Carlos Ivorra Castillo

ÁLGEBRA HOMOLÓGICA Y ÁLGEBRA CONMUTATIVA

Los geómetras se imaginan las matemáticas, los analistas las hacen y los algebristas las entienden.

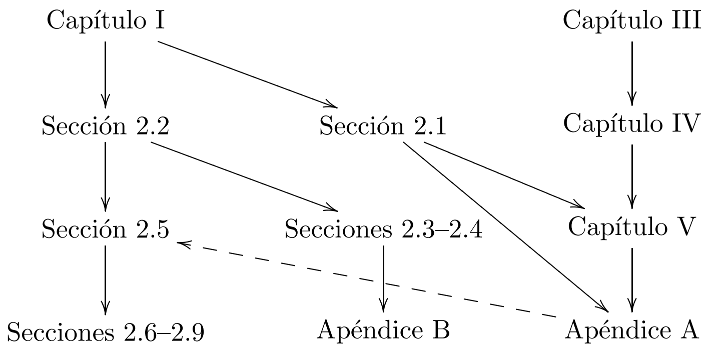
Índice General

Introducción

El propósito original de este libro era presentar los resultados sobre álgebra conmutativa necesarios para un futuro libro de geometría algebraica moderna (teoría de esquemas). Algunos de estos resultados requieren para su demostración una base de álgebra homológica, que en una primera redacción aparecía intercalada en los distintos capítulos a medida que iba siendo necesaria y, para las demostraciones, remitía a menudo a mi libro de Topología algebraica. Sin embargo, dado que la teoría de esquemas requiere una exposición más general del álgebra homológica que la que en principio exigiría la finalidad de este libro, decidí finalmente tratar esta materia con la generalidad necesaria a largo plazo en un primer capítulo preliminar. Me encontré entonces con que la teoría de este primer capítulo tiene aplicaciones a la topología algebraica y a la geometría diferencial más inmediatas que sus pretendidas aplicaciones a la teoría de esquemas, por lo que decidí incluirlas también en el presente libro. A su vez, este tratamiento del álgebra homológica hacía natural anticipar algunos resultados que en un principio pensaba introducir en el libro sobre teoría de esquemas.

El resultado final es que, formalmente, este libro ha pasado de ser un libro de álgebra conmutativa a tener dos partes de aproximadamente igual peso: una primera de álgebra homológica, dividida en dos capítulos, y una segunda de álgebra conmutativa, dividida en tres. Por otra parte, en cuanto a su contenido se pueden distinguir tres niveles, que pueden dar lugar a tres lecturas diferentes según los intereses de cada lector. En primer lugar están los resultados de álgebra homológica con aplicaciones a la topología algebraica y a la geometría diferencial; en segundo lugar están los resultados de álgebra conmutativa que incluyen una parte de álgebra homológica; y en tercer lugar están los resultados de álgebra homológica —más un apéndice en el que se combinan las dos álgebras— incluidos aquí para referirme a ellos en el citado libro de geometría algebraica, y que sería razonable omitir en una primera lectura.

Prescindiendo de algunos ejemplos y comentarios marginales, el esquema de dependencia entre las distintas partes es el que aparece en la página siguiente. La primera columna contiene los resultados de álgebra homológica (Capítulo I) y sus aplicaciones relacionadas con la geometría diferencial y la topología algebraica. En la sección 2.1 se construyen los funtores Tor, que son la única herramienta cohomológica necesaria en la parte de álgebra conmutativa, mientras que las secciones 2.3 y 2.4 contienen propiedades sobre los módulos localmente libres y sobre los funtores Ext que no tendrán ninguna aplicación en este libro, pero que son necesarios en la teoría de esquemas (y lo mismo vale para los resultados sobre los funtores f^* y f_* estudiados en el apéndice B). La tercera columna corresponde a los resultados de álgebra conmutativa propiamente dicha. En la sección 2.5 se usará un resultado sobre módulos que aparece demostrado en el apéndice A, si bien la prueba se basa únicamente en resultados elementales. Por último, las aplicaciones de las secciones 2.6–2.9 hacen referencia a los resultados de topología algebraica y geometría diferencial que aparecen demostrados en mi libro de Topología Algebraica.



El capítulo I empieza introduciendo la noción de haz sobre un espacio topológico. Se trata del concepto básico para enlazar la teoría que pretendemos desarrollar con sus aplicaciones geométricas. Un haz $\mathcal{F}$ es simplemente una estructura definida sobre un espacio topológico X, que asigna a cada uno de sus abiertos U un grupo $\mathcal{F}(U)$, o un anillo, o un módulo, o cualquier otra estructura algebraica, junto con condiciones que garanticen que los distintos grupos, anillos, etc. están relacionados de forma razonable.

Existe una infinidad de haces que aparecen de forma natural en casi todas las ramas de la matemática. Por ejemplo, a cada abierto U de una variedad diferencial X podemos asociarle la $\mathbb{R}$-álgebra $C^\infty(U)$ de sus funciones de clase C^∞ con valores en $\mathbb{R}$.

Cuando en un espacio topológico X tenemos definido un haz de anillos $\mathcal{O}_X$, podemos hablar de $\mathcal{O}_X$-módulos, que son los haces $\mathcal{M}$ sobre X tales que $\mathcal{M}(U)$ es un módulo sobre el anillo $\mathcal{O}_X(U)$, para cada abierto $U \subset X$. Por ejemplo, el haz que a cada abierto U de una variedad diferencial le asigna el $\mathbb{R}$-espacio vectorial $\Lambda^p(U)$ de sus formas diferenciales de dimensión p, es un C^∞-módulo, pues, ciertamente, $\Lambda^p(U)$ es un módulo sobre el anillo $C^\infty(U)$.

El concepto de módulo sobre un haz de anillos generaliza al de módulo sobre un anillo, pues si tomamos un espacio X con un único punto P, cada anillo A determina un haz de anillos en X (que asigna A al único abierto no vacío de X) y, análogamente, los módulos sobre este haz de anillos se corresponden con los módulos sobre A en el sentido usual. Así, toda el álgebra homológica que desarrollamos después sobre módulos sobre un espacio anillado se aplica en particular a módulos sobre un anillo. En las aplicaciones al álgebra conmutativa sólo necesitamos la teoría en este caso particular, mientras que para las aplicaciones a la geometría diferencial, a la topología algebraica o a la geometría algebraica, la generalización a módulos sobre un espacio anillado es fundamental.

El resto del capítulo está dedicado a desarrollar en este contexto la teoría de funtores derivados. Puede considerarse —y así fue, de hecho, como surgió— una versión abstracta que unifica las diversas construcciones de grupos de homología y cohomología que aparecen en topología algebraica y en geometría diferencial. En sus aplicaciones geométricas, permite asignar a cada espacio topológico X y a cada anillo A (bajo ciertas hipótesis) una sucesión de grupos de cohomología $H^p(X, A_X)$. La construcción es extremadamente abstracta, pero satisface un poderoso teorema de unicidad que hace fácil probar que $H^p(X, A_X)$ coincide con casi cualquier cosa. Así, por ejemplo, se demuestra (fácilmente) que los grupos de cohomología de De Rham de una variedad diferencial X son isomorfos a los grupos $H^p(X, \mathbb{R}_X)$, y lo mismo sucede con los grupos de cohomología singular diferenciable. Al combinar estos dos isomorfismos:

$$H^p(X) \cong H^p(X, \mathbb{R}_X) \cong H^p_\infty(X, \mathbb{R}),$$

obtenemos el teorema de De Rham. Podría pensarse que esta prueba obtenida por mediación de un concepto abstracto como $H^p(X, \mathbb{R}_X)$ es una mera prueba de existencia que no nos proporciona información explícita sobre cuál es ese isomorfismo, pero en realidad sucede justo lo contrario. Los isomorfismos individuales

$$H^p(X) \cong H^p(X, \mathbb{R}_X) \quad \text{y} \quad H^p_\infty(X, \mathbb{R}) \cong H^p(X, \mathbb{R}_X)$$

hacen partícipes a los grupos $H^p(X)$ y $H^p_\infty(X, \mathbb{R}_X)$ de la potente unicidad que satisfacen los grupos $H^p(X, \mathbb{R}_X)$, y ello implica que cualquier homomorfismo entre ellos que satisfaga unas mínimas condiciones ha de ser necesariamente un isomorfismo. Así, la prueba de que el isomorfismo explícito entre la cohomología de De Rham y la cohomología singular viene dada por la integración de formas diferenciales sobre símplices no requiere más cálculo integral que el imprescindible para definir la integración de formas sobre símplices. La parte no trivial del teorema, es decir, que esta integral induce un isomorfismo entre los grupos de cohomología, se vuelve poco menos que trivial. Más aún, esta técnica permite demostrar con sorprendente simplicidad la versión fuerte del teorema de De Rham, a saber, que los isomorfismos entre los distintos grupos de cohomología se combinan para formar un isomorfismo de álgebras

$$\bigoplus_{p=0}^{\infty} H^p(X) \cong \bigoplus_{p=0}^{\infty} H^p_\infty(X, \mathbb{R}),$$

cuando cada miembro se dota de estructura de álgebra con el correspondiente producto exterior. Nuevamente, los únicos cálculos de la prueba son los necesarios para construir los productos exteriores.

Las mismas técnicas que llevan a la construcción de los grupos $H^p(X, A_X)$ (o, más en general, $H^p(X, \mathcal{F})$, para cualquier haz $\mathcal{F}$ sobre el espacio topológico X), cuando se particularizan del contexto de los haces al contexto de los módulos sobre un anillo, dan lugar a ciertas familias de módulos asociadas a unos módulos dados y que tienen muchas aplicaciones en el álgebra conmutativa. Las más importantes son los módulos $\mathrm{Tor}_p^A(M,N)$ y $\mathrm{Ext}_p^A(M,N)$. Ambas familias están relacionadas y a menudo es posible elegir entre usar una u otra para un determinado fin. Nosotros hemos optado por utilizar Tor en todas las aplicaciones, de modo que, aunque también daremos la construcción de Ext, no veremos aplicaciones. (Al contrario que Tor, la familia Ext puede definirse para módulos sobre un espacio anillado, y pueden usarse para demostrar un profundo teorema sobre cohomología de esquemas, el teorema de dualidad.)

Si el álgebra homológica ha surgido a partir de la topología algebraica, el álgebra conmutativa ha surgido de la geometría algebraica. La geometría algebraica clásica estudia los conjuntos algebraicos afines y proyectivos, es decir, subconjuntos del espacio afín o del espacio proyectivo definidos como conjuntos de ceros de uno o varios polinomios de varias variables. Los conjuntos algebraicos pueden dotarse de una topología (la topología de Zariski) en la que cada punto tiene un entorno isomorfo a un conjunto algebraico afín, por lo que los problemas geométricos locales, es decir, los que dependen únicamente de las propiedades de un conjunto algebraico en un entorno de uno de sus puntos, pueden reducirse al estudio de conjuntos algebraicos afines. Es, precisamente, en el estudio de los conjuntos algebraicos afines donde la conexión con el álgebra conmutativa es más estrecha:

A cada conjunto algebraico afín $C \subset A^n(k)$ (un conjunto definido por polinomios con coeficientes en un cuerpo k), se le puede asignar la k-álgebra $k[C]$ de las funciones polinómicas (las funciones definidas por polinomios sobre los puntos de C). Sucede que las propiedades geométricas de C están determinadas por las propiedades del anillo $k[C]$. Para ser más precisos, podemos distinguir entre las propiedades *extrínsecas* de C, las propiedades que dependen del modo en que C está sumergido en el espacio afín $A^n(k)$, y las propiedades *intrínsecas,* las que comparten dos conjuntos algebraicos isomorfos, independientemente de cómo estén sumergidos en $A^n(k)$, incluso para distintos valores de n. Las propiedades intrínsecas son precisamente las que pueden expresarse en términos del anillo $k[C]$.

Por ejemplo, en el caso más simple, en que el cuerpo k es algebraicamente cerrado, los puntos de C se corresponden con los ideales maximales de $k[C]$, y los ideales primos de $k[C]$ se corresponden con los subconjuntos algebraicos *irreducibles* de C. (La irreducibilidad expresa que no pueden descomponerse en un número finito de conjuntos algebraicos menores. Por ejemplo, una circunferencia es irreducible, mientras que la unión de una recta y una circunferencia tiene dos componentes irreducibles.) Esto permite expresar la dimensión de C en términos de los ideales de $k[C]$: el hecho de que una esfera S tiene dimensión 2 se corresponde con el hecho de que las mayores cadenas de subconjuntos algebraicos irreducibles contenidos en una esfera tienen longitud 3, pues son necesariamente de la forma

$$\text{punto} \subset \text{curva} \subset \text{esfera}.$$

Equivalentemente, la máxima longitud de una cadena de ideales primos de $k[S]$ es 3. En vista de esto, podemos definir la *dimensión de Krull* de un anillo A como la máxima longitud (menos 1) de una cadena de ideales de A, que en general puede ser infinita. En estos términos, la dimensión de un conjunto algebraico C es una propiedad intrínseca, pues es igual a la dimensión de Krull de su álgebra $k[C]$ de funciones polinómicas.

Tenemos así un ejemplo típico de lo que se hace al estudiar el álgebra conmutativa: partimos de una propiedad geométrica como la dimensión, y pasamos a una propiedad que tiene sentido en un anillo arbitrario, como es la dimensión de Krull. La generalización de conceptos y resultados geométricos a anillos arbitrarios tiene varias razones de ser, entre las que cabe destacar:

- Facilita el empleo de técnicas algebraicas para el estudio de determinados problemas geométricos.
- Permite comprender mejor las propiedades intrínsecas de los conjuntos algebraicos.
- Flexibiliza las posibilidades de tratarlos al no estar sometidos a la necesidad de trabajar en todo momento con conjuntos definidos por polinomios.
- Permite aplicar las técnicas geométricas a otros contextos distintos de la propia geometría, como la teoría algebraica de números.

Esto se entenderá mejor si pensamos en la situación análoga en geometría diferencial. Los conjuntos algebraicos son equiparables a las variedades diferenciales definidas como subconjuntos de $\mathbb{R}^n$. Sin embargo, la noción abstracta de variedad diferencial, que permite tratar como tal a un espacio topológico que satisfaga ciertas condiciones, aunque no sea un subespacio de $\mathbb{R}^n$, presenta estas mismas ventajas. Aunque puede probarse que toda variedad diferencial puede sumergirse en $\mathbb{R}^n$, lo cierto es que hacerlo puede ser complicado y no ayudar en nada a su estudio, sino más bien al contrario. Pensemos por ejemplo en el plano proyectivo $\mathrm{P}^2(\mathbb{R})$. Es cierto que puede sumergirse en $\mathbb{R}^4$, pero es mucho más cómodo considerarla como variedad abstracta, por ejemplo, como el cociente que resulta al identificar los puntos opuestos de una esfera.

El análogo en geometría algebraica al concepto abstracto de variedad diferencial es el concepto de *esquema,* y el álgebra conmutativa es a la teoría de esquemas lo que el cálculo diferencial es a la geometría diferencial.

Respecto a las posibilidades de aplicación a la teoría de números, pensemos en la siguiente analogía: la geometría clásica puede reformularse en términos del álgebra lineal, identificando los puntos, rectas, planos, etc. con las subvariedades afines de $\mathbb{R}^n$, pero entonces estas técnicas geométricas pueden aplicarse igualmente a las subvariedades afines de k^n, donde k es un cuerpo arbitrario o, en otra dirección, pueden generalizarse a espacios de dimensión infinita (espacios de Banach o espacios de Hilbert) con numerosas aplicaciones. Igualmente, la geometría abstracta que proporciona la teoría de esquemas tiene importantes aplicaciones a la teoría de números (curvas elípticas, variedades abelianas, etc.)

En el Capítulo III exponemos simultáneamente los conceptos fundamentales de la geometría afín y del álgebra conmutativa, para mostrar cómo los segundos surgen de los primeros y los extienden. Los resultados principales de este capítulo conciernen a la dimensión de Krull de un anillo. Los análogos algebraicos de propiedades geométricamente intuitivas pueden ser difíciles de probar a causa de que un anillo arbitrario (o sujeto a hipótesis razonables, pero generales al mismo tiempo) no tiene por qué comportarse a priori como el álgebra de funciones polinómicas de un conjunto algebraico.

Veremos también que el estudio de las propiedades locales de un conjunto algebraico afín C, esto es, las propiedades que tiene C alrededor de uno de sus puntos P, pueden reducirse al estudio de un anillo asociado a $k[C]$, el anillo $\mathcal{O}_{C,P}$ de los cocientes de funciones polinómicas definidos en P. Veremos que la construcción de $\mathcal{O}_{C,P}$ a partir de $k[C]$ puede generalizarse a anillos arbitrarios (formación de anillos de fracciones), y que los anillos construidos de esta forma tienen la característica fundamental de ser *anillos locales,* es decir, anillos con un único ideal maximal (en el caso de $\mathcal{O}_{C,P}$ el ideal maximal es el ideal de las funciones que se anulan en P). El Capítulo IV está íntegramente dedicado al estudio de los anillos locales. Un ejemplo de propiedad local es la dimensión alrededor de un punto. Por ejemplo, la unión de un plano y una recta tiene, por definición, dimensión 2, pero se puede hablar de la dimensión alrededor de un punto, que en este caso será 1 para los puntos de la recta y 2 para los puntos del plano. Esto hace que los resultados principales sobre la dimensión de Krull de un anillo se apliquen a anillos locales (lo que simplifica la situación al eliminar los casos "híbridos" como el del ejemplo que acabamos de comentar). El resultado fundamental de este capítulo es el teorema de la dimensión, que da dos caracterizaciones alternativas de la dimensión de Krull de un anillo local, que resultan ser una poderosa herramienta de trabajo.

Finalmente, en el capítulo V estudiamos el álgebra subyacente al equivalente en geometría algebraica al concepto de diferenciabilidad en geometría diferencial. Estudiar la diferenciabilidad sin cálculo diferencial no es cosa fácil, y es aquí donde hacen falta las técnicas de álgebra homológica. El concepto del que hablamos recibe el nombre de regularidad, y es crucial en geometría algebraica por el mismo motivo que el concepto de diferenciabilidad es fundamental en geometría diferencial. En general, un conjunto algebraico (o un esquema) puede tener puntos "singulares" donde falla la regularidad (por ejemplo, un cono es singular en su vértice), y no es de extrañar que muchos resultados requieran la hipótesis de regularidad o, al menos, requieran distinguir los puntos regulares de los singulares. Por otra parte, las buenas propiedades de los conjuntos algebraicos regulares no son, ni mucho menos, evidentes, sino que es necesario disponer de una potente maquinaria algebraica para sacar partido de una hipótesis de regularidad. Ésta es la finalidad de este último capítulo.

El Apéndice A presenta los módulos planos, concepto que surge de forma natural en el estudio del álgebra homológica pero que tiene aplicaciones importantes en geometría algebraica. Lo hemos dejado para el final porque muchos de los resultados que probamos al respecto requieren de los teoremas técnicos que se demuestran en este libro, pero no estamos en condiciones de mostrar su interés. El lector interesado en la geometría algebraica puede relegar los dos apéndices, al igual que las secciones 2.3 y 2.4, a una segunda lectura.

Primera parte

Álgebra homológica

Capítulo I

Funtores derivados

En este capítulo expondremos la teoría de funtores derivados en el grado justo de generalidad que vamos a necesitar. Ello significa que no trabajaremos ni en el contexto —demasiado restrictivo— de las categorías de módulos sobre un anillo, ni tampoco en el contexto —inaceptablemente abstracto— de las categorías abelianas. Como término medio entre ambos extremos, hemos optado por desarrollar la teoría en el contexto de las categorías de módulos sobre un espacio anillado, así que las primeras secciones están dedicadas a presentar este concepto.

En lo sucesivo, todos los anillos se supondrán conmutativos y unitarios (y todo homomorfismo de anillos conserva la unidad por definición). Por el contrario, no supondremos que los espacios topológicos tengan la propiedad de Hausdorff salvo que lo indiquemos explícitamente.

1.1 Haces

Representaremos por $\mathbb{K}$ el cuerpo $\mathbb{R}$ o $\mathbb{C}$. Si X es un espacio topológico, para cada abierto U de X podemos considerar el conjunto $C_X(U,\mathbb{K})$ de las funciones continuas $U \longrightarrow \mathbb{K}$, que tiene una estructura de $\mathbb{K}$-álgebra con las operaciones definidas puntualmente. Estas álgebras están relacionadas entre sí: cuando $U \subset V \subset X$ son abiertos, la restricción $\rho_U^V : C_X(V,\mathbb{K}) \longrightarrow C_X(U,\mathbb{K})$ es un homomorfismo de $\mathbb{K}$-álgebras.

Éste es sólo uno de los muchos ejemplos en los que es posible asignar consistentemente de forma natural a cada abierto de un espacio topológico (tal vez dotado de estructuras más fuertes) un objeto algebraico (una $\mathbb{K}$-álgebra, un espacio vectorial, etc.). Pensemos, por ejemplo, en álgebras de funciones C^∞, u holomorfas, o espacios de tensores o formas diferenciales, etc.

La noción de haz axiomatiza este tipo de situaciones:

Definición 1.1 Un *prehaz* sobre un espacio topológico X es un par $(\mathcal{F},\rho)$, donde $\mathcal{F}$ es una aplicación que a cada abierto U de X le asigna un grupo abeliano $\mathcal{F}(U)$ y ρ es una aplicación que a cada par de abiertos $U \subset V$ de X les asigna una homomorfismo $\rho_U^V : \mathcal{F}(V) \longrightarrow \mathcal{F}(U)$ (que llamaremos restricción) de modo que se cumplan las propiedades siguientes:

a) $\mathcal{F}(\varnothing) = 0$,

b) ρ_U^U es la identidad en $\mathcal{F}(U)$,

c) si $U \subset V \subset W$ son abiertos de X, entonces $\rho_V^W \circ \rho_U^V = \rho_U^W$.

Si los grupos $\mathcal{F}(U)$ son anillos o módulos, etc. y las restricciones son homomorfismos de anillos, módulos, etc., entonces tenemos un *prehaz de anillos, módulos,* etc.

Normalmente, si $f \in \mathcal{F}(V)$ y $U \subset V$ escribiremos $f|_U = \rho_U^V(f)$.

Un *haz* sobre un espacio topológico X es un prehaz tal que si U es un abierto en X y $U = \bigcup\limits_i U_i$ es un cubrimiento abierto de U, entonces

a) Si $f \in \mathcal{F}(U)$ cumple que $f|_{U_i} = 0$ para todo i, entonces $f = 0$.

b) Para cada familia de elementos $f_i \in \mathcal{F}(U_i)$ tales que $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ para todos los índices i, j, existe un $f \in \mathcal{F}(U)$ tal que $f|_{U_i} = f_i$ para todo índice i.

Notemos que el elemento f cuya existencia se afirma en la propiedad b) es único por la propiedad a).

Ejemplos Al principio de la sección hemos definido el haz C_X de las funciones (reales o complejas) continuas sobre un espacio topológico X, que es, concretamente, un haz de $\mathbb{K}$-álgebras. Es obvio que cumple las condiciones de la definición. Similarmente podemos definir el haz C_X^∞ de las funciones de clase C^∞ sobre los abiertos de una variedad diferencial, o el haz $\mathcal{H}_X$ de las funciones holomorfas definidas sobre los abiertos de una variedad compleja.

Consideremos un espacio topológico arbitrario X, un grupo abeliano arbitrario A y fijemos punto $p \in X$. Llamaremos A_X^p al haz que a cada abierto $U \subset X$ le hace corresponder el grupo

$$A_X^p(U) = \begin{cases} A & \text{si } p \in U, \\ 0 & \text{si } p \notin U, \end{cases}$$

y en el que ρ_V^U es la identidad si $p \in V$ y el homomorfismo nulo en caso contrario. Es fácil comprobar que se trata ciertamente de un haz. Los haces de esta forma se llaman *rascacielos.*

Veamos ahora un ejemplo de prehaz que no es un haz:

Sea X un espacio topológico y sea A un grupo abeliano. Definimos el *prehaz constante* A_X^- como el dado por

$$A_X^-(U) = \begin{cases} A & \text{si } U \neq \varnothing, \\ 0 & \text{si } U = \varnothing, \end{cases}$$

en el que ρ_V^U es la identidad en A salvo si $V = \varnothing$. Obviamente A_X^- es un prehaz de grupos, pero es claro que no es un haz si $A \neq 0$ y X contiene dos abiertos disjuntos. ■

Los haces permiten relacionar las propiedades globales y locales de los espacios sobre los que están definidos. La herramienta clave para ello es el concepto siguiente:

Definición 1.2 Si $\mathcal{F}$ es un prehaz sobre un espacio topológico X y $P \in X$, definimos el *grupo de gérmenes* o *grupo local* de $\mathcal{F}$ en P como el grupo $\mathcal{F}_P$ formado por las clases de equivalencia de pares (U, f) con $P \in U$, U abierto en X, y $f \in \mathcal{F}(U)$, respecto de la relación dada por $(U, f) \sim (V, g)$ si y sólo si existe un abierto $W \subset U \cap V$ tal que $P \in W$ y $f|_W = g|_W$. La operación de grupo es la dada por

$$[(U, f)] + [(V, g)] = [(U \cap V, f|_{U\cap V} + g|_{U\cap V})].$$

Si $f \in \mathcal{F}(U)$ y $P \in U$, representaremos por $f_P = [(U, f)] \in \mathcal{F}_P$. Es claro que la aplicación $\mathcal{F}(U) \longrightarrow \mathcal{F}_P$ dada por $f \mapsto f_P$ es un homomorfismo de grupos.

Si $\mathcal{F}$ es un prehaz de anillos o módulos, etc., los grupos de gérmenes $\mathcal{F}_P$ adquieren la misma estructura de forma natural. En lo sucesivo omitiremos este tipo de observaciones, que siempre serán triviales.

Si $\mathcal{F}$ es un prehaz en un espacio topológico X y $U \subset X$ es un abierto, definimos la *restricción* de $\mathcal{F}$ a U como el prehaz $\mathcal{F}|_U$ que a cada abierto $V \subset U$ le asigna el grupo $\mathcal{F}|_U(V) = \mathcal{F}(V)$ y respecto al que las restricciones entre abiertos son las mismas que las de $\mathcal{F}$. Es obvio que si $\mathcal{F}$ es un haz su restricción a cualquier abierto también lo es. Si $P \in U$, tenemos un isomorfismo natural $(\mathcal{F}|_U)_P \longrightarrow \mathcal{F}|_P$ dado por $[(V, f)] \mapsto [(V, f)]$.

Ejemplos Si X es un espacio topológico y $p \in X$ es un punto cerrado (en particular, si X es un espacio de Hausdorff), entonces, para todo punto $q \in X$, el haz rascacielos A_X^p cumple que

$$A_{X,q}^p = \begin{cases} A & \text{si } q = p, \\ 0 & \text{si } q \neq p. \end{cases}$$

(Esta propiedad ha sugerido el nombre de "rascacielos".)

Por otra parte, el prehaz constante A_X^- cumple que $A_{X,q}^- = A$ para todo punto $q \in X$. ■

Veamos un primer ejemplo elemental de cómo un hecho global se puede probar localmente:

Teorema 1.3 *Sea $\mathcal{F}$ un haz sobre un espacio topológico X, sea U un abierto en X y sean f, $g \in \mathcal{F}(U)$ tales que $f_P = g_P$ para todo $P \in U$. Entonces $f = g$.*

DEMOSTRACIÓN: La hipótesis significa que todo punto $P \in U$ tiene un entorno $V_P \subset U$ donde $f|_{V_P} = g|_{V_P}$. Equivalentemente, $(f-g)|_{V_P} = 0$. La definición de haz implica que $f - g = 0$. ■

Definición 1.4 Sea X un espacio topológico y $\mathcal{F}$ un prehaz en X. Un *subprehaz* de $\mathcal{F}$ es un prehaz $\mathcal{G}$ en X tal que, para todo abierto $U \subset X$, se cumple que $\mathcal{G}(U)$ es un subgrupo de $\mathcal{F}(U)$ y las restricciones de $\mathcal{G}$ son las restricciones de las restricciones correspondientes de $\mathcal{F}$ (o, en otras palabras, que si $V \subset U$ y $f \in \mathcal{G}(U)$, entonces $f|_V$ es el mismo tanto si lo calculamos en $\mathcal{F}$ o en $\mathcal{G}$. Si $\mathcal{G}$ es un haz diremos que es un *subhaz* de $\mathcal{F}$.

Observemos que si $\mathcal{G}$ es un subprehaz de $\mathcal{F}$ y $P \in X$, tenemos un monomorfismo natural $\mathcal{G}_P \longrightarrow \mathcal{F}_P$ dado por $[(U,f)] \mapsto [(U,f)]$, el cual nos permite identificar a $\mathcal{G}_P$ con un subgrupo de $\mathcal{F}_P$.

Ejemplo Si X es una variedad diferencial, es claro que el haz C_X^∞ de las funciones diferenciables en X es un subhaz del haz C_X de las funciones continuas. ■

Un subhaz está determinado por sus grupos de gérmenes:

Teorema 1.5 *Sea X un espacio topológico, sea $\mathcal{F}$ un haz en X y sea $\mathcal{G}$ un subhaz. Si $U \subset X$ es un abierto y $f \in \mathcal{F}(U)$, entonces $f \in \mathcal{G}(U)$ si y sólo si $f_P \in \mathcal{G}_P$ para todo $P \in U$.*

DEMOSTRACIÓN: Una implicación es obvia. Si se cumple la condición local, cada punto $P \in U$ tiene un entorno $V_P \subset U$ tal que $f|_{V_P} = g_P$, para cierto $g_P \in \mathcal{G}(V_P)$. Como $\mathcal{G}$ es un haz, existe un $g \in \mathcal{G}(U)$ tal que $g|_{V_P} = g_P = f|_{V_P}$ para todo P y, como $\mathcal{F}$ es un haz, esto implica que $f = g \in \mathcal{G}(U)$. ■

Definición 1.6 Si $\mathcal{F}$ y $\mathcal{G}$ son dos prehaces sobre un espacio topológico X, un *homomorfismo de prehaces* (o de haces, si es que $\mathcal{F}$ y $\mathcal{G}$ son haces) $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ es una aplicación que a cada abierto U de X le asigna un homomorfismo de grupos $\alpha_U : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ tal que si $U \subset V \subset X$, el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
\mathcal{F}(V) \arrow[r, "\alpha_V"] \arrow[d, "\rho_U^V"'] & \mathcal{G}(V) \arrow[d, "\rho_U^V"] \\
\mathcal{F}(U) \arrow[r, "\alpha_U"'] & \mathcal{G}(U)
\end{tikzcd}$$

Es claro que α induce homomorfismos $\alpha_P : \mathcal{F}_P \longrightarrow \mathcal{G}_P$ entre los grupos de gérmenes, dados por $\alpha_P([(U,f)]) = [(U, \alpha_U(f))]$, de modo que si U es un abierto y $P \in U$, el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\alpha_U"] \arrow[d] & \mathcal{G}(U) \arrow[d] \\
\mathcal{F}_P \arrow[r, "\alpha_P"'] & \mathcal{G}_P
\end{tikzcd}$$

La composición de homomorfismos de prehaces se define de forma obvia, al igual que el homomorfismo identidad $1_{\mathcal{F}} : \mathcal{F} \longrightarrow \mathcal{F}$. Un homomorfismo de prehaces $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ es un *isomorfismo* si existe un homomorfismo $\beta : \mathcal{G} \longrightarrow \mathcal{F}$ tal que $\alpha \circ \beta = 1$ y $\beta \circ \alpha = 1$. Esto equivale a que todos los homomorfismos $\alpha_U : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ sean isomorfismos. El teorema siguiente nos da otra caracterización:

Teorema 1.7 *Un homomorfismo de haces $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ sobre un espacio topológico X es un isomorfismo si y sólo si para todo $P \in X$ los homomorfismos $\alpha_P : \mathcal{F}_P \longrightarrow \mathcal{G}_P$ son isomorfismos.*

Demostración: Una implicación es obvia. Supongamos que los homomorfismos α_P son isomorfismos. Sea U un abierto en X y sea $s \in \mathcal{F}(U)$ tal que $\alpha_U(s) = 0$. Entonces, para cada $P \in U$ tenemos que $\alpha_P(s_P) = \alpha_U(s)_P = 0$. Por consiguiente $s_P = 0$ para todo $P \in U$, y el teorema 1.3 nos da que $s = 0$. Esto prueba que α_U es un monomorfismo.

