}$ es un ideal de $S^{-1}A$, entonces $a \in \mathfrak{a} = \mathfrak{b} \cap A$. Así, $a/s \in \mathfrak{a}S^{-1}A$ y se tiene la inclusión $\mathfrak{b} \subset \mathfrak{a}S^{-1}A$. Por otro lado, si tomamos $a/s \in \mathfrak{a}S^{-1}A$, entonces $a \in \mathfrak{b}$, y podemos escribir $a/s = 1/s \cdot a/1 \in \mathfrak{b}$ por ser este último un ideal. Y se tiene la otra inclusión.
3. Sea $\mathfrak{p} \subset A$ un ideal primo tal que $\mathfrak{p} \cap S = \emptyset$. Entonces, $\mathfrak{p}S^{-1}A$ es un ideal estricto de $S^{-1}A$ por la parte *(1)*. Para ver que es primo, sean a/s, $a'/s' \in S^{-1}A$ tales que $aa'/ss' \in \mathfrak{p}S^{-1}A$. Por tanto, para algunos $a'' \in \mathfrak{p}$ y $s'' \in S$ se tiene $aa'/ss' = a''/s''$, así que existe un $t \in S$ tal que $(aa's'' - a''ss')t = 0$. De ahí, $aa's''t = a''ss't \in \mathfrak{p}$. Y como $\mathfrak{p} \cap S = \emptyset$, se tiene $s''t \notin \mathfrak{p}$ y al ser el ideal primo, $aa' \in \mathfrak{p}$. Por tanto, bien $a \in \mathfrak{p}$ (luego $a/s \in \mathfrak{p}S^{-1}A$), bien $a' \in \mathfrak{p}$ (luego $a'/s' \in \mathfrak{p}S^{-1}A$).

   La inclusión $\mathfrak{p} \subset \mathfrak{p}(S^{-1}A) \cap A$ es clara. Dado ahora $b \in \mathfrak{p}(S^{-1}A) \cap A$ existen ciertos $a \in \mathfrak{p}$, $s \in S$ tales que $b/1 = a/s$, esto es, para un $t \in S$, $bst = at$ y sabemos además que $at \in \mathfrak{p}$. Como $st \notin \mathfrak{p}$ entonces $b \in \mathfrak{p}$ y se tiene la otra inclusión.
4. Sea ahora $\mathfrak{q}$ un ideal primo de $S^{-1}A$. Por la observación 4.1.3 $\mathfrak{p} = \mathfrak{q} \cap A$ es un ideal primo de A por ser la imagen inversa por el homomorfismo canónico π de un ideal primo. Para ver que la extensión $\mathfrak{p}(S^{-1}A)$ coincide con $\mathfrak{q}$ basta usar la parte *(2)*. Y, como los ideales primos son estrictos, de *(1)* se tiene que $\mathfrak{p} \cap S = \emptyset$.

□

De las dos últimas propiedades de la proposición anterior se deduce que los ideales primos del anillo A que no cortan al conjunto S y los primos de su anillo de fracciones $S^{-1}A$ están relacionados biunívocamente, como explicita el corolario siguiente.

Corolario 4.3.11. *El homomorfismo canónico $\pi : A \longrightarrow S^{-1}A$ induce una biyección*

$$Spec(S^{-1}A) \xrightarrow{\sim} \{\mathfrak{p} \in Spec(A) : \mathfrak{p} \cap S = \emptyset\}, \quad \mathfrak{q} \longmapsto \mathfrak{q} \cap A$$

que, junto a su inversa, respeta la inclusión entre ideales primos.

También deducimos el resultado que anunciamos al principio de la sección: podemos construir anillos locales a partir de otros localizándolos en un ideal primo.

Corolario 4.3.12. *Dado un ideal primo $\mathfrak{p}$ de un anillo A, su localización $A_{\mathfrak{p}}$ es un anillo local de ideal maximal $\mathfrak{p}A_{\mathfrak{p}}$.*

Demostración. Basta observar que todos los elementos de $A_{\mathfrak{p}} \setminus \mathfrak{p}A_{\mathfrak{p}}$, que son del tipo a/s con $a, s \in A \setminus \mathfrak{p}$, son unidades de $A_{\mathfrak{p}}$ pues su inverso s/a pertenece a $A_{\mathfrak{p}}$.

□

Terminamos esta sección con la llamada propiedad universal de las localizaciones, que las caracteriza salvo isomorfismo canónico, y algunos resultados obtenidos a partir de ella.

Proposición 4.3.13. *El homomorfismo canónico $\pi : A \longrightarrow S^{-1}A$ verifica $\pi(S) \subset (S^{-1}A)^{\times}$ y es universal en el sentido siguiente: dado cualquier homomorfismo de anillos $\varphi : A \longrightarrow A'$ tal que $\varphi(S) \subset (A')^{\times}$, existe un único homomorfismo de anillos $\varphi' : S^{-1}A \longrightarrow A'$ tal que $\varphi = \varphi' \circ \pi$. Esto es, el diagrama*

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[d, "\varphi"] & S^{-1}A \arrow[dl, dashed, "\varphi'"] \\ A' & \end{tikzcd}$$

es conmutativo. Más aún, si $\varphi : A \longrightarrow A'$ satisface la misma propiedad universal que π, entonces $\varphi' : S^{-1}A \longrightarrow A'$ es un isomorfismo.

Demostración. Empecemos probando la unicidad del morfismo φ' del enunciado. Dados $a \in A$ y $s \in S$ cualesquiera, por la compatibilidad entre φ y φ' tenemos

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

Y como $\varphi(s)$ es invertible por hipótesis,

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

de manera que φ' queda determinado unívocamente por φ.

Para mostrar la existencia del morfismo φ', definimos

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

para $a \in A$ y $s \in S$. Veamos primero que está bien definido: si $a/s = a'/s'$, existe un $t \in S$ tal que $(as' - a's)t = 0$, y aplicando φ en dicha relación

$$(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)) \cdot \varphi(t) = 0$$

y, como $\varphi(t)$, $\varphi(s)$ y $\varphi(s')$ son unidades de A',

$$\varphi(a)\varphi(s') - \varphi(a')\varphi(s) = 0,$$

o, equivalentemente,

$$\varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}.$$

Por tanto, $\varphi'\left(\frac{a}{s}\right) = \varphi'\left(\frac{a'}{s'}\right)$ y el morfismo está bien definido y además se verifica la compatibilidad $\varphi = \varphi' \circ \pi$.

Si ahora suponemos que φ y π son universales en el sentido anterior, existen morfismos $\varphi' : S^{-1}A \longrightarrow A'$ y $\pi' : A' \longrightarrow S^{-1}A$ únicos verificando $\varphi = \varphi' \circ \pi$ y $\pi = \pi' \circ \varphi$. De la ecuación

$$\varphi = Id_{A'} \circ \varphi = \varphi' \circ \pi = (\varphi' \circ \pi') \circ \varphi,$$

deducimos que $(\varphi' \circ \pi') = Id_{A'}$ aplicando la unicidad de la propiedad universal de φ sobre sí mismo. Análogamente, se tiene que $(\pi' \circ \varphi') = Id_{S^{-1}A}$.

□

Corolario 4.3.14. *Sea $(A, \mathfrak{m})$ un anillo local. Entonces la localización en el ideal maximal es isomorfa al anillo original:*

$$A_{\mathfrak{m}} \simeq A.$$

En particular, dado un anillo A cualquiera y un ideal primo $\mathfrak{p}$ de A, se tiene que $A_{\mathfrak{p}}$ es isomorfo a $(A_{\mathfrak{p}})_{\mathfrak{p}}$.

Demostración. Basta ver que $id_A : A \longrightarrow A$ satisface la propiedad universal de la localización $A_{\mathfrak{m}}$. En primer lugar, como A es local de ideal maximal $\mathfrak{m}$, $S = A \setminus \mathfrak{m}$ son de hecho las unidades de A (ver proposición 4.3.4), de modo que $id_A(S) \subseteq A^{\times}$. Sea ahora $\varphi : A \longrightarrow A'$ un morfismo de anillos cualquiera tal que $\varphi(S) \subseteq (A')^{\times}$ (en este caso la condición es redundante pues como S son unidades de A, cualquier morfismo de anillos las enviará en unidades de B). Como el único morfismo $\varphi' : A \longrightarrow B$ que verifica $\varphi = \varphi' \circ id_A$ es el propio φ, id_A verifica la propiedad universal y por tanto $A \simeq A_{\mathfrak{m}}$, como queríamos.
La segunda parte se deduce del corolario 4.3.12, pues $A_{\mathfrak{p}}$ es un anillo local de maximal $\mathfrak{p}A_{\mathfrak{p}}$.

□

Si S y $\tilde{S}$ son dos subconjuntos multiplicativamente cerrados de un mismo anillo A, está claro que el conjunto producto

$$S\tilde{S} := \{s\tilde{s} \ : \ s \in S, \ \tilde{s} \in \tilde{S}\}$$

lo es también. En la siguiente proposición vemos que las localizaciones sucesivas «conmutan» entre sí.

Proposición 4.3.15. *Sean A un anillo y S, $\tilde{S}$ dos suconjuntos multiplicativamente cerrados del mismo. Si denotamos por $\overline{S}$ la imagen de S en $\tilde{S}^{-1}A$, entonces se tiene el isomorfismo de anillos siguiente:*

$$\overline{S}^{-1}(\tilde{S}^{-1}A) \simeq (S\tilde{S})^{-1}A.$$

Como el anillo es conmutativo, $S\tilde{S} = \tilde{S}S$ y está claro que también se tiene el isomorfismo en el otro sentido.

Demostración. La aplicación $\varphi : x \in A \longmapsto x/1 \in (S\tilde{S})^{-1}A$ verifica que $\varphi(\tilde{S})$ está compuesto por unidades de $(S\tilde{S})^{-1}A$, pues $\tilde{s} \in \tilde{S} \subseteq S\tilde{S}$, así que los elementos de la forma $\tilde{s}/1$ son efectivamente unidades. Por tanto, podemos aplicar la propiedad universal de la localización $\tilde{S}^{-1}A$ al morfismo φ: existe un único morfismo $\varphi' : \tilde{S}^{-1}A \longrightarrow (S\tilde{S})^{-1}A$ tal que $\varphi = \varphi' \circ \pi_1$, donde π_1 es la aplicación canónica de la localización $\tilde{S}^{-1}A$. De manera análoga, podemos comprobar que $\varphi'(\overline{S})$ son unidades de $(S\tilde{S})^{-1}A$, de modo que se puede aplicar la propiedad universal de la localización $\overline{S}^{-1}(\tilde{S}^{-1}A)$ a φ'. Existe por tanto un único morfismo $\varphi'' : \overline{S}^{-1}(\tilde{S}^{-1}A) \longrightarrow (S\tilde{S})^{-1}A$ que debe verificar la compatibilidad siguiente:

$$\varphi''\left(\frac{(x/\tilde{t})}{(s/\tilde{s})}\right) = (x/\tilde{t}) \cdot (s/\tilde{s})^{-1}.$$

Por otro lado, la aplicación

$$\psi : x \in A \longmapsto \frac{x/1}{1/1} \in \overline{S}^{-1}(\tilde{S}^{-1}A)$$

verifica que el conjunto $\psi(S\tilde{S})$ está compuesto por unidades de $\overline{S}^{-1}(\tilde{S}^{-1}A)$ y una vez más podemos aplicar la propiedad universal (ahora para la localización $(S\tilde{S})^{-1}A$) para garantizar la existencia y unicidad del morfismo

$$\psi' : x/(s\tilde{s}) \in (S\tilde{S})^{-1}A \longmapsto \frac{(x/\tilde{s})}{(x/s)} \in \overline{S}^{-1}(\tilde{S}^{-1}A).$$

Una simple comprobación nos muestra que ψ' y φ'' son inversos respectivos y se tiene pues el isomorfismo deseado.

$\square$

Veamos una nueva caracterización de las localizaciones que será útil en el trabajo. La demostración puede consultarse en el texto de Bosch, [2].

Lema 4.3.16. *A un anillo, $\mathcal{F} = (f_i)_{i\in I}$ una familia de elementos de A, y $S \subset A$ el sistema multiplicativamente cerrado engendrado por $\mathcal{F}$ (el conjunto de productos finitos de elementos de $\mathcal{F}$. Entonces, fijando un sistema de variables $T = (t_i)_{i\in I}$ existe un isomorfismo canónico*

$$S^{-1}A \xrightarrow{\sim} A[T]/(1 - f_i t_i; i \in I).$$

En particular, para un solo elemento $f \in A$ existe un isomorfismo canónico $A_f \simeq A[t]/(1 - ft)$.

Veamos ahora que es inmediato generalizar el proceso de localización de anillos a módulos (o también a álgebras). Sea M un A-módulo y $S \subseteq A$ un conjunto multiplicativamente cerrado. Podemos definir la relación de equivalencia $\sim$ en $M \times S$ como sigue:

$$(x, s) \sim (x', s') \Leftrightarrow \exists t \in S \;:\; (xs' - x's)t = 0.$$

Escribiendo x/s para cada clase de equivalencia, el conjunto de clases de equivalencia

$$S^{-1}M := \{x/s \;:\; x \in M, s \in S\}$$

es un $S^{-1}A$-módulo para la aritmética de fracciones usual y se denomina la localización de M por S.

Observación 4.3.17. Un caso particular es cuando el módulo B que localizamos es una A-álgebra. Sean $f : A \longrightarrow B$ el morfismo estructural, S un subconjunto de A multiplicativamente cerrado y $T = f(S)$. Por ser f un morfismo de anillos, se comprueba trivialmente que T es multiplicativamente cerrado. Además, se tiene el isomorfismo de anillos

$$S^{-1}B \simeq T^{-1}B,$$

dado por $b/s \longmapsto b/f(s)$. Se comprueba inmediatamente por la definición de las localizaciones respectivas que está bien definido y que es un isomorfismo de $S^{-1}A$-álgebras (en particular de A-álgebras). Por tanto, las dos notaciones son equivalentes al localizar álgebras.

Proposición 4.3.18. *Sea A un anillo, S un subconjunto multiplicativamente cerrado de A y M un A-módulo. Un elemento $m/s \in S^{-1}M$ es nulo si y solo si existe $t \in S$ tal que $mt = 0$. Además, si el módulo M es finitamente generado, $S^{-1}M = 0$ si y solo si existe un elemento $u \in S$ tal que $um = 0$ para todo $m \in M$.*

Demostración. La primera parte es inmediata teniendo en cuenta la relación de equivalencia que define $S^{-1}M$:

$$(m, s) \sim (0, 1) \;\Leftrightarrow\; \exists t \in S \;:\; mt = 0.$$

Para la segunda, notar que $S^{-1}M = 0$ si y solo si para todo $m \in M$ existe un $s_m \in S$ (que en principio depende de m) tal que $ms_m = 0$. Sin embargo, como M es finitamente generado, digamos con generadores $x_1, \ldots, x_n$, por linealidad basta que existan $s_i \in S$ tales que $s_i x_i = 0$ para $i = 1, \ldots, n$. Tomando $u \coloneqq \prod_{i=1}^{n} s_i$, se tiene $um = 0$ para todo $m \in M$ como queríamos. El recíproco es evidente.

□

Observación 4.3.19. Otras propiedades de la localización de anillos se generalizan con facilidad al caso de módulos. Omitimos las demostraciones, que pueden consultarse, por ejemplo, en la sección sobre localización de [10]. Sean en todos los casos A un anillo y M un A-módulo (resp. una A-álgebra):

1. Si S y $\tilde{S}$ son dos conjuntos multiplicativamente cerrados de A, entonces se tiene el isomorfismo de A-módulos (resp. A-álgebras) siguiente:

$$S^{-1}(\tilde{S}^{-1}M) \simeq (S\tilde{S})^{-1}M.$$

2. Los submódulos (resp. subálgebras) de $S^{-1}M$ son de la forma $S^{-1}N$, donde N es un submódulo (resp. subálgebra) de M.

En la subsección siguiente veremos también que la localización preserva lo que llamaremos sucesiones exactas de módulos, y de ese resultado deduciremos de manera sencilla que localizar un cociente de módulos «equivale» a localizar numerador y denominador.

Como comentábamos antes, la localización de módulos respeta la exactitud de una sucesión. Dado un subconjunto multiplicativamente cerrado S de un anillo A y un homomorfismo de A-módulos (resp. A-álgebras) $f : M \longrightarrow N$, podemos considerar el homomorfsimo de $S^{-1}A$-módulos (resp. $S^{-1}A$-álgebras) $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ que envía un elemento cualquiera $m/s \in S^{-1}M$ a $f(m)/s$. Es rutinario comprobar que se trata efectivamente de un morfismo de $S^{-1}A$-módulos (resp. álgebras)y además, si $g : N \longrightarrow T$ es otro morfismo, se tiene que

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

Decimos que la operación de localización S^{-1} es exacta, pues al aplicarla sobre una sucesión exacta de módulos, la resultante mantiene dicha propiedad.

Proposición 4.3.20. ***[Exactitud de la localización]*** *Consideremos la sucesión de A-módulos exacta (en M) siguiente:*

$$M' \xrightarrow{\;f\;} M \xrightarrow{\;g\;} M''. \tag{4.3.20.1}$$

Si S es un subconjunto multiplicativamente cerrado de A, la operación S^{-1} es exacta , esto es, la sucesión

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'', \tag{4.3.20.2}$$

sigue siendo exacta (en $S^{-1}M$).

Demostración. Como la sucesión 4.3.20.1 es exacta, $Ker(g) = Im(f)$, de donde $g \circ f = 0$ y $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$. Por tanto, $Im(S^{-1}f) \subseteq Ker(S^{-1}g)$, y nos faltaría solo obtener la inclusión inversa.

Dado $m/s \in Ker(S^{-1}g)$ cualquiera, entonces $(S^{-1}g)(m/s) = g(m)/s = 0$ en $S^{-1}M''$. Usando la proposición 4.3.18, un elemento es nulo en $S^{-1}M''$ si y solo si existe un $t \in S$ tal que $tg(m) = 0$ en M''. Pero como g es un homomorfismo de A-módulos, $tg(m) = g(tm)$ ya que $t \in S \subseteq A$. Así pues, $tm \in Ker(g) = Im(f)$ y existe $m' \in M'$ tal que $f(m') = tm$. Utilizando esta igualdad se tiene que

$$m/s = f(m')/st = (S^{-1}f)(m'/st) \in Im(S^{-1}f).$$

Por tanto $Ker(S^{-1}g) \subseteq Im(S^1 f)$ y se tiene la igualdad deseada.

$\square$

Corolario 4.3.21. *Dados dos A-módulos (resp. A-álgebras) M y N tales que N es submódulo de M, y S un suconjunto de A multiplicativamente cerrado, los $S^{-1}A$-módulos (resp. $S^{-1}A$-álgebras) $S^{-1}(M/N)$ y $(S^{-1}M)/(S^{-1}N)$ son isomorfos.*

Demostración. Basta aplicar la exactitud de la localización (4.3.20) a la sucesión exacta canónica

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

de donde se obtiene la sucesión exacta

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0,$$

que induce el isomorfismo deseado (ver observación 4.2.21).

$\square$

Corolario 4.3.22. *Dados un anillo A, un A-módulo M y S una parte multiplicativamente cerrada de A. Los $S^{-1}A$-submódulos de $S^{-1}M$ son exactamente las localizaciones en S de los A-submódulos de M. Además, si N es un A-módulo de generación finita, $S^{-1}N$ es un $S^{-1}A$-módulo de generación finita también. Y si N' es un $S^{-1}A$-módulo de generación finita, existe un A-módulo de generación finita N tal que $N' = S^{-1}N$.*

Demostración. Sea $\pi : M \longrightarrow S^{-1}M;\ \ m \longmapsto m/1$ el morfismo canónico. Comencemos tomando un submódulo N de M. Entonces $S^{-1}N$ es un $S^{-1}A$ módulo y por exactitud de la localización, de $N \hookrightarrow M$ se tiene que $S^{-1}N \hookrightarrow S^{-1}M$, así que es un submódulo de $S^{-1}M$. Si tomamos ahora N' sub-$S^{-1}A$-módulo de $S^{-1}M$, podemos considerar sus generadores (quizás una cantidad infinita), pero podemos en particular limitarnos a los de la forma $n/1$ para $n \in M$, pues estamos en un $S^{-1}A$-módulo. Ahora bien, $N := \pi^{-1}(N')$ es un submódulo de M por ser π un morfismo de A-módulos, que además contiene los elementos $n \in M$ anteriores. Por tanto, el submódulo de $S^{-1}M$ dado por $S^{-1}N$ es el generado por los $n/1$, esto es, N'.

Comentemos ahora las propiedades de finitud: si N es generado como A-módulo por elementos $x_1, \ldots, x_t$ con $t \in \mathbb{N}$, entonces $S^{-1}N$ es generado como $S^{-1}A$-módulo por los $x_1/1, \ldots, x_t/1$. Recíprocamente, si N' es un $S^{-1}A$-módulo de generación finita podemos suponer, como hemos comentado antes, que los generadores son de la forma $x_1/1, \ldots, x_t/1$, de manera que elementos $x_1, \ldots, x_t$ serán generadores de un A-módulo N tal que $S^{-1}N = N'$.

$\square$

4.4. Condiciones de finitud

Es fácil comprobar que, aunque un módulo sea finito (resp. de presentación finita), sus submódulos no tienen por qué serlo. En esta sección introducimos ciertas condiciones de finitud sobre el anillo de base que permiten mejorar este comportamiento.