Tomemos ahora $t \in \mathcal{G}(U)$. Para cada $P \in U$ existe un $f \in \mathcal{F}_P$ tal que $\alpha_P(f) = t_P$. Esto significa que existe un abierto $P \in U_P \subset U$ de forma que $f = [(U_P, s_P)]$ y $t|_{U_P} = \alpha_{U_P}(s_P)$. Entonces

$$\alpha_{U_P \cap U_Q}(s_P|_{U_P \cap U_Q}) = t|_{U_P \cap U_Q} = \alpha_{U_P \cap U_Q}(s_Q|_{U_P \cap U_Q}).$$

Ya hemos probado que $\alpha_{U_P \cap U_Q}$ es inyectiva, luego s_P y s_Q coinciden en $U_P \cap U_Q$. Por la definición de haz existe un $s \in \mathcal{F}(U)$ tal que $s|_{U_P} = s_P$ para todo $P \in U$. Ahora $\alpha_U(s)|_{U_P} = \alpha_{U_P}(s_P) = t|_{U_P}$, con lo que $\alpha_U(s) = t$. ■

Definición 1.8 Diremos que un homomorfismo de haces $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ sobre un espacio topológico X es un *monomorfismo* (resp. un *epimorfismo)* si para todo $P \in X$ se cumple que α_P es un monomorfismo (resp. un epimorfismo).

En la prueba del teorema anterior se muestra que α es un monomorfismo en este sentido si y sólo si α_U es un monomorfismo para todo abierto U de X. En cambio el ejemplo siguiente muestra que, aunque α sea un epimorfismo, los homomorfismos α_U no tienen por qué ser epimorfismos:

Ejemplos Sea $X = \mathbb{C} \setminus \{0\}$, sea $\mathcal{H}_X$ el haz de las funciones holomorfas y sea $\mathcal{H}_X^*$ el haz de las funciones holomorfas que no se anulan (que es un grupo abeliano con el producto de funciones, no con la suma). Sea $\phi : \mathcal{H}_X \longrightarrow \mathcal{H}_X^*$ el homomorfismo dado por $\phi_U(f)(z) = e^{f(z)}$. La teoría de funciones de variable compleja prueba que ϕ es un epimorfismo (porque cada función holomorfa que no se anula tiene un logaritmo holomorfo en un entorno de cada punto), mientras que la identidad $I \in \mathcal{H}_X^*(X)$ no tiene antiimagen por ϕ_X (pues no existe un logaritmo holomorfo definido sobre todo $\mathbb{C} \setminus \{0\}$).

Sea X una variedad diferencial y sea Λ_X^1 el haz de las formas diferenciales de grado 1 sobre X, es decir, para cada abierto $U \subset X$ definimos $\Lambda_X^1(U)$ como el espacio vectorial de las formas diferenciales definidas sobre U, y las restricciones son las naturales. La diferencial exterior induce un homomorfismo de haces

$$d : C_X^\infty \longrightarrow \Lambda_X^1.$$

Concretamente, para cada abierto $U \subset X$, el homomorfismo

$$d_U : C_X^\infty(U) \longrightarrow \Lambda_X^1(U)$$

es el que a cada función f le asigna su diferencial.

Si X tiene dimensión 1, entonces d es un epimorfismo. En efecto, si $P \in X$, un elemento de $\Lambda_{X,P}^1$ está determinado por una forma diferencial ω definida en un entorno V de P, que podemos tomar arbitrariamente pequeño y, en particular, contractible. Esto hace que el grupo de cohomología de De Rham $H^1(V)$ sea nulo,[1] y, como la dimensión de V es 1, toda forma ω cumple que $d\omega = 0$, (pues $\Lambda^2(V) = 0$), por lo que existe $f \in C_X^\infty(V)$ tal que $df = \omega$. El germen de f en P es, entonces una antiimagen para el germen de ω.

Sin embargo, el homomorfismo $d_X : C_X^\infty(X) \longrightarrow \Lambda_X^1(X)$ será suprayectivo si y sólo si $H^1(X) = 0$, lo cual no tiene por qué ser cierto. (No lo es, por ejemplo, si X es la circunferencia S^1.) ■

Nos encontramos así por primera vez con un fenómeno que está en el núcleo de la teoría de haces. Es el que hace que ésta no sea trivial y es la principal razón de ser del álgebra homológica sobre haces, que desarrollaremos más adelante.

Todo prehaz puede "completarse" hasta un haz:

Teorema 1.9 *Si $\mathcal{F}$ es un prehaz sobre un espacio topológico X, existe un haz $\mathcal{F}^+$ sobre X y un homomorfismo $i : \mathcal{F} \longrightarrow \mathcal{F}^+$ de modo que si $\mathcal{G}$ es un haz en X y $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ es un homomorfismo de haces, entonces existe un único homomorfismo $\alpha^+ : \mathcal{F}^+ \longrightarrow \mathcal{G}$ tal que $\alpha = i \circ \alpha^+$. Además, los homomorfismos $i_P : \mathcal{F}_P \longrightarrow \mathcal{F}_P^+$ son isomorfismos.*

Demostración: Para cada abierto U en X definimos $\mathcal{F}^+(U)$ como el conjunto de todas las funciones $f : U \longrightarrow \bigoplus_{P \in U} \mathcal{F}_P$ que cumplan lo siguiente:

Para cada $P \in U$ existe un entorno abierto V de P en U y un $s \in \mathcal{F}(V)$ de modo que para todo $Q \in V$ se cumple que $f(Q) = s_Q$.

Claramente $\mathcal{F}^+(U)$ es un grupo con la suma definida puntualmente. Como restricciones tomamos las restricciones usuales de aplicaciones. Es inmediato entonces que $\mathcal{F}^+$ es un haz en X. Definimos $i_U : \mathcal{F}(U) \longrightarrow \mathcal{F}^+(U)$ mediante $i_U(s)(P) = s_P$. Claramente es un homomorfismo de prehaces.

Si $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ es un homomorfismo de prehaces, podemos definir un homomorfismo $\alpha_U^+ : \mathcal{F}^+(U) \longrightarrow \mathcal{G}(U)$ de la forma siguiente: dado $f \in \mathcal{F}^+(U)$, consideramos pares (V, s) que cumplen la definición de $\mathcal{F}^+(U)$ para f y de modo

[1] Teorema 11.4 de mi topología algebraica.

que los abiertos V cubran U. Entonces los elementos $\alpha_V(s) \in \mathcal{G}(V)$ se extienden a un elemento $\alpha_U^+(f) \in \mathcal{G}(U)$. Este elemento está caracterizado por que $\alpha_U^+(f)_P = \alpha_P(f(P))$, luego no depende del cubrimiento elegido para calcularlo. Es claro entonces que α_U^+ es un homomorfismo de haces.

Si $s \in \mathcal{F}(U)$, entonces $\alpha_U^+(i_U(s)) = \alpha_U(s)$ (pues podemos calcularlo a partir del par (U, s)), luego $\alpha = i \circ \alpha^+$.

Si $\alpha' : \mathcal{F}^+ \longrightarrow \mathcal{G}$ cumple también que $\alpha = i \circ \alpha'$, entonces, para cada $f \in \mathcal{F}(U)$ y cada par (V, s) según la definición de $\mathcal{F}^+(U)$, tenemos que $\alpha'_U(f)|_V = \alpha'_V(f|_V) = \alpha'_V(i_V(s)) = \alpha_V(s) = \alpha^+(i_V(s)) = \alpha^+(f|_V) = \alpha^+(f)|_V$. Así pues, $\alpha'_U(f) = \alpha_U^+(f)$.

Veamos ahora que i_P es un isomorfismo. Si $i_P([(U, s)]) = [(U, i_U(s))] = 0$, entonces existe un entorno V de P tal que $i_U(s)|_V = 0$. Así $s_P = 0$ para todo $P \in V$, luego $s|_V = 0$ y $[(U, s)] = 0$. Esto prueba que i_P es inyectiva.

Dado $[(U, f)] \in \mathcal{F}_P^+$, tomamos un entorno V de P en U según la definición de $\mathcal{F}^+(U)$, y entonces $i_P([(V, s)]) = [(U, f)]$. ■

La propiedad de $\mathcal{F}^+$ implica en particular que es único salvo isomorfismo. Así mismo, si $\mathcal{F}$ es un haz, entonces $i : \mathcal{F} \longrightarrow \mathcal{F}^+$ es un isomorfismo (por el teorema 1.7). También se sigue de la construcción que si $\mathcal{F}$ es un prehaz de anillos, álgebras, etc., entonces $\mathcal{F}^+$ también lo es.

Ejemplo Sea X un espacio topológico y sea A un grupo abeliano. Definimos el *haz constante* A_X como la compleción del prehaz constante A_X^- definido en la página 4. Analizando la demostración del teorema anterior se ve fácilmente que, para cada abierto $U \subset X$ no vacío, $A_X(U)$ está formado por las funciones $U \longrightarrow A$ que son localmente constantes. Al igual que el prehaz, cumple que $A_{X,P} \cong A$ para todo punto $P \in X$.

Ahora podemos dar un ejemplo muy simple que muestra que la suprayectividad de un homomorfismo de haces no implica la suprayectividad de los homomorfismos que lo definen:

Consideremos un espacio topológico conexo X y fijemos dos puntos cerrados distintos p_1, $p_2 \in X$. Sea A un grupo abeliano y $\mathcal{F} = A_X^{p_1} \oplus A_X^{p_2}$, donde la suma directa tiene el significado obvio: para cada abierto $U \subset X$ definimos $\mathcal{F}(U) = A_X^{p_1}(U) \oplus A_X^{p_2}(U)$, y las restricciones son los homomorfismos inducidos de forma natural sobre la suma por las restricciones de los dos haces rascacielos. Es fácil ver entonces que, para cada punto $q \in X$, se tiene que

$$\mathcal{F}_q = A_{X,q}^{p_1} \oplus A_{X,q}^{p_2} \cong \begin{cases} A & \text{si } q \in \{p_1, p_2\}, \\ 0 & \text{si } q \notin \{p_1, p_2\}. \end{cases}$$

Definimos un homomorfismo $f^- : A_X^- \longrightarrow \mathcal{F}$ mediante

$$f_U^-(a) = \begin{cases} (a, a) & \text{si } p_1, p_2 \in U, \\ (a, 0) & \text{si } p_1 \in U,\ p_2 \notin U, \\ (0, a) & \text{si } p_1 \notin U,\ p_2 \in U, \\ (0, 0) & \text{si } p_1, p_2 \notin U. \end{cases}$$

Es inmediato que los homomorfismos f_U^- conmutan con las restricciones, por lo que definen ciertamente un homomorfismo de prehaces f^-, de modo que, para cada $q \in X$, el homomorfismo $f_q^- : A_{X,q}^- \longrightarrow \mathcal{F}_q$ es la identidad en A si $q \in \{p_1, p_2\}$ y el homomorfismo nulo en caso contrario. Por el teorema anterior f^- se extiende a un homomorfismo de haces $f : A_X \longrightarrow \mathcal{F}$ para el que los homomorfismos f_q son los mismos que los homomorfismos f_q^-, luego todos son epimorfismos.

Esto significa que f es un epimorfismo de haces, mientras que el homomorfismo $f_X : A_X(X) \longrightarrow \mathcal{F}(X)$ no puede ser suprayectivo (si A es razonable, por ejemplo si es un cuerpo), porque, al ser X conexo, $A_X(X) \cong A$, mientras que $\mathcal{F}(X) \cong A \oplus A$. ■

Sea X un espacio topológico, sea $\mathcal{F}$ un haz en X y sea $\mathcal{G}$ un subhaz de $\mathcal{F}$. Entonces podemos definir un prehaz $(\mathcal{F}/\mathcal{G})^-(U) = \mathcal{F}(U)/\mathcal{G}(U)$ tomando como restricciones los homomorfismos inducidos por las restricciones de $\mathcal{F}$. En general no es trata de un haz, pero definimos $\mathcal{F}/\mathcal{G} = (\mathcal{F}/\mathcal{G})^{-+}$. Es fácil ver que, para todo $P \in U$, se cumple que $(\mathcal{F}/\mathcal{G})_P \cong (\mathcal{F}/\mathcal{G})_P^- \cong \mathcal{F}_P/\mathcal{G}_P$.

La proyección canónica $\pi^- : \mathcal{F} \longrightarrow (\mathcal{F}/\mathcal{G})^-$ dada por $\pi_U^-(f) = [f]$ se extiende a un epimorfismo $\pi : \mathcal{F} \longrightarrow \mathcal{F}/\mathcal{G}$ tal que, si $P \in X$, entonces $\pi_P : \mathcal{F}_P \longrightarrow \mathcal{F}_P/\mathcal{G}_P$ es la proyección canónica.

El teorema 1.5 implica ahora que $\mathcal{F}/\mathcal{G} = 0$ si y sólo si $\mathcal{G} = \mathcal{F}$.

Si $f : \mathcal{F} \longrightarrow \mathcal{G}$ es un homomorfismo de haces sobre un espacio topológico X, podemos definir su núcleo $\mathrm{N}(f)$ como el subhaz de $\mathcal{F}$ dado por $(\mathrm{N}\, f)(U) = \mathrm{N}\, f_U$. Es claro que $(\mathrm{N}\, f)_P = \mathrm{N}\, f_P$.

En cambio, el subprehaz $(\mathrm{Im}\, f)^-$ de $\mathcal{G}$ dado por $(\mathrm{Im}\, f)^-(U) = \mathrm{Im}\, f_U$ no es en general un haz. Definimos $\mathrm{Im}\, f = (\mathrm{Im}\, f)^{-+}$. Observemos que la inclusión $j : (\mathrm{Im}\, f)^- \longrightarrow \mathcal{G}$ se extiende a un homomorfismo $j^+ : \mathrm{Im}\, f \longrightarrow \mathcal{G}$ de modo que $j = i \circ j^+$ (donde $i : (\mathrm{Im}\, f)^- \longrightarrow \mathrm{Im}\, f$). En particular, si $P \in X$ tenemos que $j_P = i_P \circ j_P^+$, de donde se sigue que j_P^+ es inyectivo. Por lo tanto los homomorfismos $j_U^+ : (\mathrm{Im}\, f)(U) \longrightarrow \mathcal{G}(U)$ son inyectivos. Esto nos permite considerar a $\mathrm{Im}\, f$ como un subhaz de $\mathcal{G}$. Esta identificación nos lleva a su vez a identificar $\mathrm{Im}\, f_P = (\mathrm{Im}\, f)_P^-$ con $(\mathrm{Im}\, f)_P$. El teorema 1.5 nos determina entonces a $\mathrm{Im}\, f$ como subhaz de $\mathcal{G}$: si $U \subset X$ es un abierto, el grupo $(\mathrm{Im}\, f)(U)$ está formado por los $s \in \mathcal{G}(U)$ tales que $s_P \in \mathrm{Im}\, f_P$ para cada $P \in U$, es decir, por los elementos de $\mathcal{G}(U)$ que localmente tienen antiimagen por f.

Ejemplos Cualquiera de los ejemplos que hemos dado de homomorfismos de haces $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ que son suprayectivos sin que todos los homomorfismos ϕ_U lo sean, sirve como ejemplo de que $(\mathrm{Im}\, \phi)^-$ no es necesariamente un haz. En efecto, si $g \in \mathcal{G}(U)$ no está en la imagen de ϕ_U, entonces podemos cubrir U con abiertos V tales que $g|_V \in (\mathrm{Im}\, \phi)^-(V)$, y estos elementos son consistentes entre sí, pero no se extienden a ningún elemento de $(\mathrm{Im}\, \phi)^-(U)$. ■

Es evidente que un homomorfismo de haces $f : \mathcal{F} \longrightarrow \mathcal{G}$ es inyectivo si y sólo si $\mathrm{N}\, f$ es el subhaz nulo de $\mathcal{F}$, y es suprayectivo si y sólo si $\mathrm{Im}\, f = \mathcal{G}$. Definimos el *conúcleo* de f como $\mathrm{CN}(f) = \mathcal{G}/\operatorname{Im} f$. Así, f es inyectivo si y sólo si $\mathrm{N}\, f = 0$ y es suprayectivo si y sólo si $\mathrm{CN}(f) = 0$.

Las propiedades elementales sobre grupos abelianos tienen su análogo para haces sobre un espacio topológico, y las demostraciones son elementales, aunque requieren cierta familiaridad con las técnicas de trabajo con haces (manejo de compleciones y localizaciones). Veamos algunos ejemplos como ilustración:

En primer lugar demostramos el teorema de isomorfía: un homomorfismo $f : \mathcal{F} \longrightarrow \mathcal{G}$ puede descomponerse como

$$\mathcal{F} \xrightarrow{\pi} \mathcal{F}/\mathrm{N}\, f \xrightarrow{\bar{f}} \operatorname{Im} f \xrightarrow{i} \mathcal{G},$$

donde el primer homomorfismo es suprayectivo (la proyección canónica), el segundo es un isomorfismo y el tercero un monomorfismo (la inclusión).

En efecto, para cada abierto $U \subset X$ definimos de forma natural el isomorfismo $\bar{f}_U^- : \mathcal{F}(U)/\mathrm{N}\, f_U \longrightarrow \operatorname{Im} f_U$. Estos isomorfismos definen un isomorfismo $\bar{f}^- : (\mathcal{F}/\mathrm{N}\, f)^- \longrightarrow (\operatorname{Im} f)^-$. Para cada $P \in X$, se comprueba inmediatamente que $\bar{f}_P^- : (\mathcal{F}/\mathrm{N}\, f)_P^- \longrightarrow \operatorname{Im} f_P$ se corresponde con el isomorfismo natural $\mathcal{F}_P/\mathrm{N}\, f_P \longrightarrow \operatorname{Im} f_P$. La composición

$$(\mathcal{F}/\mathrm{N}\, f)^- \longrightarrow (\operatorname{Im} f)^- \longrightarrow \operatorname{Im} f$$

se extiende a un homomorfismo de haces $\bar{f} : \mathcal{F}/\mathrm{N}\, f \longrightarrow \operatorname{Im} f$ tal que, para cada $P \in X$, el homomorfismo $\bar{f}_P$ se corresponde con el isomorfismo natural $\bar{f}_P : \mathcal{F}_P/\mathrm{N}\, f_P \longrightarrow \operatorname{Im} f_P$. Por lo tanto $\bar{f}$ es un isomorfismo y, puesto que $\pi_P \circ \bar{f}_P \circ i_P = f_P$, se cumple que $\pi \circ \bar{f} \circ i = f$. ■

Observemos ahora que si $\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$ son dos homomorfismos de haces, entonces $f \circ g = 0$ si y sólo si $\operatorname{Im} f$ es un subhaz de $\mathrm{N}\, g$. En efecto, $f \circ g = 0$ equivale a que $f_P \circ g_P = 0$ para todo $P \in X$, lo que equivale a que $\operatorname{Im} f_P \subset \mathrm{N}\, g_P$ y esto a su vez equivale a que $\operatorname{Im} f \subset \mathrm{N}\, g$ (por 1.5).

Diremos que la sucesión anterior es *exacta* en $\mathcal{G}$ si cumple que $\operatorname{Im} f = \mathrm{N}\, \mathcal{G}$, lo cual claramente equivale a que todas las sucesiones $\mathcal{F}_P \longrightarrow \mathcal{G}_P \longrightarrow \mathcal{H}_P$ sean exactas.

Ejemplo Ahora podemos ver ejemplos en los que los prehaces $(\mathcal{F}/\mathcal{G})^-$ no son haces. Si $\phi : \mathcal{F} \longrightarrow \mathcal{G}$ es un epimorfismo de haces, entonces

$$(\mathcal{F}/\mathrm{N}\,\phi)^-(X) = \mathcal{F}(X)/\mathrm{N}\,\phi_X \cong \operatorname{Im} \phi_X,$$

mientras que $(\mathcal{F}/\mathrm{N}\,\phi)(X) \cong \mathcal{G}(X)$, y estos isomorfismos forman el diagrama conmutativo

$$\begin{tikzcd}
(\mathcal{F}/\mathrm{N}\,\phi)(X) \arrow[r] & \mathcal{G}(X) \\
(\mathcal{F}/\mathrm{N}\,\phi)^-(X) \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Si $(\mathcal{F}/\operatorname{N}\phi)^-$ es un haz, la flecha vertical es un isomorfismo, luego los otros dos isomorfismos tendrían la misma imagen, $\operatorname{Im}\phi_X = \mathcal{G}(X)$. Así pues, si ϕ_X no es suprayectivo, entonces $(\mathcal{F}/\operatorname{N}\phi)^-$ no es un haz. ■

Hasta aquí hemos considerado haces sobre un mismo espacio topológico X. Ahora veamos que podemos transportar haces a través de aplicaciones continuas:

Definición 1.10 Sea $f : X \longrightarrow Y$ una aplicación continua entre espacios topológicos y $\mathcal{F}$ un haz sobre X. Definimos $f_*(\mathcal{F})$ como el haz sobre Y determinado por los grupos $f_*(\mathcal{F})(U) = \mathcal{F}(f^{-1}[U])$ y las restricciones $\rho_U^V = \rho_{f^{-1}[U]}^{f^{-1}[V]}$.

Para cada $P \in X$ tenemos un homomorfismo natural $f_*(\mathcal{F})_{f(P)} \longrightarrow \mathcal{F}_P$ dado por $[(U,s)] \mapsto [(f^{-1}[U],s)]$, pero en general no es un isomorfismo. Una condición suficiente para que lo sea es que las antiimágenes por f de los abiertos de Y sean una base de X, lo cual sucede, por ejemplo, si f es una inmersión, es decir, un homeomorfismo en un subespacio de Y.

En efecto, en tal caso, si $[(f^{-1}[U],s)] = 0$ existe un abierto $P \in V \subset f^{-1}[U]$ tal que $s|_V = 0$. Podemos tomar un abierto $U' \subset U$ tal que $P \in f^{-1}[U'] \subset V$, con lo que $[(U,s)] = [(U', s|_{U'})] = 0$. Esto prueba la inyectividad.

Por otra parte, dado $[(U,s)] \in \mathcal{F}_P$, podemos tomar un abierto V en Y tal que $P \in f^{-1}[V] \subset U$, con lo que $[(V, s|_{f^{-1}[V]})] \in f_*(\mathcal{F})_{f(P)}$ tiene por imagen a $[(f^{-1}[V], s|_{f^{-1}[V]})] = [(U,s)]$. Esto prueba la suprayectividad. ■

Si $f : X \longrightarrow Y$ es un homeomorfismo entre X y un cerrado de Y todavía podemos decir más:

$$f_*(\mathcal{F})_Q = \begin{cases} 0 & \text{si } Q \notin f[X], \\ \mathcal{F}_P & \text{si } Q = f(P). \end{cases}$$

En efecto, si $Q \notin f[X]$ y $[(U,s)] \in f_*(\mathcal{F})_Q$, consideramos $V = U \cap (Y \setminus f[X])$, que es un entorno de Q para el cual $s|_V \in f_*(\mathcal{F})(V) = \mathcal{F}(f^{-1}[V]) = \mathcal{F}(\varnothing) = 0$, luego $[(U,s)] = 0]$. ■

Consideremos ahora una aplicación continua $f : X \longrightarrow Y$ y sea $\mathcal{F}$ un haz sobre Y. Definimos el prehaz $f^{-1}[\mathcal{F}]^-$ en X para el que $f^{-1}[\mathcal{F}]^-(U)$ está formado por las clases de equivalencia de pares (V,s), con V abierto tal que $f[U] \subset V \subset Y$ y $s \in \mathcal{F}(V)$, respecto a la relación dada por

$$(V,s) \sim (V',s') \Leftrightarrow \text{existe un abierto } f[U] \subset W \subset V \cap V' \text{ tal que } s|_W = s'|_W.$$

La suma se define restringiendo los representantes a un abierto común y sumando. Las restricciones vienen dadas por $[(V,s)] \mapsto [(V,s)]$.

En general $f^{-1}[\mathcal{F}]^-$ no es un haz, por lo que definimos $f^{-1}[\mathcal{F}] = f^{-1}[\mathcal{F}]^{-+}$. Observemos que tenemos un isomorfismo $f^{-1}[\mathcal{F}]^-_P \longrightarrow \mathcal{F}_{f(P)}$ determinado por $[(U,[(V,s)])] \mapsto [(V,s)]$, luego también $f^{-1}[\mathcal{F}]_P \cong \mathcal{F}_{f(P)}$.

También conviene observar que si U es abierto en X e $i : U \longrightarrow X$ es la inclusión entonces $i^{-1}[\mathcal{F}] = \mathcal{F}|_U$. (En este caso $f^{-1}[\mathcal{F}]^-$ es ya un haz.)

Teorema 1.11 *Sea $f : X \longrightarrow Y$ un homeomorfismo de un espacio topológico X en un subespacio de un espacio topológico Y y sea $\mathcal{F}$ un haz en X. Entonces $\mathcal{F} \cong f^{-1}[f_*(\mathcal{F})]$.*

DEMOSTRACIÓN: Sea $\alpha : \mathcal{F} \longrightarrow f^{-1}[f_*(\mathcal{F})]^-$ definido como sigue: para cada abierto $U \subset X$ y cada $s \in \mathcal{F}(U)$, existe un abierto $V \subset Y$ tal que $U = f^{-1}[V]$, luego $f_*(\mathcal{F})(V) = \mathcal{F}(U)$. Definimos $\alpha_U(s) = [(V, s)]$. Se comprueba inmediatamente que $\alpha_U(s)$ no depende de la elección de V, así como que α es un homomorfismo de prehaces, que se extiende a un homomorfismo de haces $\alpha^+ : \mathcal{F} \longrightarrow f^{-1}[f_*(\mathcal{F})]$. Para cada punto $P \in X$ es fácil ver que el homomorfismo $\alpha^+_P : \mathcal{F}_P \longrightarrow f_*(\mathcal{F})_{f(P)} \cong \mathcal{F}_P$ es la identidad en $\mathcal{F}_P$, luego α es un isomorfismo.

■

1.2 Espacios anillados

En esta sección estudiamos los haces de anillos sobre un espacio topológico, si bien conviene asociarlos al espacio como una estructura:

Definición 1.12 Un *espacio anillado* es un par $(X, \mathcal{O}_X)$, donde X es un espacio topológico y $\mathcal{O}_X$ es un haz de anillos sobre X. Diremos que $(X, \mathcal{O}_X)$ es un *espacio anillado local* si además, para todo punto $P \in X$, el anillo $\mathcal{O}_{X,P}$ es *local,* es decir, tiene un único ideal maximal, que representaremos por $\mathfrak{m}_P$. En tal caso definimos también el cuerpo de restos $k(P) = \mathcal{O}_{X,P}/\mathfrak{m}_P$. Habitualmente escribiremos X en lugar de $(X, \mathcal{O}_X)$. Si los anillos de X son —de hecho— A-álgebras, para un cierto anillo A, diremos que el espacio anillado X está *definido sobre* A.

Si $(X, \mathcal{O}_X)$ es un espacio anillado (local) y U es un abierto en X, también lo es $(U, \mathcal{O}_X|_U)$. En lo sucesivo consideraremos a los abiertos de los espacios anillados (locales) como espacios anillados (locales) con esta estructura.

Ejemplo Todo espacio topológico X tiene una estructura de espacio anillado definido sobre $\mathbb{K}$ si lo dotamos de su haz C_X de funciones continuas con valores en $\mathbb{K}$. Se trata de un espacio anillado local, pues para cada punto $P \in X$, el anillo $C_{X,P}$ tiene un único ideal maximal, que es

$$\mathfrak{m}_P = \{[(U, f)] \mid f(P) = 0\}.$$

Es evidente que $\mathfrak{m}_P$ es un ideal propio de $C_{X,P}$ y, si $\alpha = [(U, f)] \in C_{X,P} \setminus \mathfrak{m}_P$, entonces P tiene un entorno abierto $V \subset U$ tal que $f|_V$ no se anula en ningún punto, luego podemos considerar $\beta = [(V, (f|_V)^{-1})] \in C_{X,P}$, que cumple que $\alpha\beta = 1$. Así pues, $C_{X,P} \setminus \mathfrak{m}_P$ es el conjunto de las unidades de $C_{X,P}$, luego todos los ideales de $C_{X,P}$ están contenidos en $\mathfrak{m}_P$.

El mismo razonamiento se aplica a una variedad diferencial con su haz de funciones C^∞ o a una variedad compleja con su haz de funciones holomorfas. Todos ellos son ejemplos de espacios anillados locales. ■

Definición 1.13 Un *homomorfismo de espacios anillados* $f : X \longrightarrow Y$ es un par $(f_0, f^\#)$ formado por una aplicación continua $f_0 : X \longrightarrow Y$ y un homomorfismo de haces $f^\# : \mathcal{O}_Y \longrightarrow f_*(\mathcal{O}_X)$. Si los espacios anillados son locales, diremos que f es un *homomorfismo de espacios anillados locales* si, además, para todo $P \in X$, el homomorfismo natural $f^\#_P : \mathcal{O}_{Y,f_0(P)} \longrightarrow \mathcal{O}_{X,P}$ es un *homomorfismo de anillos locales,* es decir, si cumple que $(f^\#_P)^{-1}[\mathfrak{m}_P] = \mathfrak{m}_{f_0(P)}$ (o, equivalentemente, que $f^\#_P[\mathfrak{m}_{f_0(P)}] \subset \mathfrak{m}_P$.) Si los espacios anillados están definidos sobre un anillo A, diremos que f *está definido sobre* A si $f^\#$ es un homomorfismo de haces de A-álgebras.

En definitiva, un homomorfismo de espacios anillados determina homomorfismos $f^\#_U : \mathcal{O}_Y(U) \longrightarrow \mathcal{O}_X(f_0^{-1}[U])$ de modo que los diagramas siguientes conmutan:

$$\begin{tikzcd}
\mathcal{O}_Y(V) \arrow[r, "f^\#_V"] \arrow[d, "\rho^V_U"'] & \mathcal{O}_X(f_0^{-1}[V]) \arrow[d, "\rho^{f_0^{-1}[V]}_{f_0^{-1}[U]}"] \\
\mathcal{O}_Y(U) \arrow[r, "f^\#_U"'] & \mathcal{O}_X(f_0^{-1}[U])
\end{tikzcd}$$

Es fácil definir de forma natural la composición de homomorfismos de espacios anillados, así como el homomorfismo identidad. Un *isomorfismo* f es un homomorfismo con inverso. Esto equivale a que f_0 sea un homeomorfismo y las aplicaciones $f^\#_U$ sean isomorfismos. (En el caso de espacios anillados locales, esto ya implica que los homomorfismos $f^\#_P$ son isomorfismos y, por consiguiente, que hacen corresponder los ideales maximales, tal y como exige la definición de homomorfismo de espacios anillados locales.) Por el teorema 1.7, esto equivale a su vez a que f_0 sea un homeomorfismo y los homomorfismos $f^\#_P$ sean isomorfismos.

Cuando no haya posibilidad de confusión escribiremos f en lugar de f_0. Así mismo, si hablamos de un homomorfismo entre dos espacios anillados locales, sobrentenderemos que el homomorfismo es un homomorfismo de espacios anillados locales y, si hablamos de un homomorfismo entre dos espacios anillados definidos sobre un anillo A, sobrentenderemos que está definido sobre A.

Ejemplo Sea $\phi : X \longrightarrow Y$ una aplicación continua entre dos espacios topológicos, consideramos como espacios anillados con sus haces de funciones continuas en $\mathbb{K}$. Entonces ϕ define un homomorfismo de espacios anillados en el que ella misma es ϕ_0 y, para cada abierto $U \subset Y$, el homomorfismo $\phi^\#_U : C_Y(U) \longrightarrow C_X(\phi^{-1}[U])$ es el dado por $\phi^\#_U(f) = \phi|_{\phi^{-1}[U]} \circ f$.

Observemos que ϕ es un homomorfismo de espacios anillados locales, lo cual significa únicamente que si f se anula en un punto $\phi(P)$, entonces $\phi^\#_U(f)$ se anula en P. También es obvio que ϕ está definido sobre $\mathbb{K}$ (es decir, que transforma las funciones constantes en funciones constantes).

Veamos ahora que si $\phi : (X, C_X) \longrightarrow (Y, C_Y)$ es cualquier homomorfismo de espacios anillados locales definido sobre $\mathbb{K}$, entonces $\phi^\#$ es necesariamente el homomorfismo definido por composición con ϕ_0.

En efecto, tomemos un abierto $U \subset Y$ y una función $f \in C_Y(U)$. Vamos a probar que $\phi^\#_U(f) = \phi_0|_{\phi_0^{-1}[U]} \circ f$. Tomemos un punto $P \in \phi^{-1}[U]$ y sea

$$\alpha = (\phi_0|_{\phi_0^{-1}[U]} \circ f)(P) = f(\phi_0(P)) \in \mathbb{K}.$$

Entonces $(f - \alpha)(\phi_0(P)) = 0$, luego $f - \alpha \in \mathfrak{m}_{\phi_0(P)}$, luego $\phi^\#_U(f - \alpha) \in \mathfrak{m}_P$, luego $\phi^\#_U(f)(P) = \alpha$. Esto prueba la igualdad.

Así pues, las aplicaciones continuas $\phi : X \longrightarrow Y$ entre dos espacios topológicos se corresponden biunívocamente con los homomorfismos de espacios anillados $\phi : (X, C_X) \longrightarrow (Y, C_Y)$. ■

Ejemplo Veamos ahora que si X e Y son dos variedades diferenciales existe una biyección entre las aplicaciones $\phi : X \longrightarrow Y$ de clase C^∞ y los homomorfismos de espacios anillados $\phi : (X, C^\infty_X) \longrightarrow (Y, C^\infty_Y)$.

El razonamiento es el mismo empleado en el ejemplo anterior, salvo que ahora hemos de probar que si $\phi = (\phi_0, \phi^\#)$ es un homomorfismo, entonces ϕ_0 no sólo es una aplicación continua, sino que es, de hecho, de clase C^∞. En cualquier caso, tenemos que $\phi^\#$ es necesariamente la composición con ϕ_0, por lo que si $U \subset Y$ es un abierto y $f \in C^\infty(U)$, entonces $\phi_0|_{\phi_0^{-1}[U]} \circ f \in C^\infty_X(\phi_0^{-1}[U])$. Basta tomar como U el dominio de una carta de Y y como f la propia carta.

Igualmente se prueba que las funciones holomorfas entre variedades complejas se corresponden con los homomorfismos entre las estructuras de espacio anillado definidas por sus haces de funciones holomorfas. ■

Ejercicio: Demostrar que podemos definir una variedad diferencial como un espacio anillado X tal que todo punto tiene un entorno isomorfo —como espacio anillado— a un espacio (U, C^∞_U), donde U es un abierto en $\mathbb{R}^n$.

Definición 1.14 Sea X un espacio anillado y U un abierto en X. Definimos la *inclusión* $i : U \longrightarrow X$ como el homomorfismo de espacios anillados determinado por la inclusión $i_0 : U \longrightarrow X$ (como espacios topológicos) y el homomorfismo $i^\# : \mathcal{O}_X \longrightarrow i_*(\mathcal{O}_U)$ para el que $i^\#_V : \mathcal{O}(V) \longrightarrow \mathcal{O}(U \cap V)$ es $i^\#_V = \rho^V_{U\cap V}$. Es claro que si $P \in U$ entonces $i^\#_P$ es la identidad en $\mathcal{O}_P$, luego i es ciertamente un homomorfismo de espacios anillados.

Si $f : X \longrightarrow Y$ es un homomorfismo de espacios anillados, definimos su *restricción* a U como $f|_U = i_U \circ f : U \longrightarrow Y$.

Definición 1.15 Si $(X, \mathcal{O}_X)$ es un espacio anillado, un $\mathcal{O}_X$-*módulo* es un haz $\mathcal{M}$ en X tal que, para cada abierto U de X, el grupo $\mathcal{M}(U)$ tiene una estructura adicional de $\mathcal{O}_X(U)$-módulo compatible con las restricciones, en el sentido de que, para cada $a \in \mathcal{O}_X(U)$, cada $m \in \mathcal{M}(U)$ y cada abierto $V \subset U$, se cumple que $(am)|_V = (a|_V)(m|_V)$.

Es claro entonces que para cada $P \in X$ tenemos una estructura natural de $\mathcal{O}_{X,P}$-módulo en $\mathcal{M}_P$.

Un *homomorfismo* de $\mathcal{O}_X$-módulos $f : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo de haces tal que para cada abierto $U \subset X$ se cumple que $f_U : \mathcal{M}(U) \longrightarrow \mathcal{N}(U)$ es un homomorfismo de $\mathcal{O}_X(U)$-módulos.

Aparentemente, los $\mathcal{O}_X$-módulos tienen una estructura algebraica más rica que los haces cualesquiera, pero esto es más aparente que real:

Teorema 1.16 *Sea X un espacio topológico, sea A un anillo y sea A_X el haz constante asociado. Entonces los haces en X definidos sobre A se corresponden con los A_X-módulos. En particular, todos los haces en X son $\mathbb{Z}_X$-módulos.*

Demostración: Si $U \subset X$ es un abierto no vacío, los elementos de $A_X(U)$ son las funciones $U \longrightarrow A$ localmente constantes. En particular podemos considerar que $A \subset A_X(U)$ identificando los elementos de A con las funciones constantes. Esto hace que todo A_X-módulo sea en particular un haz en X definido sobre A. Recíprocamente, si $\mathcal{M}$ es un haz en X definido sobre A y $U \subset X$ es un abierto no vacío, podemos definir como sigue un producto $A_X(U) \times \mathcal{M}(U) \longrightarrow \mathcal{M}(U)$. Tomamos $a \in A_X(U)$ y $m \in \mathcal{M}(U)$, tomamos un cubrimiento abierto $\{U_i\}_i$ de U de modo que $a|_{U_i}$ sea constante, lo que nos permite definir $a|_{U_i} m|_{U_i} \in \mathcal{M}(U_i)$. Es claro que estos elementos se extienden a un único $am \in \mathcal{M}(U)$, de modo que $\mathcal{M}(U)$ es un $A_X(U)$-módulo con este producto.

Puesto que un grupo abeliano es lo mismo que un $\mathbb{Z}$-módulo, todo haz en X está definido sobre $\mathbb{Z}$, luego puede verse como $X_{\mathbb{Z}}$-módulo. ■

Se define de forma natural la *restricción* de un $\mathcal{O}_X$-módulo a un abierto de X y la noción de *submódulo* de un $\mathcal{O}_X$-módulo.

Es fácil ver que la compleción de un prehaz de módulos sobre $\mathcal{O}_X$ (esto es, de un prehaz que cumpla la definición precedente salvo por el hecho de que no es necesariamente un haz) es un $\mathcal{O}_X$-módulo. En particular, si $\mathcal{N}$ es un $\mathcal{O}_X$-submódulo de un $\mathcal{O}_X$-módulo $\mathcal{M}$, el cociente $\mathcal{M}/\mathcal{N}$ tiene estructura natural de $\mathcal{O}_X$-módulo. Así mismo, el núcleo y la imagen de un homomorfismo de $\mathcal{O}_X$-módulos son también $\mathcal{O}_X$-módulos.

Se definen de forma natural el producto y la suma directa de una familia arbitraria de $\mathcal{O}_X$-módulos.

Si $\mathcal{M}$ y $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, los productos $\mathcal{M}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{N}(U)$, con las restricciones obvias, forman un prehaz $(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^-$, aunque no necesariamente un haz. Definimos el producto tensorial $\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}$ como la compleción de dicho prehaz. Para cada $P \in X$ se cumple que

$$(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})_P \cong \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{N}_P.$$

En efecto: para cada $P \in X$ y cada abierto $P \in U \subset X$, los homomorfismos $\mathcal{M}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{N}(U) \longrightarrow \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{N}_P$ dado por $m \otimes n \mapsto m_P \otimes n_P$ inducen un homomorfismo $(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^-_P \longrightarrow \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{N}_P$, cuyo inverso se define de forma similar. ■

Dos homomorfismos $f : M \longrightarrow \mathcal{M}'$ y $g : \mathcal{N} \longrightarrow \mathcal{N}'$, definen de forma natural un homomorfismo de prehaces $(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^- \longrightarrow (\mathcal{M}' \otimes_{\mathcal{O}_X} \mathcal{N}')^-$ que, compuesto con $(\mathcal{M}' \otimes_{\mathcal{O}_X} \mathcal{N}')^- \longrightarrow \mathcal{M}' \otimes_{\mathcal{O}_X} \mathcal{N}'$, se extiende a un homomorfismo de haces

$$f \otimes g : \mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N} \longrightarrow \mathcal{M}' \otimes_{\mathcal{O}_X} \mathcal{N}'.$$

Se prueba fácilmente que $(f \otimes g)_P = f_P \otimes g_P$ para cada $P \in X$.

Veamos que $(\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P} \cong (\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{P}) \oplus (\mathcal{N} \otimes_{\mathcal{O}_X} \mathcal{P})$. En efecto, es fácil definir homomorfismos de prehaces

$$(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{P})^- \longrightarrow ((\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P})^-, \quad (\mathcal{N} \otimes_{\mathcal{O}_X} \mathcal{P})^- \longrightarrow ((\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P})^-,$$

que se extienden a homomorfismos de haces

$$\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{P} \longrightarrow (\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P}, \quad \mathcal{N} \otimes_{\mathcal{O}_X} \mathcal{P} \longrightarrow (\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P},$$

los cuales a su vez determinan un homomorfismo

$$(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{P}) \oplus (\mathcal{N} \otimes_{\mathcal{O}_X} \mathcal{P}) \longrightarrow (\mathcal{M} \oplus \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{P},$$

que localizado a cada $P \in X$ es el isomorfismo natural

$$(\mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{P}_P) \oplus (\mathcal{N}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{P}_P) \longrightarrow (\mathcal{M}_P \oplus \mathcal{N}_P) \otimes_{\mathcal{O}_{X,P}} \mathcal{P}_P.$$

■

1.3 Categorías y funtores

Aunque la noción de categoría no va a ser esencial en la teoría que vamos a desarrollar, no está de más presentar la definición para situar debidamente nuestro marco de trabajo:

Definición 1.17 Una *categoría* $\mathcal{C}$ está determinada por:

a) Una clase, a cuyos elementos llamaremos *objetos* de $\mathcal{C}$,

b) Una función que a cada par de objetos X, Y de $\mathcal{C}$ les asigna un conjunto $\mathrm{Hom}(X, Y)$, a cuyos elementos llamaremos *morfismos* (en $\mathcal{C}$) de X en Y. Escribiremos $f : X \longrightarrow Y$ para indicar que $f \in \mathrm{Hom}(X, Y)$.

c) Una función que a cada par de morfismos $f \in \mathrm{Hom}(X, Y)$, $g \in \mathrm{Hom}(Y, Z)$ les asigna un morfismo $f \circ g \in \mathrm{Hom}(X, Z)$ de modo que se cumplan las propiedades siguientes:

1. Asociatividad: $(f \circ g) \circ h = f \circ (g \circ h)$, para todos los morfismos f, g, h para los que la composición tenga sentido.
2. Para cada objeto X, existe un morfismo $1_X \in \mathrm{Hom}(X, X)$ de manera que $1_X \circ f = f$ para todo $f \in \mathrm{Hom}(X, Y)$ y $g \circ 1_X = g$ para todo $g \in \mathrm{Hom}(Y, X)$.

Si X es un espacio anillado, representaremos por $\mathrm{Mod}(X)$ la categoría de los $\mathcal{O}_X$-módulos con los homomorfismos de $\mathcal{O}_X$-módulos y la composición usual de homomorfismos. Es obvio que $\mathrm{Mod}(X)$ cumple la definición de categoría.

Si $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, es claro que el conjunto $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$ de todos los homomorfismos $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ tiene una estructura natural de $\mathcal{O}_X(X)$-módulo con las operaciones dadas por

$$(\phi + \psi)_U = \phi_U + \psi_U, \quad (a\phi)_U = a|_U \phi_U, \quad \text{para cada abierto } U \subset X.$$

Observemos que si A es un anillo arbitrario, podemos considerar el espacio topológico $P = \{0\}$ considerado como espacio anillado con el haz constante A_P, que obviamente consta únicamente de los anillos $A_P(\varnothing) = 0$ y $A_P(P) = A$, con las restricciones obvias. Es claro entonces que la aplicación que a cada A_P-módulo $\mathcal{M}$ le asigna el A-módulo $\mathcal{M}(P)$ es biyectiva, como también lo es la aplicación que a cada homomorfismo $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ de A_P-módulos le asigna el homomorfismo de A-módulos $\phi_P : \mathcal{M}(P) \longrightarrow \mathcal{N}(P)$, de modo que todas las nociones definidas para A_P-módulos se corresponden con sus análogas para A-módulos (cocientes, núcleos, imágenes, sumas directas, etc.).

Esto significa que podemos identificar la categoría $\mathrm{Mod}(A_P)$ de los A_P-módulos con la categoría $\mathrm{Mod}(A)$ de los A-módulos, de modo que todo lo que digamos para módulos sobre un espacio anillado será válido en particular para módulos sobre un anillo.

Definición 1.18 Un *funtor covariante* $F : \mathcal{C} \longrightarrow \mathcal{C}'$ entre dos categorías es una aplicación que a cada objeto X de $\mathcal{C}$ le asigna un objeto $F(X)$ de $\mathcal{C}'$ y a cada morfismo $f : X \longrightarrow Y$ un morfismo $F(f) : F(X) \longrightarrow F(Y)$ de modo que se cumplan las propiedades siguientes:

a) $F(1_X) = 1_{F(X)}$.

b) $F(f \circ g) = F(f) \circ F(g)$ (siempre que la composición tiene sentido).

Un *funtor contravariante* se define del mismo modo, salvo que a cada morfismo $f : X \longrightarrow Y$ le hace corresponder un morfismo $F(f) : F(Y) \longrightarrow F(X)$ y la propiedad b) hay que modificarla de forma obvia.

Ejemplos Si X es un espacio anillado, cada $\mathcal{O}_X$-módulo $\mathcal{M}$ define un funtor covariante

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, -) : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X)),$$

que a cada homomorfismo $\phi : \mathcal{N} \longrightarrow \mathcal{N}'$ le hace corresponder el homomorfismo

$$\bar{\phi} : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}')$$

dado por la composición con ϕ.

Similarmente, cada $\mathcal{O}_X$-módulo $\mathcal{N}$ define un funtor contravariante

$$\mathrm{Hom}_{\mathcal{O}_X}(-, \mathcal{N}) : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X))$$

que a cada homomorfismo $\phi : \mathcal{M} \longrightarrow \mathcal{M}'$ le asigna el homomorfismo

$$\bar{\phi} : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}', \mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$$

dado también por la composición con ϕ. ■

Si X e Y son espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es un funtor, de la propia definición se sigue que F transforma isomorfismos en isomorfismos. Lo que ya no es cierto en general es que tenga que transformar monomorfismos en monomorfismos y epimorfismos en epimorfismos. Lo mejor que le puede pasar a un funtor es que sea exacto:

Definición 1.19 Sean X e Y dos espacios anillados. Un funtor covariante $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es *exacto* si para toda sucesión exacta corta de $\mathcal{O}_X$-módulos

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0,$$

también es exacta la sucesión

$$0 \longrightarrow F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P} \longrightarrow 0.$$

Análogamente se define la exactitud de un funtor contravariante, sin más que invertir el sentido en la sucesión transformada.

En realidad los funtores exactos conservan la exactitud de cualquier sucesión:

Teorema 1.20 *Sean X e Y dos espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ un funtor covariante exacto. Entonces, para toda sucesión exacta de $\mathcal{O}_X$-módulos*

$$\mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P},$$

también es exacta la sucesión $F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P}$. (Y para funtores contravariantes se cumple el resultado análogo.)

Demostración: Tenemos el siguiente diagrama conmutativo con filas y columnas exactas:

$$\begin{tikzcd}
 & 0 & & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{M}/\,\mathrm{N}\,\alpha \arrow[u] \arrow[r] & \mathcal{N} \arrow[r] \arrow[dr, "\beta"] & \mathrm{Im}\,\beta \arrow[r] \arrow[d] & 0 \\
 & \mathcal{M} \arrow[u] \arrow[ur, "\alpha"] & & \mathcal{P} &
\end{tikzcd}$$

Al aplicar F obtenemos un diagrama con las mismas características (notemos que todo monomorfismo y todo epimorfismo se extiende a una sucesión exacta corta, luego los funtores exactos conservar monomorfismos y epimorfismos). El diagrama implica que la imagen de $F\alpha$ y el núcleo de $F\beta$ son los mismos que los de los homomorfismos de la sucesión exacta horizontal, lo que prueba la exactitud de la sucesión del enunciado. La prueba para funtores contravariantes es análoga. ■

En particular los funtores exactos covariantes conservan la inyectividad y la suprayectividad de los homomorfismos, mientras que los contravariantes las intercambian.

La teoría de funtores derivados que pretendemos desarrollar tiene como finalidad estudiar la no exactitud de los funtores a los que les falta poco para ser exactos:

Definición 1.21 Sean X e Y dos espacios anillados. Un funtor covariante $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es *exacto por la izquierda* si para toda sucesión exacta corta de $\mathcal{O}_X$-módulos

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0,$$

también es exacta la sucesión

$$0 \longrightarrow F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P}.$$

El funtor es *exacto por la derecha* si proporciona sucesiones exactas

$$F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P} \longrightarrow 0.$$

Si el funtor es contravariante, diremos que es exacto por la izquierda o por la derecha si da lugar, respectivamente, a sucesiones exactas

$$0 \longrightarrow F\mathcal{P} \xrightarrow{F\beta} F\mathcal{N} \xrightarrow{F\alpha} F\mathcal{M}$$

o

$$F\mathcal{P} \xrightarrow{F\beta} F\mathcal{N} \xrightarrow{F\alpha} F\mathcal{M} \longrightarrow 0.$$

Notemos que en realidad no necesitamos suponer la exactitud de la sucesión inicial en el extremo que no se va a conservar. Por ejemplo, si F es un funtor covariante exacto por la izquierda y

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P}$$

es una sucesión exacta, aplicando la exactitud de F a la sucesión

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathrm{Im}\,\beta \longrightarrow 0$$

obtenemos igualmente la exactitud que exige la definición de funtor exacto por la izquierda, y lo mismo sucede en los otros tres casos.

Ejemplos Es fácil ver que el funtor covariante $\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, -)$ es exacto por la izquierda. En efecto, si

$$0 \longrightarrow \mathcal{N}' \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{N}'' \longrightarrow 0$$

en una sucesión exacta de $\mathcal{O}_X$-módulos, entonces la sucesión

$$0 \longrightarrow \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}') \xrightarrow{\bar{\alpha}} \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \xrightarrow{\bar{\beta}} \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}'')$$

también es exacta. Veamos, por ejemplo, la exactitud en el medio. El hecho de que $\alpha\beta = 0$ implica claramente que $\bar{\alpha}\bar{\beta} = \overline{\alpha\beta} = 0$, luego $\operatorname{Im} \bar{\alpha} \subset \mathrm{N}\, \bar{\beta}$. Tomemos ahora $\phi \in \mathrm{N}(\beta)$, es decir, $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo tal que $\phi \circ \beta = 0$. Hemos de definir $\psi : \mathcal{M} \longrightarrow \mathcal{N}'$ tal que $\psi\alpha = \phi$. Para ello tomamos un abierto $U \subset X$ y vamos a definir un homomorfismo $\psi_U : \mathcal{M}(U) \longrightarrow \mathcal{N}'(U)$.

Si $s \in \mathcal{M}(U)$, entonces $\beta_U(\phi_U(s)) = 0$, luego $\phi_U(s) \in (\mathrm{N}\,\beta)(U) = (\operatorname{Im} \alpha)(U)$. Esto no significa en principio que $\phi_U(s) \in \operatorname{Im} \alpha_U$, sino únicamente que cada punto $P \in U$ tiene un entorno $V_P \subset U$ tal que $\phi_U(s)|_{V_P} \in \operatorname{Im} \alpha_{V_P}$. Pongamos que $\phi_U(s)|_{V_P} = \alpha_{V_P}(t_P)$. El hecho de que α sea inyectivo implica que los $t_P \in \mathcal{N}'(V_P)$ se extienden a un $\psi_U(s) \in \mathcal{N}'(U)$, que claramente es el único que cumple que $\alpha_U(\psi_U(s)) = \phi_U(s)$.

Es fácil ver que ψ_U es realmente un homomorfismo de módulos que cumple $\psi_U \circ \alpha_U = \phi_U$. Se comprueba así mismo que los homomorfismos ψ_U son compatibles con las restricciones, por lo que definen un $\psi \in \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}')$ tal que $\bar{\alpha}(\psi) = \phi$. Esto prueba la exactitud en el medio.

Para que el funtor fuera exacto, haría falta que, $\mathcal{M}$ cumpliera la propiedad siguiente: para todo epimorfismo de $\mathcal{O}_X$-módulos $\mathcal{N} \longrightarrow \mathcal{N}''$ y cada homomorfismo $\mathcal{M} \longrightarrow \mathcal{N}''$, existe un homomorfismo $\mathcal{M} \longrightarrow \mathcal{N}$ que hace conmutativo el diagrama siguiente:

$$\begin{tikzcd}
\mathcal{N} \arrow[r] & \mathcal{N}'' \arrow[r] & 0 \\
& \mathcal{M} \arrow[u] \arrow[ul, dashed] &
\end{tikzcd}$$

Los $\mathcal{O}_X$-módulos $\mathcal{M}$ que cumplen esta propiedad se llaman *proyectivos,* y tendremos ocasión de estudiarlos más adelante. ■

El funtor contravariante $\operatorname{Hom}_{\mathcal{O}_X}(-, \mathcal{N})$ también es exacto por la izquierda, lo que en este caso significa que si

$$0 \longrightarrow \mathcal{M}' \xrightarrow{\alpha} \mathcal{M} \xrightarrow{\beta} \mathcal{M}'' \longrightarrow 0$$

en una sucesión exacta de $\mathcal{O}_X$-módulos, entonces también es exacta la sucesión

$$0 \longrightarrow \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}'', \mathcal{N}) \xrightarrow{\bar{\beta}} \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \xrightarrow{\bar{\alpha}} \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}', \mathcal{N})$$

Veamos también el caso menos obvio: si $\phi \in \mathrm{N}\, \bar{\alpha}$, entonces $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ cumple que $\alpha\phi = 0$. Hemos de encontrar un homomorfismo $\psi : \mathcal{M}'' \longrightarrow \mathcal{N}$ tal que $\phi = \beta\psi$. Para ello fijamos un abierto $U \subset X$ y vamos a definir un homomorfismo $\psi_U : \mathcal{M}''(U) \longrightarrow \mathcal{N}(U)$. Tomamos $s \in \mathcal{M}''(U)$. La suprayectividad de β hace que cada $P \in U$ tenga un entorno $V_P \subset U$ tal que $s|_{V_P} = \beta_{V_P}(t_P)$, para cierto $t_P \in \mathcal{M}(V_P)$. Si t'_P cumple lo mismo, entonces $\beta_{V_P}(t_P - t'_P) = 0$, luego $t_P - t'_P \in \mathrm{N}\,\beta_{V_P} = (\mathrm{Im}\,\alpha)_{V_P}$. Esto significa que cada $Q \in V_P$ tiene un entorno $W_Q \subset V_P$ tal que $t_P|_{W_Q} - t'_P|_{W_Q} = \alpha_{W_Q}(u_Q)$, para cierto $u_Q \in \mathcal{M}''(W_Q)$. Entonces $\phi_{V_P}(t_P)|_{W_Q} - \phi_{V_P}(t'_P)|_{W_Q} = \phi_{W_Q}(\alpha_{W_Q}(u_Q)) = 0$, luego llegamos a que $\phi_{V_P}(t_P) = \phi_{V_P}(t'_P)$.

Esto significa que podemos definir $v_P = \phi_{V_P}(t_P) \in \mathcal{N}(V_P)$ sin que importe la elección de t_P. Esto permite comprobar que los v_P se extienden a un único $\psi_U(s) \in \mathcal{N}(U)$ con la propiedad de que $\beta_U \circ \psi_U = \phi_U$. Además, los ψ_U son compatibles con las restricciones, por lo que determinan el homomorfismo ψ que buscábamos.

La exactitud del funtor equivale a que el $\mathcal{O}_X$-módulo $\mathcal{M}$ cumpla la propiedad siguiente: Para cada monomorfismo $\mathcal{M}' \longrightarrow \mathcal{M}$ de $\mathcal{O}_X$-módulos y cada homomorfismo $\mathcal{M}' \longrightarrow \mathcal{N}$ existe un homomorfismo $\mathcal{M} \longrightarrow \mathcal{N}$ que hace conmutativo el diagrama siguiente:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}' \arrow[r] \arrow[d] & \mathcal{M} \arrow[dl, dashed] \\
 & \mathcal{N} &
\end{tikzcd}$$

Los $\mathcal{O}_X$-módulos $\mathcal{N}$ que tienen esta propiedad se llaman *inyectivos,* y los estudiaremos en la sección siguiente. ■

Un funtor de gran importancia en la teoría que vamos a desarrollar es el funtor covariante

$$\Gamma(X, -) : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X))$$

dado por $\Gamma(X, \mathcal{M}) = \mathcal{M}(X)$ y que a cada homomorfismo de funtores $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ le asigna el homomorfismo $\phi_X : \mathcal{M}(X) \longrightarrow \mathcal{N}(X)$. Vamos a probar que también es exacto por la izquierda. Esto significa que si

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P}$$

es una sucesión exacta de $\mathcal{O}_X$-módulos, entonces

$$0 \longrightarrow \mathcal{M}(X) \xrightarrow{\alpha_X} \mathcal{N}(X) \xrightarrow{\beta_X} \mathcal{P}(X)$$

es una sucesión exacta de $\mathcal{O}_X(X)$-módulos.

En efecto, la parte menos obvia es que si $s \in \mathcal{N}(X)$ cumple que $\beta_X(s) = 0$, entonces $s \in \mathrm{Im}(\alpha)(X)$, lo que significa que cada $P \in X$ tiene un entorno V_P tal que $s|_{V_P}$ tiene una antiimagen por α_{V_P}, pero la inyectividad de α permite extender estas antiimágenes locales a un $t \in \mathcal{M}(X)$ tal que $\alpha_X(t) = s$, luego la sucesión es exacta en el centro.

El hecho de que $\Gamma(X, -)$ no sea, en general, exacto, no es sino otra forma de expresar que un epimorfismo β no tiene por qué cumplir que β_X sea suprayectivo.

■

Los funtores exactos por la izquierda satisfacen muchas propiedades:

Teorema 1.22 *Sean X e Y dos espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ un funtor exacto por la izquierda. Entonces:*

a) Si 0 es el $\mathcal{O}_X$-módulo nulo, se cumple que $F0 = 0$.

b) Si $0 : \mathcal{M} \longrightarrow N$ es el homomorfismo nulo entre dos $\mathcal{O}_X$-módulos, entonces $F0 : F\mathcal{M} \longrightarrow F\mathcal{N}$ es el homomorfismo nulo.

c) Si $\mathcal{M}_1$ y $\mathcal{M}_2$ son dos $\mathcal{O}_X$-módulos, entonces $F(\mathcal{M}_1 \oplus \mathcal{M}_2) = F\mathcal{M}_1 \oplus F\mathcal{M}_2$. Además F transforma las proyecciones $\pi_i : \mathcal{M}_1 \oplus \mathcal{M}_2 \longrightarrow \mathcal{M}_i$ en las proyecciones $\bar{\pi}_i : F\mathcal{M}_1 \oplus F\mathcal{M}_2 \longrightarrow F\mathcal{M}_i$ y las inyecciones $\iota_i : \mathcal{M}_i \longrightarrow \mathcal{M}_1 \oplus \mathcal{M}_2$ en las inyecciones $\bar{\iota}_i : F\mathcal{M}_i \longrightarrow F\mathcal{M}_1 \oplus F\mathcal{M}_2$.

d) Si $f_i : \mathcal{M} \longrightarrow \mathcal{N}_i$, para $i = 1, 2$ son homomorfismos de $\mathcal{O}_X$-módulos y $(f_1, f_2) : \mathcal{M} \longrightarrow \mathcal{N}_1 \oplus \mathcal{N}_2$ es el homomorfismo definido de forma natural, entonces $F(f_1, f_2) = (Ff_1, Ff_2)$.

e) Si $f_i : \mathcal{M}_i \longrightarrow \mathcal{N}$, para $i = 1, 2$, son dos homomorfismos de $\mathcal{O}_X$-módulos y $f_1 + f_2 : \mathcal{M}_1 \oplus \mathcal{M}_2 \longrightarrow \mathcal{N}$ es el homomorfismo definido de forma natural, entonces $F(f_1 + f_2) = Ff_1 + Ff_2$.

f) Si $f_i : \mathcal{M}_i \longrightarrow \mathcal{N}_i$, para $i = 1, 2$ son dos homomorfismos de $\mathcal{O}_X$-módulos y $(f_1, f_2) : \mathcal{M}_1 \oplus \mathcal{M}_2 \longrightarrow \mathcal{N}_1 \oplus \mathcal{N}_2$ es el homomorfismo definido de forma natural, entonces $F(f_1, f_2) = (Ff_1, Ff_2)$.

g) Si $f_i : \mathcal{M} \longrightarrow \mathcal{N}$, para $i = 1, 2$, son dos homomorfismos de $\mathcal{O}_X$-módulos, entonces $F(f_1 + f_2) = Ff_1 + Ff_2$.

Demostración: a) Consideramos la sucesión exacta

$$0 \longrightarrow 0 \xrightarrow{1} 0 \xrightarrow{1} 0 \longrightarrow 0,$$

de la que obtenemos la sucesión exacta

$$0 \longrightarrow F0 \xrightarrow{1} F0 \xrightarrow{1} F0$$

La exactitud en el $F0$ central implica que $F0 = 0$.

b) Podemos descomponer el homomorfismo 0 como $\mathcal{M} \longrightarrow 0 \longrightarrow \mathcal{N}$, luego $F0$ se descompone como $F\mathcal{M} \longrightarrow 0 \longrightarrow F\mathcal{N}$, luego necesariamente $F0$ es el homomorfismo nulo.

c) Consideramos las sucesiones exactas

$$0 \longrightarrow \mathcal{M}_1 \xrightarrow{\iota_1} \mathcal{M}_1 \oplus \mathcal{M}_2 \xrightarrow{\pi_2} \mathcal{M}_2 \longrightarrow 0,$$

$$0 \longrightarrow \mathcal{M}_2 \xrightarrow{\iota_2} \mathcal{M}_1 \oplus \mathcal{M}_2 \xrightarrow{\pi_1} \mathcal{M}_1 \longrightarrow 0,$$

que se transforman en las sucesiones exactas

$$0 \longrightarrow F\mathcal{M}_1 \xrightarrow{\bar{\iota}_1} F(\mathcal{M}_1 \oplus \mathcal{M}_2) \xrightarrow{\bar{\pi}_2} F\mathcal{M}_2,$$

$$0 \longrightarrow F\mathcal{M}_2 \xrightarrow{\bar{\iota}_2} F(\mathcal{M}_1 \oplus \mathcal{M}_2) \xrightarrow{\bar{\pi}_1} F\mathcal{M}_1.$$

(Entendemos que $\bar{\iota}_i$ y $\bar{\pi}_i$ son, por definición, las imágenes por F de ι_i y π_i.)

Claramente $\bar{\iota}_1\bar{\pi}_2 = 0$, $\bar{\iota}_2\bar{\pi}_1 = 0$, $\bar{\iota}_1\bar{\pi}_1 = 1$, $\bar{\iota}_2\bar{\pi}_2 = 1$. Sea $U \subset Y$ un abierto y tomemos un $m \in F(\mathcal{M}_1 \oplus \mathcal{M}_2)(U)$. Entonces

$$\bar{\pi}_{2U}(m - \bar{\iota}_{2U}(\bar{\pi}_{2U}(m))) = \bar{\pi}_{2U}(m) - \bar{\pi}_{2U}(m) = 0,$$

luego $m - \bar{\iota}_{2U}(\bar{\pi}_{2U}(m)) \in \mathrm{N}\,\bar{\pi}_{2U} = \mathrm{Im}\,\bar{\iota}_{1U}$, por la exactitud izquierda del funtor $\Gamma(U, -)$. Así, existe un $m' \in (F\mathcal{M}_1)(U)$ tal que $m = \bar{\iota}_{2U}(\bar{\pi}_{2U}(m)) + \bar{\iota}_{1U}(m')$. Aplicando $\bar{\pi}_{1U}$ concluimos que $m' = \bar{\pi}_{1U}(m)$, luego hemos obtenido que

$$\bar{\pi}_1\bar{\iota}_1 + \bar{\pi}_2\bar{\iota}_2 = 1.$$

Ahora es fácil comprobar que $\bar{\iota}_1 + \bar{\iota}_2 : F\mathcal{M}_1 \oplus F\mathcal{M}_2 \longrightarrow F(\mathcal{M}_1 \oplus \mathcal{M}_2)$ es un isomorfismo, a través del cual las inyecciones y proyecciones de la suma directa se corresponden con los homomorfismos $\bar{\iota}_i$ y $\bar{\pi}_i$.

d) (f_1, f_2) está completamente determinado por el hecho de que $(f_1, f_2)\circ\pi_i = f_i$, y esto implica que $F(f_1, f_2) \circ \pi_i = Ff_i$, luego $F(f_1, f_2) = (Ff_1, Ff_2)$.