Empezamos con una proposición conjuntista que será útil más adelante para caracterizar de varias maneras los módulos noetherianos y los artinianos.

Proposición 4.4.1. *Si Σ es un conjunto parcialmente ordenado por una relación $\leq$, las siguientes condiciones son equivalentes.*

1. *Cada sucesión creciente $x_1 \leq x_2 \leq \dots$ en Σ es estacionaria (i.e. existe un $n \in \mathbb{N}$ tal que $x_k = x_n\ \forall k \geq n$).*
2. *Cada subconjunto no vacío de Σ tiene un elemento maximal.*

Demostración.
1) $\Rightarrow$ 2) Si 2) es falso, existe un subconjunto $T \subset \Sigma$ no vacío que no tiene elemento maximal. Al no ser vacío, podemos coger un elemento x_1 de T y, como no tiene elemento maximal, en particular x_1 no lo es, y debe existir otro elemento $x_2 \geq x_1$ en T. Y así podemos construir por recurrencia una sucesión creciente no estacionaria de Σ, lo que va en contra de 1).
2) $\Rightarrow$ 1) Si considero el rango de una sucesión creciente $(x_n)_{n\in\mathbb{N}}$ de Σ, como es un subconjunto no vacío debe tener un elemento maximal por hipótesis, digamos x_m, a partir del cual la sucesión estaciona por ser esta creciente y x_m maximal.

□

4.4.1. Módulos noetherianos y artinianos

Definición 4.4.2. [Módulo noetheriano] Sean A un anillo y M un A-módulo. Decimos que M es *noetheriano* si todo submódulo N de M es de tipo finito.

Observación 4.4.3. ‘

1. Un anillo A es noetheriano (resp. coherente) cuando lo es como A-módulo.
2. Los submódulos de un módulo noetheriano son noetherianos también.
3. Los submódulos de tipo finito de un módulo coherente son coherentes también.

El siguiente lema muestra que los módulos noetherianos son exactamente aquellos que verifican la llamada condición de cadena ascendente (c.c.a.) y, usando la proposición 4.4.1 vemos que esto equivale a que cada familia no vacía de submódulos tenga maximal.

Lema 4.4.4. *Un A-módulo M es noetheriano si y solo si se verifica una de las propiedades siguientes:*

1. *Cualquier cadena ascendente $M_1 \subset M_2 \subset \cdots \subset M$ de submódulos de M es estacionaria, es decir, existe un índice $n_0 \in \mathbb{N}$ tal que $M_{n_0} = M_n$ para todo $n \geqslant n_0$.*
2. *Cualquier familia no vacía de submódulos de M admite un elemento maximal.*

Demostración. Vamos a probar la equivalencia de la definición y la propiedad *(1)*, pues la equivalencia entre *(1)* y *(2)* ya se ha comentado en la proposición anterior.

Si M es noetheriano, sea $M_1 \subset M_2 \subset \cdots \subset M$ una cadena ascendente de submódulos de M. Entonces $N := \bigcup_{i \in \mathbb{N}} M_i$ es un submódulo de M (la unión de submódulos no lo es en general, pero es fácil ver que sí es cierto para cadenas ascendentes). Por ser M noetheriano, N debe ser de tipo finito, digamos $N = \sum_{j=1}^{n} Ax_j$ con $x_j \in N$ para $j = 1, ..., n$. Así que existirá $n_0 \in \mathbb{N}$ tal que $x_1, ..., x_n \in M_{n_0}$, de modo que $N \subset M_n$ para todo $n \geqslant n_0$. Como también $M_n \subset N$ por definición de N, se tiene la igualdad, de modo que la cadena estaciona.

Recíprocamente, si se verifica la c.c.a., supongamos que existiera un submódulo $N \subset M$ que no fuera de tipo finito. Entonces, para todo elemento $x_1 \in N$, se tiene que $Ax_n \subsetneq N$, así que existe $x_2 \in N \setminus Ax_1$. Como N no es de tipo finito también se tendrá que $Ax_1 + Ax_2 \subsetneq N$. Continuando con este argumento podemos construir una cadena estrictamente ascendente de submódulos de M, lo que contradice la hipótesis.

□

Proposición 4.4.5. *Si A es un anillo noetheriano y S un subconjunto de A multiplicativamente cerrado, entonces su localización en S, $S^{-1}A$, es noetheriana también.*

Demostración. Como A es noetheriano, todos sus ideales son finitamente generados. En virtud del segundo apartado de la proposición 4.3.10, todos los ideales de $S^{-1}A$ son de la forma $\mathfrak{a}S^{-1}A$ para cierto ideal $\mathfrak{a}$ de A (son extensiones de ideales de A). Por tanto, si $\mathfrak{a}$ tiene generadores $b_1, \ldots, b_n$, $\mathfrak{a}S^{-1}A$ tendrá por generadores $b_1/1, \ldots, b_n/1$ y será pues de generación finita.

□

El teorema siguiente nos permite construir nuevos ejemplos de anillos noetherianos. Para su demostración puede consultarse cualquier manual de Álgebra Conmutativa, por ejemplo [2] (cap. 1, pág. 50).

Proposición 4.4.6. ***[Teorema de la Base de Hilbert]*** *Sea A un anillo noetheriano. Entonces:*

1. *El anillo de polinomios $A[X]$ es noetheriano.*
2. *En particular, cualquier cociente $A[X_1, ..., X_n]/I$ del anillo de polinomios en un número finito de variables por un ideal $I \subset A[X_1, ..., X_n]$ es noetheriano.*

Introducimos ahora el concepto de módulos artinianos, como aquellos que verifican la condición de cadena descendente en lugar de la ascendente que caracterizaba a los noetherianos.

Definición 4.4.7. [Módulo artiniano] Un A-módulo M se llama *artiniano o de Artin* si verifica la *condición de cadena descendente (c.c.d.)*, esto es, que cada cadena descendente de submódulos $M \supset M_1 \supset M_2 \supset \ldots$ es estacionaria. Equivalentemente, M es artiniano si cada familia no vacía de submódulos de M admite un elemento minimal (4.4.1).

Ejemplo 4.4.8. Un ejemplo de módulo artiniano es cualquier espacio vectorial de dimensión finita, pues cualquier cadena descendente estricta de subespacios estaciona por ser las dimensiones estrictamente decrecientes. Por otro lado, si el espacio vectorial es de dimensión infinita, entonces no es artiniano, pues podemos construir una cadena decreciente no estacionaria a partir de una familia libre infinita del mismo.

Proposición 4.4.9. *Sea A un anillo de Artin. Entonces A contiene una cantidad a lo sumo finita de ideales primos, que además son todos maximales y por tanto también todos minimales. En particular, el radical de Jacobson y el nilradical de A coinciden:*

$$\mathcal{J}(A) = \mathcal{N}(A).$$

Demostración. Sea $\mathfrak{p} \subset A$ un ideal primo. Para ver que es maximal vamos a probar que $A/\mathfrak{p}$ es un cuerpo. Sea $x \in (A/\mathfrak{p})^*$. Como A es de Artin, también lo es $A/\mathfrak{p}$, y por tanto la cadena $(x) \supset (x^2) \supset \dots$ estaciona para un cierto índice i_0, así que existe $y \in A/\mathfrak{p}$ tal que $x^{i_0+1} \cdot y = x^{i_0}$. Como $A/\mathfrak{p}$ es un dominio de integridad, la ecuación anterior implica que $x \cdot y = 1$ y, en consecuencia x es una unidad. Por tanto todos los ideales primos de A son también maximales y se concluye la igualdad del radical de Jacobson y el nilradical.

Para ver que hay una cantidad finita de ideales primos en A razonemos por reducción al absurdo. Sea $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots$ una sucesión infinita de ideales primos distintos en A. Entonces $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supset \dots$ es una cadena descendente de ideales de A, y por tanto para cierto índice i_0 se verifica que $\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{i_0} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{i_0+1}$, de manera que $\mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{i_0} \subset \mathfrak{p}_{i_0+1}$, y utilizando el lema 4.1.16 concluimos que existe $j \in \{1, \dots, i_0\}$ tal que $\mathfrak{p}_j \subset \mathfrak{p}_{i_0+1}$. Pero habíamos supuesto que todos estos ideales eran distintos y por la parte anterior son también maximales, lo que nos lleva a una contradicción.

$\square$

Teorema 4.4.10. ***[Teorema de estructura de anillos de Artin]*** *Un anillo de Artin A puede escribirse como producto (finito) de sus localizaciones en sus ideales maximales.*

Demostración. Puede consultarse, por ejemplo, en el Stacks Project [10]. $\square$

4.4.2. Longitud de un módulo y dimensión de Krull

Para acabar esta sección, vamos a incluir nuevas caracterizaciones de los módulos noetherianos y artinianos a partir del concepto conocido como longitud de un módulo. Además, veremos sin demostración que, aunque parezcan condiciones análogas, los anillos de Artin son una subclase de los anillos de Noether: aquellos cuya dimensión de Krull es nula.

Definición 4.4.11. [Longitud de un módulo] Dado un A-módulo M, una *cadena* de submódulos de M es una sucesión $(M_i)_{i=0}^n$ de submódulos de M tal que

$$M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = 0.$$

La *longitud* de la cadena es el número de eslabones n sin contar el módulo M. Una *serie de composición* de M es una cadena maximal, es decir, que no se pueden insertar otros submódulos. Finalmente, definimos *longitud de un módulo M*, y denotamos por $l(M)$, al mínimo de las longitudes de todas las series de composición del mismo o ∞ si no admite ninguna serie de composición.

Lema 4.4.12. *Una cadena de submódulos de un A-módulo M es serie de composición si y solo si cada cociente M_{i-1}/M_i para $i = 1, \dots, n$ es simple, es decir, sus únicos submódulos son el cero y él mismo.*

Demostración. Si la cadena no es serie de composición, existe un índice i tal que existe un módulo N contenido estrictamente entre M_{i-1} y M_i, es decir $M_{i-1} \supsetneq N \supsetneq M_i$. En este caso, N/M_i es un submódulo no trivial de M_{i-1}/M_i, de modo que no es simple. Para el recíproco basta notar que los submódulos del cociente son todos de la forma N/M_i, así que si hay un submódulo no trivial para algún i, puede insertarse como nuevo eslabón en la cadena.

$\square$

La siguiente proposición nos muestra que, si una serie de composición de un módulo M es de longitud finita, digamos n, entonces todas las series tienen esa misma longitud n, de modo que para calcular la longitud del módulo basta saber la de una serie de composición cualquiera.

Proposición 4.4.13. *Si un A-módulo M tiene una serie de composición de longitud $n \in \mathbb{N}$, toda serie de composición de M tiene dicha longitud n, y cada cadena en M se puede extender a una serie de composición. En este caso decimos además que M es* de longitud finita.

Demostración. Vamos a probar esta proposición en tres etapas:

1. Si N es un submódulo estricto de M, entonces $l(N) < l(M)$. Tomemos (M_i) una serie de composición de M de longitud mínima. Para cada i se considera el submódulo $N_i = N \cap M$ de N. Como $N_{i-1}/N_i = N \cap (M_{i-1}/M_i) \subset M_{i-1}/M_i$ y este último es simple, entonces N_{i-1}/N_i es un submódulo trivial: o bien $N_{i-1} = N_i$, o bien $M_{i-1}/M_i = N_{i-1}/N_i$. Así, si quitamos los términos repetidos obtenemos una serie de composición de N, de manera que $l(N) \leq l(M)$. Si $l(N) = l(M) = n$, entonces $M_{i-1}/M_i = N_{i-1}/N_i$ para todo $i = 1, \ldots, n$. Como $M_n = N_n = 0$, $M_{n-1} = N_{n-1}$, por tanto $M_{n-2} = N_{n-2}$, y así sucesivamente hasta ver que $M = N$, lo que entra en contradicción con que N sea un submódulo estricto de M.
2. Cada cadena en M (y por tanto cada serie de composición) tiene longitud menor o igual que $l(M)$. Sea $(M_i)_{i=0}^k$ una cadena de longitud k. Del apartado anterior se tiene que $l(M) > l(M_1) > \ldots > l(M_k) = 0$, y como todas las desigualdades son estrictas y las longitudes enteras se deduce que $l(M) \geq k$. Como $l(M)$ es a la vez mínimo y máximo, se deduce que todas las cadenas de M deben tener dicha longitud.
3. Dada una cadena cualquiera en M, si su longitud es $l(M)$ debe ser una serie de composición, pues si no podrían añadírsele más términos y tendríamos una cadena de M de longitud mayor que $l(M)$, contradiciendo el apartado anterior. Si su longitud es menor que $l(M)$, no puede ser una serie de composición, de manera que puede añadírsele un eslabón al menos, y por recurrencia se puede ampliar hasta tener longitud $l(M)$ y ser por tanto una serie de composición.

□

Veamos ahora que los módulos de longitud finita son exactamente los que son tanto artinianos como noetherianos (lo que, como comentamos antes, es redundante, pues los primeros son en realidad una subclase de los segundos).

Proposición 4.4.14. *Un A-módulo M tiene una serie de composición si y solo si satisface las condiciones de cadena ascendente y descendente.*

Demostración. Si M tiene una serie de composición, entonces todas las sucesiones de módulos crecientes o decrecientes en el sentido de la inclusión deben tienen longitudes acotadas por $l(M)$, pues en caso contrario podría extraerse de dichas sucesiones una cadena de longitud mayor que $l(M)$, lo que contradice la proposición anterior. Por tanto, todas son estacionarias, así que se verifican las condiciones de cadena.

Recíprocamente, si M satisface ambas condiciones de cadena, construyamos una serie de composición como sigue. Como M es noetheriano, cualquier familia de submódulos de M admite un maximal, en particular la familia de todos los submódulos estrictos. Sea dicho maximal $M_1 \subsetneq M_0 = M$. Como los submódulos de uno noetheriano lo son, M_1 verifica la misma propiedad, y así sucesivamente podemos construir una sucesión de módulos descendente estricta $M_0 \supsetneq M_1 \supsetneq \ldots$, que ha de ser finita por ser M artiniano. Por la elección de cada M_i como maximal, no se pueden añadir eslabones, por lo que se obtiene así una serie de composición de M.

□

Proposición 4.4.15. *Para K-espacios vectoriales V las siguientes condiciones son equivalentes:*

1. *Dimensión finita*

2. Longitud finita

3. Noetheriano (c.c.a.)

4. Artiniano (c.c.d.)

Además, si estas condiciones se satisfacen, la dimensión coincide con la longitud.

Demostración. La implicación (1) $\implies$ (2) se deduce de la proposición anterior, pues todos los espacios vectoriales son artinianos y noetherianos. También de dicha proposición se deducen (2) $\implies$ (3) y (2) $\implies$ (4). Falta probar que (3) y (4) implican (1). Si se supone (1) falso entonces existe una sucesión libre infinita $(x_n)_{n=1}^{\infty}$ de elementos de V. Sean U_n (resp. V_n) los espacios vectoriales engendrados por $x_1, \ldots, x_n$ (resp. $x_{n+1}, x_{n+2}, \ldots$). Entonces la cadena (U_n) (resp. (V_n)) es infinita y ascendente en el sentido estricto (resp. descendente en el sentido estricto). □

Como anunciamos, se presenta ahora el concepto de dimensión de Krull de un anillo, que permite dar una relación completa entre los noetherianos y los artinianos. De la misma manera que hablábamos de cadenas de módulos al principio de este epígrafe, una cadena de ideales primos de un anillo A es una sucesión finita creciente en sentido estricto,

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

cuya longitud, n, es uno menos que el número de eslabones.

Definición 4.4.16. [Dimensión de Krull] Sea A un anillo. Se define su *dimensión* o *dimensión de Krull* como el máximo de las longitudes de sus cadenas de ideales primos. Se denotará por *dim* A.

La demostración del siguiente teorema, que requiere introducir conceptos de descomposición primaria, puede consultarse en cualquier manual de Álgebra Conmutativa (por ejemplo [1] o [2]).

Teorema 4.4.17. *Un anillo A es artiniano si y solo si es noehteriano y $\dim A = 0$. Puede sustituirse la condición $\dim A = 0$ por que todos los ideales primos de A sean maximales, pues entonces y solo entonces todas las cadenas de ideales primos tendrán un único eslabón.*

4.5. Producto tensorial y extensión de escalares

Esta sección comienza construyendo el producto tensorial de módulos, un objeto caracterizado por una propiedad universal que a primera vista resulta bastante abstracto. Veremos en la primera parte las buenas propiedades de este objeto: es conmutativo, asociativo, respeta las sumas directas de módulos y la estructura de álgebra en caso de haberla ... En la segunda subsección se estudia el proceso de tensorización de un morfismo de módulos, a grandes rasgos, considerar el morfismo inducido al hacer el producto tensorial por un módulo fijo. Esta transformación no siempre preserva la exactitud, y de ahí el interés de los módulos planos y los fielmente planos. Terminamos con una de las principales motivaciones para presentar el producto tensorial: los procesos de extensión y restricción de escalares de un módulo. Para entender estos conceptos, podemos pensar por ejemplo en un $\mathbb{C}$-espacio vectorial, que puede considerarse también un espacio vectorial sobre $\mathbb{R}$, esto sería una restricción de escalares de dicho espacio. Si queremos hacer el proceso inverso y extender los escalares de un $\mathbb{R}$-espacio vectorial a $\mathbb{C}$, la herramienta que usaremos será el producto tensorial. En toda esta sección, se ha consultado sobre todo [2], y se refiere a él para algunas demostraciones, pues no son complicadas, pero sí tediosas de escribir por la cantidad de diagramas.

4.5.1. Producto tensorial

Definición 4.5.1. [Producto tensorial] Dados dos A-módulos M y N, un *producto tensorial* de M y N sobre A es un par (T, τ) formado por un A-módulo T y una aplicación A-bilineal $\tau : M \times N \longrightarrow T$ verificando la siguiente propiedad universal: *Para cada aplicación A-bilineal $\Phi : M \times N \longrightarrow E$ donde E es un A-módulo, existe una única aplicación A-lineal $\varphi : T \longrightarrow E$ tal que $\Phi = \varphi \circ \tau$; esto es, tal que el diagrama siguiente es conmutativo:*

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[d, "\Phi"] & T \arrow[dl, dashed, "\varphi"] \\ E & \end{tikzcd} \tag{4.5.1.1}$$

Observación 4.5.2. Usando la notación de la definición anteior, de la propiedad universal deducimos que, para cualquier A-módulo E, hay una correspondencia biyectiva entre las aplicaciones A-bilineales $M \times N \longrightarrow E$ y las aplicaciones A-lineales $T \longrightarrow E$.

Proposición 4.5.3. *Un producto tensorial está unívocamente determinado por la propiedad universal, salvo isomorfismo canónico.*

Demostración. Sean $\tau : M \times N \longrightarrow T$ y $\tau' : M \times N \longrightarrow T'$ productos tensoriales de M y N sobre A. Entonces existe un diagrama

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[d, "\tau'"] & T \arrow[dl, shift left, "\varphi"] \\ T' \arrow[ur, shift left, "\psi"] & \end{tikzcd} \tag{4.5.3.1}$$

donde φ y ψ son A-morfismos cuya existencia se deduce de las propiedades universales para τ y τ' respectivamente. Y de estas también se tienen las factorizaciones $\tau' = \varphi \circ \tau$ y $\tau = \psi \circ \tau'$, de donde

$$id_T \circ \tau = \tau = \psi \circ \tau' = (\psi \circ \varphi) \circ \tau.$$

Entonces, considerando τ como una aplicación A-bilineal y usando la propiedad universal para τ también, existe un único A-morfismo $\sigma : T \longrightarrow T$ tal que $\tau = \sigma \circ \tau$. Como tanto id_T como $\psi \circ \varphi$ verifican esta ecuación, necesariamente $id_T = \psi \circ \varphi$. Simétricamente, podemos deducir que

$\varphi \circ \psi = id_{T'}$, de modo que φ y ψ son isomorfismos inversos el uno del otro. Así concluimos que ambos productos tensoriales (T, τ) y (T', τ') son isomorfos.

□

Observación 4.5.4. Cuando consideremos un producto tensorial (T, τ) de dos A-módulos M, N escribiremos $M \otimes_A N$ en lugar de T y $x \otimes y$ en lugar de $\tau(x, y)$, para $(x, y) \in M \times N$. Llamaremos a $x \otimes y$ el *tensor* construidos a partir de x e y. A veces obviaremos la aplicación y nos referiremos a $M \otimes_A N$ como producto tensorial de M y N, o incluso $M \otimes N$ cuando no haya duda del anillo de base. Usando esta notación, como la aplicación $\tau : M \times N \longrightarrow M \otimes_A N$ es A-bilineal, los tensores $x \otimes y$ son bilineales en sus dos factores.