La prueba de e) y f) es similar a la de d), y g) se debe a que $f_1 + f_2$ puede descomponerse como

$$\mathcal{M} \xrightarrow{(f_1,f_2)} \mathcal{N} \oplus \mathcal{N} \xrightarrow{(1,1)} \mathcal{N},$$

y basta aplicar d) y e). ■

El teorema también es válido para funtores exactos por la derecha, así como para funtores contravariantes, aunque en este caso con las modificaciones obvias (por ejemplo, los funtores contravariantes exactos por la izquierda o por la derecha intercambian las proyecciones con las inyecciones en una suma directa, etc.).

1.4 Módulos inyectivos y proyectivos

Hemos definido los $\mathcal{O}_X$-módulos inyectivos como los módulos $\mathcal{N}$ para los que el funtor $\mathrm{Hom}_{\mathcal{O}_X}(-, \mathcal{N})$ es exacto, lo que equivale a que todo homomorfismo en $\mathcal{N}$ de un subhaz de un haz $\mathcal{M}$ puede extenderse hasta $\mathcal{M}$. El objetivo de esta sección es demostrar que existen muchos módulos con esta propiedad. Empezaremos estudiando los módulos inyectivos sobre un anillo A. El primer resultado es que la definición de A-módulo proyectivo es equivalente a otra más débil:

Teorema 1.23 *Un A-módulo M es inyectivo si y sólo si para todo ideal I de A se cumple que todo homomorfismo $I \longrightarrow M$ se extiende a A.*

DEMOSTRACIÓN: Una implicación es evidente. Lo que hemos de probar es que si P es un A-módulo arbitrario y N es un submódulo de P, entonces todo homomorfismo $N \longrightarrow M$ se extiende a P. Sea $\mathcal{M}$ el conjunto de todos los pares (T, α), donde T es un submódulo $N \subset T \subset N$ y $\alpha : T \longrightarrow M$ es un homomorfismo que extiende al dado. Consideramos en $\mathcal{M}$ el orden parcial dado por $(T_1, \alpha_1) \leq (T_2, \alpha_2)$ si y sólo si $T_1 \subset T_2$ y $\alpha_1 = \alpha_2|_{T_1}$. Por el lema de Zorn $\mathcal{M}$ tiene un elemento maximal (T_0, α_0). Basta probar que $T_0 = P$.

En caso contrario, existe $x \in P \setminus T_0$. Sea $I = \{a \in A \mid ax \in T_0\}$, que es claramente un ideal de A. Sea $f_0 : I \longrightarrow M$ dada por $f_0(a) = \alpha_0(ax)$. Claramente f_0 es un homomorfismo y por hipótesis se extiende a un homomorfismo $f : A \longrightarrow M$. Llamemos $T_1 = T_0 + Ax$ y definimos $\alpha_1 : T_1 \longrightarrow M$ mediante $\alpha_1(t + ax) = \alpha_0(t) + af(1)$.

En primer lugar, α_1 está bien definido, pues si $t + ax = t' + a'x$, entonces $t - t' = (a' - a)x \in T_0$, luego

$$\alpha_0(t) - \alpha_0(t') = \alpha_0((a' - a)x) = f_0(a' - a) = f(a') - f(a) = a'f(1) - af(1).$$

Por lo tanto $\alpha_0(t) + af(1) = \alpha_0(t') + a'f(1)$. Es claro que α_1 es un homomorfismo y que extiende a α_0, luego $(T_1, \alpha_1) \in \mathcal{M}$ contradice la maximalidad de (T_0, α_1). Esto prueba que $T_0 = P$ y α_0 es la extensión buscada. ■

Empezaremos estudiando la existencia de $\mathbb{Z}$-módulos inyectivos, pues tienen una caracterización sencilla:

Definición 1.24 Diremos que un $\mathbb{Z}$-módulo M es *divisible* si para todo $m \in M$ y todo $a \in \mathbb{Z}$ no nulo existe un $n \in M$ tal que $m = an$.

Teorema 1.25 *Un $\mathbb{Z}$-módulo M es inyectivo si y sólo si es divisible.*

DEMOSTRACIÓN: Supongamos en primer lugar que M es inyectivo. Sea $m \in M$ y $a \in \mathbb{Z}$ no nulo. Consideremos el homomorfismo $f_0 : (a) \longrightarrow M$ dado por $f_0(ba) = bm$ y extendámoslo a $f : \mathbb{Z} \longrightarrow M$. Entonces

$$m = f_0(a) = f(a) = af(1).$$

Supongamos ahora que M es divisible, sea $I = (a)$ un ideal de $\mathbb{Z}$ y sea $f_0 : (a) \longrightarrow M$ un homomorfismo. Existe un $x \in M$ tal que $f_0(a) = ax$. Definimos $f : \mathbb{Z} \longrightarrow M$ mediante $f(b) = bx$, de modo que $f(a) = ax = f_0(a)$, luego $f|_{(a)} = f_0$. ■

Ahora ya tenemos ejemplos de $\mathbb{Z}$-módulos inyectivos. Por ejemplo, $\mathbb{Q}$ es claramente divisible, luego es inyectivo. Más en general:

Teorema 1.26 *Para todo $\mathbb{Z}$-módulo M existe un monomorfismo $M \longrightarrow N$ con N inyectivo.*

DEMOSTRACIÓN: Podemos representar $M = L/N$, donde L es un $\mathbb{Z}$-módulo libre. Entonces L es suma directa de copias de $\mathbb{Z}$, luego puede sumergirse en una suma directa de copias de $\mathbb{Q}$, que claramente es divisible. En definitiva, tenemos $L \subset D$, con D divisible. Entonces $M = L/N \subset D/N$, y es claro que D/N también es divisible. ■

Para anillos arbitrarios tenemos lo siguiente:

Teorema 1.27 *Si D es un $\mathbb{Z}$-módulo divisible y A es un anillo arbitrario, entonces $\operatorname{Hom}_{\mathbb{Z}}(A, D)$ es un A-módulo inyectivo con el producto $(af)(b) = f(ab)$.*

DEMOSTRACIÓN: Observemos que, en general, un A-módulo M es inyectivo si, cuando $N \subset P$ son A-módulos, la restricción $\operatorname{Hom}_A(P, M) \longrightarrow \operatorname{Hom}_A(N, M)$ es un epimorfismo. En nuestro caso, tenemos un diagrama conmutativo

$$\begin{tikzcd}
\operatorname{Hom}_A(P, \operatorname{Hom}_{\mathbb{Z}}(A, D)) \arrow[r] \arrow[d] & \operatorname{Hom}_A(N, \operatorname{Hom}_{\mathbb{Z}}(A, D)) \arrow[d] \\
\operatorname{Hom}_{\mathbb{Z}}(P, D) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(N, D)
\end{tikzcd}$$

donde las flechas verticales son isomorfismos de $\mathbb{Z}$-módulos, por ejemplo, la primera es la dada por

$$\phi(f)(p) = f(p)(1)$$

y su inverso es $\psi(f)(p)(a) = f(ap)$. Como D es un $\mathbb{Z}$-módulo inyectivo, el homomorfismo horizontal inferior es un epimorfismo, luego el superior también. ■

Ahora podemos generalizar 1.26:

Teorema 1.28 *Si A es un anillo, para todo A-módulo M existe un monomorfismo $M \longrightarrow N$ con N inyectivo.*

DEMOSTRACIÓN: Considerando a M como $\mathbb{Z}$-módulo, tenemos un monomorfismo $f : M \longrightarrow D$, donde D es un $\mathbb{Z}$-módulo divisible. Consideramos el homomorfismo $\phi : M \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, D)$ dado por $\phi(m)(a) = f(am)$. Es inyectivo, pues si $\phi(m) = 0$ entonces $\phi(m)(1) = f(m) = 0$, luego $m = 0$. Es fácil ver que ϕ es un homomorfismo de A-módulos. ■

A su vez, de aquí se deduce el resultado análogo para módulos sobre cualquier espacio anillado:

Teorema 1.29 *Si X es un espacio anillado y $\mathcal{M}$ es un $\mathcal{O}_X$-módulo, entonces existe un monomorfismo $\mathcal{M} \longrightarrow \mathcal{N}$ con $\mathcal{N}$ inyectivo.*

DEMOSTRACIÓN: Para cada $P \in X$, el $\mathcal{O}_{X,P}$-módulo $\mathcal{M}_P$ puede sumergirse en un $\mathcal{O}_{X,P}$-módulo inyectivo N_P. Fijemos un monomorfismo $\alpha_P : \mathcal{M}_P \longrightarrow N_P$ y para cada abierto $U \subset X$ definimos

$$\mathcal{N}(U) = \prod_{P \in U} N_P.$$

Es fácil ver que $\mathcal{N}$, así definido (con las restricciones y las operaciones obvias), es un $\mathcal{O}_X$-módulo. Definimos $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ mediante $\phi_U(f) = (\alpha_P(f_P))_{P \in U}$.

Claramente los homomorfismos ϕ_U son inyectivos, luego ϕ también lo es. Ahora falta probar que $\mathcal{N}$ es inyectivo.

Observemos que las proyecciones $\pi_{U,P} : \mathcal{N}(U) \longrightarrow N_P$ inducen homomorfismos $\pi_P : \mathcal{N}_P \longrightarrow N_P$ independientes de U. Cada $f \in \mathcal{N}(U)$ cumple obviamente que $f = (\pi_P(f_P))_{P\in U}$.

Supongamos un monomorfismo $\psi : \mathcal{P} \longrightarrow \mathcal{Q}$ y un homomorfismo $\alpha : \mathcal{P} \longrightarrow \mathcal{N}$. Para cada $P \in X$, el homomorfismo

$$\mathcal{P}_P \xrightarrow{\alpha_P} \mathcal{N}_P \xrightarrow{\pi_P} N_P$$

se extiende a un homomorfismo $\chi_P : \mathcal{Q}_P \longrightarrow N_P$, que a su vez determina un homomorfismo $\chi : \mathcal{Q} \longrightarrow \mathcal{N}$ mediante $\chi_U(f) = (\chi_P(f_P))_{P\in U}$. Veamos que $\psi \circ \chi = \alpha$. En efecto, si U es un abierto en X y $f \in \mathcal{P}(U)$,

$$\chi_U(\psi_U(f)) = (\chi_P(\psi_P(f_P)))_{P\in U} = (\pi_P(\alpha_P(f_P)))_{P\in U} = \alpha_U(f).$$

■

La inyectividad se conserva al restringir:

Teorema 1.30 *Sea X un espacio anillado y $U \subset X$ un abierto. Si $\mathcal{I}$ es un $\mathcal{O}_X$-módulo inyectivo, entonces $\mathcal{I}|_U$ es un $\mathcal{O}_U$-módulo inyectivo.*

DEMOSTRACIÓN: En general, si $\mathcal{F}$ es un $\mathcal{O}_U$-módulo, definimos $\mathcal{F}^X$ como la compleción del prehaz dado por

$$\mathcal{F}^{X-}(V) = \begin{cases} \mathcal{F}(V) & \text{si } V \subset U, \\ 0 & \text{en caso contrario.} \end{cases}$$

Es claro que $\mathcal{F}^X_P = \mathcal{F}_P$ si $P \in U$ y $\mathcal{F}^X_P = 0$ si $P \in X \setminus U$. Todo homomorfismo de $\mathcal{O}_U$-módulos $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ se extiende a un homomorfismo de $\mathcal{O}_X$-módulos $\alpha^X : \mathcal{F}^X \longrightarrow \mathcal{G}^X$ tal que $\alpha^X_P = \alpha_P$ para todo $P \in U$. Así mismo es fácil ver que $\mathcal{F}^X|_U = \mathcal{F}$.

Pasemos ya a la demostración del teorema: supongamos dados un monomorfismo de $\mathcal{O}_U$-módulos $\mathcal{N} \longrightarrow \mathcal{P}$ y un homomorfismo $\mathcal{N} \longrightarrow \mathcal{I}|_U$. Entonces tenemos un monomorfismo de $\mathcal{O}_X$-módulos $\mathcal{N}^X \longrightarrow \mathcal{P}^X$ y un homomorfismo $\mathcal{N}^X \longrightarrow (\mathcal{I}|_U)^X$. Pero es fácil definir un monomorfismo de $\mathcal{O}_X$-módulos $(\mathcal{I}|_U)^X \longrightarrow \mathcal{I}$ que restringido a U es la identidad. Así tenemos un homomorfismo $\mathcal{N}^X \longrightarrow \mathcal{I}$, y podemos aplicar la inyectividad de $\mathcal{I}$, que nos permite extender este homomorfismo a un homomorfismo $\mathcal{P}^X \longrightarrow \mathcal{I}$. Restringiendo a U tenemos un homomorfismo $\mathcal{P} \longrightarrow \mathcal{I}|_U$ que extiende al dado sobre $\mathcal{N}$. ■

Una propiedad básica de los módulos inyectivos es la siguiente:

Teorema 1.31 *Si X es un espacio anillado y $0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$ es una sucesión exacta de $\mathcal{O}_X$-módulos en la que $\mathcal{M}$ es inyectivo, entonces se cumple que $\mathcal{N} = \mathrm{N}(\beta) \oplus \mathrm{CN}(\alpha) \cong \mathcal{M} \oplus \mathcal{P}$.*

DEMOSTRACIÓN: Existe un homomorfismo $\gamma : \mathcal{N} \longrightarrow \mathcal{M}$ tal que $\alpha \circ \gamma = 1$. Para cada $P \in X$ tenemos que $\alpha_P \circ \gamma_P = 1$ (y la sucesión localizada sigue siendo exacta), luego $\mathcal{N}_P = \mathrm{N}(\beta)_P \oplus \mathrm{CN}(\alpha)_P$. Para cada abierto U de X, si $f \in \mathrm{N}(\beta)(U) \cap \mathrm{CN}(\alpha)(U)$, entonces $f_P = 0$ para todo $P \in U$, luego $f = 0$.

Por otra parte, si $f \in \mathcal{N}(U)$ y $P \in U$, entonces $f_P = u_P + v_P$, para ciertos $u_P \in \mathrm{N}(\beta)_P$, $v_P \in \mathrm{CN}(\alpha)_P$, que serán localizaciones de elementos $u_V \in \mathrm{N}(\beta)(V)$, $v_V \in \mathrm{CN}(\alpha)(V)$, para cierto abierto $P \in V \subset U$. Podemos cubrir U con abiertos V en estas condiciones, y la unicidad de la descomposición en suma directa hace que los elementos $\{u_V\}_V$ y $\{v_V\}_V$ determinen unos $u \in \mathrm{N}(\beta)(U)$, $v \in \mathrm{CN}(\alpha)(U)$ tales que $f = u + v$. Por lo tanto $\mathcal{N}(U) = \mathrm{N}(\beta)(U) \oplus \mathrm{CN}(\alpha)(U)$, luego $\mathcal{N} = \mathrm{N}(\beta) \oplus \mathrm{CN}(\alpha)$. ■

La definición de módulo proyectivo es "dual" de la de módulo inyectivo, en el sentido de que una se obtiene de la otra sin más que intercambiar sistemáticamente el sentido de todos los homomorfismos que intervienen en ella (lo que supone cambiar también "inyectivo" por "suprayectivo"). Sin embargo, esto no significa que todos los resultados válidos para módulos inyectivos valgan también para proyectivos sin más que intercambiar las flechas en los enunciados y las demostraciones. De hecho, el "dual" del teorema es falso en general, y sólo podemos demostrar el dual de 1.28 que, por contrapartida, es mucho más sencillo de probar, debido a que los módulos proyectivos sobre un anillo tienen una caracterización muy simple:

Teorema 1.32 *Sea A un anillo y M un A-módulo. Las afirmaciones siguientes son equivalentes:*

a) M es proyectivo.

b) Toda sucesión exacta de módulos $0 \longrightarrow C \xrightarrow{\beta} N \xrightarrow{\alpha} M \longrightarrow 0$ se escinde, es decir, existe un homomorfismo $\gamma : M \longrightarrow N$ tal que $\gamma \circ \alpha = 1$ (lo que, a su vez, implica que $N = \operatorname{Im} \beta \oplus \operatorname{Im} \gamma \cong C \oplus M$).

c) Existe un A-módulo M' tal que $M \oplus M'$ es libre.

DEMOSTRACIÓN:

a) $\Rightarrow$ b) aplicamos la proyectividad a la identidad $M \longrightarrow M$. La descomposición se debe a que si $n \in N$, entonces $\alpha(n - \gamma(\alpha(n)) = 0$, luego $b = n - \gamma(\alpha(n)) \in \operatorname{Im} \beta$ y $n = b + \gamma(\alpha(n))$. Por otra parte, si $\beta(c) = \gamma(m)$, aplicando α obtenemos que $m = 0$, luego la suma es directa.

b) $\Rightarrow$ c) Podemos formar una sucesión exacta como la de b) con N libre. Entonces $N = C \oplus \gamma[M]$.

c) $\Rightarrow$ a) Consideremos un epimorfismo $\alpha : N \longrightarrow P$ y un homomorfismo $\beta : M \longrightarrow P$. Extendemos trivialmente β a $M \oplus M'$. Consideramos una base de este módulo y a cada uno de sus elementos le asignamos una antiimagen en N de su imagen en P. Esta asignación se extiende a un homomorfismo γ, el cual se restringe a su vez a un homomorfismo sobre M que cumple lo requerido. ■

La condición c) implica en particular que todo módulo libre es proyectivo. En la prueba del teorema anterior se ve que si M es un módulo proyectivo finitamente generado, entonces el módulo M' tal que $M \oplus M'$ es libre se puede tomar también finitamente generado. También es obvio que la suma directa de módulos proyectivos es proyectiva y que todo sumando directo de un módulo proyectivo es proyectivo. En particular, es evidente que todo A-módulo M es imagen de un A-módulo proyectivo, pues todo A-módulo M es imagen de un módulo libre.

1.5 Complejos

Definición 1.33 Si X es un espacio anillado, un *complejo directo* de $\mathcal{O}_X$-módulos $\mathcal{C}$ es una sucesión

$$\cdots \longrightarrow \mathcal{C}_2 \xrightarrow{\partial_1} \mathcal{C}_1 \xrightarrow{\partial_0} \mathcal{C}_0 \longrightarrow 0$$

de $\mathcal{O}_X$-módulos y homomorfismos tal que $\partial_{i+1} \circ \partial_i = 0$ para todo i. Un *complejo inverso* es de la forma

$$0 \longrightarrow \mathcal{C}_0 \xrightarrow{d_0} \mathcal{C}_1 \xrightarrow{d_1} \mathcal{C}_2 \longrightarrow \cdots$$

de modo que $d_i \circ d_{i+1} = 0$.

Un *homomorfismo* $\phi : \mathcal{C} \longrightarrow \mathcal{D}$ entre dos complejos directos es una sucesión de homomorfismos $\phi_i : \mathcal{C}_i \longrightarrow \mathcal{D}_i$ tal que el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
\cdots \arrow[r] & \mathcal{C}_2 \arrow[r, "\partial_1"] \arrow[d, "\phi_2"] & \mathcal{C}_1 \arrow[r, "\partial_0"] \arrow[d, "\phi_1"] & \mathcal{C}_0 \arrow[r] \arrow[d, "\phi_0"] & 0 \\
\cdots \arrow[r] & \mathcal{D}_2 \arrow[r, "\partial_1"'] & \mathcal{D}_1 \arrow[r, "\partial_0"'] & \mathcal{C}_0 \arrow[r] & 0
\end{tikzcd}$$

Los homomorfismos de complejos inversos se definen análogamente. Es fácil ver que los complejos directos de $\mathcal{O}_X$-módulos con los homomorfismos de complejos forman una categoría, y lo mismo vale para los complejos inversos.

Diremos que una sucesión de homomorfismos de complejos

$$0 \longrightarrow \mathcal{C} \xrightarrow{\phi} \mathcal{D} \xrightarrow{\psi} \mathcal{E} \longrightarrow 0$$

es *exacta* si lo son todas las sucesiones

$$0 \longrightarrow \mathcal{C}_i \xrightarrow{\phi_i} \mathcal{D}_i \xrightarrow{\psi_i} \mathcal{E}_i \longrightarrow 0.$$

Los *grupos de homología* de un complejo directo $\mathcal{C}$ se definen como los $\mathcal{O}_X$-módulos

$$H_i(\mathcal{C}) = \mathrm{N}(\partial_{i-1}) / \operatorname{Im} \partial_i.$$

Similarmente, los *grupos de cohomología* de un complejo inverso $\mathcal{C}$ se definen como los $\mathcal{O}_X$-módulos

$$H^i(\mathcal{C}) = \mathrm{N}(d_i)/\operatorname{Im} d_{i-1}.$$

Si $\alpha, \beta : \mathcal{C} \longrightarrow \mathcal{D}$ son dos homomorfismos de complejos inversos de $\mathcal{O}_X$-módulos. Una *homotopía* Δ entre α y β es una sucesión de homomorfismos de $\mathcal{O}_X$-módulos $\Delta^n : \mathcal{C}_{n+1} \longrightarrow \mathcal{D}_n$ tal que

$$\alpha^n - \beta^n = \Delta^{n-1} d_{n-1} + d_n \Delta^n.$$

Si existe una homotopía entre α y β se dice que son homomorfismos *homotópicos.* Las homotopías entre homomorfismos de complejos directos se definen análogamente, sin más que invertir la ordenación de los índices.

Observemos que la única diferencia entre los complejos directos y los inversos es la ordenación de los índices, por lo que todo concepto o resultado general sobre complejos directos puede reformularse en términos de complejos inversos, y viceversa. En lo sucesivo enunciaremos y probaremos los resultados únicamente para complejos inversos.

Teorema 1.34 *Si X es un espacio anillado, todo homomorfismo de complejos inversos de $\mathcal{O}_X$-módulos $\alpha : \mathcal{C} \longrightarrow \mathcal{C}'$ induce homomorfismos*

$$\bar{\alpha}^n : H^n(\mathcal{C}) \longrightarrow H^n(\mathcal{C}')$$

determinados por que, para cada $P \in X$, el homomorfismo

$$\bar{\alpha}_P : (\mathrm{N}\, d_n)_P/(\operatorname{Im} d_{n-1})_P \longrightarrow (\mathrm{N}\, d'_n)_P/(\operatorname{Im} d'_{n-1})_P$$

es el inducido por la restricción $\alpha_P|_{(\mathrm{N}\, d_n)_P} : (\mathrm{N}\, d_n)_P \longrightarrow (\mathrm{N}\, d'_n)_P$. Dos homomorfismos homotópicos inducen los mismos homomorfismos sobre los grupos de cohomología.

Demostración: Sea $U \subset X$ un abierto y tomemos $s \in (\mathrm{N}\, d_n)(U)$. Es claro entonces que $\alpha^n_U(s) \in (\mathrm{N}\, d'_n)(U)$, luego podemos considerar su clase de equivalencia $[\alpha^n_U(s)] \in (\mathrm{N}\, d'_n)(U)/(\operatorname{Im} d'_{n-1})(U)$.

Tomemos ahora $s \in (\mathrm{Im} d_{n-1})(U)$. La única complicación que hace que el teorema no sea trivial es que esto no implica que s esté en la imagen de $d_{n-1,U}$. Lo que sabemos es que, para cada $P \in U$, se cumple que $s_P \in \operatorname{Im} d_{n-1,P}$, por lo que $\alpha^n_U(s)_P \in \operatorname{Im} d'_{n-1,P}$, lo que a su vez implica que $\alpha^n_U(s) \in (\operatorname{Im} d'_{n-1})(U)$.

Esto nos permite definir un homomorfismo de $\mathcal{O}_X(U)$-módulos:

$$(\mathrm{N}\, d_n)(U)/(\operatorname{Im} d_{n-1})(U) \longrightarrow (\mathrm{N}\, d'_n)(U)/(\operatorname{Im} d'_{n-1})(U).$$

Estos homomorfismos definen un homomorfismo de prehaces

$$(\mathrm{N}\, d_n/\mathrm{Im} d_{n-1})^- \longrightarrow (\mathrm{N}\, d'_n/\mathrm{Im} d'_{n-1})^-,$$

que a su vez se extiende a un homomorfismo de haces $H^n(\mathcal{C}) \longrightarrow H^n(\mathcal{C}')$. Claramente cumple lo pedido. La última afirmación del enunciado es inmediata.

■

Ahora es claro que podemos considerar a cada H^n como un funtor de la categoría de complejos inversos de $\mathcal{O}_X$-módulos en la categoría de los $\mathcal{O}_X$-módulos.

Ahora vamos a probar el resultado fundamental sobre complejos, para lo que necesitamos un hecho previo:

Teorema 1.35 *Sea X un espacio anillado, consideremos el siguiente diagrama conmutativo de $\mathcal{O}_X$-módulos y supongamos que sus filas son exactas.*

$$\begin{tikzcd} & Z_1' \arrow[r, "\phi'"] \arrow[d, "d_1"] & Z_2' \arrow[r, "\psi'"] \arrow[d, "d_2"] & Z_3' \arrow[r] \arrow[d, "d_3"] & 0 \\ 0 \arrow[r] & Z_1 \arrow[r, "\phi"'] & Z_2 \arrow[r, "\psi"'] & Z_3 & \end{tikzcd}$$

Entonces existe un homomorfismo $\delta_* : \mathrm{N}(d_3) \longrightarrow Z_1/\operatorname{Im} d_1$ tal que la sucesión

$$\mathrm{N}(d_1) \xrightarrow{\phi''} \mathrm{N}(d_2) \xrightarrow{\psi''} \mathrm{N}(d_3) \xrightarrow{\delta_*} Z_1/\operatorname{Im} d_1 \xrightarrow{\bar{\phi}} Z_2/\operatorname{Im} d_2 \xrightarrow{\bar{\psi}} Z_3/\operatorname{Im} d_3$$

es exacta, donde ϕ'' y ψ'' son las restricciones de ϕ' y ψ' a $\mathrm{N}(d_1)$ y $\mathrm{N}(d_2)$ y $\bar{\phi}$, $\bar{\psi}$ son los homomorfismos inducidos de forma natural.

DEMOSTRACIÓN: Los homomorfismos $\bar{\phi}$ y $\bar{\psi}$ son los construidos como en el teorema anterior. Para construir δ_* fijamos un abierto $U \subset X$ y un elemento $s_3' \in Z_3'(U)$. Entonces $s_3' \in \operatorname{Im} \psi'$, lo que significa que, para cada $P \in U$, $s_{3P}' \in \operatorname{Im} \psi_P'$. Existe un abierto $P \in V_P \subset U$ y un $s_2' \in Z_2'(V_P)$ tal que $\psi_{V_P}'(s_2') = s_3'|_{V_P}$. Sea $s_2 = d_{2V_P}(s_2') \in Z_2(V_P)$. Entonces $s_2 \in (\mathrm{N}\,\psi)(V_P) = (\operatorname{Im} \phi)(V_P)$. Por consiguiente, podemos tomar otro abierto $P \in W_P \subset V_P$ y un $s_1 \in Z_1(W_P)$ de modo que $\phi_{W_P}(s_1) = s_2|_{W_P}$.

En resumen: para cada $P \in U$ existe un abierto $P \in W_P \subset U$ tal que $s_3'|_{W_P}$ tiene una antiimagen $s_2' \in Z_2'(W_P)$, cuya imagen $s_2 = d_{2W_P}(s_2')$ tiene una antiimagen $s_1 \in Z_1(W_p)$. Llamamos $\delta_P(s_3) = [s_1] \in Z_1(W_P)/(\operatorname{Im} d_1)(W_P)$.

Supongamos que elegimos otros $\bar{W}_P$, $\bar{s}_2'$ y $\bar{s}_1$ que cumplan lo mismo. Entonces, $s_2'|_{W_P \cap \bar{W}_P} - \bar{s}_2'|_{W_P \cap \bar{W}_P} \in \mathrm{N}\,\psi' = \operatorname{Im} \phi'$, luego para cada $Q \in W_P \cap \bar{W}_P$ tenemos que $s_{2Q}' - \bar{s}_{2Q}' \in \operatorname{Im} \phi_Q'$, luego $s_{2Q} - \bar{s}_{2Q} \in \operatorname{Im}(d_{1Q} \circ \phi_Q)$, luego $s_1 - \bar{s}_1 \in \operatorname{Im} d_{1Q}$, luego $s_1|_{W_P \cap \bar{W}_P} - \bar{s}_1|_{W_P \cap \bar{W}_P} \in (\operatorname{Im} d_1)(W_P \cap \bar{W}_P)$, luego $\delta_P(s_3)|_{W_P \cap \bar{W}_P} = \bar{\delta}_P(s_3)|_{W_P \cap \bar{W}_P}$.

El mismo argumento prueba que $\delta_P(s_3)|_{W_P \cap W_Q} = \delta_Q(s_3)|_{W_P \cap W_Q}$. Sea $\hat{\delta}_P(s_3)$ la imagen de $\delta_P(s_3)$ en $(Z_1/\operatorname{Im} d_1)(W_P)$. Entonces

$$\hat{\delta}_P(s_3)|_{W_P \cap W_Q} = \hat{\delta}_Q(s_3)|_{W_P \cap W_Q},$$

luego estos elementos se extienden un $\delta_*(s_3) \in (Z_1/\operatorname{Im} d_1)(U)$ que es independiente de todas las elecciones intermedias, pues hemos probado que todas determinan el mismo $\delta_*(s_3)_P$.

De hecho, es claro que $\delta_*(s_3)_P$ es el homomorfismo de conexión usual obtenido a partir de s_{3P} con el diagrama del enunciado localizado en P, es decir, se toma una antiimagen de s_{3P} en Z'_{2P}, se toma su imagen en Z_{2P}, se toma una antiimagen en Z_{1P} y se toma la clase módulo $\operatorname{Im} d_{1P}$. Como cada elemento de $Z'_3(U)$ está determinado por sus localizaciones, esto prueba el resto del teorema, a saber, que δ_* es un homomorfismo de $\mathcal{O}_X$-módulos y que la sucesión del enunciado es exacta.[2] ■

Teorema 1.36 *Sea X un espacio anillado y $0 \longrightarrow \mathcal{A} \xrightarrow{\phi} \mathcal{B} \xrightarrow{\psi} \mathcal{C} \longrightarrow 0$ una sucesión exacta de complejos de $\mathcal{O}_X$-módulos. Entonces existen homomorfismos*

$$\delta_*^n : H^n(\mathcal{C}) \longrightarrow H^{n+1}(\mathcal{A})$$

tales que la sucesión siguiente es exacta:

$$\cdots \longrightarrow H^n(\mathcal{A}) \xrightarrow{\bar{\phi}^n} H^n(\mathcal{B}) \xrightarrow{\bar{\psi}^n} H^n(\mathcal{C}) \xrightarrow{\delta_*^n} H^{n+1}(\mathcal{A}) \xrightarrow{\bar{\phi}^{n+1}} H^{n+1}(\mathcal{B}) \longrightarrow \cdots$$

DEMOSTRACIÓN: Basta comprobar que el diagrama siguiente satisface las hipótesis del teorema anterior.

$$\begin{tikzcd}
 & \mathcal{A}^n/\operatorname{Im} d_{n-1} \arrow[r, "\phi^n"] \arrow[d, "d_n"'] & \mathcal{B}^n/\operatorname{Im} d_{n-1} \arrow[r, "\psi^n"] \arrow[d, "d_n"'] & \mathcal{C}^n/\operatorname{Im} d_{n-1} \arrow[r] \arrow[d, "d_n"'] & 0 \\
0 \arrow[r] & \operatorname{N} d_{n+1} \arrow[r, "\phi^{n+1}"] & \operatorname{N} d_{n+1} \arrow[r, "\psi^{n+1}"] & \operatorname{N} d_{n+1} &
\end{tikzcd}$$

Ahora bien, todas las comprobaciones pueden reducirse a las propiedades análogas sobre los diagramas que resultan de localizar en un punto arbitrario $P \in X$, y entonces son las comprobaciones usuales cuando en lugar de $\mathcal{O}_X$-módulos tenemos módulos ordinarios.[3] ■

La sucesión exacta dada por el teorema anterior se llama *sucesión exacta larga de cohomología* asociada a la sucesión exacta corta dada de homomorfismos de complejos.

Nota Se comprueba fácilmente que los homomorfismos de conexión dados por el teorema anterior conmutan con los homomorfismos inducidos por homomorfismos de sucesiones exactas de complejos, es decir, que si tenemos un diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{A} \arrow[r] \arrow[d] & \mathcal{B} \arrow[r] \arrow[d] & \mathcal{C} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{A}' \arrow[r] & \mathcal{B}' \arrow[r] & \mathcal{C}' \arrow[r] & 0
\end{tikzcd}$$

[2]Para los detalles ver el teorema 2.24 de mi Topología Algebraica.

[3]Para los detalles ver el teorema 2.25 de mi Topología algebraica. Nótese que dicho teorema está enunciado para complejos directos y no inversos, lo que supone únicamente que los homomorfismos d disminuyen el grado en lugar de aumentarlo. Los cambios que ello supone son meramente de notación.

con filas exactas, entonces los homomorfismos entre los grupos de cohomología inducidos por las flechas verticales determinan un diagrama conmutativo entre sus sucesiones exactas largas de cohomología. (Una vez más, todas las comprobaciones se reducen a comprobar la conmutatividad de diagramas de homomorfismos de módulos sobre un anillo y no sobre un espacio anillado.) ■

Los funtores exactos por la izquierda o la derecha cumplen que $F0 = 0$, y esto basta para concluir que transforman complejos inversos en complejos inversos en el caso de los funtores covariantes y complejos inversos en complejos directos en el caso de los contravariantes. Además, su aditividad (teorema 1.22 g) implica que transforman homotopías en homotopías. Los funtores exactos, además, conservan la cohomología:

Teorema 1.37 *Sean X e Y dos espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ un funtor exacto. Sea $\mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P}$ una sucesión de homomorfismos de $\mathcal{O}_X$-módulos tal que $\mathrm{Im}\,\alpha \subset \mathrm{N}\,\beta$. Entonces la sucesión $F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P}$ cumple lo mismo y además*

$$\mathrm{N}(F\beta)/\,\mathrm{Im}(F\alpha) \cong F(\mathrm{N}\,\beta/\,\mathrm{Im}\,\alpha).$$

Demostración: De $\alpha\beta = 0$ se deduce que $F\alpha F\beta = 0$, es decir, que $\mathrm{Im}(F\alpha) \subset \mathrm{N}(F\beta)$. Aplicando F al diagrama conmutativo

$$\begin{tikzcd}
\mathcal{M} \arrow[r, "\alpha"] \arrow[d] & \mathcal{N} \\
\mathrm{Im}\,\alpha \arrow[ur, "i"'] &
\end{tikzcd}$$

se conserva la suprayectividad de la flecha vertical y la inyectividad de i, lo que implica que $Fi : F\,\mathrm{Im}\,\alpha \longrightarrow \mathrm{Im}(F\alpha)$ es un isomorfismo. Por otra parte, al aplicar F a la sucesión exacta

$$0 \longrightarrow \mathrm{N}\,\beta \xrightarrow{j} \mathcal{N} \xrightarrow{\beta} \mathcal{P}$$

obtenemos el isomorfismo $Fj : F(\mathrm{N}\,\beta) \longrightarrow \mathrm{N}(F\beta)$. Por otra parte, al aplicar F al diagrama conmutativo

$$\begin{tikzcd}
\mathrm{Im}\,\alpha \arrow[r, "k"] \arrow[d, "i"'] & \mathrm{N}\,\beta \arrow[dl, "j"'] \\
\mathcal{N} &
\end{tikzcd}$$

obtenemos un diagrama conmutativo que puede descomponerse en

$$\begin{tikzcd}
0 \arrow[r] & F(\mathrm{Im}\,\alpha) \arrow[r, "Fk"] \arrow[d, "Fi"'] & F(\mathrm{N}(\beta)) \arrow[r] \arrow[d, "Fj"] & F(\mathrm{N}\,\beta/\,\mathrm{Im}\,\alpha) \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{Im}(F\alpha) \arrow[r] & \mathrm{N}(F\beta) \arrow[r] & \mathrm{N}(F\beta)/\,\mathrm{Im}(F\alpha) \arrow[r] & 0
\end{tikzcd}$$

Como las filas son exactas, los isomorfismos Fj y Fi inducen el isomorfismo buscado. ■

Nuestro propósito es estudiar la inexactitud de un funtor exacto por la izquierda o por la derecha estudiando como alteran los grupos de (co)homología de ciertos complejos, complejos que vamos a construir en la sección siguiente:

1.6 Resoluciones inyectivas y proyectivas

Definición 1.38 Sea X un espacio anillado y $\mathcal{M}$ un $\mathcal{O}_X$-módulo. Una *resolución inversa* de $\mathcal{M}$ es una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{I}^0 \longrightarrow \mathcal{I}^1 \longrightarrow \mathcal{I}^2 \longrightarrow \cdots$$

La resolución es *inyectiva* si los $\mathcal{O}_X$-módulos $\mathcal{I}^i$ son inyectivos. Similarmente, una *resolución directa* de $\mathcal{M}$ es una sucesión exacta

$$\cdots \longrightarrow \mathcal{P}^2 \longrightarrow \mathcal{P}^1 \longrightarrow \mathcal{P}^0 \longrightarrow \mathcal{M} \longrightarrow 0,$$

y la resolución es *proyectiva* si los $\mathcal{O}_X$-módulos $\mathcal{P}^i$ son proyectivos.

A partir del teorema 1.29 es fácil probar que todo $\mathcal{O}_X$-módulo $\mathcal{M}$ admite una resolución inyectiva, pero vamos a demostrar algo más preciso:

Teorema 1.39 *Sea X un espacio anillado y*

$$0 \longrightarrow \mathcal{M}_1 \xrightarrow{\alpha} \mathcal{M}_2 \xrightarrow{\beta} \mathcal{M}_3 \longrightarrow 0$$

una sucesión exacta de $\mathcal{O}_X$-módulos. Entonces existen sendas resoluciones inyectivas $(\mathcal{I}_j^i)_i$, para $j = 1, 2, 3$, tales que $\mathcal{I}_2^i = \mathcal{I}_1^i \oplus \mathcal{I}_3^i$ y el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}_1 \arrow[r] \arrow[d, "\alpha"'] & \mathcal{I}_1^0 \arrow[r] \arrow[d] & \mathcal{I}_1^1 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathcal{M}_2 \arrow[r] \arrow[d, "\beta"'] & \mathcal{I}_2^0 \arrow[r] \arrow[d] & \mathcal{I}_2^1 \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathcal{M}_3 \arrow[r] & \mathcal{I}_3^0 \arrow[r] & \mathcal{I}_3^1 \arrow[r] & \cdots
\end{tikzcd}$$

donde las flechas verticales son los homomorfismos naturales

$$0 \longrightarrow \mathcal{I}_1^i \longrightarrow \mathcal{I}_1^1 \oplus \mathcal{I}_3^i \longrightarrow \mathcal{I}_3^i \longrightarrow 0.$$

Demostración: Sea $\eta_1 : \mathcal{M}_1 \longrightarrow \mathcal{I}_1^0$ un monomorfismo en un módulo inyectivo $\mathcal{I}_1^0$ y consideremos el homomorfismo

$$(\alpha, -\eta_1) : \mathcal{M}_1 \longrightarrow \mathcal{M}_2 \oplus \mathcal{I}_1^0.$$

Sea $\mathcal{G} = \mathrm{CN}(\alpha, -\eta_1)$ y sea $\mathcal{G} \longrightarrow \mathcal{I}$ un monomorfismo en un módulo inyectivo $\mathcal{I}$. Definimos $\bar{\alpha}^0$ como la composición $\mathcal{I}_1^0 \longrightarrow \mathcal{M}_2 \oplus \mathcal{I}_1^0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{I}$ y $\bar{\eta}_2$ como la composición $\mathcal{M}_2 \longrightarrow \mathcal{M}_2 \oplus \mathcal{I}_1^0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{I}$.

Observemos que ambos homomorfismos son inyectivos. Por ejemplo, si tomamos $P \in X$ y $f \in \mathcal{I}_{1,P}^0$ tales que $\bar{\alpha}_P^0(f) = 0$, entonces $(0, f) \in \mathrm{Im}(\alpha_P, -\eta_{1,P})$, es decir que existe un $g \in \mathcal{M}_{1,P}$ tal que $\alpha_P(g) = 0$ y $-\eta_{1,P}(g) = f$, pero entonces $g = 0$ y también $f = 0$. Por el teorema 1.31 tenemos que $\mathcal{I} = \mathrm{Im}(\bar{\alpha}^0) \oplus \mathrm{CN}(\bar{\alpha}^0)$.

Llamemos $\mathcal{H} = \mathrm{CN}(\bar{\alpha}^0)$ y sea $\bar{\beta}^0 : \mathcal{I} \longrightarrow \mathcal{H}$ el epimorfismo canónico. Es inmediato que todo sumando directo de un módulo inyectivo es inyectivo, luego $\mathcal{H}$ es inyectivo. Tenemos la situación siguiente:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & \mathcal{M}_1 \arrow[r, "\alpha"] \arrow[d, "\eta_1"'] & \mathcal{M}_2 \arrow[r, "\beta"] \arrow[d, "\bar{\eta}_2"'] & \mathcal{M}_3 \arrow[r] & 0 \\
0 \arrow[r] & \mathcal{I}_1^0 \arrow[r, "\bar{\alpha}^0"'] & \mathcal{I} \arrow[r, "\bar{\beta}^0"'] & \mathcal{H} \arrow[r] & 0
\end{tikzcd}$$

donde el cuadrado es conmutativo y las filas y columnas son exactas. Como $\mathrm{Im}(\alpha) \subset \mathrm{N}(\bar{\eta}_2 \circ \bar{\beta}^0)$, podemos definir un homomorfismo $\mathrm{CN}(\alpha) \longrightarrow \mathcal{H}$ tal que $\mathcal{M}_2 \longrightarrow \mathrm{CN}(\alpha) \longrightarrow \mathcal{H}$ sea $\bar{\eta}_2 \circ \bar{\beta}^0$. Este homomorfismo se extiende a un homomorfismo $\bar{\eta}_3 : \mathcal{M}_3 \longrightarrow \mathcal{H}$ tal que

$$\mathcal{M}_2 \longrightarrow \mathrm{CN}(\alpha) \longrightarrow \mathcal{M}_3 \xrightarrow{\bar{\eta}_3} \mathcal{H}$$

sea $\bar{\eta}_2 \circ \bar{\beta}^0$, es decir, tal que $\bar{\eta}_3$ hace el diagrama conmutativo (aunque no es necesariamente inyectivo). Sea $\nu : \mathcal{M}_3 \longrightarrow \mathcal{K}$ un monomorfismo en un módulo inyectivo. Definimos $\mathcal{I}_3^0 = \mathcal{H} \oplus \mathcal{K}$, $\mathcal{I}_2^0 = \mathcal{I} \oplus \mathcal{K}$, $\eta_3 = (\bar{\eta}_3, \nu) : \mathcal{M}_3 \longrightarrow \mathcal{I}_3^0$, $\eta_2 = (\bar{\eta}_2, \beta \circ \nu) : \mathcal{M}_2 \longrightarrow \mathcal{I}_2^0$, $\alpha^0 = (\bar{\alpha}^0, 0) : \mathcal{I}_1^0 \longrightarrow \mathcal{I}_2^0$, $\beta^0 = (\bar{\beta}^0, 1) : \mathcal{I}_2^0 \longrightarrow \mathcal{I}_3^0$. Ahora el diagrama siguiente es conmutativo con filas y columnas exactas:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{M}_1 \arrow[r, "\alpha"] \arrow[d, "\eta_1"'] & \mathcal{M}_2 \arrow[r, "\beta"] \arrow[d, "\eta_2"'] & \mathcal{M}_3 \arrow[r] \arrow[d, "\eta_3"'] & 0 \\
0 \arrow[r] & \mathcal{I}_1^0 \arrow[r, "\alpha^0"'] & \mathcal{I}_2^0 \arrow[r, "\beta^0"'] & \mathcal{I}_3^0 \arrow[r] & 0
\end{tikzcd}$$

Los módulos $\mathcal{I}_i^0$ son inyectivos porque es evidente que la suma directa de módulos inyectivos es inyectiva, y también es claro que $\mathcal{I}_2^0 \cong \mathcal{I}_1^0 \oplus \mathcal{I}_3^0$, de modo que α^0 y β^0 se corresponden con la inmersión y la proyección natural.

Sea ahora $\mathcal{G}_i = \mathrm{CN}(\eta_i)$, para $i = 1, 2, 3$. El diagrama anterior nos da una sucesión exacta

$$0 \longrightarrow \mathcal{G}_1 \xrightarrow{\bar{\alpha}} \mathcal{G}_2 \xrightarrow{\bar{\beta}} \mathcal{G}_3 \longrightarrow 0.$$

Repitiendo todo el argumento anterior obtenemos un diagrama conmutativo con filas y columnas exactas

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{G}_1 \arrow[r, "\bar{\alpha}"] \arrow[d, "\bar{\delta}_1"'] & \mathcal{G}_2 \arrow[r, "\bar{\beta}"] \arrow[d, "\bar{\delta}_2"'] & \mathcal{G}_3 \arrow[r] \arrow[d, "\bar{\delta}_3"'] & 0 \\
0 \arrow[r] & \mathcal{I}_1^1 \arrow[r, "\bar{\alpha}_1"'] & \mathcal{I}_2^1 \arrow[r, "\bar{\beta}_1"'] & \mathcal{I}_3^1 \arrow[r] & 0
\end{tikzcd}$$

Llamando δ_i^0 a las composiciones $\mathcal{I}_i^0 \longrightarrow \mathcal{G}_i \xrightarrow{\bar{\delta}_i} \mathcal{I}_i^1$ obtenemos un peldaño más del trío de sucesiones exactas del enunciado del teorema. El proceso se puede repetir indefinidamente para obtener las sucesiones exactas completas. ■

Nota Supongamos que partimos de un diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}_1 \arrow[r] \arrow[d, "\phi_1"'] & \mathcal{M}_1 \arrow[r] \arrow[d, "\phi_2"'] & \mathcal{M}_3 \arrow[r] \arrow[d, "\phi_3"'] & 0 \\
0 \arrow[r] & \mathcal{M}_1' \arrow[r] & \mathcal{M}_2' \arrow[r] & \mathcal{M}_3' \arrow[r] & 0
\end{tikzcd}$$

con filas exactas. Entonces existe un diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & (\mathcal{I}_1^i)_i \arrow[r] \arrow[d] & (\mathcal{I}_2^i)_i \arrow[r] \arrow[d] & (\mathcal{I}_3^i)_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (\mathcal{I}_1'^i)_i \arrow[r] & (\mathcal{I}_2'^i)_i \arrow[r] & (\mathcal{I}_3'^i)_i \arrow[r] & 0
\end{tikzcd}$$

donde las filas son las resoluciones inyectivas construidas en el teorema anterior para las dos filas del diagrama de partida (donde entendemos que $\mathcal{I}_j^{-1} = \mathcal{M}_j$). En efecto, consideremos el diagrama siguiente, donde falta definir los homomorfismos ϕ_1^0, $\bar{\phi}_2^0$ y $\bar{\phi}_3^0$.

$$\begin{tikzcd}
 & \mathcal{M}_1' \arrow[rr, "\alpha'"] \arrow[dd, "\eta_1'"] & & \mathcal{M}_2' \arrow[rr, "\beta'"] \arrow[dd, "\bar{\eta}_2'"] & & \mathcal{M}_3' \arrow[dd, "\bar{\eta}_3'"] \\
\mathcal{M}_1 \arrow[ur, "\phi_1"] \arrow[rr, "\alpha"] \arrow[dd, "\eta_1"'] & & \mathcal{M}_2 \arrow[ur, "\phi_2"] \arrow[rr, "\beta"] \arrow[dd, "\bar{\eta}_2"] & & \mathcal{M}_3 \arrow[ur, "\phi_3"] \arrow[dd, "\bar{\eta}_3"] & \\
 & \mathcal{I}_1'^0 \arrow[rr, "\bar{\alpha}_0'"'] & & \mathcal{I}' \arrow[rr, "\bar{\beta}'^0"'] & & \mathcal{H}' \\
\mathcal{I}_1^0 \arrow[ur, "\phi_1^0"] \arrow[rr, "\bar{\alpha}^0"'] & & \mathcal{I} \arrow[ur, "\bar{\phi}_2^0"] \arrow[rr, "\bar{\beta}^0"'] & & \mathcal{H} \arrow[ur, "\bar{\phi}_3^0"] &
\end{tikzcd}$$

La inyectividad de η_1 nos permite tomar ϕ_1^0 que haga conmutativa la cara izquierda del diagrama. Entonces $(\phi_2, \phi_1^0) : \mathcal{M}_2 \oplus \mathcal{I}_1^0 \longrightarrow \mathcal{M}_2' \oplus \mathcal{I}_1'^0$ induce un homomorfismo $\mathcal{G} \longrightarrow \mathcal{G}'$, a partir del cual podemos tomar un homomorfismo $\bar{\phi}_2^0 : \mathcal{I} \longrightarrow \mathcal{I}'$ que haga conmutativo el diagrama

$$\begin{tikzcd}
\mathcal{G} \arrow[r] \arrow[d] & \mathcal{I} \arrow[d] \\
\mathcal{G}' \arrow[r] & \mathcal{I}'
\end{tikzcd}$$

Las definiciones de $\bar{\alpha}^0$ y $\bar{\eta}_2$ implican inmediatamente que tanto la cara inferior izquierda como la cara central del diagrama son conmutativas. Las filas del diagrama forman sucesiones exactas cortas, por lo que existe un $\bar{\phi}_3^0$ que hace conmutativa la cara inferior derecha. La exactitud de las filas implica también la conmutatividad de la cara derecha. Por último tomamos un homomorfismo $\mathcal{K} \longrightarrow \mathcal{K}'$ que conmute con ϕ_3, ν y ν'. Es fácil definir entonces homomorfismos ϕ_2^0 y ϕ_3^0 de forma obvia que hacen conmutativo el diagrama que resulta de sustituir $\mathcal{I}$, $\mathcal{K}$, $\mathcal{I}'$, $\mathcal{K}'$ por $\mathcal{I}_0^2$, $\mathcal{I}_0^3$, $\mathcal{I}_0'^2$, $\mathcal{I}_0'^2$. La continuación del argumento del teorema no presenta ninguna dificultad. ■

La prueba anterior es "dualizable", en el sentido de que sigue siendo válida si invertimos el sentido de todas las flechas, salvo por el hecho de que el dual del teorema 1.29 sólo lo tenemos demostrado para categorías de módulos sobre un anillo. Vamos a enunciar el teorema dual en este contexto, aunque es válido (con la misma prueba) para cualquier categoría de $\mathcal{O}_X$-módulos que tenga "suficientes proyectivos", en el sentido de que todo $\mathcal{O}_X$-módulo sea imagen de un $\mathcal{O}_X$-módulos proyectivo. Demostraremos el teorema como ilustración de lo que supone dualizar un argumento, pero ya no volveremos a demostrar teoremas duales de teoremas ya demostrados:

Teorema 1.40 *Sea A un anillo y*

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

una sucesión exacta de A-módulos. Entonces existen sendas resoluciones proyectivas $(P_j^i)_i$, para $j = 1, 2, 3$, tales que $P_2^i = P_1^i \oplus P_3^i$ y el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
\cdots \arrow[r] & P_1^1 \arrow[r] \arrow[d] & P_1^0 \arrow[r] \arrow[d] & M_1 \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_2^1 \arrow[r] \arrow[d] & P_2^0 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & P_3^1 \arrow[r] & P_3^0 \arrow[r] & M_3 \arrow[r] & 0
\end{tikzcd}$$

donde las flechas verticales son los homomorfismos naturales

$$0 \longrightarrow P_1^i \longrightarrow P_1^1 \oplus P_3^i \longrightarrow P_3^i \longrightarrow 0.$$

Demostración: Sea $\eta_3 : P_3^0 \longrightarrow M_3$ un epimorfismo, donde P_3^0 es un A-módulo proyectivo y consideremos el homomorfismo

$$\beta - \eta_3 : M_2 + P_3^0 \longrightarrow M_3.$$

Sea $G = \mathrm{N}(\beta - \eta_3)$ y sea $P \longrightarrow G$ un epimorfismo con P proyectivo. Definimos $\bar{\beta}^0$ como la composición $P \longrightarrow G \longrightarrow M_2 \oplus P_3^0 \longrightarrow P_3^0$ y $\bar{\eta}_2$ como la composición $P \longrightarrow G \longrightarrow M_2 \oplus P_3^0 \longrightarrow M_2$.

Observemos que ambos homomorfismos son suprayectivos. Por ejemplo, si tomamos $f \in P_3^0$, entonces $\eta_3(f) = \beta(m)$, para cierto $m \in M_2$, de modo que $(m, f) \in G$, por lo que tiene una antiimagen $p \in P$ que cumple $\bar{\beta}^0(p) = f$.

Por el teorema 1.32 tenemos que $P = \mathrm{N}(\bar{\beta}^0) \oplus \mathrm{Im}\,\bar{\beta}^0$. Llamemos $H = \mathrm{N}(\bar{\beta}^0)$ y sea $\bar{\alpha}_0 : H \longrightarrow P$ la inyección canónica. Es inmediato que todo sumando directo de un módulo proyectivo es proyectivo, luego $\mathcal{H}$ es proyectivo. Tenemos la situación siguiente:

$$\begin{tikzcd}
 & & 0 & 0 & \\
0 \arrow[r] & M_1 \arrow[r, "\alpha"] & M_2 \arrow[r, "\beta"] \arrow[u] & M_3 \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & H \arrow[r, "\bar{\alpha}^0"'] & P \arrow[r, "\bar{\beta}^0"'] \arrow[u, "\bar{\eta}_2"'] & P_3^0 \arrow[r] \arrow[u, "\eta_3"'] & 0
\end{tikzcd}$$

donde el cuadrado es conmutativo y las filas y columnas son exactas. Como $\mathrm{Im}(\bar{\beta}^0 \circ \bar{\eta}_2) \subset \mathrm{N}\,\beta$, podemos definir un homomorfismo $\bar{\eta}_1 : H \longrightarrow M_1$ que haga el cuadrado conmutativo (aunque no es necesariamente suprayectivo).

Sea $\nu : K \longrightarrow M_1$ un epimorfismo con K proyectivo. Definimos $P_1^0 = H \oplus K$, $P_2^0 = P \oplus K$, $\eta_1 = \bar{\eta}_1 + \nu : P_1^0 \longrightarrow M_1$, $\eta_2 = \bar{\eta}_2 + \beta \circ \nu : P_2^0 \longrightarrow M_2$, $\beta^0 = \bar{\beta}^0 : P_2^0 \longrightarrow P_3^0$, $\alpha^0 = \bar{\alpha}^0 + 1 : P_1^0 \longrightarrow P_2^0$. Ahora el diagrama siguiente es conmutativo con filas y columnas exactas:

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[u] & M_2 \arrow[r, "\beta"] \arrow[u] & M_3 \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & P_1^0 \arrow[r, "\alpha^0"'] \arrow[u, "\eta_1"'] & P_2^0 \arrow[r, "\beta^0"'] \arrow[u, "\eta_2"'] & P_3^0 \arrow[r] \arrow[u, "\eta_3"'] & 0
\end{tikzcd}$$

Los módulos P_i^0 son proyectivos porque es evidente que la suma directa de módulos proyectivos es proyectiva, y también es claro que $P_2^0 \cong P_1^0 \oplus P_3^0$, de modo que α^0 y β^0 se corresponden con la inmersión y la proyección natural.

La sucesión se prolonga dualizando los argumentos del teorema anterior tal y como hemos venido haciendo hasta ahora. ■

Nota Igualmente se demuestra la versión dual de la nota posterior a 1.39. ■

La característica principal de las resoluciones inyectivas y proyectivas es que permiten extender homomorfismos de módulos a homomorfismos de complejos, tal y como prueba el teorema siguiente. Lo demostramos para resoluciones inyectivas, pero su dual para resoluciones proyectivas se demuestra sin dificultad:

Teorema 1.41 *Si X es un espacio anillado, $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo de $\mathcal{O}_X$-módulos y $(\mathcal{I}_i)$, $(\mathcal{J}_i)$ son resoluciones de $\mathcal{M}$ y $\mathcal{N}$ respectivamente, con $\mathcal{J}$ inyectiva, entonces α se extiende a un homomorfismo entre ambas resoluciones, y dos extensiones cualesquiera son homotópicas.*

Demostración: Hemos de construir homomorfismos $\alpha^i : \mathcal{I}^i \longrightarrow \mathcal{J}^i$ que hagan conmutativo el diagrama

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r, "\eta"] \arrow[d, "\alpha"'] & \mathcal{I}^0 \arrow[r, "\delta^0"] \arrow[d, "\alpha^0"'] & \mathcal{I}^1 \arrow[r, "\delta^1"] \arrow[d, "\alpha^1"'] & \mathcal{I}^2 \arrow[r] \arrow[d, "\alpha^2"'] & \cdots \\
0 \arrow[r] & \mathcal{N} \arrow[r, "\eta'"'] & \mathcal{J}^0 \arrow[r, "\delta'^0"'] & \mathcal{J}^1 \arrow[r, "\delta'^1"'] & \mathcal{J}^2 \arrow[r] & \cdots
\end{tikzcd}$$

Obtenemos α_0 por la inyectividad de $\mathcal{J}^0$, luego obtenemos α_1 por la inyectividad de $\mathcal{J}^1$ aplicada al monomorfismo $\mathrm{CN}(\eta) \longrightarrow \mathcal{I}^1$ y al homomorfismo $\mathrm{CN}(\eta) \longrightarrow \mathcal{J}^1$ inducido por $\alpha_0 \circ \delta_0'$, y así sucesivamente.

Supongamos ahora que tenemos otra sucesión de homomorfismos (α'^i). Definimos $\Delta^{-1} = 0$, con lo que hemos de construir homomorfismos $\Delta^i : \mathcal{I}^{i+1} \longrightarrow \mathcal{J}^i$ tales que

$$\alpha^0 - \alpha'^0 = \delta^0\Delta^0 \quad \text{y} \quad \alpha^i - \alpha'^i = \Delta^{i-1}\delta'^{i-1} + \delta^i\Delta^i \quad \text{para } i \geq 1.$$

En primer lugar, obtenemos Δ^0 aplicando la inyectividad de $\mathcal{J}^0$ al monomorfismo $\mathrm{CN}(\eta) \longrightarrow \mathcal{J}^0$ y el homomorfismo $\mathrm{CN}(\eta) \longrightarrow \mathcal{J}^0$ inducido por $\alpha^0 - \alpha'^0$. A continuación observamos que

$$\delta^0(\alpha^1 - \alpha'^1 - \Delta^0\delta'^0) = \delta^0\alpha^1 - \delta^0\alpha'^1 - (\alpha^0 - \alpha'^0)\delta'^0 = 0,$$

luego $\alpha^1 - \alpha'^1 - \Delta^0\delta'^0$ induce un homomorfismo $\mathrm{CN}(\delta^0) \longrightarrow \mathcal{J}^1$. La inyectividad de $\mathcal{J}^1$ nos da entonces Δ^1 tal que $\alpha^1 - \alpha'^1 - \Delta^0\delta'^0 = \delta^1\Delta^1$. La construcción puede prolongarse así indefinidamente. ■

1.7 Funtores derivados

Llegamos finalmente al objetivo de este capítulo: la definición de la sucesión de funtores derivados de un funtor dado, que ha de ser exacto por la izquierda o por la derecha. Consideramos en primer lugar el caso de un funtor covariante

$F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$, donde X e Y son espacios anillados. Para cada $\mathcal{O}_X$-módulo $\mathcal{M}$, podemos considerar una resolución inyectiva

$$0 \longrightarrow \mathcal{M} \xrightarrow{\eta} \mathcal{I}^0 \xrightarrow{d_0} \mathcal{I}^1 \xrightarrow{d_1} \mathcal{I}^2 \xrightarrow{d_2} \cdots$$

Si eliminamos a $\mathcal{M}$ tenemos el *complejo reducido:*

$$0 \longrightarrow \mathcal{I}^0 \xrightarrow{d_0} \mathcal{I}^1 \xrightarrow{d_1} \mathcal{I}^2 \xrightarrow{d_2} \cdots$$

que ya no es exacto en $\mathcal{I}^0$. Si ahora aplicamos F, obtenemos un complejo de $\mathcal{O}_Y$-módulos

$$0 \longrightarrow F\mathcal{I}^0 \xrightarrow{Fd_0} F\mathcal{I}^1 \xrightarrow{Fd_1} F\mathcal{I}^2 \xrightarrow{Fd_2} \cdots$$

que ya no tiene por qué ser exacto en ningún sitio. Para cada $n \geq 0$, definimos $D^nF(\mathcal{M})$ como el n-simo grupo de cohomología de este complejo. Hemos de demostrar que este $\mathcal{O}_Y$-módulo no depende (salvo isomorfismo) de la elección de la resolución inyectiva, pero antes consideremos otro $\mathcal{O}_X$-módulo $\mathcal{N}$, con otra resolución inyectiva,

$$0 \longrightarrow \mathcal{N} \xrightarrow{\eta'} \mathcal{J}^0 \xrightarrow{d'_0} \mathcal{J}^1 \xrightarrow{d'_1} \mathcal{J}^2 \xrightarrow{d'_2} \cdots$$

y un homomorfismo $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$. Por el teorema 1.41, α se extiende a un homomorfismo de complejos

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r, "\eta"] \arrow[d, "\alpha"'] & \mathcal{I}^0 \arrow[r, "d_0"] \arrow[d, "\alpha^0"'] & \mathcal{I}^1 \arrow[r, "d_1"] \arrow[d, "\alpha^1"'] & \mathcal{I}^2 \arrow[r] \arrow[d, "\alpha^2"'] & \cdots \\
0 \arrow[r] & \mathcal{N} \arrow[r, "\eta'"'] & \mathcal{J}^0 \arrow[r, "d'_0"'] & \mathcal{J}^1 \arrow[r, "d'_1"'] & \mathcal{J}^2 \arrow[r] & \cdots
\end{tikzcd}$$

en el que podemos eliminar $\mathcal{M}$ y $\mathcal{N}$ para obtener un homomorfismo entre los complejos reducidos y luego aplicar F. Así obtenemos el homomorfismo

$$\begin{tikzcd}
0 \arrow[r] & F\mathcal{I}^0 \arrow[r, "Fd_0"] \arrow[d, "F\alpha^0"'] & F\mathcal{I}^1 \arrow[r, "Fd_1"] \arrow[d, "F\alpha^1"'] & F\mathcal{I}^2 \arrow[r] \arrow[d, "F\alpha^2"'] & \cdots \\
0 \arrow[r] & F\mathcal{J}^0 \arrow[r, "Fd'_0"'] & F\mathcal{J}^1 \arrow[r, "Fd'_1"'] & F\mathcal{J}^2 \arrow[r] & \cdots
\end{tikzcd}$$

De acuerdo con el teorema 1.34, llamamos $D^nF(\alpha) : D^nF(\mathcal{M}) \longrightarrow D^nF(\mathcal{N})$ al homomorfismo inducido sobre los grupos de cohomología. También hemos de demostrar que este homomorfismo no depende de la elección de las resoluciones inyectivas ni de la extensión de α.

Empezamos suponiendo que tenemos dos extensiones de α, digamos (α^i) y (α'^i), con lo que el teorema 1.41 nos da una homotopía entre ellas:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r, "\eta"] \arrow[d, "\alpha"'] & \mathcal{I}^0 \arrow[r, "d_0"] \arrow[d, shift right, "\alpha^0"'] \arrow[d, shift left, "\alpha'^0"] \arrow[dl, "\Delta^{-1}"'] & \mathcal{I}^1 \arrow[r, "d_1"] \arrow[d, shift right, "\alpha^1"'] \arrow[d, shift left, "\alpha'^1"] \arrow[dl, "\Delta^0"'] & \mathcal{I}^2 \arrow[r] \arrow[d, shift right, "\alpha^2"'] \arrow[d, shift left, "\alpha'^2"] \arrow[dl, "\Delta^1"'] & \cdots \\
0 \arrow[r] & \mathcal{N} \arrow[r, "\eta'"'] & \mathcal{J}^0 \arrow[r, "d'_0"'] & \mathcal{J}^1 \arrow[r, "d'_1"'] & \mathcal{J}^2 \arrow[r] & \cdots
\end{tikzcd}$$

En la demostración de 1.41 se ve que podemos tomar $\Delta^{-1} = 0$, por lo que seguimos teniendo una homotopía al reducir los complejos, y es evidente que F transforma dicha homotopía en una homotopía entre los homomorfismos $(F\alpha^i)$ y $(F\alpha'^i)$, luego ambos inducen el mismo homomorfismo $D^nF(\alpha)$.

Observemos ahora que si tenemos una sucesión $\mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P}$ y fijamos sendas resoluciones inyectivas de los tres módulos, al componer una extensión de α con una de β obtenemos una extensión de $\alpha\beta$, por lo que, usando ésta para hacer los cálculos, vemos que

$$D^nF(\alpha\beta) = D^nF(\alpha)D^nF(\beta).$$

Por otra parte, si fijamos una resolución inyectiva $(\mathcal{I}^i)$ de un módulo $\mathcal{M}$, entonces una extensión de la identidad en $\mathcal{M}$ está formada por las identidades en los módulos $\mathcal{I}^i$, de donde deducimos que $D^nF(1) = 1$.