Proposición 4.5.5. *El producto tensorial $T = M \otimes_A N$ existe para cualesquiera A-módulos M y N.*

Demostración. Consideramos $A^{M\times N}$ como una A-módulo,

$$e_{(x,y)} = (\delta_{x,x'} \cdot \delta_{y,y'})_{(x',y')\in M\times N}, \quad x \in M, y \in N,$$

el sistema generador libre del módulo. Escribiendo (x, y) en lugar de $e_{(x,y)}$ podemos ver $A^{M\times N}$ como el A-módulo generado por los pares $(x, y) \in M \times N$. Ahora vamos a reducir módulo el menor $Q \subset A^{M\times N}$ submódulo tal que las clases $\overline{(x, y)}$ adquieran la propiedad universal de los tensores. Es decir, consideramos el submódulo $Q \subset A^{M\times N}$ generado por los elementos de tipo

$$(x + x', y) - (x, y) - (x', y),\ (x, y + y') - (x, y) - (x, y'),\ (ax, y) - a(x, y),\ (x, ay) - a(x, y),$$

donde $a \in A$, $x, x' \in M$, $y, y' \in N$, Poniendo $T := A^{M\times N}/Q$, el homomorfismo canónico $\tau : M \times N \longrightarrow T$, $(x, y) \mapsto \overline{(x, y)}$ es A-bilineal. Veamos que además verifica la propiedad universal de un tensor.
Sea entonces $\Phi : M \times N \longrightarrow E$ una aplicación A-bilineal con E un A-módulo. Podemos considerar la aplicación A-lineal asociada $\hat{\varphi} : A^{M\times N} \longrightarrow E$ definida fijando $\hat{\varphi}(x, y) = \Phi(x, y)$ donde los (x, y) son los $e_{(x,y)} \in A^{M\times N}$ de antes y para el resto de elementos de $A^{M\times N}$, la aplicación queda determinada por extensión A-lineal. Además, como Φ es A-bilineal, $ker\hat{\varphi}$ contiene todos los generadores de Q que enumeramos arriba, luego $Q \subset ker\hat{\varphi}$ y por el teorema de factorización deducimos la existencia de un aplicación A-lineal $\varphi : A^{M\times N}/Q \longrightarrow E$ verificando $\Phi = \varphi \circ \tau$:

$$\begin{tikzcd}
\tau : M \times N \arrow[r] \arrow[d, "\Phi"'] & A^{M\times N} \arrow[r] \arrow[dl, "\hat{\varphi}"] & A^{M\times N}/Q \arrow[dll, "\varphi"] \\
E & &
\end{tikzcd} \tag{4.5.5.1}$$

Para acabar basta observar que φ está unívocamente determinada por la relación $\Phi = \varphi \circ \tau$, ya que las clases $\overline{(x, y)}$ para $(x, y) \in M \times N$ engendran $A^{M\times N}/Q$ como A-módulo y tenemos además

$$\varphi(\overline{(x, y)}) = \varphi(\tau(x, y)) = \Phi(x, y).$$

De modo que φ está unívocamente determinada en un conjunto de generadores de $T = A^{M\times N}/Q$ y, por tanto, unívocamente determinada también en todo T.

□

De ahora en adelante, para manejar los productos tensoriales, su construcción explícita no tendrá demasiada importancia: en casi todos los casos es posible deducir la información que necesitamos de la propiedad universal. Por ejemplo, aunque el siguiente resultado se deduce inmediatamente de la construcción anterior, lo vamos a obtener razonando con la propiedad universal.

Proposición 4.5.6. *Sean M y N dos A-módulos. Entonces cualquier elemento $z \in M \otimes_A N$ puede expresarse como suma finita de tensores, esto es, de la forma $z = \sum_{i=1}^{r} x_i \otimes y_i$ con $x_i \in M$ e $y_i \in N$.*

Demostración. Consideramos el submódulo $T \subset M \otimes_A N$ engendrado por todos los tensores $x \otimes y$ con $x \in M$ e $y \in N$. Entonces la aplicación $\tau : M \times N \longrightarrow M \otimes_A N$ del producto tensorial se puede restringir a una aplicación A-bilineal $\tau' : M \times N \longrightarrow T$ que, al igual que τ, satisface la propiedad universal del producto tensorial. Efectivamente, dada $\Phi : M \times N \longrightarrow E$ una aplicación A-bilineal a un A-módulo E, existe una aplicación A-lineal $\varphi : M \otimes_A N \longrightarrow E$ tal que $\Phi = \varphi \circ \tau$. Entonces la restricción $\varphi' = \varphi_{|T}$ satisface $\Phi = \varphi' \circ \tau'$. Además, φ' está unívocamente determinada por esta propiedad ya que los tensores $\tau'(x, y)$ para $x \in M, y \in N$ su imagen viene dada por $\varphi'(\tau'(x, y)) = \Phi(x, y)$. Así, T es un producto tensorial de M y N sobre A, y por la unicidad demostrada antes se tiene la igualdad $T = M \otimes_A N$.

□

Corolario 4.5.7. *Sean $(x_i)_{i \in I}$ y $(y_j)_{j \in J}$ sistemas de generadores de dos A-módulos M y N. Entonces $(x_i \otimes y_j)_{i \in I, j \in J}$ es un sistema de generadores de $M \otimes_A N$. En particular, si M y N son de tipo finito, también lo es su producto tensorial.*

Demostración. Dados $x \in M$ e $y \in N$, podemos expresarlos en los respectivos sistemas de generadores de la forma

$$x = \sum_{i \in I} a_i x_i, \quad y = \sum_{j \in J} b_j y_j$$

con coeficientes $a_i, b_j \in A$, de modo que

$$x \otimes y = \sum_{i \in I, j \in J} a_i b_j x_i \otimes y_j.$$

Finalmente, usando la proposición anterior, cada elemento de $M \otimes_A N$ se puede escribir como combinación lineal finita de tensores como el anterior, de donde se tiene que $(x_i \otimes y_j)_{i \in I, j \in J}$ es un sistema de generadores de $M \otimes_A N$.

□

La siguiente observación, que no es más que una reformulación de la propiedad universal de los productos tensoriales, teniendo en cuenta el corolario anteior, será útil más adelante para definir aplicaciones A-lineales de un producto tensorial en otro A-módulo.

Observación 4.5.8. Sean M y N dos A-módulos y $(z_{x,y})_{x \in M, y \in N}$ una familia de elementos de un A-módulo E.

1. Si $\varphi : M \otimes_A N \longrightarrow E$ es una aplicación A-lineal que verifica $\varphi(x \otimes y) = z_{x,y} \in E$ para todos $x \in M$, $y \in N$, entonces φ es única.
2. Si la aplicación $\Phi : M \times N \longrightarrow E$ dada por $\Phi(x, y) = z_{x,y}$ es A-bilineal, entonces existe una aplicación A-lineal $\varphi : M \otimes_A N \longrightarrow E$ tal que $\varphi(x \otimes y) = z_{x,y} \in E$ para todos $x \in M$, $y \in N$, y φ es única gracias al apartado anterior.

Veamos ahora algunas propiedades elementales del producto tensorial (conmutatividad, asociatividad, compatibilidad con la suma directa de módulos...)

Lema 4.5.9. *Sean M, N, P tres A-módulos y $F \simeq A$ un A-módulo libre generado por un elemento $e \in F$. Entonces existen los isomorfismos canónicos de A-módulos siguientes:*

1. $F \otimes_A M \xrightarrow{\sim} M, \;\; ae \otimes x \mapsto ax,$
2. [Conmutatividad] $\;M \otimes_A N \xrightarrow{\sim} N \otimes_A M, \;\; x \otimes y \mapsto y \otimes x,$
3. [Asociatividad] $\;(M \otimes_A N) \otimes_A P \xrightarrow{\sim} M \otimes_A (N \otimes_A P), \;\; (x \otimes y) \otimes z \mapsto x \otimes (y \otimes z).$

Demostración.
(1) La aplicación $F \times M \longrightarrow M$, $(ae, x) \mapsto ax$ es A-bilineal de modo que, por la observación anterior, induce una aplicación A-lineal $\varphi : F \otimes_A M \longrightarrow M$, $ae \otimes x \mapsto ax$.. También podemos considerar la aplicación A-lineal $\psi : M \longrightarrow F \otimes_A M$, $x \mapsto e \otimes x$, que verifica $\varphi \circ \psi = id_M$ y, usando la A-bilinearidad del producto tensorial,

$$\psi \circ \varphi(ae \otimes x) = \psi(ax) = e \otimes (ax) = a(e \otimes x) = ae \otimes x$$

para $a \in A$, $x \in M$. De modo que $\psi \circ \varphi = id_{F \otimes_A M}$, así que son inversas la una de la otra, y por tanto biyectivas.

(2) Consideremos la aplicación A-bilineal $\Phi : M \times N \longrightarrow N \otimes_A M$, $(x, y) \mapsto y \otimes x$. De la propiedad universal para el producto tensorial $(M \otimes_A N, \tau)$ deducimos que existe una única aplicación A-lineal $\varphi : M \otimes_A N \longrightarrow N \otimes_A M$ tal que $\Phi = \varphi \circ \tau$. Razonando de manera análoga para $(N \otimes_A M, \tau')$ y $\Phi' : N \times M \longrightarrow M \otimes_A N$, $(y, x) \mapsto x \otimes y$ obtenemos una aplicación A-lineal $\varphi' : N \otimes_A M \longrightarrow M \otimes_A N$ con la propiedad $\Phi' = \varphi' \circ \tau'$. Además,

$$\varphi' \circ \varphi(x \otimes y) = \varphi' \circ \varphi(\tau(x, y)) = \varphi' \circ (\Phi(x, y)) = \varphi'(y \otimes x) = \varphi'(\tau'(y, x)) = x \otimes y.$$

Y razonando idénticamente para $\varphi \circ \varphi'$, como los tensores $x \otimes y$ (resp. $y \otimes x$) con $x \in M$, $y \in N$ engendran $M \otimes_A N$ (resp. $N \otimes_A M$), concluimos que son inversas la una de la otra, y por tanto biyectivas.

(3) Fijamos $x \in M$ y definimos la aplicación bilineal $N \times P \longrightarrow (M \otimes_A N) \otimes_A P$, $(y, z) \mapsto (x \otimes y) \otimes z$. De la propiedad universal del producto tensorial $N \otimes_A P$ deducimos la existencia de una aplicación A-lineal $\varphi_x : N \otimes_A P \longrightarrow (M \otimes_A N) \otimes_A P$ tal que $\varphi_x(y \otimes z) = (x \otimes y) \otimes z$ para $y \in N, z \in P$. Ahora definimos la aplicación bilineal

$$M \times (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes_A P,$$

$$(x, \sum_{i=1}^{n} (y_i \otimes z_i)) \mapsto \varphi_x(\sum_{i=1}^{n} (y_i \otimes z_i)).$$

Por la propiedad universal de $M \otimes_A (N \otimes_A P)$ existe una única aplicación A-lineal $\varphi : M \otimes_A (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes_A P$ tal que $\varphi(x \otimes (y \otimes z)) = (x \otimes y) \otimes z$ para todos $(x, y, z) \in M \times N \times P$. Un razonamiento simétrico nos garantiza también la existencia y unicidad de una aplicación A-lineal $\psi : (M \otimes_A N) \otimes_A P \longrightarrow M \otimes_A (N \otimes_A P)$ verificando $\psi((x \otimes y) \otimes z) = x \otimes (y \otimes z)$ para todos $(x, y, z) \in M \times N \times P$. Deducimos una vez más que son inversas la una de la otra y, por tanto, isomorfismos.

(Nótese que en las dos demostraciones anteriores, los tensores del tipo $a \otimes b$ que han ido apareciendo pertenecen en cada caso a un producto tensorial distinto.)

$\square$

Proposición 4.5.10. *Sea $(M_i)_{i \in I}$ una familia de A-módulos y N otro A-módulo. Entonces existe un isomorfismo canónico*

$$(\bigoplus_{i \in I} M_i) \otimes_A N \xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes_A N), \;\; (x_i)_{i \in I} \otimes y \mapsto (x_i \otimes y)_{i \in I}.$$

Demostración. La aplicación

$$(\bigoplus_{i\in I} M_i)\times N \longrightarrow \bigoplus_{i\in I}(M_i\otimes_A N),\ ((x_i)_{i\in I},y)\mapsto (x_i\otimes y)_{i\in I},$$

es A-bilineal, de modo que invocando la propiedad universal una vez más, existe una aplicación A-lineal

$$\varphi : (\bigoplus_{i\in I} M_i)\otimes_A N \longrightarrow \bigoplus_{i\in I}(M_i\otimes_A N)$$

de la forma de la del enunciado. Para encontrar su inversa, consideremos las inclusiones $Mj \hookrightarrow \oplus_{i\in I}M_i$ para cada $j\in I$, y las aplicaciones inducidas

$$M_j\times N \hookrightarrow (\bigoplus_{i\in I} M_i)\times N \longrightarrow (\bigoplus_{i\in I} M_i)\otimes_A N.$$

Son aplicaciones A-bilineales que inducen aplicaciones A-lineales

$$\psi_j : M_j\otimes_A N \longrightarrow (\bigoplus_{i\in I} M_i)\otimes_A N,\ j\in I,$$

$$x_j\otimes y \longmapsto (0,...,x_j,...,0,...)\otimes y$$

de donde deducimos una aplicación A-lineal

$$\psi : \bigoplus_{i\in I}(M_i\otimes_A N) \longrightarrow (\bigoplus_{i\in I} M_i)\times N,\ z_i := (x_i\otimes y_i)_{i\in I} \longmapsto \sum_{i\in I}\psi_i(z_i) = (x_i)_{i\in I}\otimes \sum_{i\in I} y_i.$$

Y observamos que φ y ψ son inversas la una de la otra.

□

Corolario 4.5.11. *Sea M un A-módulo libre y sea $(x_i)_{i\in I}$ una base del mismo. Entonces para cualquier A-módulo N se tienen los siguientes isomorfismos.*

$$M\otimes_A N \simeq \bigoplus_{i\in I}(Ax_i\otimes_A N)\simeq N^{(I)}.$$

Demostración. Como $(x_i)_{i\in I}$ es una base de M, podemos escribir $M = \oplus_{i\in I}Ax_i$. Reescrito así vemos que el primer isomorfismo es consecuencia de la proposición anterior. Teniendo en cuenta además que Ax_i es un A-módulo de rango 1, del primer apartado de 4.5.9 deducimos que $(Ax_i\otimes_A N)\simeq N$ de donde se tiene el segundo isomorfismo.

□

Corolario 4.5.12. *Sea A un anillo y N un A-módulo cualquiera. Si $X = (X_i)_{i\in I}$ es una familia de indeterminadas, se tiene que $A[X]\otimes_A N\simeq N[X]$.*

Demostración. Basta usar el corolario anterior, 4.5.11, pues $A[X]$ es un A-módulo libre. Como $N^{(I)}\simeq N[X]$, se concluye el isomorfismo pedido.

□

Para acabar remarcamos que, si los módulos para los que calculamos el producto tensorial tienen además estructura de A-álgebra, dicho producto tensorial también la tiene.

Proposición 4.5.13. *Sea A un anillo y B y C dos A-álgebras de morfismos estructurales $f : A\longrightarrow B$ y $g : A\longrightarrow C$ respectivamente. El A-módulo $D := B\otimes_A C$ puede dotarse de una estructura de A-álgebra de neutro multiplicativo $1\otimes 1$ y tal que $\phi : A\longrightarrow D;\ \ a\longmapsto f(a)\otimes g(a)$ es un homomorfismo de anillos.*

Demostración. Como ya sabemos que el producto tensorial de A-módulos tiene estructura de A-módulo también, basta ver que es un anillo con un producto compatible con el producto por escalares.

Se considera la aplicación

$$B \times C \times B \times C \longrightarrow D; \quad (b, c, b', c') \longmapsto bb' \otimes cc',$$

que es A lineal en cada factor. Por tanto, usando tres veces la propiedad universal del producto tensorial y su asociatividad (lema 4.5.9) deducimos la existencia y unicidad de un homomorfismo de A-módulos

$$D \otimes_A D \longrightarrow D.$$

Ahora bien, como se comentó en la observación 4.5.2, este A-morfismo induce una aplicación A-bilineal

$$D \times D \longrightarrow D; \quad (b \otimes c, b' \otimes c') \longmapsto bb' \otimes cc',$$

que será el producto en el anillo D. Además, de la bilinealidad anterior se deduce en particular que es compatible con la estructura de A-módulo, de modo que D es una A-álgebra. Comprobar que $1 \otimes 1$ es el neutro multiplicativo y ϕ un morfismo de anillos es rutinario y se omite.

□

Proposición 4.5.14. *Sea A un anillo, $\mathfrak{a}$ un ideal suyo y B una A-álgebra de morfismo estructural $f : A \longrightarrow B$. Entonces se tiene el morfismo de A-álgebras siguiente:*

$$B \otimes_A A/\mathfrak{a} \longleftrightarrow B/\mathfrak{a}B.$$

Demostración. Consideremos la aplicación A-bilineal siguiente:

$$B \times A/\mathfrak{a} \longrightarrow B/\mathfrak{a}B; \quad (b, a + \mathfrak{a}) \longmapsto f(a)b + \mathfrak{a}B.$$

Por la propiedad universal del producto tensorial, esta aplicación induce un homomorfismo de A-módulos

$$\rho : B \otimes_A A/\mathfrak{a} \longrightarrow B/\mathfrak{a}B; \quad b \otimes (a + \mathfrak{a}) \longmapsto f(a)b + \mathfrak{a}B.$$

Notemos que, por A-bilinealidad del producto tensorial $b \otimes (a + \mathfrak{a}) = a(b \otimes (1 + \mathfrak{a})$ para cualesquiera $b \in B$ y $a \in A$. Si definimos, para cada $b \in B$, $\psi(b + \mathfrak{a}B) = b \otimes (1 + \mathfrak{a})$, ψ puede extenderse a un morfismo A-lineal de $B/\mathfrak{a}B$ en $B \otimes_A A/\mathfrak{a}B$ que resulta ser la inversa del morfismo ρ anterior. Basta notar que, dado $f(a)b \in B$, $\psi(f(a)b) = a\psi(b) = a(b \otimes (1 + \mathfrak{a})) = (b \otimes (a + \mathfrak{a}))$.

□

El siguiente lema, que presenta una propiedad universal para los morfismos de inclusión de álgebras en su producto tensorial, se utilizará para estudiar las extensiones de escalares en anillos de polinomios.

Lema 4.5.15. *Sea A un anillo y sean B y C dos A-álgebras. Entonces los homomorfismos canónicos*

$$\sigma_B : B \longrightarrow B \otimes_A C, \quad b \longmapsto b \otimes 1,$$
$$\sigma_C : C \longrightarrow B \otimes_A C, \quad c \longmapsto 1 \otimes c,$$

verfican la propiedad universal siguiente: «Para cualquier A-álgebra D y para cualesquiera homomorfismos de A-álgebras $\varphi_B : B \longrightarrow D$ y $\varphi_C : C \longrightarrow D$ existe un único homomorfismo de A-álgebras $\varphi : B \otimes_A C \longrightarrow D$ tal que el diagrama siguiente es conmutativo»:

$$\begin{tikzcd}
C \arrow[d, "\sigma_C"] \arrow[dr, "\varphi_C"] & \\
B \otimes_A C \arrow[r, dashed, "\varphi"] & D \\
B \arrow[u, "\sigma_B"] \arrow[ur, "\varphi_B"] &
\end{tikzcd}$$

Demostración. Para todos $b \in B$ y $c \in C$ se tiene que

$$\varphi(b \otimes c) = \varphi((b \otimes 1) \cdot (1 \otimes c)) = \varphi(b \otimes 1) \cdot \varphi(1 \otimes c) = \varphi_B(b) \cdot \varphi_C(c),$$

Por tanto, el morfismo φ queda unívocamente determinado por φ_B y φ_C, de donde se tiene la unicidad. Para la existencia basta considerar la aplicación A-bilineal siguiente:

$$B \times C \longrightarrow D, \quad (b, c) \longmapsto \varphi_B(b) \cdot \varphi_C(c),$$

la cual induce, por la propiedad universal del producto tensorial, un A-morfismo

$$\varphi : B \otimes_A C \longrightarrow D, \quad b \otimes c \longmapsto \varphi_B(b) \cdot \varphi_C(c).$$

Esta aplicación es de hecho un homomorfismo de A-álgebras y hace el diagrama anterior conmutativo. Veamos por ejemplo que $\varphi \circ \sigma_B = \varphi_B$ (el resto de comprobaciones son similares o rutinarias). Dado $b \in B$, $\sigma_B(b) = b \otimes 1$ y $\varphi(b \otimes 1) = \varphi_B(b) \cdot \varphi_C(1) = \varphi_B(b)$, como queríamos.

□

4.5.2. Platitud

Dados dos morfismos de A-módulos $\varphi : M \longrightarrow M'$ y $\psi : N \longrightarrow N'$, es inmediato comprobar que el morfismo

$$M \times N \longrightarrow M' \otimes_A N'; \;\; x \times y \longmapsto \varphi(x) \otimes \psi(y)$$

es A-bilineal en x e y. Usando la propiedad universal del producto tensorial, podemos garantizar la existencia de un A-morfismo

$$\varphi \otimes \psi : M \otimes_A N \longrightarrow M' \otimes_A N', \;\; x \otimes y \longmapsto \varphi(x) \otimes \psi(y),$$

que llamaremos producto tensorial de los morfismos φ y ψ sobre A. En particular, es de especial interés el caso en que uno de los morfismos considerados es la identidad.

Definición 4.5.16. [Tensorización de un morfismo con un módulo] Dado un morfismo de A-módulos $\varphi : M \longrightarrow M'$ y un A-módulo N, llamamos *tensorización de φ con N sobre A* al morfismo de A-módulos resultante de tensorizar φ con id_N, esto es,

$$\varphi \otimes id_N : M \otimes_A N \longrightarrow M' \otimes_A N; \;\; x \otimes y \longmapsto \varphi(x) \otimes y.$$

De la misma manera podemos tensorizar sucesiones de A-morfismos, proceso que respeta las composiciones de morfismos, como explicitamos en el lema siguiente.

Lema 4.5.17. *Sea*

$$M \xrightarrow{\varphi} M' \xrightarrow{\psi} M'',$$

una sucesión de A-morfismos y N un A-módulo. Entonces $(\psi \circ \varphi) \otimes id_N = (\psi \otimes id_N) \circ (\varphi \otimes id_N)$.

Demostración. Basta probar que ambos morfismos coinciden para tensores del tipo $x \otimes y$ con $x \in M$ e $y \in N$, pues los elementos del producto tensorial $M \otimes_A N$ son suma de tensores de esa forma y por linealidad de los morfismos se concluye. Dados pues $x \in M$ e $y \in N$, basta aplicar la definición del producto tensorial de morfismos para concluir:

$$(\psi \circ \varphi) \otimes id_N(x \otimes y) = (\psi \circ \varphi)(x) \otimes y = (\psi \otimes id_N) \circ (\varphi \otimes id_N)(x \otimes y).$$

□

Si ahora tomamos una sucesión exacta de módulos, es natural preguntarse si la sucesión tensorizada mantendrá esta propiedad. En el caso general se tiene «exactitud a derechas», pero no se preserva la inyectividad de los morfismos. De ahí el interés de los módulos planos que definiremos después, que son los que la mantienen.

Proposición 4.5.18. ***[Exactitud a derechas del producto tensorial]*** *Sea*

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \xrightarrow{0} 0,$$

una sucesión exacta de A-módulos. Entonces, para cada A-módulo N, la sucesión

$$M' \otimes_A N \xrightarrow{\varphi \otimes id_N} M \otimes_A N \xrightarrow{\psi \otimes id_N} M'' \otimes_A N \longrightarrow 0,$$

obtenida al tensorizar con N sobre A, es exacta también.

Demostración. Por la exactitud de la primera sucesión se tiene que $Im(\varphi) = Ker(\psi)$, de modo que, en virtud del lema 4.5.17, se tiene que

$$(\psi \circ \varphi) \otimes id_N = (\psi \otimes id_N) \circ (\varphi \otimes id_N) = 0,$$

y por tanto $Im(\varphi \otimes id_N) \subseteq Ker(\psi \otimes id_N)$. Así pues, por el primer teorema de isomorfía para módulos, $\psi \otimes id_N$ admite una factorización

$$\begin{tikzcd} M \otimes_A N \arrow[r, "\psi \otimes id_N"] \arrow[d, "\pi"] & M'' \otimes_A N \\ (M \otimes_A N)/Im(\varphi \otimes id_N). \arrow[ur, "\overline{\psi}"] & \end{tikzcd}$$

También por el primer teorema de isomorfía se tienen las equivalencias siguientes:

1. $Im(\varphi \otimes id_N) = Ker(\psi \otimes id_N)$ si y solo si $\overline{\psi}$ es inyectiva.
2. $\psi \otimes id_N$ es sobreyectiva si y solo si $\overline{\psi}$ lo es.

Por tanto, para ver que la sucesión tensorizada es exacta bastará ver que $\overline{\psi}$ es un isomorfismo. Consideramos la aplicación $\sigma : M'' \times N \longrightarrow (M \otimes_A N)/Im(\varphi \otimes id_N)$; $(x'', y) \longmapsto \overline{\rho(x'') \otimes y}$, donde $\rho(x'') \in M$ denota una ψ-preimagen cualquiera de $x'' \in M''$ (siempre existe puesto que ψ es sobreyectiva por la exactitud de la sucesión inicial). Esta aplicación está bien definida y es un morfismo de A-módulos inverso de $\overline{\psi}$, de donde se deduce que es un isomorfismo, como queríamos. Los detalles son sencillos pero tediosos de escribir y pueden consultarse en [2].

$\square$

Ejemplo 4.5.19. Vemos ahora un ejemplo sencillo de un caso en el que la tensorización de un morfismo no preserva la inyectividad.
Sea $\varphi : 2\mathbb{Z} \hookrightarrow \mathbb{Z}$ la inyección canónica. Como $\mathbb{Z} \simeq 2\mathbb{Z}$ como $\mathbb{Z}$-módulos, la aplicación tensorizada

$$\varphi \otimes id : 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$$

corresponde a la aplicación nula $0 : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$, que obviamente no es inyectiva. Aquí hemos usado la proposición 4.5.9 para probar que $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, y que cada elemento $2k \otimes \bar{z}$ se envía a $k \otimes 2\bar{z} = k \otimes 0$ por $\mathbb{Z}$-bilinealidad de los tensores.

Como acabamos de ver en el ejemplo anterior, si M_1 es un submódulo de M_2 nada nos garantiza que al tensorizar por otro módulo N, $M_1 \otimes_A N$ vaya a ser submódulo de $M_2 \otimes_A N$. Como parece algo deseable, vamos a introducir el concepto de platitud, que nos permitirá distinguir aquellos módulos que sí mantienen la inyectividad de un morfismo al tensorizarlos por él.

Definición 4.5.20. **[Módulo plano]** Un A-módulo N se llama *plano sobre A o A-plano* si para cada morfismo de A-módulos inyectivo $M' \longrightarrow M$, el A-morfismo $M' \otimes_A N \longrightarrow M \otimes_A N$ obtenida haciendo el producto tensorial con N sobre A es inyectivo. Si no hay confusión con el anillo de base se dirá simplemente que N es plano. Un homomorfismo de anillos $\varphi : A \longrightarrow A'$ se llama *plano* si A', visto como A-módulo a través de φ, es plano.

Proposición 4.5.21. *Sea A un anillo.*

1. *El anillo A visto como A-módulo es plano.*
2. *La suma directa de A-módulos planos es plana.*
3. *Cualquier A-módulo libre es plano.*
4. *Un anillo de polinomios $A[(X_i)_{i\in I}]$ en un número cualquiera de variables es plano.*

Demostración. .

1. En virtud del lema 4.5.9, para cada A-módulo N se tiene que $N \otimes_A A \simeq N$. Por tanto, si $M' \hookrightarrow M$ es un morfismo de A-módulos inyectivo, al tensorizarlo por A se mantiene la inyectividad, pues los tensorizados son isomorfos a M' y M.
2. Sean $(N_i)_{i\in I}$ una familia de A-módulos planos y $M' \hookrightarrow M$ un morfismo de A-módulos inyectivo. Queremos ver que el morfismo tensorizado
$$(\oplus_{i\in I} N_i) \otimes_A M' \longrightarrow (\oplus_{i\in I} N_i) \otimes_A M$$
sigue siendo inyectivo. Como los N_i son planos sabemos que los morfismos $N_i \otimes_A M' \longrightarrow N_i \otimes_A M$ son inyectivos, y usando la proposición 4.5.10 se deduce que $(\oplus_{i\in I} N_i) \otimes_A M \simeq \oplus_{i\in I}(N_i \otimes_A M)$ y lo mismo sustituyendo M por M' y se deduce la inyectividad deseada.
3. Un A-módulo libre M será isomorfo a un $A^{(I)}$ para un cierto conjunto I. Esto es, M es suma directa de copias de A, que es plano por la parte 1. Así que usando la parte 2, M es plano como suma directa de módulos planos.
4. Basta notar que un anillo de polinomios en las variables $(X_i)_{i\in I}$ es suma directa de A-módulos monógenos del tipo AX_i^n para $i \in I$ y $n \in \mathbb{N}$.

□

Proposición 4.5.22. ***[Caracterización de módulos planos]*** *Sea A un anillo. Para un A-módulo N las siguientes condiciones son equivalentes:*

1. *N es plano.*
2. *Si*
$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$
es una sucesión exacta de A-módulos, entonces la sucesión
$$0 \longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0,$$
obtenida al tensorizar con N sobre A, es exacta.

3. Si

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

es una sucesión exacta de A-módulos, entonces la sucesión

$$M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N,$$

obtenida al tensorizar con N sobre A, es exacta.

Demostración.
(1) $\Longrightarrow$ (2) Basta usar la exactitud a derechas del producto tensorial (4.5.18) para ver la exactitud de la sucesión deseada salvo el primer eslabón, que a su vez no es más que la definición de módulo plano.
(2) $\Longrightarrow$ (3) Consideramos la sucesión exacta

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'',$$

de manera que $Ker(\psi) = Im(\varphi)$ y se tiene el diagrama conmutativo siguiente de filas exactas:

$$\begin{tikzcd}
M' \arrow[r] \arrow[drr] & Im(\varphi) \arrow[r] \arrow[d, equal, "\varphi"] & 0 & & \\
0 \arrow[r] & Ker(\psi) \arrow[r] & M \arrow[r] \arrow[drr] & Im(\psi) \arrow[r] \arrow[d, equal, "\psi"] & 0 \\
 & & 0 \arrow[r] & Im(\psi) \arrow[r] & M''.
\end{tikzcd}$$

Completando la primera y tercera filas a sucesiones exactas cortas estamos en las condiciones de aplicar (2) y obtener un nuevo diagrama de filas exactas

$$\begin{tikzcd}
M' \otimes_A N \arrow[r] \arrow[drr] & Im(\varphi) \times_A N \arrow[r] \arrow[d, equal, "\varphi\otimes id_N"] & 0 & & \\
0 \arrow[r] & Ker(\psi) \otimes_A N \arrow[r] & M \otimes_A N \arrow[r] \arrow[drr] & Im(\psi) \otimes_A N \arrow[r] \arrow[d, equal, "\psi\otimes id_N"] & 0 \\
 & & 0 \arrow[r] & Im(\psi) \otimes_A N \arrow[r] & M'' \otimes_A N.
\end{tikzcd}$$

En particular se tiene que la exactitud de

$$M' \otimes_A N \xrightarrow{\varphi\otimes id_N} M \otimes_A N \xrightarrow{\psi\otimes id_N} M'' \otimes_A N,$$

como queríamos.
(3) $\Rightarrow$ (1) Si $M' \longrightarrow M$ es un morfismo inyectivo de A-módulos, entonces la sucesión $0 \longrightarrow M' \longrightarrow M$ es exacta, y se puede aplicar (3) para ver que $0 \longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N$, es exacta también, de donde se tiene otra vez la inyectividad y N es plano.

$\square$

Corolario 4.5.23. *Sea N un A-módulo plano y $\varphi : M \longrightarrow M'$ un morfismo de A-módulos. Entonces el producto tensorial $\cdot \otimes_A N$ conmuta con la formación de $Ker\varphi$ y $im\varphi$, es decir, existen isomorfismos canónicos de A-módulos*

$$Ker\varphi \otimes_A N \simeq Ker(\varphi \otimes id_N)\ ;\ Im\varphi \otimes_A N \simeq Im(\varphi \otimes id_N).$$

Demostración. Es consecuencia de la caracterización 4.5.22 anterior aplicada a las sucesiones exactas

$$0 \longrightarrow Ker(\varphi) \hookrightarrow M \longrightarrow M'$$

y

$$\begin{tikzcd}
M \arrow[r, two heads] \arrow[drr] & Im(\varphi) \arrow[r] \arrow[d, equal, "\varphi"] & 0 \\
0 \arrow[r] & Im(\varphi) \arrow[r, hook] & M'.
\end{tikzcd}$$

□

Finalmente, presentamos la platitud fiel, un caso particular de la anterior en la que además de preservarse la exactitud al tensorizar se tiene una especie de recíproco: si la sucesión tensorizada es exacta debe serlo también la original.

Definición 4.5.24. **[Módulo fielmente plano]** Un A-módulo N se llama *fielmente plano* si verifica las condiciones siguientes:

1. N es plano
2. Si M es un A-módulo tal que $M \otimes_A N = 0$, entonces $M = 0$.

Un homomorfismo de anillos $\varphi : A \longrightarrow A'$ se llama *fielmente plano* si A', visto como A-módulo via φ, es fielmente plano.

Observación 4.5.25. La segunda condición de la definición de fielmente plano implica en particular que *un módulo nulo no puede ser fielmente plano*, pues dado un A-módulo $M \neq 0$, $M \otimes_A 0 = 0$ de todas maneras.

Para módulos fielmente planos tenemos una caracterización similar a la que teníamos para módulos planos. La demostración puede consultarse por ejemplo en [2].

Proposición 4.5.26. ***[Caracterización de módulos fielmente planos]*** *Sea A un anillo. Para un A-módulo N las siguientes condiciones son equivalentes:*

1. *N es fielmente plano.*
2. *N es plano y, dado $\varphi : M' \longrightarrow M$ morfismo de A-módulos tal que $\varphi \otimes id_N : M' \otimes_A N \longrightarrow M \otimes_A N$ es el morfismo nulo, entonces $\varphi = 0$ también. De hecho $\varphi = 0 \Longleftrightarrow \varphi \otimes id_N = 0$.*
3. *Una sucesión de A-módulos*

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

es exacta si y solo si la sucesión obtenida al tensorizar con N sobre A,

$$M \otimes_A N \longrightarrow M' \otimes_A N \longrightarrow M'' \otimes_A N,$$

lo es.

Corolario 4.5.27. *Un anillo A visto como A-módulo es fielmente plano. En particular un módulo libre sobre un anillo no nulo es fielmente plano si y solo si no es nulo.*

Demostración. Sea A es no nulo. Cualquier A-módulo libre $A^{(I)}$ es un módulo plano como vimos en 4.5.21. Además, por el corolario 4.5.11, dado un A-módulo M cualquiera, se tienen el isomorfismo

$$A^{(I)} \otimes_A N \simeq N^{(I)}.$$

Y como $N = 0$ si y solo si $N^{(I)} = 0$, se tiene la fiel platitud buscada.

□

4.5.3. Extensión y restricción de escalares

Dado $\varphi : A \longrightarrow A'$ un morfismo de anillos, cualquier módulo N' sobre A' puede verse también como A-módulo via φ. Basta dotarlo del producto por escalares siguiente

$$A \times N' \longrightarrow N'; \;\; (a, n) \longmapsto \varphi(a) \cdot n,$$

donde el último producto, $\cdot$, es el producto por escalares de N' como A'-módulo. Decimos que esta estructura de A-módulo sobre N' se obtiene por ***restricción de escalares/coeficientes con respecto a*** *φ. En particular, el propio anillo A' puede verse como A-módulo via φ (que es de hecho su morfismo estructural como A-álgebra) y, por tanto, para un A-módulo cualquiera M, el producto tensorial $M \otimes_A A'$ puede entenderse como A-módulo también.*

Por otro lado, este producto tensorial $M \otimes_A A'$ puede entenderse también como A'-módulo como detallamos a continuación. Dado $a' \in A'$ cualquiera pero fijo, consideramos el morfismo A-bilineal

$$M \times A' \longrightarrow M \otimes_A A'; \;\; (x, b') \longmapsto x \otimes a'b',$$

y el A-morfismo inducido por la propiedad universal del producto tensorial:

$$M \otimes_A A' \longrightarrow M \otimes_A A'; \;\; x \otimes b' \longmapsto x \otimes a'b'.$$

Definamos pues el siguiente morfismo como producto por escalares de $M \otimes_A A'$ como A'-módulo:

$$A' \times (M \otimes_A A') \longrightarrow M \otimes_A A'; \;\; (a', x \otimes b') \longmapsto x \otimes a'b'.$$

En estas condiciones, el A'-módulo $M \otimes_A A'$ se denomina ***extensión de escalares/coeficientes de M con respecto a*** *φ. Más generalmente, dado cualquier A'-módulo N', podemos ver el producto tensorial $M \otimes_A N'$ como A'-módulo usando el producto por escalares siguiente*

$$A' \times (M \otimes_A N') \longrightarrow M \otimes_A N'; \;\; (a', x \otimes y') \longmapsto x \otimes a'y'.$$

Lema 4.5.28. *Sea $\varphi : A \longrightarrow A'$ un homomorfismo de anillos, 1 el neutro multiplicativo de A y M un A-módulo.*

1. *Si $(x_i)_{i\in I}$ es un sistema de generadores de M sobre A, entonces $(x_i \otimes 1)_{i\in I}$ es un sistema de generadores de $M \otimes_A A'$ sobre A'.*
2. *Si $(x_i)_{i\in I}$ es un sistema de generadores libre de M sobre A, entonces $(x_i \otimes 1)_{i\in I}$ es un sistema de generadores libre de $M \otimes_A A'$ sobre A'.*

Demostración. 1. Sabemos que los elementos de cualquier producto tensorial se pueden escribir como sumas de tensores, en este caso $x \otimes y$ con $x \in M$, $y \in A'$. Como los $(x_i)_{i\in I}$ son generadores de M, existe $J \subseteq I$ finito y coeficientes $\alpha_j \in A$ tales que

$$x = \sum_{j\in J} \alpha_j x_j.$$

Por tanto, usando la A-bilinealidad del producto tensorial y la estructura de A'-módulo de la extensión de escalares, tenemos que

$$x \otimes y = (\sum_{j\in J} \alpha_j x_j) \otimes y = \sum_{j\in J} (y\alpha_j)(x_j \otimes 1),$$

así que los tensores $(x_i \otimes 1)_{i\in I}$ son generadores de la extensión de escalares como A'-módulo.

2. Sabemos que $M = \oplus_{i\in I} Ax_i$, así que usando el corolario 4.5.11, se tienen los isomorfismos siguientes:
$$(M \otimes_A A') \simeq \bigoplus_{i\in I} (Ax_i \otimes_A A') \simeq (A')^{(I)},$$
esto es, $M \otimes_A A'$ es un A'-módulo libre de base $(x_i \otimes 1)_{i\in I}$.

□

Lema 4.5.29. *Sean $A \longrightarrow A' \longrightarrow A''$ homomorfismos de anillos y M un A-módulo. Entonces existe un isomorfismo canónico de A''-módulos*

$$(M \otimes_A A') \otimes_{A'} A'' \longrightarrow M \otimes_A A''; \ \ (x \otimes a') \otimes a'' \longmapsto x \otimes a'a''.$$

De manera similar, para cada A'-módulo N' hay un isomorfismo canónico

$$(M \otimes_A A') \otimes_{A'} N' \longrightarrow M \otimes_A N'; \ \ (x \otimes a') \otimes y' \longmapsto x \otimes a'y'.$$

Demostración. Se basa esencialmente en aplicar un par de veces la propiedad universal del producto tensorial a los morfismos A-bilineales apropiados. Los detalles están una vez más en la sección de Extensión de Coeficientes de [2].

□

Proposición 4.5.30. ***[Propiedad universal de la extensión de escalares]*** *Sea $\varphi : A \longrightarrow A'$ un morfismo de anillos y sea M un A-módulo, y N' un A'-módulo. Denotamos en este teorema con $N'|_A$ la restricción de escalares de N' a A. Se tiene entonces la biyección canónica siguiente:*

$$Hom_{A'}(M \otimes_A A', N') \simeq Hom_A(M, N'|_A).$$

Si los módulos son de hecho álgebras sobre los anillos correspondientes, el resultado puede extenderse a homomorfismos de A- y A'-álgebras respectivamente.

Demostración. Denotemos $M' := M \otimes_A A'$. Entonces se puede considerar M' como A' módulo por extensión de escalares. Sea ahora $u \in Hom_A(M, N'|_A)$. Entonces, tensorizando u con A' sobre A se tiene el homomorfismo de A'-módulos $u \otimes id_{A'} : M' \longrightarrow N'|_A \otimes_A A'$. Sea ahora $z : N'|_A \otimes A' \longrightarrow N'$ el morfismo de A'-módulos que envía $n' \otimes a'$ en $a'n'$. Entonces su composición $z \circ u \otimes id_{A'}$ pertenece a $Hom_{A'}(M \otimes_A A', N')$.

Veamos ahora como definir la inversa de esta aplicación. Si $v \in Hom_{A'}(M \otimes_A A', N')$, lo enviamos al homomorfismo de A-módulos dado por

$$v \circ (id_M \otimes \varphi) \circ \pi : M \longrightarrow M \otimes_A A \longrightarrow M \otimes_A A' \longrightarrow N'|_A\,,$$

donde $\pi : M \longrightarrow M \otimes_A A;\ m \longmapsto m \otimes 1$ es el isomorfismo canónico dado en el lema 4.5.9, y ahora v se considera como morfismo de A- (y no de A'-) módulos.

Por construcción, estas correspondencias son inversas la una de la otra: probemos por ejemplo que al actuar la segunda correspondencia sobre $z \circ (u \otimes id_{A'}$ recuperamos u. Queremos estudiar, considerando todas las aplicaciones como homomorfismos de A-módulos, la composición

$$z \circ (u \otimes id_{A'} \circ (id_M \otimes \varphi) \circ \pi : M \longrightarrow N'|_A\,.$$

Basta notar que $(u \otimes id_{A'}) \circ (id_M \otimes \varphi) = u \otimes \varphi$, y componiendo con las restantes aplicaciones (recordamos que z se considera ahora morfismo de A-módulos) vemos que la resultante es de nuevo u como queríamos.