Combinando estos dos hechos, concluimos que si $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$ es un isomorfismo entre dos módulos y tomamos resoluciones inyectivas arbitrarias de cada uno de ellos, entonces los homomorfismos $D^nF(\alpha)$ son isomorfismos, ya que cumplen

$$D^nF(\alpha)D^nF(\alpha^{-1}) = D^nF(1) = 1, \quad D^nF(\alpha^{-1})D^nF(\alpha) = D^nF(1) = 1.$$

En particular, tomando $\mathcal{M} = \mathcal{N}$, concluimos que distintas resoluciones inyectivas de un mismo módulo $\mathcal{M}$ dan lugar a grupos $D^nF(\mathcal{M})$ isomorfos, que es lo que queríamos probar.

Definición 1.42 Si X e Y son espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es un funtor covariante exacto por la izquierda, se llama *funtor derivado (derecho) n-simo* de F al funtor $D^nF : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ que acabamos de construir.[4]

En la construcción de los funtores derivados no hemos usado en ningún momento que F sea exacto por la izquierda (hemos usado las propiedades que da el teorema 1.22, pero todas ellas las tienen también los funtores exactos por la derecha). La razón por la que esta construcción tiene interés especialmente en el caso de funtores exactos por la izquierda es el teorema siguiente:

Teorema 1.43 *Si X e Y son espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es un funtor covariante exacto por la izquierda, para cada $\mathcal{O}_X$-módulo $\mathcal{M}$ existe un isomorfismo natural $D^0F(\mathcal{M}) \cong F\mathcal{M}$, de modo que si $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo de $\mathcal{O}_X$-módulos, el diagrama siguiente es conmutativo:*

$$\begin{tikzcd} F\mathcal{M} \arrow[r, "F\alpha"] \arrow[d] & F\mathcal{N} \arrow[d] \\ D^0F(\mathcal{M}) \arrow[r, "D^0F(\alpha)"] & D^0F(\mathcal{N}) \end{tikzcd}$$

[4]En realidad $D^nF(\mathcal{M})$ sólo está definido salvo isomorfismo, pero esto es un tecnicismo sin ninguna trascendencia en la teoría que vamos a desarrollar.

Demostración: Para calcular $D^0F(\mathcal{M})$ partimos de una resolución inyectiva

$$0 \longrightarrow \mathcal{M} \xrightarrow{\eta} \mathcal{I}^0 \xrightarrow{d_0} \mathcal{I}^1 \xrightarrow{d_1} \mathcal{I}^2 \xrightarrow{d_2} \cdots$$

Aplicando F a la sucesión exacta

$$0 \longrightarrow \mathcal{M} \xrightarrow{\eta} \mathcal{I}^0 \xrightarrow{d_0} \operatorname{Im} d_0 \longrightarrow 0$$

obtenemos una sucesión exacta

$$0 \longrightarrow F\mathcal{M} \xrightarrow{F\eta} F\mathcal{I}^0 \xrightarrow{Fd_0} F \operatorname{Im} d_0.$$

Por otra parte, $D^0F(\mathcal{M})$ se obtiene a partir del complejo

$$0 \longrightarrow F\mathcal{I}^0 \xrightarrow{Fd_0} F\mathcal{I}^1 \longrightarrow \cdots$$

En definitiva, tenemos que $D^0F(\mathcal{M}) = \mathrm{N}(Fd_0) = \operatorname{Im}(F\eta) \cong F\mathcal{M}$. Concretamente, el isomorfismo no es más que $F\eta : F\mathcal{M} \longrightarrow D^0F(\mathcal{M})$. Teniendo esto en cuenta, la conmutatividad del diagrama del enunciado es trivial. ■

En suma, que el funtor derivado D^0F es esencialmente el propio F. A su vez, esto tiene interés a causa de la conexión entre los funtores derivados que proporciona el teorema siguiente:

Teorema 1.44 *Si X e Y son espacios anillados, $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es un funtor covariante exacto por la izquierda y $0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$ es una sucesión exacta de $\mathcal{O}_X$-módulos, entonces existen homomorfismos de $\mathcal{O}_Y$-módulos $\delta^n : D^nF(\mathcal{P}) \longrightarrow D^{n+1}F(\mathcal{M})$ que forman una sucesión exacta*

$$0 \longrightarrow D^0F(\mathcal{M}) \xrightarrow{D^0F\alpha} D^0F(\mathcal{N}) \xrightarrow{D^0F\beta} D^0F(\mathcal{P})$$

$$\xrightarrow{\delta^0} D^1F(\mathcal{M}) \xrightarrow{D^1F\alpha} D^1F(\mathcal{N}) \xrightarrow{D^1F\beta} D^1F(\mathcal{P}) \xrightarrow{\delta^1} \cdots$$

Demostración: Consideramos las resoluciones inyectivas dadas por el teorema 1.39. Los tres complejos reducidos forman una sucesión exacta:

$$0 \longrightarrow \mathcal{I}_1^n \longrightarrow \mathcal{I}_1^n \oplus \mathcal{I}_3^n \longrightarrow \mathcal{I}_3^n \longrightarrow 0,$$

donde los homomorfismos son la inyección y la proyección canónicas. Al aplicar F obtenemos una nueva sucesión exacta de complejos:

$$0 \longrightarrow F\mathcal{I}_1^n \longrightarrow F\mathcal{I}_1^n \oplus F\mathcal{I}_3^n \longrightarrow F\mathcal{I}_3^n \longrightarrow 0,$$

a la que podemos aplicar el teorema 1.36. ■

Nota Observemos que si partimos de un diagrama conmutativo

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{M} \arrow[r] \arrow[d] & \mathcal{N} \arrow[r] \arrow[d] & \mathcal{P} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathcal{M}' \arrow[r] & \mathcal{N}' \arrow[r] & \mathcal{P}' \arrow[r] & 0 \end{tikzcd}$$

con filas exactas, aplicando la nota posterior a 1.39 y luego la nota posterior a 1.36, concluimos que los homomorfismos inducidos por las flechas verticales entre los grupos de cohomología conmutan con los homomorfismos de conexión dados por el teorema o, lo que es lo mismo, que determinan un homomorfismo entre las sucesiones exactas largas correspondientes a cada una de las filas del diagrama. ■

Combinando los dos teoremas precedentes vemos que si tenemos un funtor covariante $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ exacto por la izquierda y

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$$

es una sucesión exacta de $\mathcal{O}_X$-módulos, entonces tenemos una sucesión exacta de $\mathcal{O}_Y$-módulos

$$0 \longrightarrow F\mathcal{M} \xrightarrow{F\alpha} F\mathcal{N} \xrightarrow{F\beta} F\mathcal{P} \xrightarrow{\delta^1} D^1F\mathcal{M} \longrightarrow D^1F\mathcal{N} \longrightarrow D^1F\mathcal{P} \longrightarrow \cdots,$$

de modo que los funtores derivados "completan" la inexactitud de F. Es claro entonces que si $D^1F = 0$ entonces F es exacto. Más aún, es fácil ver que los funtores exactos cumplen que $D^nF = 0$ para todo $n \geq 1$.

Observemos ahora que si $\mathcal{I}$ es un $\mathcal{O}_X$-módulo inyectivo, entonces una resolución inyectiva de $\mathcal{I}$ es simplemente

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{I} \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

Al reducir la resolución y aplicar F obtenemos

$$0 \longrightarrow F\mathcal{I} \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

de donde concluimos que $D^nF(\mathcal{I}) = 0$ para $i \geq 1$.

Aunque hemos definido los funtores derivados en términos de módulos inyectivos, a la hora de hacer cálculos concretos, éstos no son fáciles de manejar explícitamente, pero a continuación demostramos que es posible sustituirlos por otros que puedan ser más convenientes.

Definición 1.45 Sean X e Y espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ un funtor covariante exacto por la izquierda. Un $\mathcal{O}_X$-módulo $\mathcal{M}$ es *acíclico* para F si $D^nF(\mathcal{M}) = 0$ para todo $i \geq 1$.

Así, acabamos de probar que los $\mathcal{O}_X$-módulos inyectivos son acíclicos para cualquier funtor.

Una *resolución acíclica* de $\mathcal{M}$ (para un funtor F) es una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{I}^0 \longrightarrow \mathcal{I}^1 \longrightarrow \mathcal{I}^2 \longrightarrow \cdots$$

tal que todos los módulos $\mathcal{I}^i$ son acíclicos.

Teorema 1.46 *Si X e Y son espacios anillados y $F : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ es un funtor exacto por la izquierda, los funtores derivados de F pueden calcularse a partir de cualquier resolución acíclica de un $\mathcal{O}_X$-módulo $\mathcal{M}$ dado, no necesariamente inyectiva.*

Demostración: Consideremos una resolución acíclica

$$0 \longrightarrow \mathcal{M} \xrightarrow{\epsilon} \mathcal{I}^0 \xrightarrow{d_0} \mathcal{I}^1 \xrightarrow{d_1} \mathcal{I}^2 \xrightarrow{d_2} \cdots$$

Calcular los funtores derivados con ella significa pasar al complejo

$$0 \longrightarrow F\mathcal{I}^0 \xrightarrow{Fd_0} F\mathcal{I}^1 \xrightarrow{Fd_1} F\mathcal{I}^2 \xrightarrow{Fd_2} \cdots$$

y calcular

$$\mathcal{F}^0 = \mathrm{N}\, F(d_0), \quad \mathcal{F}^i = \mathrm{N}\, F(d_i)/\operatorname{Im} Fd_{i-1}, \text{ para } i \geq 1.$$

Hemos de probar que $\mathcal{F}^i \cong D^iF(\mathcal{M})$ para $i \geq 0$. El mismo argumento empleado en el teorema 1.43 prueba que $\mathcal{F}^0 \cong F\mathcal{M} \cong D^0F(\mathcal{M})$, luego nos queda probar el isomorfismo para $i \geq 1$.

Sea $\mathcal{N}^i = \mathrm{N}(d_i)$. Tenemos una sucesión exacta

$$0 \longrightarrow \mathcal{N}^{i-1} \longrightarrow \mathcal{I}^{i-1} \xrightarrow{d_{i-1}} \mathcal{N}^i \longrightarrow 0,$$

de la que obtenemos una sucesión exacta

$$0 \longrightarrow D^0F(\mathcal{N}^{i-1}) \xrightarrow{\alpha} D^0F(\mathcal{I}^{i-1}) \xrightarrow{\beta} D^0F(\mathcal{N}^i) \xrightarrow{\delta} D^1F(\mathcal{N}^{i-1}) \longrightarrow 0,$$

así como isomorfismos $D^jF(\mathcal{N}^i) \cong D^{j+1}F(\mathcal{N}^{i-1})$, para $j \geq 1$.

Así pues, para $i \geq 1$,

$$D^iF(\mathcal{M}) \cong D^iF(\mathcal{N}^0) \cong D^{i-1}F(\mathcal{N}^1) \cong \cdots \cong D^1F(\mathcal{N}^{i-1}) \cong D^0F(\mathcal{N}^i)/\operatorname{Im}\beta.$$

Por otra parte, consideramos el diagrama conmutativo

$$\begin{tikzcd}
& D^0F(\mathcal{N}^{i-1}) \arrow[dr, "\alpha"] & & & \\
D^0F(\mathcal{I}^{i-2}) \arrow[ur] \arrow[rr, "D^0F(d_{i-2})"] & & D^0F(\mathcal{I}^{i-1}) \arrow[rr, "D^0F(d_{i-1})"] \arrow[dr, "\beta"'] & & D^0F(\mathcal{I}^i) \\
& & & D^0F(\mathcal{N}^i) \arrow[ur, "\alpha'"'] &
\end{tikzcd}$$

donde convenimos que $\mathcal{I}^{-1} = \mathcal{M}$ y $d_{-1} = \epsilon$. Sabemos que α es inyectiva, y también lo es α', pues es el homomorfismo análogo a α con i en lugar de $i-1$. Así pues,

$$\operatorname{Im}\beta \cong \operatorname{Im} D^0F(d_{i-1}), \qquad \operatorname{Im}\alpha \cong \operatorname{N} D^0F(d_{i-1}).$$

Ahora bien, el segundo isomorfismo es válido también cambiando α por α' e $i-1$ por i, de modo que α' determina un isomorfismo entre $D^0F(\mathcal{N}^i)$ y $\operatorname{N} D^0F(d_i)$, que se restringe a un isomorfismo entre $\operatorname{Im}\beta$ e $\operatorname{Im} D^0F(d_{i-1})$. Consecuentemente,

$$\begin{aligned} D^iF(\mathcal{M}) &\cong D^0F(\mathcal{N}^i)/\operatorname{Im}\beta \cong \operatorname{N} D^0F(d_i) \,/\, \operatorname{Im} D^0F(d_{i-1}) \\ &\cong \operatorname{N} F(d_i)/\operatorname{Im} F(d_{i-1}) \cong \mathcal{F}^i. \end{aligned}$$

■

Definición 1.47 Si X e Y son espacios anillados y $F : \operatorname{Mod}(X) \longrightarrow \operatorname{Mod}(Y)$ es un funtor contravariante exacto por la derecha, sus *funtores derivados (izquierdos)* I^nF se definen de forma completamente análoga a los funtores derivados derechos de un funtor covariante exacto por la izquierda. La única diferencia es que al aplicar F a una resolución inyectiva de un módulo pasamos a un complejo directo, pero esto no afecta en nada a ninguno de los argumentos que hemos empleado y todos los resultados siguen siendo válidos. Los funtores I^nF son ahora contravariantes, como F.

Por el contrario, los *funtores derivados izquierdos* de un funtor covariante exacto por la derecha y los *funtores derivados derechos* de un funtor contravariante exacto por la izquierda han de definirse con resoluciones proyectivas en lugar de inyectivas, por lo que sólo existen en la medida en que la categoría $\operatorname{Mod}(X)$ tenga suficientes proyectivos. En particular, podemos definirlos para funtores sobre la categoría de los módulos sobre un anillo.

1.8 Caracterización axiomática

Podría pensarse que la construcción de los funtores derivados de un funtor dado es un tanto caprichosa o arbitraria, pero en esta sección demostraremos que estos funtores están completamente determinados por sus propiedades fundamentales, de modo que la forma concreta de construirlos pasa a ser irrelevante. El primer paso para aislar estas propiedades fundamentales que determinan a los funtores derivados es definir con precisión la noción de "homomorfismo de conexión" que aparece implícita en el teorema 1.44:

Definición 1.48 Sean X e Y dos espacios anillados y $(T^n)_{n\geq 0}$ una sucesión de funtores covariantes $T^n : \operatorname{Mod}(X) \longrightarrow \operatorname{Mod}(Y)$. Un *homomorfismo de conexión derecho* para dicha sucesión es una aplicación que a cada sucesión exacta

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$$

de $\mathcal{O}_X$-módulos le hace corresponder una sucesión de homomorfismos de $\mathcal{O}_Y$-módulos $\delta_n : T^n\mathcal{P} \longrightarrow T^{n+1}\mathcal{M}$ tales que la sucesión

$$0 \longrightarrow T^0\mathcal{M} \xrightarrow{T^0\alpha} T^0\mathcal{M} \xrightarrow{T^0\beta} T^0\mathcal{P} \xrightarrow{\delta_0} T^1\mathcal{M} \xrightarrow{T^1\alpha} T^1\mathcal{N} \xrightarrow{T^1\beta} T^1\mathcal{P} \xrightarrow{\delta_1} \cdots$$

es exacta y, para todo homomorfismo de sucesiones exactas

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r, "\alpha"] \arrow[d, "\phi"] & \mathcal{N} \arrow[r, "\beta"] \arrow[d, "\chi"] & \mathcal{P} \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & \mathcal{M}' \arrow[r, "\alpha'"'] & \mathcal{N}' \arrow[r, "\beta'"'] & \mathcal{P}' \arrow[r] & 0
\end{tikzcd}$$

el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & T^0\mathcal{M} \arrow[r, "T^0\alpha"] \arrow[d, "T^0\phi"] & T^0\mathcal{N} \arrow[r, "T^0\beta"] \arrow[d, "T^0\chi"] & T^0\mathcal{P} \arrow[r, "\delta_0"] \arrow[d, "T^0\psi"] & T^1\mathcal{M} \arrow[r] \arrow[d, "T^1\phi"] & \cdots \\
0 \arrow[r] & T^0\mathcal{M} \arrow[r, "T^0\alpha"] & T^0\mathcal{N} \arrow[r, "T^0\beta"] & T^0\mathcal{P} \arrow[r, "\delta_0"] & T^1\mathcal{M} \arrow[r] & \cdots
\end{tikzcd}$$

Los homomorfismos de conexión izquierdos se definen análogamente, salvo que las sucesiones exactas largas forman complejos directos en lugar de inversos. Así mismo se definen de forma obvia los homomorfismos de conexión derechos e izquierdos de una familia de funtores contravariantes.

El teorema 1.44 y la nota posterior demuestran que los funtores derivados derechos de un funtor covariante exacto por la izquierda tienen un homomorfismo de conexión derecha, y lo mismo es válido *mutatis mutandis* en los otros tres casos posibles.

El siguiente elemento que necesitamos es la noción de isomorfismo entre dos funtores. Más en general:

Definición 1.49 Sean X e Y dos espacios anillados y consideremos dos funtores covariantes T, $T' : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$. Una *transformación natural* $\eta : T \longrightarrow T'$ es una aplicación que a cada $\mathcal{O}_X$-módulo $\mathcal{M}$ le asigna un homomorfismo de $\mathcal{O}_Y$-módulos $\eta_{\mathcal{M}} : T\mathcal{M} \longrightarrow T'\mathcal{M}$ de modo que si $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo de $\mathcal{O}_X$-módulos el diagrama siguiente es conmutativo:

$$\begin{tikzcd}
T\mathcal{M} \arrow[r, "\eta_{\mathcal{M}}"] \arrow[d, "T\alpha"'] & T'\mathcal{M} \arrow[d, "T'\alpha"] \\
T\mathcal{N} \arrow[r, "\eta_{\mathcal{N}}"'] & T'\mathcal{N}
\end{tikzcd}$$

Si los homomorfismos $\eta_{\mathcal{M}}$ son isomorfismos diremos que η es un *isomorfismo*[5] entre los dos funtores. La composición de transformaciones naturales se define

[5] Los isomorfismos de funtores se llaman también *equivalencias naturales,* y cuando dos funtores son isomorfos se dice también que son *naturalmente equivalentes.*

de forma obvia, así como la transformación identidad de un funtor en sí mismo. Es fácil ver que η es un isomorfismo si y sólo si existe $\eta^{-1} : T' \longrightarrow T$ tal que $\eta \circ \eta^{-1} = 1_T$ y $\eta^{-1} \circ \eta = 1_{T'}$.

Las transformaciones naturales entre dos funtores contravariantes se definen sin más que invertir el sentido de las flechas verticales (no de las horizontales) en el diagrama conmutativo anterior.

Por ejemplo, en estos términos, el teorema 1.43 afirma que D^0F es isomorfo a F. Ahora podemos dar la definición que recoge la propiedad que nos proponemos demostrar para los funtores derivados:

Diremos que una sucesión de funtores $(T^n)_{n\geq 0}$ dotada de un homomorfismo de conexión por la derecha es *universal* si cuando $(T'^n)_{n\geq 0}$ es otra sucesión de funtores (de la misma varianza) dotada también de un homomorfismo de conexión y $\eta_0 : T^0 \longrightarrow T'^0$ es una transformación natural, existe una única sucesión de transformaciones naturales $\eta_n : T^n \longrightarrow T'^n$ (que empieza con el η_0 dado) tal que, para cada sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0,$$

los diagramas siguientes son conmutativos:

$$\begin{tikzcd}
T^n\mathcal{P} \arrow[r, "\delta_n"] \arrow[d, "\eta_{n\mathcal{P}}"'] & T^{n+1}\mathcal{M} \arrow[d, "\eta_{n+1\mathcal{M}}"] \\
T'^n\mathcal{P} \arrow[r, "\delta'_n"'] & T'^{n+1}\mathcal{M}
\end{tikzcd}$$

La definición se adapta de forma obvia al caso en que los homomorfismos de conexión son izquierdos.

Observemos que si (T^n) y (T'^n) son dos sucesiones universales de funtores dotados de un homomorfismo de conexión y $\eta_0 : T^0 \longrightarrow T'^0$ es un isomorfismo, entonces todas las transformaciones naturales $\eta_n : T^n \longrightarrow T'^n$ son isomorfismos, cuyos inversos son las transformaciones naturales η_n^{-1} obtenidas a partir de η_0^{-1} por la universalidad de (T'_n). En efecto, se comprueba inmediatamente que las transformaciones naturales $\eta_n \circ \eta_n^{-1}$ cumplen la definición anterior para la identidad $T^0 \longrightarrow T^0$, luego por la unicidad ha de ser $\eta_n \circ \eta_n^{-1} = 1$, e igualmente $\eta_n^{-1} \circ \eta_n = 1$.

Esto significa que en un sistema $(T^n)_{n\geq 0}$ universal, tanto los funtores T^n, para $n \geq 1$, como el homomorfismo de conexión, están completamente determinados (salvo isomorfismo) por el funtor T^0. Los funtores $(T^n)_{n\geq 1}$ se llaman *satélites* de T^0. El teorema que vamos a probar es una condición suficiente para que un sistema de funtores sea universal.

Teorema 1.50 *Sean X e Y dos espacios anillados y $(T^n)_{n\geq 0}$ una sucesión de funtores covariantes $T^n : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ dotada de un homomorfismo* *de conexión derecho. Supongamos que para cada $\mathcal{O}_X$-módulo $\mathcal{M}$ y cada $n \geq 1$ existe un monomorfismo $\mathcal{M} \longrightarrow \mathcal{I}$, donde $\mathcal{I}$ es un $\mathcal{O}_X$-módulo tal que $T^n\mathcal{I} = 0$. Entonces la sucesión dada es universal.*

Demostración: Sea $(T'^n)_{n\geq 0}$ otra sucesión de funtores covariantes dotada también de un homomorfismo de conexión derecho y sea $\eta_0 : T^0 \longrightarrow T'^0$ una transformación natural.

Dado un $\mathcal{O}_X$-módulo $\mathcal{M}$, podemos formar una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{I} \longrightarrow \mathcal{C} \longrightarrow 0,$$

donde $T^1\mathcal{I} = 0$ y $\mathcal{C} = \mathcal{I}/\mathcal{M}$. A partir de ella obtenemos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & T^0\mathcal{M} \arrow[r] \arrow[d, "\eta_{0\mathcal{M}}"'] & T^0\mathcal{I} \arrow[r] \arrow[d, "\eta_{0\mathcal{I}}"'] & T^0\mathcal{C} \arrow[r, "\delta_1"] \arrow[d, "\eta_{0\mathcal{C}}"'] & T^1\mathcal{M} \arrow[r] \arrow[d, dashed, "\eta_{1\mathcal{M}}"'] & 0 \\
0 \arrow[r] & T'^0\mathcal{M} \arrow[r] & T'^0\mathcal{I} \arrow[r] & T'^0\mathcal{C} \arrow[r, "\delta'_1"'] & T'^1\mathcal{M} \arrow[r] & T'^1\mathcal{I}
\end{tikzcd}$$

Es claro que existe un único homomorfismo $\eta_{1\mathcal{M}} : T^1\mathcal{M} \longrightarrow T'^1\mathcal{M}$ que hace conmutativo el último cuadrado.

Observemos que el funtor T^0 es exacto por la izquierda, lo que nos permite aplicar esto en particular al caso en que (T'^n) es la sucesión de funtores derivados de T^0 y η_0 es el isomorfismo natural. Entonces las tres primeras flechas verticales del diagrama anterior son isomorfismos y es claro que la cuarta es, al menos, un monomorfismo. Si, más en particular, aplicamos esto al caso en que $\mathcal{M}$ es un $\mathcal{O}_X$-módulo inyectivo, entonces $T'^1\mathcal{M} = 0$, luego también $T^1\mathcal{M} = 0$.

Así pues, hemos probado que T^1 se anula sobre los módulos inyectivos. Por consiguiente, podemos volver a empezar tomando como $\mathcal{I}$ un módulo inyectivo.

En el caso particular en que (T'^n) sea la sucesión de funtores derivados de T^0, ahora tenemos que $T'^1\mathcal{I} = 0$, luego el diagrama anterior nos da que $\eta_{1\mathcal{M}}$ es un isomorfismo.

Consideremos ahora un homomorfismo de $\mathcal{O}_X$-módulos $\alpha : \mathcal{M} \longrightarrow \mathcal{N}$. Sumergiendo ambos en sendos módulos inyectivos obtenemos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r] \arrow[d, "\alpha"'] & \mathcal{I} \arrow[r] \arrow[d] & \mathcal{C} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{N} \arrow[r] & \mathcal{I}' \arrow[r] & \mathcal{C}' \arrow[r] & 0
\end{tikzcd}$$

(El homomorfismo $\mathcal{I} \longrightarrow \mathcal{I}'$ se obtiene por la inyectividad de $\mathcal{I}'$, que a su vez induce un homomorfismo entre los cocientes $\mathcal{C}$ y $\mathcal{C}'$.)

Ahora tenemos los dos diagramas conmutativos correspondientes a la construcción de $\eta_{1\mathcal{M}}$ y $\eta_{1\mathcal{N}}$ así como los dos diagramas conmutativos correspondientes a la definición de homomorfismo de conexión y al homomorfismo α. Todos ellos se combinan en un diagrama en forma de tres cubos yuxtapuestos, cuyas caras comunes conmutan, además, por la naturalidad de η_0. De ahí se sigue fácilmente la conmutatividad de la última cara, que es

$$\begin{tikzcd}
T^1\mathcal{M} \arrow[r, "T^1\alpha"] \arrow[d, "\eta_{1\mathcal{M}}"'] & T^1\mathcal{N} \arrow[d, "\eta_{1\mathcal{N}}"] \\
T'^1\mathcal{M} \arrow[r, "T'^1\alpha"'] & T'^1\mathcal{N}
\end{tikzcd}$$

Si aplicamos esto en particular cuando α es la identidad en $\mathcal{M}$ vemos que $\eta_{1\mathcal{M}}$ no depende de la elección del módulo inyectivo $\mathcal{I}$, luego tenemos una transformación natural bien definida $\eta_1 : T^1 \longrightarrow T'^1$ que, por construcción, es la única que conmuta con ciertos homomorfismos de conexión (los asociados a inmersiones de un módulo dado en un módulo inyectivo). Si probamos que conmuta con todos los homomorfismos de conexión, obviamente será la única que lo haga.

Fijemos, pues una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0$$

y consideremos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M} \arrow[r] \arrow[d, "1"'] & \mathcal{N} \arrow[r] \arrow[d, "\phi"'] & \mathcal{P} \arrow[r] \arrow[d, "\chi"'] & 0 \\
0 \arrow[r] & \mathcal{M} \arrow[r] & \mathcal{I} \arrow[r] & \mathcal{C} \arrow[r] & 0
\end{tikzcd}$$

donde $\mathcal{I}$ es un $\mathcal{O}_X$-módulo inyectivo. De él obtenemos a su vez el diagrama

$$\begin{tikzcd}
T^0\mathcal{P} \arrow[r, "T^0\chi"] \arrow[d, "\eta_{0\mathcal{P}}"'] & T^0\mathcal{C} \arrow[r, "\delta_0"] \arrow[d, "\eta_{0\mathcal{C}}"'] & T^1\mathcal{M} \arrow[d, "\eta_{1\mathcal{M}}"'] \\
T'^0\mathcal{P} \arrow[r, "T'^0\chi"'] & T'^0\mathcal{C} \arrow[r, "\delta'_0"'] & T'^1\mathcal{M}
\end{tikzcd}$$

El primer cuadrado conmuta por la naturalidad de η_0, mientras que el segundo conmuta por la construcción de η_1. Por otra parte, la definición de homomorfismo de conexión aplicada al homomorfismo $(1, \phi, \chi)$ de sucesiones exactas nos da que las composiciones de las dos filas del diagrama anterior son precisamente los homomorfismos de conexión para la sucesión exacta de partida. Esto termina la construcción de η_1. Ahora procedemos por inducción y suponemos construidas transformaciones naturales $\eta_0, \ldots, \eta_n$ que conmuten con los homomorfismos de conexión. También podemos suponer que los funtores $T^1, \ldots, T^n$ son isomorfos a los funtores derivados de T^0.

Fijado un $\mathcal{O}_X$-módulo $\mathcal{M}$, formamos nuevamente una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{I} \longrightarrow \mathcal{C} \longrightarrow 0,$$

donde $T^{n+1}\mathcal{I} = 0$ y $\mathcal{C} = \mathcal{I}/\mathcal{M}$, de la que deducimos el diagrama conmutativo

$$\begin{tikzcd}
T^n\mathcal{I} \arrow[r] \arrow[d, "\eta_{n\mathcal{I}}"'] & T^n\mathcal{C} \arrow[r, "\delta_n"] \arrow[d, "\eta_{n\mathcal{C}}"'] & T^{n+1}\mathcal{M} \arrow[r] \arrow[d, dashed, "\eta_{n+1\mathcal{M}}"'] & 0 \\
T'^n\mathcal{I} \arrow[r] & T'^n\mathcal{C} \arrow[r, "\delta'_{n+1}"'] & T'^{n+1}\mathcal{M} \arrow[r] & T'^{n+1}\mathcal{I}
\end{tikzcd}$$

que nos da un homomorfismo $\eta_{n+1\mathcal{M}}$, el único que conmuta con los homomorfismos de conexión.

En el caso particular en que (T'_n) es la sucesión de los funtores derivados de T^0, tenemos, por hipótesis de inducción, que $\eta_{n\mathcal{C}}$ es un isomorfismo, por lo que $\eta_{n+1\mathcal{M}}$ es un monomorfismo, y si $\mathcal{M}$ es inyectivo resulta que $T^{n+1}\mathcal{M} = 0$. Empezamos de nuevo tomando $\mathcal{I}$ inyectivo, y entonces $T^n\mathcal{I} = 0$ en el diagrama anterior. Todas las comprobaciones que faltan son más sencillas que las que hemos hecho en el caso $n = 0$. ■

Este teorema implica, en particular, que si T es un funtor covariante exacto por la izquierda, entonces la sucesión de sus funtores derivados es universal, la única sucesión universal con T^0 isomorfo a T.

Nota La prueba del teorema anterior se adapta de forma obvia al caso de una sucesión de funtores contravariantes con un homomorfismo de conexión izquierdo, mientras que los otros dos casos posibles (funtores covariantes con homomorfismo de conexión izquierdo y contravariantes con homomorfismo de conexión derecho) requieren que la categoría tenga suficientes proyectivos, lo cual se cumple, en particular, en el caso de categorías de módulos sobre un anillo. ■

Capítulo II

Ejemplos de funtores derivados

En este capítulo construiremos tres familias de funtores derivados: los funtores Tor, los funtores de cohomología y los funtores Ext. En las últimas secciones mostraremos que las cohomologías clásicas de la topología algebraica y la geometría diferencial son casos particulares de los funtores de cohomología que definimos aquí, y como aplicación demostraremos la versión fuerte del teorema de De Rham.

2.1 Los funtores Tor

Consideremos el funtor covariante

$$\otimes_A N : \mathrm{Mod}(A) \longrightarrow \mathrm{Mod}(A)$$

que a cada A-módulo M le asigna el A-módulo $M \otimes_A N$ y a cada homomorfismo de A-módulos $\phi : M \longrightarrow M'$ le asigna $\phi \otimes 1 : M \otimes_A N \longrightarrow M' \otimes_A N$. Vamos a probar que es exacto por la derecha:

Teorema 2.1 *Si A es un anillo, N es un A-módulo y*

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

es una sucesión exacta de A-módulos, entonces también es exacta la sucesión

$$M' \otimes_A N \xrightarrow{\alpha\otimes 1} M \otimes_A N \xrightarrow{\beta\otimes 1} M'' \otimes_A N \longrightarrow 0.$$

Demostración: Lo único que no es obvio es que $\mathrm{N}(\beta \otimes 1) \subset \mathrm{Im}(\alpha \otimes 1)$. Basta probar que $\mathrm{N}(\beta\otimes 1)$ está generado por los tensores de la forma $m\otimes n$ con $m \in \mathrm{N}\,\beta$, pues todos ellos tienen antiimagen en $M' \otimes_A N$. En efecto, llamemos

D al submódulo generado por estos tensores y sea $p : M \otimes_A N \longrightarrow (M \otimes_A N)/D$ la proyección. Podemos definir una aplicación bilineal

$$M'' \times N \longrightarrow (M \otimes_A N)/D$$

mediante $(m'', n) \mapsto p(m \otimes n)$, donde $\beta(m) = m''$. Es fácil ver que esta bien definida, y se extiende a un homomorfismo

$$\psi : M'' \otimes_A N \longrightarrow (M \otimes_A N)/D.$$

Claramente, $p = (\beta \otimes 1) \circ \psi$, de donde se sigue inmediatamente que el núcleo de $\beta \otimes 1$ está contenido en D. La otra inclusión es obvia. ■

Definición 2.2 Si A es un anillo y N es un A-módulo, llamamos $\mathrm{Tor}_n^A(-, N)$ a los funtores derivados izquierdos del funtor $\otimes_A N$.

Explícitamente, si

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

es una resolución proyectiva de un A-módulo M, entonces $\mathrm{Tor}_n^A(M, N)$ es el n-simo grupo de homología del complejo

$$\cdots \longrightarrow P_2 \otimes_A N \longrightarrow P_1 \otimes_A N \longrightarrow P_0 \otimes_A N \longrightarrow 0.$$

Sabemos que $\mathrm{Tor}_0^A(M, N) \cong M \otimes_A N$ y que cada sucesión exacta corta de A-módulos

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

da lugar a una sucesión exacta larga

$$\cdots \longrightarrow \mathrm{Tor}_1^A(M'', N) \longrightarrow M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0.$$

En este punto se plantea de forma natural una cuestión: podemos considerar el funtor $M\otimes_A$, que tiene las mismas características que $\otimes_A N$ (por la conmutatividad del producto tensorial), con el cual podemos definir los funtores derivados derechos $\mathrm{Tor}_n^A(M, -)$, lo que nos da dos definiciones distintas para $\mathrm{Tor}_n^A(M, N)$. Vamos a probar que en realidad nos llevan al mismo módulo.

Para ello observamos en primer lugar que si L es un A-módulo libre, entonces el funtor $L\otimes_A$ es exacto. Ello se debe a que, si B es una base de L, entonces $L \cong A^B$ (la suma directa de tantas copias de A como elementos tiene B), de donde se sigue que $L \otimes_A M \cong M^B$, lo que nos da fácilmente un isomorfismo entre el funtor $L\otimes_A$ y el funtor $M \mapsto M^B$, claramente exacto.

Fijemos ahora una resolución libre

$$\cdots \longrightarrow L_2 \longrightarrow L_1 \longrightarrow L_0 \longrightarrow N \longrightarrow 0$$

de un A-módulo N y, para cada A-módulo M, llamamos T^nM al n-simo grupo de homología del complejo

$$\cdots \longrightarrow M \otimes_A L_2 \longrightarrow M \otimes_A L_1 \longrightarrow M \otimes_A L_0 \longrightarrow 0.$$

Cada homomorfismo de módulos $\phi : M \longrightarrow M'$ induce obviamente un homomorfismo de complejos $M \otimes_A (L_i) \longrightarrow M' \otimes_A (L_i)$ que a su vez induce homomorfismos $T^n\phi : T^nM \longrightarrow T^nM'$, de modo que $T^n : \mathrm{Mod}(A) \longrightarrow \mathrm{Mod}(A)$ es un funtor covariante.

Observemos que T^nM no es sino el funtor $\mathrm{Tor}_n^A(M, -)$ actuando sobre N, por lo que si probamos que $T^n = \mathrm{Tor}_n^A(-, N)$, habremos probado que $\mathrm{Tor}_n^A(M, N)$ es el mismo, tanto si se calcula mediante una resolución de M como si se calcula con una resolución de N.

Vamos a aplicar la versión dual del teorema 1.50. Veamos en primer lugar que los funtores T^n tienen un homomorfismo de conexión. En efecto, si

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

es una sucesión exacta, el hecho de que los módulos L_i sean libres hace que también sea exacta la sucesión de complejos

$$0 \longrightarrow M' \otimes_A (L_i) \longrightarrow M \otimes_A (L_i) \longrightarrow M'' \otimes_A (L_i) \longrightarrow 0,$$

y esta sucesión da lugar a una sucesión exacta larga entre los grupos de homología, que son los módulos T^nM', T^nM y T^nM''. También es obvio que un homomorfismo entre dos sucesiones exactas cortas induce un homomorfismo entre las sucesiones exactas de complejos que, a su vez, induce un isomorfismo entre las sucesiones de homología. También es evidente que $T^nL = 0$ cuando L es libre y $n \geq 1$, luego la familia (T^n) es universal. Sólo falta probar que $T^0 \cong \otimes_A N$. Para ello aplicamos a la sucesión exacta

$$L_1 \xrightarrow{\partial_0} L_0 \xrightarrow{\epsilon} N \longrightarrow 0$$

la exactitud de $M\otimes_A$, que nos da una sucesión exacta

$$M \otimes_A L_1 \xrightarrow{1\otimes\partial_0} M \otimes_A L_0 \xrightarrow{1\otimes\epsilon} M \otimes_A N \longrightarrow 0.$$

Tenemos que $T^0M = (M \otimes_A L_0)/\,\mathrm{Im}(1 \otimes \partial_0) \cong M \otimes_A N$, y el isomorfismo es el inducido por $1 \otimes \epsilon$, lo que implica fácilmente que se trata de un isomorfismo de funtores. ■

Como consecuencia obtenemos la conmutatividad de Tor:

Teorema 2.3 *Sea A un anillo y M y N dos A-módulos. Entonces*

$$\mathrm{Tor}_n^A(M, N) \cong \mathrm{Tor}_n^A(N, M).$$

DEMOSTRACIÓN: Es claro que $\mathrm{Tor}_n^A(M, N)$, calculado con una resolución proyectiva de M, es isomorfo a $\mathrm{Tor}_n^A(N, M)$ calculado también con una resolución de M, pero hemos visto que no importa qué resolución proyectiva se calcula. ■

Por ejemplo, ahora es claro que el funtor $\otimes_A P$ es exacto cuando P es proyectivo, pues $\mathrm{Tor}_1^A(P, N) = 0$ para todo A-módulo N.

2.2 Grupos de cohomología

Sea X un espacio anillado. Ahora vamos a estudiar los funtores derivados del funtor covariante

$$\Gamma(X, -) : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X))$$

dado por $\Gamma(X, \mathcal{M}) = \mathcal{M}(X)$ y que a cada homomorfismo de funtores $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ le asigna el homomorfismo $\phi_X : \mathcal{M}(X) \longrightarrow \mathcal{N}(X)$.

En la página 22 hemos probado que es exacto por la izquierda. Sus funtores derivados se representan por $H^n(X, -)$. Para cada $\mathcal{O}_X$-módulo $\mathcal{M}$, los $\mathcal{O}_X(X)$-módulos $H^n(X, \mathcal{M})$ se llaman *grupos de cohomología* de $\mathcal{M}$.

Explícitamente, para calcularlos partimos de una resolución inyectiva

$$0 \longrightarrow \mathcal{M} \xrightarrow{\eta} \mathcal{I}^0 \xrightarrow{d_0} \mathcal{I}^1 \xrightarrow{d_1} \mathcal{I}^2 \xrightarrow{d_2} \cdots$$

la reducimos eliminando $\mathcal{M}$ y pasamos al complejo

$$0 \longrightarrow \mathcal{I}^0(X) \xrightarrow{d_{0X}} \mathcal{I}^1(X) \xrightarrow{d_{1X}} \mathcal{I}^2(X) \xrightarrow{d_{2X}} \cdots$$

Entonces $H^n(X, \mathcal{M}) = \mathrm{N}\, d_{nX} / \operatorname{Im} d_{n-1X}$.

Notemos que si U es un abierto en X podríamos considerar el funtor $\Gamma(U, -)$ en lugar de $\Gamma(X, -)$, que claramente es también exacto por la izquierda, pero es fácil ver que los $\mathcal{O}_X(U)$-módulos que obtendríamos de esta manera no son sino $H^n(U, \mathcal{M}) = H^n(U, \mathcal{M}|_U)$. En efecto, basta tomar como resolución inyectiva de $\mathcal{M}|_U$ la resolución

$$0 \longrightarrow \mathcal{M}|_U \xrightarrow{\eta|_U} \mathcal{I}^0|_U \xrightarrow{d_0|_U} \mathcal{I}^1|_U \xrightarrow{d_1|_U} \mathcal{I}^2|_U \xrightarrow{d_2|_U} \cdots$$

y la igualdad es inmediata.

Vamos a introducir ahora una familia de módulos acíclicos mucho más manejable que la de los módulos inyectivos:

Definición 2.4 Si X es un espacio anillado, diremos que un $\mathcal{O}_X$-módulo $\mathcal{M}$ es *diseminado* si para todo par de abiertos $U \subset V \subset X$ se cumple que la restricción $\rho_U^V : \mathcal{M}(V) \longrightarrow \mathcal{M}(U)$ es suprayectiva.

Observemos que para que X sea diseminado basta con que sean suprayectivas las restricciones ρ_U^X. En primer lugar probamos que esta familia incluye a la de los módulos inyectivos:

Teorema 2.5 *Si X es un espacio anillado, todo $\mathcal{O}_X$-módulo inyectivo es diseminado.*

Demostración: Sea U un abierto en X y consideremos el prehaz $\mathcal{F}_U^-$ en X dado por

$$\mathcal{F}_U^-(W) = \begin{cases} \mathcal{O}_X(W) & \text{si } W \subset U, \\ 0 & \text{en otro caso,} \end{cases}$$

con las restricciones obvias. Llamemos $\mathcal{F}_U$ a su compleción. Es inmediato que si $P \in X$, entonces

$$\mathcal{F}_{U,P} = \begin{cases} \mathcal{O}_{X,P} & \text{si } P \in U, \\ 0 & \text{en otro caso.} \end{cases}$$

Si $U \subset V \subset X$, tenemos un homomorfismo natural $\mathcal{F}_U^- \longrightarrow \mathcal{F}_V^-$, que se extiende a un homomorfismo de haces $i : \mathcal{F}_U \longrightarrow \mathcal{F}_V$. Es claro que si $P \in U$ entonces $i_P = 1$, mientras que si $P \in X \setminus U$ entonces $i_P = 0$, pero en ambos casos i_P es inyectivo, luego i es inyectivo.

Por otra parte, $\mathcal{F}_U^-$ tiene una estructura natural de $\mathcal{O}_X$-módulo, luego $\mathcal{F}_U$ también la tiene.

Si $\mathcal{I}$ es un $\mathcal{O}_X$-módulo arbitrario y $f \in \mathcal{I}(U)$, podemos definir un homomorfismo $\phi_f : \mathcal{F}_U^- \longrightarrow \mathcal{I}$ mediante

$$\phi_{f,W}(a) = \begin{cases} af|_W & \text{si } W \subset U, \\ 0 & \text{en otro caso.} \end{cases}$$

Así, si $P \in X$ se cumple que

$$\phi_{f,P}(1) = \begin{cases} f_P & \text{si } P \in U, \\ 0 & \text{en otro caso.} \end{cases}$$

La compleción $\phi_f^+ : \mathcal{F}_U \longrightarrow \mathcal{I}$ cumple esto mismo, de donde se sigue que $\phi_{f,U}^+(1) = f$.

Si $\mathcal{I}$ es inyectivo podemos extender ϕ_f^+ a un homomorfismo $\phi_V : \mathcal{F}_V \longrightarrow \mathcal{I}$. Sea $g = \phi_V(1) \in \mathcal{I}(V)$. Entonces

$$g|_U = \phi_V(1)|_U = \phi_U(1) = \phi_U(i_U(1)) = \phi_{f,U}^+(1) = f.$$

Por lo tanto la restricción es suprayectiva. ■

Ahora vamos a demostrar que los módulos diseminados son acíclicos. Necesitamos algunos resultados previos:

Teorema 2.6 *Sea X un espacio anillado y $0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$ una sucesión exacta de $\mathcal{O}_X$-módulos. Si $\mathcal{M}$ es diseminado, la sucesión*

$$0 \longrightarrow \mathcal{M}(X) \xrightarrow{\alpha_X} \mathcal{N}(X) \xrightarrow{\beta_X} \mathcal{P}(X) \longrightarrow 0$$

también es exacta.

Demostración: La sucesión $0 \longrightarrow \mathcal{M}(X) \longrightarrow \mathcal{N}(X) \longrightarrow \mathcal{P}(X)$ es exacta (para un módulo $\mathcal{M}$ arbitrario) por la exactitud izquierda de $\Gamma(X, -)$ Basta probar que β_X es suprayectivo.

Fijemos $u \in \mathcal{P}(X)$ y sea Σ el conjunto de los pares (V, t), donde V es un abierto en X y $t \in \mathcal{N}(V)$ cumple $\beta_V(t) = u|_V$. Definimos en Σ el orden parcial dado por $(V, t) \leq (V', t')$ si $V \subset V'$ y $t'|_V = t$. Obviamente $(\varnothing, 0) \in \Sigma$ y, por el lema de Zorn, Σ tiene un elemento maximal (U, t). Basta probar que $U = X$.

En caso contrario existe $P \in X \setminus U$. Como β_P es suprayectiva, existe un entorno V de P y un $t' \in \mathcal{N}(V)$ tal que $\beta_V(t') = u|_V$. Entonces $t|_{U\cap V} - t'|_{U\cap V}$ está en el núcleo de $\beta_{U\cap V}$ y la sucesión

$$0 \longrightarrow \mathcal{M}(U \cap V) \longrightarrow \mathcal{N}(U \cap V) \longrightarrow \mathcal{P}(U \cap V)$$

es exacta por el mismo motivo que para X. Existe, pues, un $s \in \mathcal{M}(U \cap V)$ tal que $t|_{U\cap V} - t'|_{U\cap V} = \alpha_{U\cap V}(s)$. Como $\mathcal{M}$ es diseminado, existe un $s' \in \mathcal{M}(X)$ tal que $s = s'|_{U\cap V}$. Ahora definimos $\bar{t} \in \mathcal{N}(U \cup V)$ por $\bar{t}|_U = t$ y $\bar{t}|_V = t' + \alpha_V(s'|_V)$. Es claro entonces que $(U \cup V, \bar{t})$ contradice la maximalidad de (U, t). ■

Teorema 2.7 *Si X es un espacio anillado y $0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0$ es una sucesión exacta de $\mathcal{O}_X$-módulos donde $\mathcal{M}$ y $\mathcal{N}$ son diseminados, entonces $\mathcal{P}$ también lo es.*

DEMOSTRACIÓN: Si $U \subset V$ son dos abiertos de X, tenemos el siguiente diagrama conmutativo, en el que las filas son exactas por el teorema anterior (observemos que la restricción de un módulo diseminado es trivialmente diseminada):

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{M}(V) \arrow[r] \arrow[d] & \mathcal{N}(V) \arrow[r] \arrow[d] & \mathcal{P}(V) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{M}(U) \arrow[r] & \mathcal{N}(U) \arrow[r] & \mathcal{P}(U) \arrow[r] & 0
\end{tikzcd}$$

El hecho de que la restricción en $\mathcal{N}$ sea suprayectiva implica ahora que también lo es la de $\mathcal{P}$. ■

Teorema 2.8 *Si X es un espacio anillado, todo $\mathcal{O}_X$-módulo diseminado es acíclico.*

DEMOSTRACIÓN: Sea $\mathcal{M} \longrightarrow \mathcal{I}$ un monomorfismo en un módulo inyectivo y formemos una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{I} \longrightarrow \mathcal{J} \longrightarrow 0.$$

Los teoremas anteriores nos dan que tanto $\mathcal{I}$ como $\mathcal{J}$ son diseminados, así como que tenemos una sucesión exacta

$$0 \longrightarrow \mathcal{M}(X) \longrightarrow \mathcal{I}(X) \longrightarrow \mathcal{J}(X) \longrightarrow 0.$$

Por otra parte, sabemos que $H^i(X, \mathcal{I}) = 0$ para todo $i \geq 1$. La sucesión exacta larga de homología implica entonces que $H^1(X, \mathcal{M}) = 0$, así como que $H^i(X, \mathcal{M}) \cong H^{i-1}(X, \mathcal{J})$. De aquí se sigue inductivamente que todos los grupos de cohomología (menos el primero) son nulos. ■

Esto tiene una consecuencia notable, y es que los grupos de cohomología $H^n(X, \mathcal{M})$ no dependen de la estructura de espacio anillado que estemos considerando en X, sino únicamente de su estructura topológica. En efecto, dado un espacio anillado $(X, \mathcal{O}_X)$, podemos considerar también a X como espacio anillado con el haz constante $\mathbb{Z}_X$, de modo que todo $\mathcal{O}_X$-módulo $\mathcal{M}$ es también un $\mathbb{Z}_X$-módulo. Ahora bien, $\mathcal{M}$ es diseminado como $\mathcal{O}_X$-módulo si y sólo si lo es como $\mathbb{Z}_X$-módulo. Por consiguiente, una resolución inyectiva de $\mathcal{M}$ como $\mathcal{O}_X$-módulo sigue siendo una resolución diseminada de $\mathcal{M}$ como $\mathbb{Z}_X$-módulo, luego, al aplicarle el funtor $\Gamma(X, -)$, los grupos de cohomología del complejo resultante son los grupos $H^n(X, \mathcal{M})$ considerando indistintamente a $\mathcal{M}$ como $\mathcal{O}_X$-módulo o como $\mathbb{Z}_X$-módulo.

También tenemos que los homomorfismos entre los grupos de cohomología son independientes de la estructura algebraica de $\mathcal{M}$, aunque para probarlo hemos de recurrir a la propiedad universal de los funtores derivados. En efecto, tenemos que $\mathrm{Mod}(X, \mathcal{O}_X) \subset \mathrm{Mod}(X, \mathbb{Z}_X)$, luego en $\mathrm{Mod}(X, \mathcal{O}_X)$ podemos considerar las dos familias de funtores $H^n(X, -)$, según consideremos a los módulos de $\mathrm{Mod}(X, \mathcal{O}_X)$ como $\mathcal{O}_X$-módulos o como $\mathbb{Z}_X$-módulos (hemos probado que ambas familias de funtores coinciden sobre los módulos, pero nos falta probar que coinciden sobre los homomorfismos). Ambas familias están dotadas de sendos homomorfismos de conexión, ambas se anulan (para $n \geq 1$) sobre los $\mathcal{O}_X$-módulos diseminados, luego ambas son universales. Puesto que obviamente coinciden (incluso en los homomorfismos) para $n = 0$, concluimos que son isomorfas.

Desde otro punto de vista, para cada haz de grupos abelianos $\mathcal{M}$ sobre el espacio topológico X, hemos definido los grupos de cohomología $H^n(X, \mathcal{M})$, que son grupos abelianos, pero si $\mathcal{M}$ tiene una estructura adicional de $\mathcal{O}_X$-módulo para cierto haz de anillos $\mathcal{O}_X$ sobre X, entonces los grupos $H^n(X, \mathcal{M})$ heredan una estructura de $\mathcal{O}_X(X)$-módulo.

2.3 Módulos localmente libres

Antes de estudiar los funtores Ext en la sección siguiente conviene demostrar algunos resultados sobre módulos localmente libres y su relación con los módulos de homomorfismos.

Si X es un espacio anillado y $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, en el capítulo anterior hemos visto que el conjunto $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$ tiene una estructura natural de $\mathcal{O}_X(X)$-módulo.

Notemos ahora que podemos definir un $\mathcal{O}_X$-módulo $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$ que a cada abierto $U \subset X$ le asigna el $\mathcal{O}_X(U)$-módulo

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})(U) = \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{M}|_U, \mathcal{N}|_U),$$

con las restricciones naturales. (Se comprueba sin dificultad que ciertamente es un haz.)

Un homomorfismo $\alpha : \mathcal{O}_X \longrightarrow \mathcal{M}$ de $\mathcal{O}_X$-módulos está completamente determinado por $\alpha_X(1) \in \mathcal{M}(X)$, de donde se sigue inmediatamente que

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{M}) \cong \mathcal{M}(X),$$

y esto a su vez implica que, para todo $\mathcal{O}_X$-módulo $\mathcal{M}$,

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{M}) \cong \mathcal{M}.$$

Definimos el $\mathcal{O}_X$-módulo *dual* de un $\mathcal{O}_X$-módulo $\mathcal{M}$ como

$$\mathcal{M}^* = \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{O}_X).$$

Hemos probado que $\mathcal{O}_X^* \cong \mathcal{O}_X$.

Diremos que un $\mathcal{O}_X$-módulo $\mathcal{L}$ es *libre* de rango $n \geq 0$ si es isomorfo a $\mathcal{O}_X^n$ (la suma directa de n copias de $\mathcal{O}_X$). Notemos que el rango de $\mathcal{L}$ coincide con el rango de $\mathcal{L}(X)$ como $\mathcal{O}_X(X)$-módulo (libre), luego está completamente determinado por $\mathcal{L}$. Diremos que $\mathcal{L}$ es *localmente libre* (de rango n) si todo punto $P \in X$ tiene un entorno abierto U tal que $\mathcal{L}|_U$ es libre (de rango n). En tal caso, los abiertos $U \subset X$ tales que $\mathcal{L}|_U$ es libre forman una base de X.

Es inmediato que si $\mathcal{L}_1$ es localmente libre de rango r y $\mathcal{L}_2$ es localmente libre de rango s, entonces $\mathcal{L}_1 \oplus \mathcal{L}_2$ es localmente libre de rango $r+s$, y $\mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$ es localmente libre de rango rs.

Veamos que si $\mathcal{L}$ es un $\mathcal{O}_X$-módulo localmente libre de rango r, entonces $\mathcal{L}^*$ también lo es. En efecto: si $U \subset X$ es un abierto tal que $\mathcal{L}|_U \cong \mathcal{O}_U^r$, entonces

$$\mathcal{L}^*|_U = (\mathcal{L}|_U)^* \cong (\mathcal{O}_U^r)^* = \mathcal{H}\mathrm{om}_{\mathcal{O}_U}(\mathcal{O}_U^r, \mathcal{O}_U) \cong \mathcal{O}_U^r,$$

pues un homomorfismo $\mathcal{O}_U^r \longrightarrow \mathcal{O}_U$ está completamente determinado por la imagen de la base canónica de $\mathcal{O}_U^r(U) = \mathcal{O}_U(U)^r$. ■

Teorema 2.9 *Si X es un espacio anillado y $\mathcal{L}$ es un $\mathcal{O}_X$-módulo localmente libre de rango finito, entonces $\mathcal{L}^{**} \cong \mathcal{L}$.*

Demostración: Construyamos un homomorfismo $\phi : \mathcal{L} \longrightarrow \mathcal{L}^{**}$. Para ello fijamos un abierto $U \subset X$ y definimos $\phi_U : \mathcal{L}(U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}^*|_U, \mathcal{O}_X|_U)$. Para ello fijamos un $s \in \mathcal{L}(U)$ y hemos de definir $\phi_U(s) : \mathcal{L}^*|_U \longrightarrow \mathcal{O}_X|_U$. Para ello fijamos un abierto $V \subset U$ y hemos de definir un homomorfismo

$$\phi_U(s)_V : \mathrm{Hom}_{\mathcal{O}_V}(\mathcal{L}|_V, \mathcal{O}_X|_V) \longrightarrow \mathcal{O}_X(V).$$

Si $\alpha : \mathcal{L}|_V \longrightarrow \mathcal{O}_X|_V$, definimos $\phi_U(s)_V(\alpha) = \alpha_V(s|_V)$. Se comprueba fácilmente que $\phi_V(s)_V$ así definido es un homomorfismo de $\mathcal{O}_X(V)$-módulos que conmuta con las restricciones, por lo que define ciertamente un homomorfismo $\phi_U(s)$ de $\mathcal{O}_U$-módulos, de modo que ϕ_U resulta ser un homomorfismo de $\mathcal{O}_X(U)$-módulos que conmuta con las restricciones, por lo que define ciertamente el homomorfismo ϕ que buscábamos.

Ahora hemos de ver que ϕ es un isomorfismo. Para ello basta probar que si $\mathcal{L}|_U$ es libre, entonces ϕ_U es un isomorfismo.

Fijemos un isomorfismo $\mathcal{L}|_U \cong \mathcal{O}_X^r|_U$ y sean $s_1, \ldots, s_r \in \mathcal{L}(U)$ las imágenes de la base canónica de $\mathcal{O}_X^r(U)$. Así, para cada abierto $V \subset U$, los elementos $s_i|_V$ son una base de $\mathcal{L}(V)$ como $\mathcal{O}_X(V)$-módulo. Esto hace que si $\alpha : \mathcal{L}|_V \longrightarrow \mathcal{O}_X|_V$ es un homomorfismo de $\mathcal{O}_V$-módulos, cada α_W, para cada abierto $W \subset V$, está determinado por los elementos $\alpha_W(s_i|_W)$, que a su vez están determinados por los elementos $\alpha_V(s_i|_V)$. Esto nos proporciona isomorfismos de $\mathcal{O}_X(V)$-módulos

$$\mathcal{L}^*(V) = \operatorname{Hom}_{\mathcal{O}_V}(\mathcal{L}|_V, \mathcal{O}_X|_V) \cong \mathcal{O}_X(V)^r,$$

que a su vez determinan un isomorfismo de $\mathcal{O}_U$-módulos $\mathcal{L}^*|_U \cong \mathcal{O}_X^r|_U$. A través de este isomorfismo, la base canónica de $\mathcal{O}_X^r(U)$ se corresponde con los elementos $\delta^i \in \mathcal{L}^*(U)$ determinados por que

$$\delta_U^i(s_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Igualmente, cada homomorfismo de $\mathcal{O}_U$-módulos $\alpha : \mathcal{L}^*|_U \longrightarrow \mathcal{O}_X|_U$ está determinado por los elementos $\alpha_U(\delta^i)$, lo que nos da un isomorfismo

$$\mathcal{L}^{**}(U) = \operatorname{Hom}_{\mathcal{O}_U}(\mathcal{L}^*|_U, \mathcal{O}_X|_U) \cong \mathcal{O}_X^r(U).$$

Finalmente observamos que

$$\phi_U(s_j)_U(\delta^i) = \delta_U^i(s_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Esto significa que los elementos $\phi_U(s_j)$ se corresponden con la base canónica de $\mathcal{O}_X^r(U)$ a través del isomorfismo anterior, y por otra parte los s_j se corresponden con la base canónica a través del isomorfismo $\mathcal{L}(U) \cong \mathcal{O}_X^r|_U$. De este modo, ϕ_U resulta ser la composición de los dos isomorfismos

$$\mathcal{L}(U) \longrightarrow \mathcal{O}_X^r(U) \longrightarrow \mathcal{L}^{**}(U),$$

luego ϕ_U es un isomorfismo. ■

Teorema 2.10 *Sea X un espacio anillado, sea $\mathcal{L}$ un $\mathcal{O}_X$-módulo localmente libre de rango finito y sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo arbitrario. Entonces*

$$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{M}) \cong \mathcal{L}^* \otimes_{\mathcal{O}_X} \mathcal{M}.$$

DEMOSTRACIÓN: Vamos a definir un homomorfismo de prehaces

$$\phi^- : (\mathcal{L}^* \otimes_{\mathcal{O}_X} \mathcal{M})^- \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{M}),$$

para lo cual fijamos un abierto $U \subset X$ y vamos a definir un homomorfismo

$$\phi_U^- : \mathcal{L}^*(U) \otimes_{\mathcal{O}_X(U)} \mathcal{M}(U) \longrightarrow \operatorname{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{M}|_U),$$

para lo cual fijamos $\alpha \in \mathcal{L}^*(U) = \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{O}_X|_U)$ y $m \in \mathcal{M}(U)$ y vamos a definir un homomorfismo $\psi^{\alpha,m} : \mathcal{L}|_U \longrightarrow \mathcal{M}|_U$, para lo cual fijamos un abierto $V \subset U$ y definimos $\psi_V^{\alpha,m} : \mathcal{L}(V) \longrightarrow \mathcal{M}(V)$ mediante $\psi_V^{\alpha,m}(l) = \alpha_V(l)m|_V$.

Se comprueba que $\psi_V^{\alpha,m}$ es un homomorfismo de $\mathcal{O}_X(V)$-módulos que conmuta con las restricciones, por lo que define un homomorfismo de $\mathcal{O}_U$-módulos $\psi^{\alpha,m}$, lo que nos permite definir $\phi_U^-(\alpha \otimes m) = \psi^{\alpha,m}$. Los homomorfismos ϕ_U^- son compatibles con las restricciones, por lo que definen un homomorfismo ϕ^-, que a su vez se extiende a un homomorfismo de haces

$$\phi : \mathcal{L}^* \otimes_{\mathcal{O}_X} \mathcal{M} \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{M}).$$

Basta probar que si $\mathcal{L}|_U$ es libre entonces ϕ_U^- es un isomorfismo. Fijemos un isomorfismo $\mathcal{L}|_U \cong \mathcal{O}_X^r|_U$ y sean $s_1, \ldots, s_r \in \mathcal{L}(U)$ las imágenes de la base canónica de $\mathcal{O}_X^r(U)$. Como en el teorema anterior, tenemos entonces un isomorfismo $\mathcal{L}^*|_U \cong \mathcal{O}_X^r|_U$ en el que la base canónica de $\mathcal{O}_X^r(U)$ se corresponde con los elementos $\delta^i \in \mathcal{L}^*(U)$.

Entonces todo elemento de $\mathcal{L}^*(U) \otimes_{\mathcal{O}_X(U)} \mathcal{M}(U)$ se expresa de forma única como $\delta^1 \otimes m_1 + \cdots + \delta^r \otimes m_r$, para ciertos $m_i \in \mathcal{M}(U)$, y esto nos da un isomorfismo $\mathcal{L}^*(U) \otimes_{\mathcal{O}_X(U)} \mathcal{M}(U) \cong \mathcal{M}(U)^r$.

Por otra parte, también $\mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{M}|_U) \cong \mathcal{M}(U)^r$ donde el isomorfismo viene dado por $\alpha \mapsto (\alpha_U(s_i))_i$.

De la definición de ϕ_U^- se sigue que $\phi_U^-(\delta^i \otimes m)_U(s_j) = \delta^i(s_j)m$, lo que significa que ϕ_U^- es la composición de los isomorfismos

$$\mathcal{L}^*(U) \otimes_{\mathcal{O}_X(U)} \mathcal{M}(U) \cong \mathcal{M}(U)^r \cong \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{M}|_U).$$

■

En particular vemos que si $\mathcal{L}_1$ y $\mathcal{L}_2$ son $\mathcal{O}_X$-módulos localmente libres de rangos r y s, entonces $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}_1, \mathcal{L}_2)$ es localmente libre de rango rs.

Teorema 2.11 *Si X es un espacio anillado y $\mathcal{L}$ es un $\mathcal{O}_X$-módulo localmente libre de rango 1, entonces $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{L}) \cong \mathcal{O}_X$.*

Demostración: Vamos a definir $\phi : \mathcal{O}_X \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{L})$, para lo cual fijamos un abierto $U \subset X$ y definimos un homomorfismo de $\mathcal{O}_X(U)$-módulos $\phi_U : \mathcal{O}_X(U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{L}|_U)$. Para ello, a su vez, fijamos $s \in \mathcal{O}_X(U)$ y vamos a definir un homomorfismo $\phi_U(s) : \mathcal{L}|_U \longrightarrow \mathcal{L}|_U$, para lo cual fijamos un abierto $V \subset U$ y definimos $\phi_U(s)_V : \mathcal{L}(V) \longrightarrow \mathcal{L}(V)$ mediante $\phi_U(s)_V(l) = s|_V l$.

Basta probar que ϕ_U es un isomorfismo cuando $\mathcal{L}|_U \cong \mathcal{O}_U$. Sea $s \in \mathcal{L}(U)$ la imagen de 1 por este isomorfismo. Entonces, como en los teoremas anteriores, cada $\alpha : \mathcal{L}|_U \longrightarrow \mathcal{L}|_U$ está determinado por $\alpha_U(s)$, que puede ser cualquier elemento de $\mathcal{L}(U)$, de la forma $\alpha_U(s) = as$, para cierto $a \in \mathcal{O}_X(U)$. Esto determina un isomorfismo $\mathcal{O}_X(U) \cong \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{L}|_U, \mathcal{L}|_U)$, dado por $a \leftrightarrow \alpha$, que no es sino el propio ϕ_U, pues $\phi_U(a)_U(s) = as$. ■

Definición 2.12 Si X es un espacio anillado, llamaremos $\mathcal{S}(X)$ al conjunto de las clases de isomorfía de $\mathcal{O}_X$-módulos localmente libres de rango finito. Es claro que el producto tensorial $\otimes_{\mathcal{O}_X}$ induce una ley de composición interna conmutativa en $\mathcal{S}(X)$ en la que la clase de $\mathcal{O}_X$, es decir, la clase de los $\mathcal{O}_X$-módulos libres de rango 1, es el elemento neutro.