□

Proposición 4.5.31. ***[Extensión de escalares en anillos de polinomios]*** *Sea A un anillo, B una A-álgebra, X una familia de variables y $\mathfrak{a} \subseteq A[X]$ un ideal. Entonces se tienen los isomorfismos canónicos de B-álgebras siguientes:*

$$A[X] \otimes_A B \longrightarrow B[X], \quad f \otimes b \longmapsto bf,$$
$$(A[X]/\mathfrak{a}) \otimes_A B \longrightarrow B[X]/\mathfrak{a}B[X], \quad \bar{f} \otimes b \longmapsto \overline{bf}.$$

Demostración. Sean $\varphi' : A[X] \longrightarrow B[X]$ el morfismo de A-álgebras deducido del morfismo estructural de B como A-álgebra y $\varphi'' : B \longrightarrow B[X]$ la inclusión canónica vista como morfismo de A-álgebras. Utilizando el lema 4.5.15, estos morfismos inducen un homomorfismo de A-álgebras

$$\varphi : A[X] \otimes_A B \longrightarrow B[X], \;\; f \otimes b \longmapsto bf.$$

Por otro lado, el homomorfismo de anillos

$$B \longrightarrow A[X] \otimes_A B, \;\; b \longmapsto 1 \otimes b$$

puede extenderse a otro homomorfismo de anillos

$$\psi : B[X] \longrightarrow A[X] \otimes_A B,$$

enviando X en $X \otimes 1$. Ambos pueden entenderse como morfismos de A-álgebras, y de hecho son inversos el uno del otro, de donde se tiene el primer isomorfismo.

Para la segunda parte basta adaptar la demostración de la proposición 4.5.14 sustituyendo el anillo A, su ideal $\mathfrak{a}$ y el A-módulo B por $A[X]$, $\mathfrak{a}[X]$ y $B[X]$. El isomorfismo se obtiene de la misma manera que en dicha prueba teniendo también en cuenta el corolario 4.5.12, sobre el producto tensorial de anillos de polinomios.

□

Acabamos con este lema, extraído del capítulo sobre el Teorema del descenso fielmente plano de [2], que es utilizado para demostrar unas propiedades de finitud para morfismos étale.

Lema 4.5.32. *Sean A un anillo y A' una A-álgebra fielmente plana sobre A, con $i : A \longrightarrow A'$ morfismo estructural. Definamos $A'' := A' \otimes_A A'$, y consideremos los morfismos*

$$i_1 : A' \longrightarrow A''; \; a \longmapsto a \otimes 1,$$

$$i_1 : A' \longrightarrow A''; \; a \longmapsto 1 \otimes a.$$

En estas condiciones el diagrama

$$0 \longrightarrow A \xrightarrow{\;\;i\;\;} A' \xrightarrow{i_1 - i_2} A'',$$

es exacto. De hecho sigue siendo exacto cuando tensorizamos sobre A con un A-módulo M cualquiera, y en particular el morfismo de extensión de escalares $M \longrightarrow M' = M \otimes_A A'$; $m \longmapsto m \otimes 1$ es inyectivo.

4.6. Dependencia entera

En esta sección introducimos el concepto de elemento entero de un álgebra sobre un anillo, que generaliza el de elemento algebraico de una extensión de cuerpos. Nos basamos en [1] y en el inicio del capítulo 5 del texto de Álgebra Conmutativa de Bourbaki, [3], pues luego nos apoyaremos en la segunda parte de este capítulo para poder demostrar más fácilmente algunos resultados del libro de Raynaud.

Dado A un anillo (como siempre, conmutativo y unitario), x un elemento de una A-álgebra R, vamos a utilizar la siguiente notación

$$A[x] := \Big\{\sum_{i=0}^{n} a_i x^i,\ n \in \mathbb{N},\ a_i \in A\Big\} \subset R,$$

esto es, la sub-A-álgebra de R formada por los polinomios en la variable x con coeficientes en A. Análogamente, se definen $A[x_1, \ldots, x_n]$ para familias finitas de elementos $x_i \in R$ como los polinomios en dichas variables con coeficientes en A.

Necesitaremos también introducir la noción de módulo fiel, que nos dará una de las caracterizaciones de elementos enteros que veremos.

Definición 4.6.1. **[Módulo fiel]** Se dice que un A-módulo M es *fiel* si $Ann(M) = 0$, esto es, el único elemento $a \in A$ tal que $a \cdot m = 0$ para todo $m \in M$ es el cero .

Definición 4.6.2. **[Enteros]** Sean A un anillo (conmutativo), R una A-álgebra (no necesariamente conmutativa) y $x \in R$. Si x cumple alguna de las propiedades equivalentes siguientes, decimos que x es *entero sobre A*.

E1. El elemento x es raíz de un polinomio mónico de $A[X]$.

E2. La subálgebra $A[x]$ de R es un A-módulo de tipo finito.

E3. La subálgebra $A[x]$ de R está contenida en una subálgebra B de R tal que B es un A-módulo de tipo finito.

E4. Existe un $A[x]$-módulo fiel M que es un A-módulo de tipo finito.

Demostración.
$(E1) \implies (E2)$ Sea $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$ un polinomio mónico de $A[X]$ tal que

$$P(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 = 0.$$

Para cada $q \in \mathbb{N}_0$, sea M_q el sub-A-módulo de R engendrado por $1, x, ..., x^{n+q}$. Entonces, multiplicando por x^q a ambos miembros de la ecuación anterior y despejando el término líder x^{n+q}, tenemos

$$x^{n+q} = -a_{n-1}x^{n-1+q} - ... - a_0 x^q \in M_{q-1}.$$

De aquí, por recurrencia sobre q, se tiene la cadena

$$M_q = M_{q-1} = ... = M_0.$$

De modo que cualquier polinomio con coeficientes en A está en M_0, i.e. $A[x] = M_0$, y concluimos que $A[x]$ es un A-módulo de tipo finito, como queríamos.

$(E2) \implies (E3)$ Basta tomar $B = A[x]$.

$(E3) \implies (E4)$ El módulo B es un $A[x]$-módulo de tipo finito por hipótesis y fiel porque si existe $y \in A$ tal que $yB = 0$ en particular $y \cdot 1 = 0$, luego $y = 0$.

$(E3) \implies (E1)$ Es consecuencia de 4.2.14. Basta tomar como endomorfismo el producto por x, y como ideal el propio anillo A (se tiene la inclusión $xM \subset M$ del enunciado puesto que M es un $A[x]$-módulo). Como M es fiel por hipótesis, solo puede anularse multiplicándolo por 0, luego $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$ para los $a_i \in A$ de 4.2.14.

□

Observación 4.6.3. Una relación de la forma $P(x) = 0$ donde P es un polinomio mónico de $A[X]$ se denomina *ecuación de dependencia entera con coeficientes en A.*

Lema 4.6.4. *Dada R una A-álgebra, $x_1, ..., x_n$ elementos de R enteros sobre A. Entonces $A[x_1, ..., x_n]$ es un A-módulo de tipo finito.*

Demostración. Basta aplicar inducción sobre $n \in \mathbb{N}$ teniendo en cuenta la transitividad de la propiedad de ser de tipo finito (ver 4.2.7).

□

Corolario 4.6.5. *Dada R una A-álgebra, el conjunto de elementos de R enteros sobre A forman un subanillo B de R que contiene a A y se llama* clausura íntegra de A en R. *Si además $B = A$, decimos que el anillo A es* íntegramente cerrado en R.

Demostración. Está claro que $A \subset B$, pues cualquier elemento $a \in A$ es raíz de $X - a \in A[X]$. Por otro lado, dados $x, y \in B$, del lema anterior se deduce que $A[x, y]$ es un A-módulo de tipo finito y, por la caracterización *E3* de elemento entero $x - y$, $xy \in A[x, y]$ son enteros sobre A (así que elementos de B también).

□

Definición 4.6.6. **[Álgebra entera]** Dado A un anillo, una A-álgebra R se dice *entera sobre A* si todo elemento de R es entero sobre A.

Lema 4.6.7. *Sea A un anillo y R una A-álgebra. Entonces R es finita si y solo si es de tipo finito y entera sobre A.*

Demostración.
$\Longrightarrow$ Si R es una A-álgebra finita, en particular es de tipo finito. Además, dado $x \in R$ cualquiera, R es un $A[x]$-módulo fiel puesto que $1_B \in B$. Así pues, cada $x \in R$ es entero sobre A.

$\Longleftarrow$ Si R es de tipo finito como A-álgebra, es de la forma $R \simeq A[x_1, \ldots, x_n]$ para ciertos elementos $x_i \in R$. Pero como R es entera sobre A, los x_i son enteros, y usando el lema 4.6.4, R es finita sobre A.

□

Lema 4.6.8. ***[Transitividad de la dependencia entera]*** *Sean A un anillo, B una A-álgebra y C una B-álgebra. Si C es entera sobre B y esta lo es sobre A, entonces C es entera sobre A.*

Demostración. Dado $x \in C$ entero sobre B, queremos ver que es entero sobre A. Sabemos que x es raíz de un polinomio mónico $P(X) = p_0 + p_1 X + ... + X^n \in B[X]$, y por hipótesis cada uno de sus coeficientes p_i es entero sobre A, luego $B' = A[p_0, .., p_{n-1}]$ es un A-módulo de tipo finito por el lema precedente. Además, como x es entero sobre B' por construcción, entonces $B'[x]$ es un B'-módulo de tipo finito. Por la transitividad de la propiedad de ser de tipo finito (4.2.7), $B'[x]$ es un A-módulo de tipo finito. Y como $A[x] \subset B'[x]$, usando la tercera caracterización de elementos enteros, x es entero sobre A.

$\square$

Ejemplo 4.6.9. Si el anillo de base es un cuerpo K, entonces la condición de ser mónico no es relevante: basta que sea no constante. Notar también que, en particular, si tenemos una extensión L de dicho cuerpo , esta es una K-álgebra, y resulta que los elementos enteros coinciden con los *elementos algebraicos* de la extensión.

Observación 4.6.10. Sea R una álgebra sobre el anillo A:

1. Si A' es el subanillo de R imagen de A por el homomorfismo $A \longrightarrow R$ que da la estructura de A-álgebra a R, entonces los enteros de R sobre A coinciden con los enteros de R sobre A'.
2. Si R' es una sub-A-álgebra de R, los elementos enteros de R' sobre A son los enteros de R sobre A que pertenecen a R'.

Proposición 4.6.11. *Dados A,A' dos anillos; R, R' álgebras sobre cada uno de ellos; $f : A \longrightarrow A'$ y $g : R \longrightarrow R'$ dos homomorfismos de anillos tales que, si $e : A \longrightarrow R$ y $e' : A' \longrightarrow R'$ son los homomorfismos estructurales correspondientes, entonces $e' \circ f = g \circ e$, es decir, el siguiente diagrama es conmutativo.*

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle e'} \\ R & \xrightarrow{g} & R' \end{array}$$

Entonces, si $x \in R$ es entero sobre A, $g(x) \in R'$ lo es sobre A'.

Demostración. Si tomamos la ecuación de dependencia entera para un $x \in R$ entero sobre A,

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$$

con $a_i \in A$, por ser f y g morfismos de anillos y la compatibilidad dada en el enunciado tenemos la ecuación siguiente:

$$g(x)^n + f(a_{n-1})g(x)^{n-1} + ... + f(a_0) = 0,$$

donde $f(a_i) \in A'$, y por tanto $g(x)$ es entero sobre A'.

$\square$

Corolario 4.6.12. *Sean A un anillo, B una A-álgebra y C una B-álgebra. Entonces, todo elemento $x \in C$ entero sobre A es entero sobre B. En particular, si C es entera sobre A, entonces también lo es sobre B.*

Demostración. Basta aplicar la proposición anterior notando que los morfismos entre los anillos y los estructurales de las álgebras coinciden.

$\square$

4.7. Levantamiento de ideales primos

Esta sección, cuyos resultados provienen mayoritariamente del capítulo 5 del libro de Álgebra Conmutativa de Bourbaki ([3]), presenta la noción de ideales por encima de otro a través de un morfismo de anillos. Estudiaremos en qué casos podemos garantizar que se mantengan la primalidad o la maximalidad y acabaremos hablando de preservación de la integridad por cocientes y localizaciones.

Definición 4.7.1. [Ideal por encima] Dados A, A' dos anillos, $h : A \longrightarrow A'$ un homomorfismo entre ellos, decimos que un ideal $\mathfrak{a}'$ de A' está *por encima de* un ideal $\mathfrak{a}$ de A (respecto del homomorfismo h) si $\mathfrak{a} = h^{-1}(\mathfrak{a}')$. También es frecuente decir que $\mathfrak{a}$ es la *contracción de* $\mathfrak{a}'$ *por* h y se puede denotar $\mathfrak{a} = \mathfrak{a}'^c$.

Lema 4.7.2. *Para que exista un ideal de A' sobre el ideal* (0) *de A, es condición necesaria y suficiente que el morfismo h sea inyectivo*

Demostración. Si h es inyectivo, entonces $h^{-1}(0) = (0)$. Si no lo fuera, $h^{-1}(0)$ contendría elementos distintos del 0, y cualquier otro ideal va a contener siempre al 0, así que su imagen inversa también contendrá elementos distintos de 0.

□

Observación 4.7.3. Dado $\mathfrak{a}$ un ideal de A, tomando cocientes, el homomorfismo h induce un homomorfismo $h_1 : A/\mathfrak{a} \longrightarrow A'/\mathfrak{a}A'$, donde $\mathfrak{a}A'$ es el ideal de A' engendrado por la imagen de $\mathfrak{a}$ por h. Entonces, un ideal $\mathfrak{a}'$ es un ideal de A' por encima de $\mathfrak{a}$ si y solo si $\mathfrak{a}A' \subset \mathfrak{a}'$ y además $\mathfrak{a}'/\mathfrak{a}A'$ es un ideal de $A'/\mathfrak{a}A'$ sobre el (0)).

Las proposiciones siguientes, que usaremos al introducir la noción de anillo henseliano, necesitan de los lemas que incluimos a continuación, cuyas demostraciones se han adaptado de los textos de Bourbaki, [3] y [4].

Lema 4.7.4. *Sea A una álgebra finita sobre un cuerpo K. Los elementos de A no divisores de cero son también inversibles en A. En particular, si A es un dominio de integridad, es necesariamente un cuerpo.*

Demostración. Basta notar que, por ser A finita, el K-espacio vectorial correspondiente es de dimensión finita. Además, para cada $a \in A$ no divisor de cero, la aplicación lineal $x \mapsto ax$ de A en A es inyectiva y, por igualdad de dimensiones vectoriales, biyectiva, luego a es invertible en A. □

Lema 4.7.5. *Sean B un dominio de integridad y A un subanillo de B tal que B es entero sobre A. Entonces B es un cuerpo si y solo si A es un cuerpo.*

Demostración. Si A es un cuerpo, entonces para todo $y \neq 0$ en B, $A[y]$ es un A-módulo de tipo finito por la caracterización $E2$ de elemento entero que dimos en la sección anterior. Como $A[y] \subset B$ es también un dominio, es un cuerpo como resultado del lema anterior. En particular, y es invertible en $B \supset A[y]$, luego B es un cuerpo. Recíprocamente, si B es un cuerpo y $z \neq 0$ es un elemento de A, como $z^{-1} \in B$, entonces es entero sobre A, de donde obtenemos una ecuación de dependencia entera

$$z^{-n} + a_{n-1}z^{-(n-1)} + ... + a_0 \;=\; 0$$

con $a_i \in A$ y $n \in \mathbb{N}$. Multiplicando dicha relación por z^{n-1} y despejando tenemos

$$-z^{-1} = a_{n-1} + a_{n-2}z + ... + a_0 z^{n-1} \in A,$$

de modo que A es un cuerpo.

□

Proposición 4.7.6. *Sean $h : A \longrightarrow A'$ un homomorfismo de anillos tal que A' es entero sobre A, $\mathfrak{p}'$ un ideal primo de A', y $\mathfrak{p} = h^{-1}(\mathfrak{p}')$. Entonces, $\mathfrak{p}$ es maximal si y solo si $\mathfrak{p}'$ es maximal. En particular, el resultado es cierto si A' es finita sobre A, pues en tal caso también A' es entera sobre A.*

Demostración. Denotemos $B := A/\mathfrak{p}$, y $B' := A'/\mathfrak{p}'$, que serán ambos dominios por ser los ideales $\mathfrak{p}$ y $\mathfrak{p}'$ primos. Como $\mathfrak{p} = h^{-1}(\mathfrak{p}')$, de la propiedad universal del cociente se deduce un homomorfismo $\bar{h} : B \longrightarrow B'$. Además, utilizando la proposición 4.6.11, B' es entero sobre B (basta tomar como par de anillos A y B y como álgebras sobre ellos A' y B', considerando las estructuras de álgebra inducidas por los morfismos h y $\bar{h}$; entonces, como A' es entero sobre A por hipótesis, B' lo es sobre B).

Ahora bien, el ideal $\mathfrak{p}$ (resp $\mathfrak{p}'$) es maximal si y solo si B (resp. B') es un cuerpo. Como acabamos de ver que B' es entero sobre B, el lema previo (4.7.5) nos garantiza que B' es cuerpo si y solo si B es cuerpo, luego $\mathfrak{p}$ es maximal si y solo si lo es $\mathfrak{p}'$.

□

Proposición 4.7.7. *Sea $h : A \longrightarrow A'$ un homomorfismo de anillos tal que A' es un A-módulo de tipo finito. Entonces, para cada ideal primo $\mathfrak{p}$ de A, el conjunto de ideales primos de A' por encima de $\mathfrak{p}$ es finito.*

Demostración. Como $\mathfrak{p}$ es primo, podemos considerar el conjunto $S = A \backslash \mathfrak{p}$, la localización $A_\mathfrak{p}$ de A en $\mathfrak{p}$ y la correspondiente en A', que denotaremos $S^{-1}A'$. Sea también $\tilde{h} : A_\mathfrak{p} \longrightarrow S^{-1}A'$; $a/s \longmapsto h(a)/s$, la aplicación que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc} A & \xrightarrow{h} & A' \\ \downarrow & & \downarrow \\ A_\mathfrak{p} & \xrightarrow{\tilde{h}} & S^{-1}A', \end{array}$$

donde las flechas verticales corresponden a los morfismos de localización. Sabemos que este anillo $S^{-1}A'$ sigue siendo finito sobre $A_\mathfrak{p}$ (lema 4.3.22) y que $A_\mathfrak{p}$ es un anillo local de ideal maximal $\mathfrak{p}A_\mathfrak{p}$. Los conjuntos

$$\{\mathfrak{q} \in Spec(A') \ : \ h^{-1}(\mathfrak{q}) = \mathfrak{p}\}$$

$$\{\tilde{\mathfrak{q}} \in Spec(S^{-1}A') \ : \ \tilde{h}^{-1}(\tilde{\mathfrak{q}}) = \mathfrak{p}A_\mathfrak{p}\}$$

están en biyección, y por tanto podemos reducirnos al segundo caso, y suponer que el ideal $\mathfrak{p}$ es maximal. En ese caso $A/\mathfrak{p}$ es un cuerpo y $A'/\mathfrak{p}A'$ es aún una álgebra finita sobre $A/\mathfrak{p}$, y por tanto un anillo de Artin por la proposición 4.4.15. Así que el número de ideales primos de $A'/\mathfrak{p}A'$ es finito, o lo que es lo mismo, hay una cantidad finita de ideales primos de A' por encima de $\mathfrak{p}$ (ver observación 4.7.3).

□

Introducimos para acabar un resultado que permite extender la dependencia entera por localizaciones y por cocientes, extraído del texto de Atiyah-Macdonald [1]

Proposición 4.7.8. *Sea B una A-álgebra entera.*

1. *Si $\mathfrak{b}$ es un ideal de B por encima del ideal $\mathfrak{a}$ de A (el ideal $\mathfrak{b}$ también se denota a veces por $\mathfrak{a}B$), entonces $B/\mathfrak{b}$ es entera sobre $A/\mathfrak{a}$.*
2. *Si S es un subconjunto de A multiplicativamente cerrado, entonces $S^{-1}B$ es entera sobre $S^{-1}A$.*

Demostración. .

1. Como B es entera sobre A, dado $x \in B$ existen $n \in \mathbb{N}$ y $a_i \in A$ para $i = 0, \ldots, n-1$ tales que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Para ver que $x + \mathfrak{b}$ es entero sobre $A/\mathfrak{a}$ basta reducir la ecuación anterior módulo $\mathfrak{b}$.
2. Siguiendo con la notación del punto anterior, dado $x/s \in S^{-1}B$, con $x \in B, s \in S$, dividiendo por s^n y reagrupando en la ecuación anterior se obtiene
$$(x/s)^n + (a_{n-1}/s)(x/s)^{n-1} + \cdots + a_0/s^n = 0,$$
que prueba que x/s es entero sobre $S^{-1}A$.

□

Corolario 4.7.9. *Sea B una A-álgebra y sea C la clausura íntegra de A en B. Si S es un subconjunto de A multiplicativamente cerrado, $S^{-1}C$ es la clausura íntegra de $S^{-1}A$ en $S^{-1}B$. En particular, si A es íntegramente cerrado en B, entonces $S^{-1}A$ también lo es en $S^{-1}B$.*

Demostración. Como la clausura íntegra es entera por definición, de la segunda parte de la proposición anterior (4.7.8) se tiene que $S^{-1}C$ es entera sobre $S^{-1}A$. Queremos ver ahora que cada elemento de $b/s \in S^{-1}B$ entero sobre $S^{-1}A$ está en $S^{-1}C$. De la integridad de b/s se tiene una ecuación de dependencia entera con coeficientes en $S^{-1}A$:
$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + a_0/s_0 = 0,$$
donde $a_i \in A$ y $s_i \in S$, $i = 0, \ldots, n-1$. Tomamos $t := \prod_{i=0}^{n-1} s_i$ y mutiplicamos la ecuación por $(st)^n$, obteniendo la siguiente:
$$(tb)^n + (tb)^{n-1}(sa_{n-1} \prod_{i \neq n-1} s_i) + \cdots + ((st)^n a_0/s_0) = 0,$$
que es una ecuación de dependencia entera para bt sobre A. Por tanto, $bt \in C$ y $st \in S$ por ser S estable por multiplicación; así, $b/s = (bt)/(st) \in S^{-1}C$.

□

4.8. Sistemas y límites inductivos

Esta sección introduce el concepto de límite inductivo de módulos y algunas propiedades que se utilizan en el resto del trabajo. Aunque este concepto admite una formulación más general en el marco de la teoría de categorías (ver por ejemplo [2] o [10]), para nuestra memoria es suficiente trabajar en el caso de módulos. Para elaborar esta sección se han seguido algunos de los ejercicios de la página 37 de la versión española del libro de Atiyah-Macdonald [1].

Antes de poder definir los límites inductivos vamos a necesitar un conjunto I equipado con una relación $\leq$ de orden parcial, es decir, una relación binaria cumpliendo las propiedades reflexiva y transitiva. También supondremos que $I \neq \emptyset$ y que es dirigido, esto es, que para cada par $(i, j) \in I^2$ existe $k \in I$ tal que $i \leq k$ y $j \leq k$.

Definición 4.8.1. [Sistema directo o inductivo] Sea A un anillo, I un conjunto dirigido y $(M_i)_{i\in I}$ una familia de A-módulos indexada por I. Para cada par $(i, j) \in I^2$ tal que $i \leq j$ se tienen los A-homomorfismos $\mu_{ij} : M_i \longrightarrow M_j$ (denominados *morfismos de transición*), verificando los siguientes axiomas:

1. Para todo $i \in I$, la aplicación μ_{ii} es la identidad en M_i.
2. Si $i \leq j \leq k$, se tiene $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$.

En este caso, decimos que $\mathbf{M} = (M_i, \mu_{ij})$ es un *sistema inductivo o directo* sobre el conjunto dirigido I.

Definición 4.8.2. [Límite directo o inductivo] En las condiciones de la definición anterior, sea $C = \oplus_{i\in I} M_i$ e identifíquese cada módulo M_i con su imagen canónica en C. Sea D el submódulo de C engendrado por los elementos de la forma $x_i - \mu_{ij}(x_i)$ con $i \leq j$ y $x_i \in M_i$. Definimos el cociente $M := C/D$, $\mu : C \longrightarrow M$ el epimorfismo canónico y μ_i su restricción a M_i para cada $i \in I$. El par formado por el A-módulo M y la familia de homomorfismos de A-módulos $\mu_i : M_i \longrightarrow M$ se denomina *límite inductivo o directo del sistema* $\boldsymbol{M}$ y lo denotaremos por $\varinjlim M_i$.

Observación 4.8.3. Usando la notación de las definiciones de arriba, se deduce que, para $i \leq j$ índices de I, $\mu_i = \mu_j \circ \mu_{ij}$. Para verlo, basta tomar un elemento $m_i \in M_i$ cualquiera y notar que $\mu_i(m_i)$ es su clase en $\varinjlim M_i$ y $\mu_j \circ \mu_{ij}(m_i)$ es la clase de $\mu_{ij}(m_i)$. Pero $m_i - \mu_{ij}(m_i)$ resulta ser uno de los generadores de D, y por tanto nulo, así que ambos elementos son iguales.

Observación 4.8.4. Cabe destacar también que todos los elementos del límite inductivo M anterior pueden escribirse en la forma $\mu_i(x_i)$ para un cierto $i \in I$ y $x_i \in M_i$. Concretamente, dado $\bar{m} \in M$, sea $m \in C$ un representante de su clase de equivalencia módulo D (es decir, tal que $\mu(m) = \bar{m}$). Por pertenecer a la suma directa, existe un subconjunto $J \subseteq I$ finito tal que $m = \sum_{j\in J} m_j$ para ciertos $m_j \in M_j$. Como I es dirigido, por recurrencia existe un $k \in I$ tal que $k \geq j$ para todos los $j \in J$ (y por tanto $mu_j = \mu_k \circ \mu_{jk}$ para todo $j \in J$). Si denotamos $m' := \sum_{j\in J} \mu_{jk}(x_j) \in M_k$, veamos que $\bar{m} = \mu_k(m')$:

$$\bar{m} = \mu(m) = \mu(\sum_{j\in J} m_j) = \sum_{j\in J} \mu_j(x_j) = \sum_{j\in J} \mu_k(\mu_{jk}(x_j)) = \mu_k(m'),$$

donde en la última igualdad se ha utilizado la linealidad de μ_k.

Veamos la propiedad universal de este módulo que acabamos de definir. Para su demostración usaremos esencialmente la propiedad universal de la suma directa de módulos.

Proposición 4.8.5. ***[Propiedad universal del límite inductivo]*** *Dado un anillo A y $\boldsymbol{M} = ((M_i)_{i\in I}, \mu_{ij})$ un sistema inductivo de A-módulos, su límite inductivo $M = C/D$ está caracterizado (salvo isomorfismo) por la siguiente propiedad:*

«Sean N un A-módulo y, para cada $i \in I$, $\alpha_i : M_i \longrightarrow N$ un homomorfismo de A-módulos tal que $\alpha_i = \alpha_j \circ \mu_{ij}$ si $i \leq j$. Entonces existe un único homomorfismo $\alpha : M \longrightarrow N$ tal que $\alpha_i = \alpha \circ \mu_i$ para todo $i \in I$.» *Donde los $\mu_i : M_i \longrightarrow M$ son las restricciones a los M_i del epimorfismo canónico $\mu : \oplus_{i\in I} M_i \longrightarrow M$.*

Demostración. Nuestro objetivo es encontrar el (único) morfismo α que hace conmutativos los diagramas siguientes (para $i \leq j$, ambos índices en I):

$$\begin{tikzcd}
M_i \arrow[dd, "\mu_{ij}"'] \arrow[dr, "\mu_i"] \arrow[drr, bend left, "\alpha_i"] & & \\
& M \arrow[r, dashed, "\alpha"] & N. \\
M_j \arrow[ur, "\mu_j"] \arrow[urr, bend right, "\alpha_j"'] & &
\end{tikzcd} \qquad (4.8.5.1)$$

Por la propiedad universal de la suma directa de módulos 4.2.12, sabemos que existe un único morfismo de A-módulos $\beta : C = \oplus_{i\in I} M_i \longrightarrow N$ tal que $\alpha_i = \beta \circ \pi_i$ para cada $i \in I$ (donde los $\pi : M_i \hookrightarrow C$ son las inyecciones canónicas. Si ahora vemos que el submódulo D está contenido en el $Ker(\beta)$, por el primer teorema de isomorfía podremos concluir que existe un morfismo de A-módulos $\alpha : M = C/D \longrightarrow N$ con $\alpha \circ \mu = \beta$. Sean $i \leq j$ en I y tomemos un generador de D cualquiera, $x_i - \mu_{ij}(x_i)$. Notemos que hay cierto abuso de notación y que x_i es de hecho $\pi_i(x_i)$ y $\mu_{ij}(x_i)$ es $\pi_j(\mu_{ij}(x_i))$ en este caso, ya que los estamos observando en la suma directa. Así las cosas, como β verifica la propiedad universal de la suma directa (en particular, $\beta \circ \pi_k = \alpha_k$ para todo $k \in I$) y usando la linealidad de β, se tiene que

$$\beta(x_i - \mu_{ij}(x_i)) = \beta(\pi_i(x_i)) - \beta(\pi_j(\mu_{ij}(x_i))) = \alpha_i(x_i) - (\alpha_j \circ \mu_{ij})(x_i) = 0.$$

La última igualdad se deduce de la compatibilidad de las aplicaciones α_k y las μ_{ij} dada en el enunciado ($\alpha_i = \alpha_j \circ \mu_{ij}$ si $i \leq j$). Este morfismo α verifica además que $\alpha_i = \alpha \circ \mu_i$ pues $\mu_i = \mu \circ \pi_i$, $\alpha \circ \mu = \beta$ (primer teorema de isomorfía) y $\beta \circ \pi_i = \alpha_i$ (propiedad universal de la suma directa):

$$\alpha_i = \beta \circ \pi_i = \alpha \circ \mu \circ \pi_i = \alpha \circ \mu_i.$$

Finalmente veamos que el morfismo α obtenido es el único con estas propiedades: supongamos por reducción al absurdo que hubiera dos morfismos de dicha forma, $\alpha, \alpha' : M \longrightarrow N$. El conjunto de los elementos $\mu_i(x_i)$, para $x_i \in M_i$ cualquiera, engendra el A-módulo $M = C/D$. Por tanto, si vemos que los dos morfismos coinciden sobre estos elementos, deben coincidir siempre. Sin embargo, como $\alpha_i = \alpha' \circ \mu_i = \alpha \circ \mu_i$ para todo $i \in I$, vemos que efectivamente son iguales sobre tales elementos y se concluye.

Nos falta ver que el límite inductivo está de hecho caracterizado por esta propiedad salvo isomorfismo. Sea pues T otro A-módulo que verifique la propiedad universal anterior. Necesitaremos además que haya unos morfismos $\tilde{\mu}_i : M_i \longrightarrow T$ para todo $i \in I$ verificando $\tilde{\mu}_i = \tilde{\mu}_j \circ \mu_{ij}$ si $i \leq j$. Aplicamos ahora la propiedad universal de T sobre (M, μ_i), de manera que existe (un único) morfismo de A-módulos $\gamma : T \longrightarrow M$ tal que

$$\mu_i = \gamma \circ \tilde{\mu}_i, \qquad (4.8.5.2)$$

para todo $i \in I$. Haciendo lo mismo con M sobre $(T, \tilde{\mu}_i)$ garantizamos la existencia (y unicidad) de un morfismo $\epsilon : M \longrightarrow T$ tal que

$$\tilde{\mu}_i = \epsilon \circ \mu_i, \tag{4.8.5.3}$$

para todo $i \in I$. Combinando las ecuaciones 4.8.5.3 y 4.8.5.2, obtenemos $\mu_i = (\gamma \circ \epsilon) \circ \mu_i$ y $\tilde{\mu}_i = (\epsilon \circ \gamma) \circ \tilde{\mu}_i$ para todo $i \in I$. Finalmente, si aplicamos la propiedad universal de M sobre sí mismo, deducimos que hay un único morfismo de A-módulos $\theta : M \longrightarrow M$ tal que $\mu_i = \theta \circ \mu_i$ para todo $i \in I$, y como id_M lo verifica, $\theta = id_M = \gamma \circ \epsilon$. Y análogamente se tiene que $\epsilon \circ \gamma = id_T$, de modo que $M \simeq T$, como queríamos.

□

Introducimos ahora un caso particular de sistema inductivo formado por submódulos de uno dado en el que el límite coincidirá con la suma de la familia de submódulos. De aquí deduciremos luego que todo módulo es límite inductivo de sus submódulos finitamente generados, considerando el orden parcial dado por la inclusión.

Proposición 4.8.6. *Sea M un A-módulo y $(M_i)_{i\in I}$ una familia de submódulos suyos tal que, para cada par de índices $i, j \in I$ existe $k \in I$ de manera que $M_i + M_j \subseteq M_k$. Definimos $i \leq j$ cuando $M_i \subseteq M_j$ y los morfismos $\mu_{ij} : M_i \longrightarrow M_j$ como las inclusiones de M_i en M_j para cada $i, j \in I$. Entonces el límite inductivo del sistema inductivo $((M_i)_{i\in I}, \mu_{ij})$ coincide con la suma o unión de los submódulos, esto es*

$$\varinjlim M_i = \sum_{i\in I} M_i = \bigcup_{i\in I} M_i.$$

Demostración. Veamos primero que, en este caso, la suma de los submódulos coincide con su unión. En general se tiene que la unión está contenida en la suma. Para la otra contención, tomemos $m \in \sum_{i\in I} M_i$, que puede escribirse como suma finita (no única en general) de elementos de los M_i. Digamos pues que existe $J \subseteq I$ finito tal que $m = \sum_{j\in J} m_j$. Como para cada par de índices $(i, j) \in I^2$ existe otro $k \in I$ tal que $M_i + M_j \subseteq M_k$, usando esta propiedad recursivamente concluimos que existe un índice $k_J \in I$ tal que $m \in \sum_{j\in J} M_j \subseteq M_{k_J} \subseteq \cup_{i\in I} M_i$, como queríamos.

Ahora, como la propiedad universal 4.8.5 caracteriza al límite inductivo, basta probar que $\cup_{i\in I} M_i$ la verifica para tener la igualdad deseada. Así pues, dado un A-módulo N cualquiera y una familia de homomorfismos $\alpha_i : M_i \longrightarrow N$ para cada $i \in I$ tales que $\alpha_i = \alpha_j \circ \mu_{ij}$ si $i \leq j$, queremos ver que existe un único homomorfismo $\alpha : \cup_{i\in I} M_i \longrightarrow N$ tal que $\alpha_i = \alpha \circ \mu_i$ para todo $i \in I$.
Dado $m \in \cup_{i\in I} M_i$ cualquiera, existe $s \in I$ tal que $m \in M_s$. Definamos pues $\alpha(m) \coloneqq \alpha_s(m)$ y veamos que esta definición no depende del s elegido. Concretamente, si $m \in M_j$ con $j \neq s$, sabemos que existe $k \in I$ tal que $M_s + M_j \subseteq M_k$, de modo que $s \leq k$ y $j \leq k$. Por tanto, $\alpha_s = \alpha_k \circ \mu_{sk}$ y $\alpha_j = \alpha_k \circ \mu_{jk}$, pero como μ_{sk} y μ_{jk} no son más que inclusiones, deducimos que $\alpha_s(m) = \alpha_k(m) = \alpha_j(m)$.

Veamos ahora que la aplicación α así definida es un morfismo de A-módulos. Sean $a \in A$ y $m, m' \in \cup_{i\in I} M_i$. Por un lado, si $m \in M_s$,

$$\alpha(am) = \alpha_s(am) = a\alpha_s(m) = a\alpha(m),$$

pues los α_i son morfismos de A-módulos para $i \in I$. Por otro lado, si $m \in M_s$ y $m' \in M_j$ sabemos que existe un M_k con $k \in I$ que contiene a ambos, luego

$$\alpha(m + m') = \alpha_k(m + m') = \alpha_k(m) + \alpha_k(m') = \alpha(m) + \alpha(m').$$

Finalmente, basta notar que la condición $\alpha_i = \alpha \circ \mu_i$ hace que el morfismo α que hemos encontrado sea único, pues cualquier otro verificándola coincidirá con α sobre los módulos M_i para todo $i \in I$, en particular serán el mismo morfismo.

$\square$

Corolario 4.8.7. *En las condiciones de la proposición anterior, un A-módulo M es límite directo de sus submódulos de generación finita.*

Demostración. Basta notar que la familia $(M_i)_{i\in I}$ formada por todos los submódulos finitamente generados de M verifica las hipótesis de la proposición 4.8.6: dados dos submódulos M_i, M_j de generación finita, su suma $M_i + M_j$ lo es todavía y sigue siendo un submódulo de M así que existe un cierto $k \in I$ tal que $M_k = M_i + M_j$. Así, el límite directo de los submódulos de generación finita de un módulo es su suma (o unión), la cual coincide con el módulo total M.

$\square$

Terminamos esta sección viendo que el límite inductivo conmuta con el producto tensorial con un módulo fijo cualquiera. Para la demostración usaremos los dos lemas siguientes, que solo requieren razonamientos sencillos de Álgebra Lineal.

Lema 4.8.8. *Sean M, N, P, T cuatro módulos sobre un anillo A. Si $f : M \times N \longrightarrow P$ es una aplicación A-bilineal y $g : P \longrightarrow T$ una aplicación A-lineal, entonces $g \circ f$ es A-bilineal.*

Demostración. Sean $a, b \in A$, $x, x' \in M$ e $y \in N$ cualesquiera. Veamos que $g \circ f$ es lineal respecto de su primera variable (la linealidad respecto de la segunda se prueba exactamente igual):

$$(g \circ f)(ax + bx', y) = g(af(x, y) + bf(x', y)) = a(g \circ f)(x, y) + b(g \circ f)(x', y).$$

Se ha usado la A-bilinealidad de f para la primera igualdad y la A-linealidad de g para la segunda.

$\square$

Lema 4.8.9. *Sean M, N, P tres A-módulos. Entonces el A-módulo de aplicaciones A-bilineales de $M \times N$ en P es isomorfo al A-módulo de aplicaciones A-lineales de M en $Hom_A(N, P)$. Esto es,*

$$Bil_A(M \times N, P) \simeq Hom_A(M, Hom_A(N, P)).$$

Demostración. Sea $\phi : M \times N \longrightarrow P$ una aplicación A-bilineal. Hagámosle corresponder la aplicación $\tilde{\phi} : M \longrightarrow Hom_A(N, P)$ que a cada $m \in M$ le asocia el A-morfismo $\tilde{\phi}(m) : n \in N \longmapsto \phi(m, n) \in P$. Es fácil comprobar que es una aplicación A-lineal, y su inversa se obtiene análogamente: $\tilde{\phi} \in Hom_A(M, Hom_A(N, P))$ se envía a $\phi \in Bil_A(M \times N, P)$ tal que $\forall (m, n) \in M \times N$ se tiene que $\phi(m, n) = \tilde{\phi}(m)(n)$.

$\square$

Proposición 4.8.10. *Sean A un anillo, $\boldsymbol{M} = ((M_i)_{i\in I}, \mu_{ij})$ un sistema inductivo de A-módulos y N otro A-módulo cualquiera. Entonces $((M_i \otimes_A N)_{i\in I}, \mu_{ij} \otimes id_N)$ es un sistema inductivo cuyo límite verifica*

$$\varinjlim (M_i \otimes_A N) \simeq (\varinjlim M_i) \otimes_A N.$$

Demostración. En primer lugar, fijemos las notaciones a utilizar: $M \coloneqq \varinjlim M_i$, $P \coloneqq \varinjlim (M_i \otimes_A N)$ los morfismos $\mu_i : M_i \longrightarrow M$ serán las restricciones sobre cada M_i del epimorfismo canónico $\mu : \oplus_{i\in I} M_i \longrightarrow M$ y los morfismos $\tilde{\mu}_i : M_i \otimes_A N \longrightarrow P$ las propias de $\tilde{\mu} : \oplus_{i\in I}(M_i \otimes_A N) \longrightarrow P$. Por la observación 4.8.3, sabemos además que

$$\mu_i = \mu_j \circ \mu_{ij}; \quad \tilde{\mu}_i = \tilde{\mu}_j \circ (\mu_{ij} \otimes id_N) \quad \forall\, i \leq j. \tag{4.8.10.1}$$

Por otro lado, tenemos morfismos de A-módulos $\mu_i \otimes id_N : M_i \otimes_A N \longrightarrow M \otimes_A N$ para todo $i \in I$, y además $\mu_i \otimes id_N = (\mu_j \otimes id_N) \circ (\mu_{ij} \circ id_N)$ para $i \leq j$ en virtud de la ecuación 4.8.10.1. Por tanto, podemos invocar para P la propiedad universal del límite inductivo (4.8.5) y garantizar así la existencia y unicidad de un morfismo de A-módulos $\psi : P \longrightarrow M \otimes_A N$ tal que $\mu_i \otimes id_N = \psi \circ \tilde{\mu}_i$ para todo $i \in I$.
Consideremos ahora las aplicaciones canónicas bilineales

$$g_i : M_i \times N \longrightarrow M_i \otimes_A N; \quad (m_i, n) \longmapsto m_i \otimes n,$$

para todo $i \in I$; y sean $\tilde{g}_i \coloneqq \tilde{\mu}_i \circ g_i : M_i \times N \longrightarrow P$. Como $\tilde{\mu}_i$ es A-lineal y g_i A-bilineal, usando el lema 4.8.8, concluimos que $\tilde{g}_i$ es A-bilineal. Utilizando ahora el lema 4.8.9, consideramos los A-morfismos $\xi_i : M_i \longrightarrow Hom_A(N, P)$ correspondientes a los $\tilde{g}_i$; esto es, para cada $i \in I$, $\xi_i(m_i) : N \longrightarrow P$; $\ n \longmapsto \tilde{g}_i(m_i, n)$. Queremos aplicar la propiedad universal de M como límite inductivo sobre el A-módulo $Hom_A(N, P)$ y los morfismos ξ_i, y para eso nos falta ver que $\xi_i = \xi_j \circ \mu_{ij}$ para índices $i \leq j$ en I. Sea pues $m_i \in M_i$ cualquiera; por un lado el morfismo $\xi_i(m_i)$ envía un elemento $n \in N$ en $\tilde{g}_i(m_i, n) = \tilde{\mu}_i(m_i \otimes n)$, donde la última igualdad se deduce de la definición de $\tilde{g}_i$. Por otro lado, el morfismo $(\xi_j \circ \mu_{ij})(m_i)$ envía n en $\tilde{g}_j(\mu_{ij}(m_i), n) = \tilde{\mu}_j(\mu_{ij}(m_i) \otimes n)$, pero este elemento coincide con el anterior gracias a la segunda ecuación en 4,8,10,1.

Por la propiedad universal del límite inductivo M sabemos que existe un único A-morfismo $\tilde{\beta} : M \longrightarrow Hom_A(N, P)$ tal que $\xi_i = \tilde{\beta} \circ \mu_i$ para todo $i \in I$. Usando de nuevo la correspondencia del lema 4.8.9, podemos asociar a $\tilde{\beta}$ el morfismo A-bilineal $\beta : M \times N \longrightarrow P$. Más aún, por la propiedad universal del producto tensorial, existe un único morfismo A-lineal $\phi : M \otimes_A N \longrightarrow P$ tal que $\phi \circ g = \beta$, donde $g : M \times N \longrightarrow M \otimes_A N$ es la aplicación bilineal canónica.

Finalmente, nos falta ver que las aplicaciones ψ y ϕ que acabamos de obtener son inversas la una de la otra y se tiene por tanto el isomorfismo deseado. Para simplificar los cálculos usaremos la observación 4.8.4, gracias a la cual sabemos que los elementos de M son de la forma $\mu_i(m_i)$ para ciertos $i \in I$ y $m_i \in M_i$. Por tanto, los elementos $\mu_i(m_i) \otimes n$ (con $n \in N$) son generadores de $M \otimes_A N$, y basta estudiar este caso:

$$\begin{aligned}(\psi \circ \phi)(\mu_i(m_i) \otimes n) &= (\psi \circ \phi)(g(\mu_i(m_i), n)) = \psi(\beta(\mu_i(m_i), n)) \\ &= \psi(\tilde{\beta}(\mu_i(m_i))(n)) = \psi(\xi_i(m_i)(n)) \\ &= \psi(\tilde{g}_i(m_i, n)) = \psi(\tilde{\mu}_i(m_i \otimes n)) = \mu_i(m_i) \otimes n,\end{aligned} \tag{4.8.10.2}$$

donde se han utilizado las definiciones de g, β y ξ_i y las identidades siguientes: $\phi \circ g = \beta$ en la segunda igualdad, $\tilde{\beta} \circ \mu_i = \xi_i$ en la cuarta igualdad, $\tilde{g}_i = \tilde{\mu}_i \circ g_i$ en la sexta igualdad y $\psi \circ \tilde{\mu}_i = \mu_i \otimes id_N$ en la última.

Por otro lado, usando de nuevo la observación 4.8.4, concluimos que los elementos de P serán de la forma $\tilde{\mu}_j(\tilde{m}_j)$ con $j \in I$ y $\tilde{m}_j \in M_j \otimes_A N$. Sin embargo, como los tensores $m_j \otimes n$ con $m_j \in M_j$ y $n \in N$ son generadores del producto tensorial anterior y las aplicaciones consideradas son lineales, basta estudiar $\phi \circ \psi$ sobre elementos de la forma $\tilde{\mu}_j(m_j \otimes n)$. Usando las mismas identidades y definiciones que antes se obtienen las igualdades siguientes, que concluyen que ψ y ϕ son efectivamente inversas la una de la otra:

$$(\phi \circ \psi)(\tilde{\mu}_j(m_j \otimes n)) = \phi(\mu_j(m_j) \otimes n) = \beta(\mu_j(m_j), n) = \tilde{\mu}_j(m_j \otimes n).$$

□

Otra propiedad interesante del límite inductivo de módulos es su exactitud, esto es, que si tomamos límites inductivos en una sucesión exacta de módulos, la resultante preservará la exactitud.

La demostración puede encontrarse, por ejemplo, en el sitio web del Stacks Project ([10]) o en el libro de Bosch ([2]).

Proposición 4.8.11. *Sean I un conjunto dirigido y $(M_i)_{i\in I}$, $(M'_i)_{i\in I}$ y $(M''_i)_{i\in I}$ tres sistemas inductivos de A-módulos indexados por I y tales que, para cada $i \in I$, la sucesión*

$$0 \longrightarrow M'_i \longrightarrow M_i \longrightarrow M''_i \longrightarrow 0$$

es exacta. Entonces la sucesión de A-módulos

$$0 \longrightarrow \varinjlim M'_i \longrightarrow \varinjlim M_i \longrightarrow \varinjlim M''_i \longrightarrow 0$$

es exacta también.

Observación 4.8.12. Las definiciones y resultados de esta sección pueden adaptarse sin mucha dificultad a un sistema inductivo compuesto por A-álgebras (en particular anillos o ideales) y los morfismos de álgebras correspondientes, teniendo en cuenta su estructura de módulo subyacente. En este caso, se puede probar que el límite inductivo hereda la estructura de A-álgebra de la familia, y que los morfismos que van apareciendo son todos morfismos de álgebras. En este trabajo usaremos de hecho la versión para álgebras de los resultados expuestos arriba, cuya adaptación es sencilla pero tediosa y por eso la omitimos. En particular, nos será útil la siguiente proposición.

Proposición 4.8.13. *Sea A un anillo, B una A-álgebra y $((B_i)_{i\in I}, \mu_{ij})$ el sistema inductivo formado por todas las sub-A-álgebras finitas de B con los morfismos de inclusión respectivos. Entonces su límite inductivo coincide con B. En particular, si tomamos como sistema inductivo las subálgebras de tipo finito o presentación finita, que contienen a las finitas, su límite inductivo también coincidirá con B.*

4.9. Completaciones y topología $\mathfrak{a}$-ádica

Esta sección es un poco especial en este anexo ya que su interés en esta memoria se reduce a uno de los ejemplos de anillos henselianos: «dado un anillo local $(A, \mathfrak{m})$ *(Hausdorff para la topología* $\mathfrak{m}$*-ádica), su completado* $\mathfrak{m}$*-ádico es henseliano » (proposición 1.2.7). Así pues, aunque se puede hacer un tratamiento muy general de los sistemas y límites proyectivos (en el marco de la teoría de categorías) o de los grupos topológicos, vamos aquí a restringirnos a los conceptos y resultados indispensables para probar dicha proposición (sin detallar demasiado las demostraciones) que han sido extraídos esencialmente de los manuales de Atiyah y Matsumura ([1] y [5]). Comenzamos viendo grupos con una topología compatible con la estructura de grupo y definimos en ellos la noción de sucesión de Cauchy y completación.*

Definición 4.9.1. [**Grupo topológico**] Un espacio topológico sobre un grupo abeliano $(G, +)$ se llama *grupo (abeliano) topológico* si las aplicaciones

$$f : G \times G \longrightarrow G\ ;\ (x, y) \longmapsto x + y, \qquad g : G \longrightarrow G\ ;\ x \longmapsto -x$$

son continuas para dicha topología.

Si un grupo topológico es anillo con un producto continuo para la topología, se llama en particular *anillo topológico*, y añadiendo la continuidad de un producto por escalares se pueden definir *álgebras o módulos topológicos.*

Lema 4.9.2. *Sea G un grupo topológico y $a \in G$ un elemento fijo. Entonces la traslación $T_a : G \longrightarrow G\ ;\ x \mapsto x + a$ es un homeomorfismo.*

Demostración. Basta ver que es continua, pues T_{-a} es su inversa, y su continuidad se deduce de la misma manera. La aplicación $G \longrightarrow G \times G\ ;\ x \mapsto (x, a)$ es continua por serlo sus componentes, y T_a es la composición de esta aplicación y la aplicación f de la definición 4.9.1, que es continua también.

□

Observación 4.9.3. Como T_a es abierta, dado $a \in G$ y U un entorno de 0 en G (i.e. existe V un abierto tal que $0 \in V \subset U$) entonces $T_a(U) = U + a$ es un entorno de a en G, pues es un abierto que contiene a dicho punto. Razonando igual para un entorno cualquiera de un punto a y la aplicación T_{-a} se puede ver que *los entornos de cualquier punto pueden obtenerse por traslación de los entornos del cero.* Así que la topología de G estará totalmente determinada por los entornos del cero.

Introducimos ahora la noción de sucesión de Cauchy en grupos topológicos y, de la mano, la de completado como grupo formado por las clases de equivalencia de dichas sucesiones, de manera similar a las asignaturas de Análisis.

Definición 4.9.4. [**Sucesión de Cauchy**] Una sucesión $(x_n)_n$ de elementos de un grupo topológico G se dice que es *de Cauchy* si para cada entorno U del 0 existe un $n_U \in \mathbb{N}$ tal que si $n, m \geq n_U$, entonces $x_n - x_m \in U$. Dos sucesiones de Cauchy $(x_n)_n$, $(y_n)_n$ en G son *equivalentes* si $(x_n - y_n)_n$ converge hacia 0. El conjunto de clases de equivalencia de sucesiones de Cauchy de G se denota $\hat{G}$ y se denomina *completado de G*.

Lema 4.9.5. *La equivalencia de sucesiones de Cauchy en un grupo topológico es una relación de equivalencia. Además, si $(x_n)_n$, $(y_n)_n$ son sucesiones de Cauchy de un grupo topológico G, $(x_n+y_n)_n$ lo es también y su clase de equivalencia en $\hat{G}$ está determinada por las de $(x_n)_n$, $(y_n)_n$. Por tanto, tenemos definida una suma en $\hat{G}$ con respecto a la cual este es un grupo abeliano. Si es un anillo topológico, $(x_ny_n)_n$ es también de Cauchy y el completado tiene estructura de anillo.*

Demostración.

1. La propiedad reflexiva es clara. Si $x_n \sim y_n$, sea U un abierto genérico y sea $V = U \cap (-U)$. Como $0 \in V$ y $x_n - y_n$ converge a 0, existe n_V tal que $x_m - y_m \in V$ para todo $m \geq n_V$. Pero como V está formado por elementos cuyo inverso también está en V, $y_m - x_m \in V$ para todo $m \geq n_V$ también, así que $y_n \sim x_n$ y se tiene la propiedad simétrica. Para la transitividad sean $x_n - y_n$ e $y_n - z_n$ dos sucesiones que convergen a 0 y sea U un entorno abierto del cero cualquiera. Tomando de nuevo la aplicación de suma f de 4.9.1, se tiene que $f^{-1}(U)$ es abierto por ser ella continua, así que existen abiertos U_1, U_2 de G tales que $U_1 \times U_2 \subseteq f^{-1}(U)$ (base de la topología producto). Pero por definición de f se deduce que las sumas de elementos de U_1 y U_2, que denotaremos $U_1 + U_2$, están contenidas en U. Tomando $V = U_1 \cap U_2$, podemos encontrar un índice común n_V tal que $x_m - y_m \in V$ e $y_m - z_m \in V$ para todo $m \geq n_V$. Sumando, $(x_m - y_m) - (y_m - z_m) = x_m - z_m$, que es por tanto un elemento de $V + V \subseteq U_1 + U_2 \subseteq U$. De modo que para $m \geq n_V$, $x_m - z_m \in U$ y se tiene la propiedad transitiva.

2. Para ver que $x_n - y_n$ es de Cauchy usamos la misma estrategia que arriba. Sean pues U un entorno abierto del cero cualquiera, U_1, U_2 dos abiertos de G tales que $U_1 + U_2 \subseteq U$ y $V = U_1 \cap U_2$. Sean n_V tal que para todos $n, m \geq n_V$ se tiene que $x_n - x_m \in V$ e $y_n - y_m \in V$. Sumando ambas, $(x_n + y_n) - (x_m + y_m) \in V + V \subseteq U_1 + U_2 \subseteq U$. Esta claro que $(-x_n)$ es de Cauchy si lo es (x_n) y la suma de sucesiones es conmutativa, así que efectivamente $\hat{G}$ es un grupo abeliano para la suma.

3. En el caso de un anillo topológico A, se prueba de manera totalmente análoga (introduciendo unos términos cruzados de la forma x_ny_m) que $(x_ny_n)_n$ también es de Cauchy y por tanto el completado $\hat{A}$ es también un anillo con la suma y producto de sucesiones definidos elemento a elemento.

□

Observación 4.9.6. Para cada elemento $x \in G$ la sucesión constante igual a x es de Cauchy y podemos considerar su clase $\phi(x)$ en $\hat{G}$, luego el morfismo

$$\phi : G \longrightarrow \hat{G}; \quad x \mapsto \phi(x) = (x, x, \dots)$$

está bien definido y es un morfismo de grupos (o de anillos en caso de que G sea un anillo topológico). En general, no es inyectivo: su núcleo está compuesto por los elementos $y \in G$ tales que la sucesión $(y, y, y, \dots)$ es equivalente a la nula, esto es, tales que y está en todos los entornos abiertos del 0 en G. Cuando este morfismo ϕ sea un isomorfismo de grupos (resp. anillos, módulos, etc) diremos que G es *completo*.

Vamos ahora a construir el ejemplo de grupo topológico que nos interesa. Sean pues A un anillo, M un A-módulo y $\mathfrak{a}$ un ideal de A. Por la observación 4.9.3, si queremos dar una estructura de grupo topológico a M, bastará con dar una base de entornos (abiertos) del 0 y obtener el resto de ellos por traslaciones: tomemos $\mathfrak{a}^nM$, con n natural, como base de entornos (abiertos) del cero y veamos entonces que $\{m + \mathfrak{a}^nM \ : \ m \in M, n \geq 1\}$ es base de una topología en M. Para que M sea un A-módulo topológico tendremos además que comprobar que las operaciones del mismo son continuas en esta topología que acabamos de definir: la $\mathfrak{a}$-ádica.

Proposición 4.9.7. ***[Topología $\mathfrak{a}$-ádica]*** *Sean M un A-módulo y $\mathfrak{a}$ un ideal de A. Tomando*

$$M \supseteq \mathfrak{a}M \supseteq \cdots \supseteq \mathfrak{a}^n M \supseteq \mathfrak{a}^{n+1} M \supseteq \ldots$$

como base de entornos abiertos del cero, se obtiene una estructura de A-módulo topológico en M que se llamará topología $\mathfrak{a}$-ádica.

Demostración.

1. Comencemos viendo que $\{m + \mathfrak{a}^n M \,:\, m \in M, n \geq 1\}$ es base de una topología en M. Por un lado, está claro que la unión de dichos submódulos coincide con M y falta ver que, dados $n_1 \geq n_2$ cualesquiera y $m \in (m_1 + \mathfrak{a}^{n_1} M) \cap (m_2 + \mathfrak{a}^{n_2} M)$, existen $m_3 \in M$ y un índice n_3 tales que
$$m \in (m_3 + \mathfrak{a}^{n_3} M) \subseteq (m_1 + \mathfrak{a}^{n_1} M) \cap (m_2 + \mathfrak{a}^{n_2} M).$$
Como hemos supuesto (sin pérdida de generalidad) que $n_1 \geq n_2$, se tiene que $\mathfrak{a}^{n_1} M \subseteq \mathfrak{a}^{n_2} M$. Pero además, por estar en la intersección, m puede escribirse como $m = m_i + s_i$ con $s_i \in \mathfrak{a}^{n_i} M$ para $i = 1, 2$. Así que
$$m_1 - m_2 = s_2 - s_1 \in \mathfrak{a}^{n_2} M,$$
y de ahí $m_1 \in m_2 + \mathfrak{a}^{n_2} M$. Finalmente, se tiene que
$$m \in (m_1 + \mathfrak{a}^{n_1} M) = (m_1 + \mathfrak{a}^{n_1} M) \cap (m_2 + \mathfrak{a}^{n_2} M).$$

2. Antes de ver la continuidad, recalcar que la topología que se está suponiendo en A también es la $\mathfrak{a}$-ádica. Para ver la continuidad del producto por escalares, sea $(a, m) \in A \times M$ cualquiera. Una base de entornos de su imagen am será de la forma $am + \mathfrak{a}^n M$ con n natural, y sus imágenes inversas por dicha aplicación contendrán a los entornos del producto del tipo $(a + \mathfrak{a}^n) \times (m + \mathfrak{a}^n M)$, así que serán entornos de (a, m) también. La prueba de la continuidad de la suma es análoga.

□

A continuación probamos que la topología $\mathfrak{a}$-ádica es de Hausdorff si y solo si la intersección de la base de entornos del 0 que tenemos es el módulo nulo. Este resultado es válido para grupos topológicos cualesquiera y puede consultarse por ejemplo en [1].

Proposición 4.9.8. *Sea M un A-módulo con la topología $\mathfrak{a}$-ádica. Entonces es un espacio de Hausdorff si y solo si $\bigcap_{n \geq 1} \mathfrak{a}^n M = (0)$.*

Demostración. Si la intersección es nula, dados $m \neq m'$, como $m - m' \neq 0$, existe $n \in \mathbb{N}$ tal que $m - m' \notin \mathfrak{a}^n M$. Esto equivale a que los puntos estén separados, esto es,

$$(m + \mathfrak{a}^n M) \cap (m' + \mathfrak{a}^n M) = \emptyset,$$

pues si existiera un m'' en dicha intersección, podría escribirse como $m'' = m + b = m' + b'$, con $b, b' \in \mathfrak{a}^n M$. Y en tal caso $m - m' = b' - b \in \mathfrak{a}^n M$ que contradice lo supuesto.

Si M es de Hausdorff, supongamos que existiera $m \neq 0$ en la intersección. Entonces existe n natural tal que
$$(m + \mathfrak{a}^n M) \cap (\mathfrak{a}^n M) = \emptyset,$$
pero esto supone que $m \notin \mathfrak{a}^n M$, contradiciendo que esté en la intersección.

□

En el caso de la topología $\mathfrak{a}$-ádica (y de cualquier otra que tenga una base de entornos numerable del 0 formada por una cadena descendente de subgrupos), se puede dar una definición equivalente de sucesión de Cauchy: las sucesiones coherentes. Para introducirlas, veamos también una noción simplificada de sistema proyectivo.

Definición 4.9.9. [Sucesiones coherentes. Límites proyectivos] Sean $(A_n)_n$ una sucesión de grupos y $(\theta_n)_n$ una familia de homomorfismos de la forma

$$\theta_{n+1} : A_{n+1} \longrightarrow A_n.$$

1. El par $((A_n)_n, (\theta_n)_n)$ se llama *sistema proyectivo o inverso.*
2. Decimos que una sucesión $(a_n)_n$ es una *sucesión coherente* para el sistema proyectivo anterior si $a_n \in A_n$ y $\theta_{n+1}a_{n+1} = a_n$ para todo n.
3. El *límite proyectivo o inverso* del sistema anterior se define como el grupo formado por todas las sucesiones coherentes del mismo y se denota por $\varprojlim A_n$.

Observación 4.9.10. Volviendo a nuestra topología $\mathfrak{a}$-ádica sobre el A-módulo M, una sucesión $(x_n)_n$ de M es de Cauchy si $\forall n \in \mathbb{N}$ existe un $s_n \in \mathbb{N}$ de manera que si $m, k \geq s_n$ entonces $x_k - x_m \in \mathfrak{a}^n M$ (equivalentemente, $x_m \equiv x_k \; mod \, \mathfrak{a}^n M$). Es decir, las sucesiones de Cauchy son aquellas constantes para cada $M/\mathfrak{a}^n M$ de un s_n en adelante. Denotemos por ξ_n la clase de equivalencia módulo $\mathfrak{a}^n M$ donde estaciona.

Como $\mathfrak{a}^{n+1}M \subseteq \mathfrak{a}^n M$ para cada n, partiendo del epimorfismo canónico $M \longrightarrow M/\mathfrak{a}^n M$ se puede obtener otro epimorfismo

$$\theta_{n+1} : M/\mathfrak{a}^{n+1}M \longrightarrow M/\mathfrak{a}^n M; \;\; m + \mathfrak{a}^{n+1}M \longmapsto m + \mathfrak{a}^n M.$$

Además, de la contención de los submódulos se tiene también (usando la notación del inicio de esta observación) que $s_{n+1} \geq s_n$, esto es, la sucesión de clases de equivalencia estaciona antes módulo $\mathfrak{a}^n M$ que módulo $\mathfrak{a}^{n+1}M$, como era de esperar. Por tanto, $\theta_{n+1}(\xi_{n+1}) = \xi_n$, así que cada sucesión de Cauchy define una sucesión coherente para el sistema proyectivo $(M/\mathfrak{a}^n M, \theta_n)_n$. También observamos que las sucesiones de Cauchy equivalentes tiene la misma sucesión coherente asociada. Más aún, dada una sucesión coherente $(\xi_n)_n$ podemos crear una sucesión de Cauchy $(x_n)_n$ tomando un elemento x_n de cada clase ξ_n (de manera que $x_n - x_{n+1} \in \mathfrak{a}^n M$). Por tanto, $\hat{M}$ puede definirse también como el grupo de las sucesiones coherentes con las operaciones naturales.

Así, usando la notación de la definición 4.9.9,

$$\hat{M} = \varprojlim M/\mathfrak{a}^n M$$

Acabamos con un par de proposiciones que usaremos en el texto principal.

Proposición 4.9.11. *Sean (A_n, θ_n) y (B_n, ϕ_n) dos sistemas proyectivos de álgebras sobre un anillo común. Si consideramos el sistema inductivo formado por los productos $(A_n \times B_n, \theta_n \times \phi_n)$, entonces se tiene el isomorfismo siguiente entre sus límites proyectivos*

$$\varprojlim A_n \times \varprojlim B_n \simeq \varprojlim (A_n \times B_n).$$

Demostración. Notemos que por las aplicaciones del sistema producto nos referimos a

$$\theta_n \times \phi_n : A_n \times B_n \longrightarrow A_{n-1} \times B_{n-1}; \;\; (x, y) \longmapsto (\theta_n(x), \phi_n(y)),$$

para cada n natural. Como todas las aplicaciones son morfismos de álgebras, las aplicaciones producto así definidas también lo son, y cada par de sucesiones coherentes para cada sistema está biunívocamente relacionado con una sucesión coherente en el producto. (El resultado no es exclusivo de álgebras pero es la versión que emplearemos en el texto.)

$\square$

Si consideramos en un anillo A la topología $\mathfrak{a}$-ádica dada por un ideal $\mathfrak{a}$ de A, el homomorfismo natural $A \longrightarrow \hat{A}$ nos permite considerar $\hat{A}$ como una A-álgebra y entonces cada A-módulo M puede verse como $\hat{A}$ módulo si se considera su extensión de escalares $\hat{A} \otimes_A M$. Queremos ver ahora su relación con el $\hat{A}$-módulo $\hat{M}$ obtenido como completado $\mathfrak{a}M$-ádico de M. El A-morfismo $M \longrightarrow \hat{M}$ induce el $\hat{A}$-morfismo

$$\hat{A} \otimes_A M \longrightarrow \hat{A} \otimes_A \hat{M} \longrightarrow \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M},$$

que en general no es ni inyectivo ni sobreyectivo, pero se tiene el resultado siguiente, cuya demostración puede consultarse en el manual de Atiyah-Macdonald, [1].

Proposición 4.9.12. *Para cualquier anillo A, si M es un A-módulo finitamente generado, el A-morfismo*

$$\hat{A} \otimes_A M \longrightarrow \hat{M}$$

es sobreyectivo (donde se han considerado los completados de A y M respecto a las topologías $\mathfrak{a}$-ádica respectivas). Si A es además noetheriano, entonces es biyectivo. En particular, si A es completo para la topología $\mathfrak{a}$-ádica, se deduce que $M \simeq \hat{M}$.

4.10. Topología de Zariski

Dado un anillo A, denotamos con $Spec(A)$ a su espectro primo, esto es, el conjunto de ideales primos de A. En esta sección, vamos a dar una topología a este conjunto que se utilizará en numerosas ocasiones a lo largo del texto. Esta no es para nada un ejemplo anecdótico, sino el primer enlace del Álgebra Conmutativa con la Geometría Algebraica. Para esta sección se han utilizado esencialmente los recursos web del Stacks Project ([10]). Antes de empezar, recordemos las siguientes caracterizaciones del nilradical de un ideal $\mathfrak{a}$ de A (ver observación 4.1.14):

$$\sqrt{\mathfrak{a}} = \{a \in A \ : \ \exists n \in \mathbb{N} \ con \ a^n \in \mathfrak{a}\} = \bigcap_{\mathfrak{p} \in Spec(A) \, : \, \mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}.$$

Definición 4.10.1. Dado un anillo A, se definen los conjuntos siguientes:

1. Para cada subconjunto $T \subseteq A$ se define
$$V(T) = \{\mathfrak{p} \in Spec(A) \ : \ T \subseteq \mathfrak{p}\}.$$
2. Para cada elemento $f \in A$ se define
$$D(f) = \{\mathfrak{p} \in Spec(A) \ : \ f \notin \mathfrak{p}\}.$$

Proposición 4.10.2. ***[Topología de Zariski]*** *Dado un anillo A, la familia de partes de $Spec(A)$ dada por los conjuntos $V(T)$, con $T \subseteq A$, verifica las propiedades siguientes:*

1. *$Spec(A)$ y $\emptyset$ pertenecen a la familia.*
2. *Dada una familia arbitraria de subconjuntos de A, $\{T_j\}_{j\in J}$, se tiene que $\cap_{j\in J} V(T_j) = V(\cup_{j\in J} T_j)$, y por tanto la familia es estable por intersecciones arbitrarias.*
3. *Dada una familia finita de subconjuntos de A, $\{T_i\}_{i=1}^n$, se tiene que $\cup_{i=1}^n V(T_i) = V(\prod_{i=1}^n T_i)$, donde $\prod_{i=1}^n T_i = \{\prod_{i=1}^n f_i \ : \ f_i \in T_i \ \forall i = 1, \dots, n\}$. Por tanto la familia es estable también por uniones finitas.*

Estas tres propiedades nos permiten por tanto concluir que los conjuntos $V(T)$ con $T \subseteq A$ son los cerrados de una topología sobre $Spec(A)$ que se llamará topología de Zariski de A.

Demostración.

1. Basta notar que $Spec(A) = V(0)$ y que $\emptyset = V(A)$, pues todo ideal contiene al cero y ningún ideal primo contiene al anillo por definición.
2. Sea $\mathfrak{p} \in Spec(A)$. Se tienen las equivalencias siguientes:
$$\mathfrak{p} \in \cap_{j\in J} V(T_j) \ \Leftrightarrow \ \forall j \in J, \ \mathfrak{p} \in V(T_j) \ \Leftrightarrow \ T_j \subseteq \mathfrak{p} \ \ \forall j \in J \ \Leftrightarrow \ \cup_{j\in J} T_j \subseteq \mathfrak{p} \ \Leftrightarrow \ \mathfrak{p} \in V(\cup_{j\in J}).$$
3. Probamos ahora cada contención por separado. Sea $\mathfrak{p} \in \cup_{i=1}^n V(T_i)$. Entonces existe un índice $i \in \{1, \dots, n\}$ tal que $\mathfrak{p} \in V(T_i)$, esto es, tal que $T_i \subseteq \mathfrak{p}$. En particular se tiene que $\prod_{i=1}^n T_i \subseteq \mathfrak{p}$, ya que $\mathfrak{p}$ es un ideal. Por tanto $\mathfrak{p} \in V(\prod_{i=1}^n T_i)$. Pongamos ahora que $\mathfrak{p} \in V(\prod_{i=1}^n T_i)$ y supongamos que no pertenece a $\cup_{i=1}^n V(T_i)$ (reducción al absurdo). Como $\mathfrak{p}$ no pertenece a la unión, $\forall i = 1, \dots, n$ se tiene que $T_i \nsubseteq \mathfrak{p}$. Por tanto, para cada i existe un $f_i \in T_i \setminus \mathfrak{p}$. Sin embargo, $\prod_{i=1}^n f_i \in \mathfrak{p}$ puesto que $\prod_{i=1}^n T_i \subseteq \mathfrak{p}$, y como $\mathfrak{p}$ es un ideal primo, debe existir un $j \in \{1, \dots, n\}$ tal que $f_j \in \mathfrak{p}$, lo que es absurdo.

$\square$

Acabamos de ver que las uniones de los cerrados de Zariski para distintos T_i coinciden con el cerrado de Zariski correspondiente al «producto» de dichos conjuntos. Sin embargo, cuando los conjuntos son ideales, ese producto puede sustituirse por una intersección. Veremos en la proposición siguiente esta y otras propiedades de los cerrados de Zariski, pero antes introducimos el siguiente lema, que nos será útil en la demostración de la proposición.

Lema 4.10.3. *Sea A un anillo cualquiera y sean $\mathfrak{a}, \mathfrak{b}, \mathfrak{p}$ tres ideales de A. Si $\mathfrak{p}$ es primo y $\mathfrak{ab} \subseteq \mathfrak{p}$ entonces bien $\mathfrak{a} \subseteq \mathfrak{p}$ o bien $\mathfrak{b} \subseteq \mathfrak{p}$.*

Demostración. Supongamos, sin pérdida de generalidad, que $\mathfrak{a} \not\subseteq \mathfrak{p}$ y veamos que se tiene la otra contención. Sea pues $a \in \mathfrak{p} \setminus \mathfrak{a}$. Entonces, para cada $b \in \mathfrak{b}$, $ab \in \mathfrak{p}$. Como este ideal es primo y a no está contenido en él, se deduce que $b \in \mathfrak{p}$ para todo $b \in \mathfrak{b}$.

□

Proposición 4.10.4. *Sea A un anillo.*

1. *Dados dos subconjuntos T, S de A, si $T \subseteq S$, entonces $V(S) \subseteq V(T)$.*
2. *Dado un subconjunto $T \subseteq A$, si $< T >$ es el ideal engendrado por dicho conjunto entonces $V(T) = V(< T >)$.*
3. *Dado un ideal $\mathfrak{a}$ de A, entonces $V(\mathfrak{a}) = \emptyset$ si y solo si $\mathfrak{a} = A$.*
4. *Dado $\mathfrak{a}$ un ideal de A, se tiene que $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.*
5. *Dados dos ideales $\mathfrak{a}, \mathfrak{b}$ de A, se tiene que $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b})$. Por recurrencia, puede generalizarse el resultado para cualquier familia finita de ideales de A.*
6. *Dada una familia cualquiera de ideales de A, $(\mathfrak{a}_s)_{s \in S}$, entonces $\cap_{s \in S} V(\mathfrak{a}_s) = V(\cup_{s \in S} \mathfrak{a}_s) = V(\sum_{s \in S} \mathfrak{a}_s)$.*

Demostración. La primera es inmediata usando la definición de los cerrados de Zariski. Para la segunda basta recordar que $< T >$ es el ideal más pequeño que contiene a T, luego si $T \subseteq \mathfrak{p}$, entonces $< T > \subseteq \mathfrak{p}$ también por ser $\mathfrak{p}$ un ideal. La otra contención se deduce del punto 1. En el tercer apartado basta aplicar que cualquier ideal de A está contenido en uno maximal (en particular primo) salvo el propio A.
Para el punto 4, notemos primero que cualquier ideal $\mathfrak{a}$ de A está contenido en su nilradical, de modo que podemos usar el punto 1 para probar que $V(\sqrt{\mathfrak{a}}) \subseteq V(\mathfrak{a})$. Para la otra contención, sea $\mathfrak{p} \in V(\mathfrak{a})$. Entonces $\mathfrak{a} \subseteq \mathfrak{p}$ y $\mathfrak{p}$ es primo. Dado $a \in \sqrt{\mathfrak{a}}$, existe un n natural para el cual $a^n \in \mathfrak{a}$. De la contención anterior se tiene que $a^n \in \mathfrak{p}$, y como este ideal es primo se deduce que $a \in \mathfrak{p}$ también y de ahí la otra contención.

Para la parte 5, la contención $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{ab})$ se deduce de que para ideales cualesquiera su producto está contenido en su intersección. Dado ahora $\mathfrak{p} \in V(\mathfrak{ab})$, se tiene que $\mathfrak{ab} \subseteq \mathfrak{p}$, y como es primo, usando el lema 4.10.3 se tiene que bien $\mathfrak{a} \subseteq \mathfrak{p}$ o bien $\mathfrak{b} \subseteq \mathfrak{p}$. En cualquier caso, la intersección $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ y por tanto $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$.

En el último punto basta notar que la suma de ideales es el ideal engendrado por la unión de los mismos y por tanto se puede aplicar el punto 2 a la parte 2 de la proposición 4.10.2.

□

Proposición 4.10.5. ***[Abiertos principales de Zariski]*** *Dado un anillo A y una familia $\{f_i\}_{i \in I}$ de elementos de A, entonces $\cup_{i \in I} D(f_i)$ es el complementario de $V(\{f_i\}_{i \in I})$ en $Spec(A)$. En particular $Spec(A) \setminus V(f) = D(f)$ para cada $f \in A$.*

Por tanto, los complementarios de los cerrados de Zariski son uniones de los conjuntos $D(f)$, con $f \in A$. Así, el conjunto $\{D(f)\}_{f\in A}$ es una base de abiertos para la topología de Zariski, llamados abiertos principales.

Demostración. Sea $\mathfrak{p} \in Spec(A)$. Se tienen las equivalencias siguientes:

$$\mathfrak{p} \in \cup_{i\in I} D(f_i) \Leftrightarrow \exists i \in I : \mathfrak{p} \in D(f_i) \Leftrightarrow \exists i \in I : f_i \notin \mathfrak{p}$$

$$\Leftrightarrow \{f_i\}_{i\in I} \nsubseteq \mathfrak{p} \Leftrightarrow \mathfrak{p} \in Spec(A) \setminus V(\{f_i\}_{i\in I}).$$

□

Proposición 4.10.6. *Dado un anillo A cualquiera, su espectro Spec(A) es un espacio topológico casi-compacto (es decir, que cada recubrimiento de Spec(A) por abiertos admite un subrecubrimiento finito, sin ser necesariamente de Hausdorff).*

Demostración. Como los abiertos principales forman una base de la topología de Zariski, basta probar que de un recubrmiento cualquiera de $Spec(A)$ con estos abiertos se puede extraer un subrecubrimiento finito. Sea pues $Spec(A) = \cup_{i\in I} D(f_i)$ para $f_i \in A$ para todo $i \in I$. Como $V(f_i) = Spec(A) \setminus D(f_i)$, entonces

$$\bigcap_{i\in I} V(f_i) = \bigcap_{i\in I} D(f_i)^c = (\bigcup_{i\in I} D(f_i))^c = Spec(A)^c = \emptyset,$$

donde ^{c} denota el complementario conjuntista en $Spec(A)$. Utilizando ahora el punto 6 de la proposición 4.10.4, $V(\{f_i\}_{i\in I}) = \emptyset$, pero por el punto 3 de la misma proposición se deduce que $< \{f_i\}_{i\in I} >= A$. Así pues, el 1 de A debe poder escribirse como combinación A-lineal finita de elementos f_i: existe $J \subseteq I$ finito tal que $1 = \sum_{j\in J} a_j f_j$ para ciertos $a_j \in A$. Dado $\mathfrak{p} \in Spec(A)$ cualquiera, como es primo $1 \notin \mathfrak{p}$, luego alguno de los f_j no está en $\mathfrak{p}$ (si todos lo estuvieran también lo estaría el 1 por ser combinación alineal suya). Por tanto $\mathfrak{p} \subseteq D(f_{j_0})$ para ese cierto $f_{j_0} \notin \mathfrak{p}$, con $j_0 \in J$. Así se concluye que $Spec(A) = \cup_{j\in J} D(f_j)$ y el espectro es casi-compacto.

□

Proposición 4.10.7. *Sea A un anillo. Los puntos cerrados de su espectro son justamente los ideales maximales del mismo.*

Demostración. Dado $\mathfrak{p} \in Spec(A)$ cualquiera, veamos que su adherencia es exactamente el conjunto $V(\mathfrak{p})$. Como dicho conjunto es un cerrado que contiene a $\mathfrak{p}$ basta ver que es minimal entre ellos: otro cerrado de Zariski que contenga a $\mathfrak{p}$ cualquiera debe contener a $V(\mathfrak{p})$ o, equivalentemente, a cualquier primo $\mathfrak{q}$ tal que $\mathfrak{p} \subseteq \mathfrak{q}$. Sea C un cerrado con $\mathfrak{p} \in C$. Su complementario es abierto y por tanto puede escribirse como unión de abiertos principales, es decir, existen elementos de A, $(f_i)_{i\in I}$ tales que

$$Spec(A) \setminus C = \bigcup_{i\in I} D(f_i).$$

Por tanto, un ideal primo $\mathfrak{d}$ pertenece a C si y solo si para todo $i \in I$ se tiene que $f_i \in \mathfrak{d}$, esto es $\cup_{i\in I} f_i \subseteq \mathfrak{d}$. Como $\mathfrak{p} \in C$, la unión de los f_i está contenida en él, pero entonces cualquier ideal $\mathfrak{q}$ que lo contenga también tendrá a la unión, y por tanto será un elemento de C, como queríamos.

Una vez probado que $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, este punto es cerrado si y solo si el único ideal primo que lo contiene es él mismo, es decir, si y solo si es maximal.

□

Veamos ahora cómo se transforman los espectros de anillos a través de morfismos y localizaciones.

Proposición 4.10.8. ***[Funtorialidad del espectro]*** *Dado un morfismo de anillos $\varphi : A \longrightarrow A'$, el morfismo inducido entre los espectros,*

$$Spec(\varphi) : Spec(A') \longrightarrow Spec(A); \;\; \mathfrak{p} \in Spec(A') \longmapsto \varphi^{-1}(\mathfrak{p}).$$

es continuo para las topologías de Zariski respectivas. En particular, para cada elemento $f \in A$, $Spec(\varphi)^{-1}(D(f)) = D(\varphi(f))$.

Demostración. Utilizando la observación 4.1.3 notamos que la aplicación está bien definida porque la imagen inversa de un ideal primo a través de un morfismo de anillos sigue siendo un ideal primo. Para la segunda parte, basta notar que, para todo $f \in A$,

$$Spec(\varphi)^{-1}(D(f)) = \{\mathfrak{p}' \in Spec(A') \; : \; Spec(\varphi)(\mathfrak{p}') \in D(f)\} = \{\mathfrak{p}' \in Spec(A') \; : \; \varphi(f) \notin \mathfrak{p}'\} = D(\varphi(f)).$$

Así pues las imágenes inversas de abiertos principales son abiertos también y se deduce la continuidad de la aplicación.

$\square$

Lema 4.10.9. *Sean A un anillo y $f, g \in A$. Si son elementos asociados (difieren en una unidad) entonces $D(f) = D(g)$.*

Demostración. Supongamos que $g = uf$ con u una unidad de A. Entonces para cualquier ideal primo $\mathfrak{p}$ de A, se tiene que $f \in \mathfrak{p} \Leftrightarrow g = uf \in \mathfrak{p}$, pues una unidad nunca puede pertenecer a un ideal primo. Equivalentemente, los primos que no contengan a f no contendrán tampoco a g, de modo que $D(f) = D(g)$ como queríamos.

$\square$

Proposición 4.10.10. *Sean A un anillo y S un conjunto multiplicativamente cerrado. La aplicación canónica $A \longrightarrow S^{-1}A$ induce, por la funtorialidad del espectro, un homeomorfismo*

$$Spec(S^{-1}A) \longrightarrow \{\mathfrak{p} \in Spec(A) \; : \; S \cap \mathfrak{p} = \emptyset\},$$

donde la topología en el lado derecho es la inducida por la de Zariski en $Spec(A)$. El inverso de esta aplicación viene dado por $\mathfrak{p} \longmapsto S^{-1}\mathfrak{p}$.

Demostración. Ya hemos visto en la sección de localización que es una biyección (4.3.11), por la proposición anterior (4.10.8) sabemos que es continua por ser restricción en el espacio de llegada de una continua. Veamos que es abierta para concluir. Sea $D(g)$ un abierto principal de $Spec(S^{-1}A)$, con $g \in S^{-1}A$. Podemos escribir $g = h/s$ para ciertos $h \in A$ y $s \in S$, y como $1/s$ es una unidad de $S^{-1}A$, $h/1$ y g son asociados y el lema 4.10.9 nos dice que $D(g) = D(h/1)$. La proposición 4.10.8 en este caso nos dice que las imágenes inversas de abiertos principales de $Spec(S^{-1}A)$ son de la forma $D(f/1)$ para $f \in A$. Uniendo esto a la biyectividad de nuestra aplicación, deducimos que la imagen de $D(g) = D(h/1)$ es justamente $D(h) \cap \{\mathfrak{p} \in Spec(A) \; : \; S \cap \mathfrak{p} = \emptyset\}$, y esto es un abierto de la topología de subespacio, así que la aplicación es abierta.

$\square$

Corolario 4.10.11. *Sean A un anillo y f un elemento cualquiera de A. Entonces la aplicación $A \longrightarrow A_f$ induce, por la funtorialidad del espectro, un homeomorfismo*

$$Spec(A_f) \longrightarrow D(f) \subseteq Spec(A),$$

cuya inversa viene dada por $\mathfrak{p} \longmapsto \mathfrak{p} \cdot A_f$.

Demostración. Basta usar la proposición anterior (4.10.10) aplicada a $S = \{f^i \,:\, i = 0, 1, 2, \dots\}$, pues en ese caso los ideales primos que no contienen a S son justamente los que no contienen a f, esto es, $D(f)$.

$\square$

Incluimos también esta proposición extraída de los apuntes de Milne ([6]), que se utiliza en la sección de álgebras quasifinitas. La demostración puede consultarse en ese libro y, aunque no es complicada, es laboriosa pues hay que incluir otra correspondencia más relacionada con idempotentes y hacer la demostración a partir de las tres.

Proposición 4.10.12. *Sea A un anillo y denotemos por X su espectro $Spec(A)$. Se tienen entonces correspondencias biyectivas naturales entre los objetos siguientes:*

1. *Descomposiciones de X es una unión finita disjunta de abiertos.*
2. *Descomposiciones de A en un producto finito de subanillos.*

Bibliografía

[1] *M. F. Atiyah and I. G. Macdonald.* Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.*

[2] *Siegfried Bosch.* Algebraic geometry and commutative algebra*. Universitext. Springer, London, [2022] ©2022. Second edition.*

[3] *Nicolas Bourbaki.* Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 5 à 7. [Commutative algebra. Chapters 5–7], Reprint.*

[4] *Nicolas Bourbaki.* Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 1 à 4. [Commutative algebra. Chapters 1–4], Reprint.*

[5] *Hideyuki Matsumura.* Commutative ring theory*, volume 8 of* Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Translated from the Japanese by M. Reid.*

[6] *James S. Milne. A Primer in Commutative Algebra.* `https://www.jmilne.org/math/xnotes/CA.pdf`*, 2020.*

[7] *Christian Peskine. Une généralisation du "main theorem" de Zariski.* Bull. Sci. Math. (2)*, 90:119–127, 1966.*

[8] *Massimo Pippi. Proper base change over henselian pairs. ALGANT Master's thesis.* `https://www.math.u-bordeaux.fr/~ybilu/algant/documents/theses/Pippi.pdf`*, 2017.*

[9] *Michel Raynaud.* Anneaux locaux henséliens*, volume Vol. 169 of* Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1970.*

[10] *The Stacks Project Authors. Stacks Project.* `https://stacks.math.columbia.edu`*, 2018.*