El hecho de que el producto multiplique los rangos hace que sólo las clases de rango 1 puedan tener inverso, y ciertamente lo tienen, pues si $\mathcal{L}$ es un $\mathcal{O}_X$-módulo localmente libre de rango 1, entonces los teoremas precedentes nos dan que

$$\mathcal{L}^* \otimes_{\mathcal{O}_X} \mathcal{L} \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}, \mathcal{L}) \cong \mathcal{O}_X.$$

Por ello, los $\mathcal{O}_X$-módulos localmente libres de rango 1 se llaman $\mathcal{O}_X$-módulos *inversibles*, y el conjunto $\mathrm{Pic}(X)$ de clases de isomorfía de módulos inversibles forma un grupo, que recibe el nombre de *grupo de Picard* del espacio anillado X.

En resumen, el producto en el grupo de Picard es $[\mathcal{L}_1][\mathcal{L}_2] = [\mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2]$, el elemento neutro es $[\mathcal{O}_X]$ y la clase inversa de una clase es $[\mathcal{L}]^{-1} = [\mathcal{L}^*]$.

Veamos un par de resultados más sobre módulos de homomorfismos que necesitaremos más adelante:

Teorema 2.13 *Sea X un espacio anillado y sean $\mathcal{M}$, $\mathcal{N}$, $\mathcal{P}$ tres $\mathcal{O}_X$-módulos. Entonces*

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}, \mathcal{P}) \cong \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P})).$$

Demostración: Vamos a definir un homomorfismo

$$\phi : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P})) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}, \mathcal{P}),$$

para lo cual tomamos $\alpha : \mathcal{M} \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P})$ y vamos a definir un homomorfismo de prehaces

$$\phi(\alpha)^- : (\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^- \longrightarrow \mathcal{P}.$$

Para ello tomamos un abierto $U \subset X$ y consideramos el homomorfismo $\phi(\alpha)^-_U : \mathcal{M}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{N}(U) \longrightarrow \mathcal{P}(U)$ dado por $\phi(\alpha)^-_U(m \otimes n) = \alpha_U(m)_U(n)$.

Se comprueba fácilmente que $\phi(\alpha)^-$ es realmente un homomorfismo de prehaces, y lo extendemos a un homomorfismo de haces $\phi(\alpha)$. Se comprueba que ϕ, así definido, es un homomorfismo de $\mathcal{O}_X(X)$-módulos.

Ahora definimos

$$\psi : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}, \mathcal{P}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P})),$$

para lo cual tomamos $\beta : \mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N} \longrightarrow \mathcal{P}$ y vamos a definir

$$\psi(\beta) : \mathcal{M} \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P}),$$

para lo cual tomamos un abierto $U \subset X$ y definimos un homomorfismo

$$\psi(\beta)_U : \mathcal{M}(U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{N}|_U, \mathcal{P}|_U),$$

para lo cual tomamos $m \in \mathcal{M}(U)$ y definimos $\psi(\beta)_U(m) : \mathcal{N}|_U \longrightarrow \mathcal{P}|_U$, para lo cual tomamos un abierto $V \subset U$ y definimos $\psi(\beta)_U(m)_V : \mathcal{N}(V) \longrightarrow \mathcal{P}(V)$ mediante $\psi(\beta)_U(m)_V(n) = \beta_V((m|_V \otimes n)^+)$ (donde el signo $+$ denota el homomorfismo $(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^- \longrightarrow \mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}$).

Basta comprobar que ϕ y ψ son mutuamente inversos. Si $\beta : \mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N} \longrightarrow \mathcal{P}$, entonces

$$\phi(\psi(\beta))^-_U(m \otimes n) = \psi(\beta)_U(m)_U(n) = \beta_U((m \otimes n)^+).$$

Esto implica que $\phi(\psi(\beta)) = \beta$.

Recíprocamente, si $\alpha : \mathcal{M} \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{N}, \mathcal{P})$, entonces

$$\psi(\phi(\alpha))_U(m)_V(n) = \phi(\alpha)_V((m|_V \otimes n)^+) = \phi(\alpha)^-_V(m|_V \otimes n) = \alpha_V(m|_V)_V(n),$$

luego $\psi(\phi(\alpha))_U(m)_V = \alpha_V(m|_V)_V = \alpha_U(m)|_V$, luego $\psi(\phi(\alpha)) = \alpha$. ■

Cuando el módulo $\mathcal{N}$ es localmente libre de rango finito, el teorema 2.10 nos proporciona una versión más simétrica del teorema anterior:

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}, \mathcal{P}) \cong \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}^* \otimes_{\mathcal{O}_X} \mathcal{P}).$$

Teorema 2.14 *Sea X un espacio anillado, sea $\mathcal{L}$ un $\mathcal{O}_X$-módulo localmente libre de rango finito y sean $\mathcal{M}$, $\mathcal{N}$ dos $\mathcal{O}_X$-módulos arbitrarios. Entonces*

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{L}, \mathcal{N}) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{L}^* \otimes_{\mathcal{O}_X} \mathcal{N}) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{L}^*.$$

Demostración: El primer isomorfismo es consecuencia inmediata del isomorfismo indicado previamente al teorema, junto con el hecho de que éste es compatible con las restricciones. Para probar el segundo podemos sustituir $\mathcal{L}^*$ por $\mathcal{L}$ y vamos a construir un isomorfismo

$$\phi : \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{L} \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N}),$$

para lo cual definimos un homomorfismo

$$\phi^- : (\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \otimes_{\mathcal{O}_X} \mathcal{L})^- \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N}),$$

para lo cual fijamos un abierto $U \subset X$ y definimos un homomorfismo

$$\phi^-_U : \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, \mathcal{N}|_U) \otimes_{\mathcal{O}_X(U)} \mathcal{L}(U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})|_U),$$

para lo cual tomamos un $\alpha : \mathcal{M}|_U \longrightarrow \mathcal{N}|_U$ y un $l \in L(U)$ y definimos un homomorfismo $\phi^-_U(\alpha \otimes l) : \mathcal{M}|_U \longrightarrow (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})|_U$, para lo cual tomamos un abierto $V \subset U$ y definimos $\phi^-_U(\alpha \otimes l)_V : \mathcal{M}(V) \longrightarrow (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})(V)$ mediante $\phi^-_U(\alpha \otimes l)_V(m) = (l|_V \otimes \alpha_V(m))^+$.

Se comprueba que esto define realmente un homomorfismo ϕ, y ahora vamos a probar que ϕ_U es un isomorfismo cuando $\mathcal{L}|_U$ es libre. Ello se debe a que si $\mathcal{L}|_U \cong \mathcal{O}^r_U$, entonces,

$$\mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, \mathcal{N}|_U) \otimes_{\mathcal{O}_X(U)} \mathcal{L}(U) \cong \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, \mathcal{N}|_U)^r,$$

e igualmente $\mathcal{L}(V) \otimes_{\mathcal{O}_X(V)} \mathcal{N}(V) \cong \mathcal{N}(V)^r$ para todo abierto $V \subset U$, y los isomorfismos son compatibles con las restricciones, por lo que inducen un isomorfismo $(\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})^-|_U \cong \mathcal{N}|_U^r$, lo que prueba que el prehaz $(\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})^-|_U$ es ya un haz y así $(\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})|_U \cong \mathcal{N}|_U^r$. Esto implica a su vez que

$$\mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{N})|_U) \cong \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, \mathcal{N}|_U)^r,$$

y es fácil ver que ϕ_U^- es la composición de estos dos isomorfismos. ■

2.4 Los funtores Ext

En el capítulo anterior hemos visto que, si X es un espacio anillado, los módulos de homomorfismos definen dos funtores $\mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X))$, uno covariante, $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, -)$ y otro contravariante, $\mathrm{Hom}_{\mathcal{O}_X}(-, \mathcal{N})$.

En la sección anterior hemos definido el $\mathcal{O}_X$-módulo $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$, que nos permite definir igualmente dos funtores $\mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(X)$: el funtor covariante $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, -)$ y el funtor contravariante $\mathcal{H}om_{\mathcal{O}_X}(-, \mathcal{N})$. (Su acción sobre un homomorfismo se define de forma natural, por composición.) Vamos a ver que ambos son exactos por la izquierda.

Consideremos una sucesión exacta de $\mathcal{O}_X$-módulos

$$0 \longrightarrow \mathcal{N}' \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{N}'' \longrightarrow 0.$$

Hemos de probar la exactitud de

$$0 \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}') \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}'').$$

Probaremos el caso menos obvio, que, como es habitual, se trata de la inclusión $\mathrm{N}(\bar{\beta}) \subset \mathrm{Im}\,\bar{\alpha}$. Sea $U \subset X$ un abierto y sea $\phi \in \mathrm{N}(\bar{\beta})(U)$. Esto significa que $\phi : \mathcal{M}|_U \longrightarrow \mathcal{N}|_U$ y $\phi \circ \beta|_U = 0$. Ahora usamos que la restricción a U de la sucesión exacta de partida sigue siendo exacta, así como que el funtor $\mathrm{Hom}_{\mathcal{O}_U}(\mathcal{M}|_U, -)$ es exacto por la izquierda. Esto quiere decir que la sucesión

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}|_U, \mathcal{N}'|_U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}|_U, \mathcal{N}|_U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}|_U, \mathcal{N}''|_U)$$

es exacta y tenemos que ϕ está en el núcleo del segundo homomorfismo. Por consiguiente, existe un $\psi : \mathcal{M}|_U \longrightarrow \mathcal{N}'|_U$ tal que $\phi = \psi \circ \alpha|_U$. Así pues, $\phi = \bar{\alpha}_U(\psi) \in \mathrm{Im}\,\bar{\alpha}_U \subset (\mathrm{Im}\,\bar{\alpha})(U)$.

La exactitud de $\mathcal{H}om_{\mathcal{O}_X}(-, \mathcal{N})$ se prueba análogamente.

Definición 2.15 Si X es un espacio anillado y $\mathcal{M}$ es un $\mathcal{O}_X$-módulo, llamaremos $\mathrm{Ext}_X^n(\mathcal{M}, -) : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(\mathcal{O}_X(X))$ a los funtores derivados del funtor $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, -)$, y $\mathcal{E}xt_X^n : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(X)$ a los funtores derivados del funtor $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{M}, -)$.

El funtor $\mathcal{E}xt$ es local:

Teorema 2.16 *Sea X un espacio anillado, sea $U \subset X$ un abierto y sean $\mathcal{M}$ y $\mathcal{N}$ dos $\mathcal{O}_X$-módulos. Entonces $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},\mathcal{N})|_U \cong \mathcal{E}\mathrm{xt}^n_U(\mathcal{M}|_U,\mathcal{N}|_U)$.*

Demostración: Podemos considerar a $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},-)|_U$ y a $\mathcal{E}\mathrm{xt}^n_U(\mathcal{M}|_U,-|_U)$ como funtores $\mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(U)$, y es claro que ambos están dotados de un homomorfismo de conexión.

Por definición, $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M},\mathcal{N})|_U = \mathcal{H}\mathrm{om}_{\mathcal{O}_U}(\mathcal{M}|_U,\mathcal{N}|_U)$, y es fácil ver, más en general, que los funtores $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M},-)|_U$ y $\mathcal{H}\mathrm{om}_{\mathcal{O}_U}(\mathcal{M}|_U,-|_U)$ son iguales (es decir, que no sólo coinciden al actuar sobre módulos, sino también sobre homomorfismos). Equivalentemente, tenemos un isomorfismo entre los dos funtores del enunciado para $n = 0$.

Por otra parte, si $\mathcal{N}$ es un $\mathcal{O}_X$-módulo inyectivo, entonces $\mathcal{N}|_U$ es un $\mathcal{O}_U$-módulo inyectivo, luego ambos miembros se anulan en $\mathcal{N}$. El teorema 1.50 implica entonces que existe un isomorfismo para cada n. ■

Veamos ahora un resultado elemental:

Teorema 2.17 *Si X es un espacio anillado y $\mathcal{N}$ es un $\mathcal{O}_X$-módulo, entonces:*

a) $\mathcal{E}\mathrm{xt}^0_X(\mathcal{O}_X,\mathcal{N}) \cong \mathcal{N}$.

b) $\mathcal{E}\mathrm{xt}^n_X(\mathcal{O}_X,\mathcal{N}) = 0$ *para* $n > 0$.

c) $\mathrm{Ext}^n_X(\mathcal{O}_X,\mathcal{N}) \cong H^n(X,\mathcal{N})$ *para todo* $n \geq 0$.

Demostración: Esto es consecuencia de que

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X,\mathcal{N}) \cong \mathcal{N}(X) = \Gamma(X,\mathcal{N}),$$

de donde se sigue fácilmente que el funtor $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X,-)$ es isomorfo al funtor $\Gamma(X,-)$ y el funtor $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{O}_X,-)$ es isomorfo a la identidad. Por consiguiente, los funtores derivados del primero son los derivados de $\Gamma(X,-)$ (y esto nos da el apartado c) y los derivados del segundo son los derivados de la identidad (lo que claramente nos da a y b). ■

Es fácil ver que los funtores derivados conservan sumas directas (porque la suma de dos resoluciones inyectivas de dos módulos es una resolución inyectiva de la suma). El teorema anterior implica entonces que si $\mathcal{L}$ es un $\mathcal{O}_X$-módulo libre de rango finito, entonces $\mathcal{E}\mathrm{xt}^n_X(\mathcal{L},\mathcal{N}) = 0$ para todo $n \geq 1$ y todo $\mathcal{O}_X$-módulo $\mathcal{N}$. Por el teorema 2.16 basta, en realidad, con que $\mathcal{L}$ sea localmente libre. Esto, a su vez, equivale a que el funtor $\mathcal{H}\mathrm{om}_X(\mathcal{L},-)$ es exacto.

Observemos ahora que, en general, no podemos definir los funtores derivados de los funtores $\mathrm{Hom}_{\mathcal{O}_X}(-,\mathcal{N})$ y $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(-,\mathcal{N})$, porque requieren resoluciones proyectivas, que no tienen por qué existir. Dichos funtores derivados existen, por ejemplo, en la categoría de los módulos sobre un anillo A, en cuyo caso los funtores $\mathrm{Hom}_A(-,N)$ y $\mathcal{H}\mathrm{om}_A(-,N)$ son el mismo. Sin embargo, vamos a demostrar que en este caso los funtores derivados nos dan los mismos módulos $\mathrm{Ext}_A(M,N)$. En realidad obtendremos un resultado más general.

Observemos que si tenemos un homomorfismo $\phi : \mathcal{M} \longrightarrow \mathcal{M}'$ de $\mathcal{O}_X$-módulos y fijamos una resolución inyectiva de otro $\mathcal{O}_X$-módulo $\mathcal{N}$:

$$0 \longrightarrow \mathcal{N} \longrightarrow \mathcal{I}^0 \longrightarrow \mathcal{I}^1 \longrightarrow \mathcal{I}^2 \longrightarrow \cdots,$$

entonces ϕ induce homomorfismos de complejos

$$\bar{\phi} : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}', (\mathcal{I}^n)_n) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, (\mathcal{I}^n)_n),$$

$$\bar{\Phi} : \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}', (\mathcal{I}^n)_n) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, (\mathcal{I}^n)_n),$$

los cuales, a su vez, inducen homomorfismos

$$\mathrm{Ext}^n_X(\mathcal{M}', \mathcal{N}) \longrightarrow \mathrm{Ext}^n_X(\mathcal{M}, \mathcal{N}) \quad \text{y} \quad \mathcal{E}\mathrm{xt}^n_X(\mathcal{M}', \mathcal{N}) \longrightarrow \mathcal{E}\mathrm{xt}^n_X(\mathcal{M}, \mathcal{N}).$$

Los argumentos usuales prueban que estos homomorfismos no dependen de la elección de la resolución inyectiva de $\mathcal{N}$, así como que son funtoriales, es decir, que podemos considerar a $\mathrm{Ext}^n_X(-, \mathcal{N})$ y $\mathcal{E}\mathrm{xt}^n_X(-, \mathcal{N})$ como funtores contravariantes $\mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(X)$. El teorema siguiente prueba que ambos tienen homomorfismos de conexión.

Teorema 2.18 *Sea X un espacio anillado, sea $0 \longrightarrow \mathcal{M}' \longrightarrow \mathcal{M} \longrightarrow \mathcal{M}'' \longrightarrow 0$ una sucesión exacta de $\mathcal{O}_X$-módulos y sea $\mathcal{N}$ otro $\mathcal{O}_X$-módulo. Entonces existen sucesiones exactas*

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}'', \mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}', \mathcal{N})$$

$$\longrightarrow \mathrm{Ext}^1_X(\mathcal{M}'', \mathcal{N}) \longrightarrow \mathrm{Ext}^1_X(\mathcal{M}, \mathcal{N}) \longrightarrow \mathrm{Ext}^1_X(\mathcal{M}', \mathcal{N}) \longrightarrow \cdots$$

y

$$0 \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}'', \mathcal{N}) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}', \mathcal{N})$$

$$\longrightarrow \mathcal{E}\mathrm{xt}^1_X(\mathcal{M}'', \mathcal{N}) \longrightarrow \mathcal{E}\mathrm{xt}^1_X(\mathcal{M}, \mathcal{N}) \longrightarrow \mathcal{E}\mathrm{xt}^1_X(\mathcal{M}', \mathcal{N}) \longrightarrow \cdots$$

DEMOSTRACIÓN: Sea $0 \longrightarrow \mathcal{N} \longrightarrow \mathcal{I}^0 \longrightarrow \mathcal{I}^1 \longrightarrow \cdots$ una resolución inyectiva de $\mathcal{N}$. A partir de ella obtenemos, por la propia definición de inyectividad, una sucesión exacta de complejos

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}'', (\mathcal{I}^n)) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}, (\mathcal{I}^n)) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}', (\mathcal{I}^n)) \longrightarrow 0$$

Los grupos de cohomología de estos tres complejos son, por definición de los funtores derivados, los funtores Ext^n_X que aparecen en la primera sucesión del enunciado, que no es sino la sucesión exacta de cohomología dada por el teorema 1.36. La prueba para $\mathcal{E}\mathrm{xt}$ es idéntica. (Para probar la exactitud de la sucesión de complejos en este segundo caso basta tener presente que la restricción de un módulo inyectivo es inyectiva.) ■

Nota La segunda condición que exige la definición de homomorfismo de conexión se demuestra sin dificultad alguna. ■

En definitiva, los funtores $\mathrm{Ext}^n_X(-,\mathcal{N})$ y $\mathcal{E}\mathrm{xt}^n_X(-,\mathcal{N})$ se comportan como funtores derivados de $\mathrm{Hom}_{\mathcal{O}_X}(-,\mathcal{N})$ y $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(-,\mathcal{N})$, aunque tales derivados no tengan por qué existir.

En la categoría de los módulos sobre un anillo A, hemos demostrado que $\mathrm{Ext}_A(L,N)=0$ siempre que L es un módulo libre, luego el teorema 1.50 (en su forma dual) prueba que los funtores $\mathrm{Ext}_A(-,N)$ forman una sucesión universal, luego son los derivados del funtor $\mathrm{Hom}_A(-,N)$.

En particular tenemos que $\mathrm{Ext}_A(M,N)$ puede calcularse indistintamente con una resolución proyectiva de M o con una resolución inyectiva de N. El teorema siguiente generaliza ligeramente este hecho a otras categorías de $\mathcal{O}_X$-módulos.

Teorema 2.19 *Sea X un espacio anillado y $\mathcal{M}$ un $\mathcal{O}_X$-módulo que admita una resolución localmente libre de rango finito*

$$\cdots \longrightarrow \mathcal{L}_1 \longrightarrow \mathcal{L}_0 \longrightarrow \mathcal{M} \longrightarrow 0$$

(es decir, una sucesión exacta donde cada $\mathcal{L}_i$ es localmente libre de rango finito). Entonces, para cada $\mathcal{O}_X$-módulo $\mathcal{N}$, los módulos $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},\mathcal{N})$ pueden calcularse como los grupos de cohomología del complejo

$$0 \longrightarrow \mathcal{H}\mathrm{om}_X(\mathcal{L}_0,\mathcal{N}) \longrightarrow \mathcal{H}\mathrm{om}_X(\mathcal{L}_1,\mathcal{N}) \longrightarrow \cdots$$

Demostración: Llamemos $T^n\mathcal{N}$ al n-simo grupo de cohomología del complejo del enunciado. Es claro que un homomorfismo $\mathcal{N} \longrightarrow \mathcal{N}'$ induce un homomorfismo de complejos, que a su vez induce homomorfismos entre los grupos de cohomología, por lo que tenemos funtores $T^n : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(X)$.

Estos funtores tienen un homomorfismo de conexión. En efecto, si

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0$$

es una sucesión exacta de $\mathcal{O}_X$-módulos, según hemos observado tras 2.17 el funtor $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_n,-)$ es exacto, luego nos da sucesiones exactas

$$0 \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_n,\mathcal{M}) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_n,\mathcal{N}) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_n,\mathcal{P}) \longrightarrow 0,$$

que forman una sucesión exacta de complejos cuyos grupos de cohomología son los módulos $T^n(\mathcal{M})$, $T^n(\mathcal{N})$, $T^n(\mathcal{M})$, y la sucesión exacta dada por 1.36 proporciona los homomorfismos de conexión. La segunda propiedad de la definición de homomorfismo de conexión es una comprobación rutinaria.

Observemos ahora que si $\mathcal{I}$ es inyectivo, entonces $T^n\mathcal{I}=0$ para todo $n \geq 1$. En efecto, tenemos que $\mathcal{E}\mathrm{xt}^1_X(\mathcal{M},\mathcal{I})=0$ para todo $\mathcal{O}_X$-módulo $\mathcal{M}$ (por las propiedades de los funtores derivados), luego el teorema anterior implica que el funtor $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(-,\mathcal{I})$ es exacto. Esto se traduce en que conserva *todas* las sucesiones exactas, luego la sucesión

$$\mathcal{H}\mathrm{om}(\mathcal{L}_n,\mathcal{I}) \longrightarrow \mathcal{H}\mathrm{om}(\mathcal{L}_{n+1},\mathcal{I}) \longrightarrow \mathcal{H}\mathrm{om}(\mathcal{L}_{n+2},\mathcal{I}),$$

es exacta para todo $n \geq 0$, de donde $T^{n+1}\mathcal{N}=0$.

El teorema 1.50 nos da que la sucesión de funtores (T^n) es universal, al igual que lo es la sucesión de funtores derivados $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},-)$. Basta probar que coinciden para $n=0$. Ahora bien, la sucesión exacta

$$0 \longrightarrow \mathcal{L}_1/\,\mathrm{N}\,\delta_1 \longrightarrow \mathcal{L}_0 \xrightarrow{\eta} \mathcal{M} \longrightarrow 0$$

nos da la sucesión exacta

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M},\mathcal{N}) \arrow[r, "\bar\eta"] & \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_0,\mathcal{N}) \arrow[r] \arrow[dr] & \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_1/\,\mathrm{N}\,\delta_1,\mathcal{N}) \arrow[d] \\ & & & \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{L}_1,\mathcal{N}) \end{tikzcd}$$

La flecha vertical es un monomorfismo, por lo que $T^0\mathcal{N}$, que es el núcleo del homomorfismo oblicuo, es también la imagen de $\bar\eta$, luego

$$T^0\mathcal{N} \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M},\mathcal{N}) \cong \mathcal{E}\mathrm{xt}^0_X(\mathcal{M},\mathcal{N}),$$

y es fácil ver que estos isomorfismos determinan un isomorfismo entre los funtores. ■

Para terminar vamos a generalizar el teorema 2.14, para lo que necesitamos un resultado previo:

Teorema 2.20 *Sea X un espacio anillado. Si $\mathcal{L}$ es un $\mathcal{O}_X$-módulo localmente libre de rango finito y $\mathcal{I}$ es un $\mathcal{O}_X$-módulo inyectivo, entonces $\mathcal{L}\otimes_{\mathcal{O}_X}\mathcal{I}$ es también inyectivo.*

DEMOSTRACIÓN: Observemos en primer lugar que, según la observación tras el teorema 2.10, para cualquier $\mathcal{O}_X$-módulo $\mathcal{M}$ se cumple que

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M},\mathcal{L}\otimes_{\mathcal{O}_X}\mathcal{I}) \cong \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}\otimes_{\mathcal{O}_X}\mathcal{L}^*,\mathcal{I}).$$

Más aún, es fácil ver que, si consideramos a ambos miembros como funtores en la variable $\mathcal{M}$, en realidad tenemos un isomorfismo de funtores, es decir, los isomorfismos son compatibles con los homomorfismos determinados por ambos funtores. La inyectividad de $\mathcal{L}\otimes_{\mathcal{O}_X}\mathcal{I}$ equivale a la exactitud del funtor $\mathrm{Hom}_{\mathcal{O}_X}(-,\mathcal{L}\otimes_{\mathcal{O}_X}\mathcal{I})$ y, a causa del isomorfismo anterior, ésta equivale a su vez a la exactitud del funtor $\mathrm{Hom}_{\mathcal{O}_X}(-\otimes_{\mathcal{O}_X}\mathcal{L}^*,\mathcal{I})$. Ahora bien, si tenemos una sucesión exacta

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0,$$

también es exacta la sucesión

$$0 \longrightarrow \mathcal{M}\otimes_{\mathcal{O}_X}\mathcal{L}^* \longrightarrow \mathcal{N}\otimes_{\mathcal{O}_X}\mathcal{L}^* \longrightarrow \mathcal{P}\otimes_{\mathcal{O}_X}\mathcal{L}^* \longrightarrow 0,$$

pues $\mathcal{L}^*$ es localmente libre, luego los módulos $\mathcal{L}^*_P$, con $P\in X$, son planos. Ahora, la inyectividad de $\mathcal{I}$ equivale a la exactitud del funtor $\mathrm{Hom}_{\mathcal{O}_X}(-,\mathcal{I})$, luego tenemos la exactitud de la sucesión

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{P}\otimes_{\mathcal{O}_X}\mathcal{L}^*,\mathcal{I}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{N}\otimes_{\mathcal{O}_X}\mathcal{L}^*,\mathcal{I}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M}\otimes_{\mathcal{O}_X}\mathcal{L}^*,\mathcal{I}) \longrightarrow 0.$$

■

Teorema 2.21 *Sea X un espacio anillado, sea $\mathcal{L}$ un $\mathcal{O}_X$-módulo localmente libre de rango finito y sean $\mathcal{M}$, $\mathcal{N}$ dos $\mathcal{O}_X$-módulos arbitrarios. Entonces*

$$\operatorname{Ext}^n_X(\mathcal{M}\otimes_{\mathcal{O}_X}\mathcal{L},\mathcal{N})\cong \operatorname{Ext}^n_X(\mathcal{M},\mathcal{L}^*\otimes_{\mathcal{O}_X}\mathcal{N}),$$

$$\mathcal{E}\mathrm{xt}^n_X(\mathcal{M}\otimes_{\mathcal{O}_X}\mathcal{L},\mathcal{N})\cong \mathcal{E}\mathrm{xt}^n_X(\mathcal{M},\mathcal{L}^*\otimes_{\mathcal{O}_X}\mathcal{N})\cong \mathcal{E}\mathrm{xt}^n_X(\mathcal{M},\mathcal{N})\otimes_{\mathcal{O}_X}\mathcal{L}^*.$$

Demostración: Los isomorfismos para $n=0$ están demostrados en el teorema 2.14 y en la observación previa. Es fácil ver además que son isomorfismos de funtores considerando a $\mathcal{N}$ como variable.

Por otra parte, los cinco funtores tienen homomorfismos de conexión. Esto es obvio para el primero de cada línea, pues ambos son funtores derivados. Respecto a $\operatorname{Ext}^n_X(\mathcal{M},\mathcal{L}^*\otimes_{\mathcal{O}_X}-)$ y $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},\mathcal{L}^*\otimes_{\mathcal{O}_X}-)$, observamos que una sucesión exacta corta de $\mathcal{O}_X$-módulos sigue siendo exacta al multiplicarla por $\mathcal{L}^*$, por ser localmente libre, luego los homomorfismos de conexión de $\operatorname{Ext}^n_X(\mathcal{M},-)$ y $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},-)$ nos dan homomorfismos de conexión para los dos funtores considerados. Para $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},-)\otimes_{\mathcal{O}_X}\mathcal{L}^*$, los homomorfismos de conexión de $\mathcal{E}\mathrm{xt}^n_X(\mathcal{M},-)$ nos dan una sucesión exacta que sigue siendo exacta cuando la multiplicamos por $\mathcal{L}^*$.

Ahora basta probar que los cinco funtores se anulan sobre $\mathcal{O}_X$-módulos inyectivos, lo cual es evidente para tres de ellos y consecuencia inmediata del teorema anterior para los otros dos.

En definitiva, los cinco funtores son universales y tenemos los isomorfismos indicados. ■

2.5 Cohomología en espacios paracompactos

En esta sección y en las siguientes daremos aplicaciones de la teoría de funtores derivados a la topología algebraica y a la geometría diferencial. Vamos a estudiar con más detalle los grupos de cohomología definidos en la sección 2.2 en el caso de haces sobre un espacio paracompacto X. Para definir esta clase de espacios hemos de recordar algunos conceptos:

Definición 2.22 Sea X un espacio topológico. Un cubrimiento abierto de X es *localmente finito* si cada punto de X está contenido tan sólo en un número finito de abiertos del cubrimiento.

El *soporte* de una función continua $f: X\longrightarrow \mathbb{R}$ es la clausura del conjunto de puntos donde f no se anula.

Una *partición de la unidad* en X es una familia $\{f_i\}_{i\in I}$ de funciones continuas $f_i: X\longrightarrow [0,1]$ tales que, cada punto $P\in X$ tiene un entorno U tal que el conjunto $\{i\in I\mid f_i|_U\neq 0\}$ es finito y $\sum\limits_i f_i|_U=1$.

Una partición de la unidad *subordinada* a un cubrimiento abierto $\{U_i\}_{i\in I}$ es una partición de la unidad de la forma $\{f_i\}_{i\in I}$ (es decir, con el mismo conjunto de índices) tal que $\operatorname{sop} f_i\subset U_i$.

Un espacio topológico de Hausdorff X es *paracompacto* si cumple las dos propiedades siguientes:

a) Todo cubrimiento abierto $\mathcal{U}$ de X tiene un refinamiento $\mathcal{V}$ localmente finito. (Que $\mathcal{V}$ sea un refinamiento significa que todo abierto de $\mathcal{V}$ está contenido en un abierto de $\mathcal{U}$.)

b) Todo cubrimiento abierto de X tiene una partición de la unidad subordinada.

Nota En realidad, la topología general demuestra que las dos propiedades a) y b) son equivalentes (de modo que bastaría exigir una de las dos en la definición), así como que la clase de los espacios paracompactos incluye a todos los espacios métricos y a todos los espacios compactos. Sin embargo, las demostraciones de estos hechos son muy técnicas y no necesitamos para nada tal grado de generalidad. Para nuestros fines será más que suficiente este teorema:

Teorema 2.23 *Se cumple:*

a) Toda variedad diferencial es paracompacta, y en este caso las particiones de la unidad pueden tomarse de clase C^∞.

b) Toda variedad topológica es paracompacta.

c) Todo espacio métrico localmente compacto y con una base numerable es paracompacto.

Demostración: Hemos de entender que en la definición de variedad topológica y variedad diferencial exigimos que sean espacios de Hausdorff con una base numerable.

El teorema 1.17 de mi Topología algebraica prueba que en los tres casos se cumple la propiedad a) de la definición de espacio paracompacto. El teorema 9.6 *ibid.* prueba que las variedades diferenciales tienen particiones de la unidad de clase C^∞ subordinadas a cualquier cubrimiento abierto. La demostración es válida literalmente para variedades topológicas, salvo, naturalmente, por el hecho de que las particiones que se obtienen ya no son diferenciables. Más en general, la prueba se adapta fácilmente al caso de un espacio métrico localmente compacto sin más que sustituir el teorema 9.4 (que proporciona funciones "meseta" diferenciables) por el teorema de Tietze (1.12 *ibid.*) que proporciona funciones continuas con las mismas características. ■

Nota En toda esta sección supondremos tácitamente que todos los espacios topológicos considerados son paracompactos. Necesitaremos la siguiente consecuencia de la paracompacidad:

Teorema 2.24 *Si X es un espacio paracompacto, $U \subset X$ es un subconjunto abierto y $P \in U$, entonces existe un abierto V tal que $P \in V \subset \overline{V} \subset U$.*

Demostración: Por la propiedad de Hausdorff, cada $Q \in X \setminus U$ tiene un entorno abierto U_Q tal que $P \notin \overline{U}_Q$. Los abiertos U_Q junto con U forman un cubrimiento abierto de X, y por la paracompacidad tiene un refinamiento localmente finito $\{V_i\}_{i\in I}$. Sea $J = \{i \in I \mid V_i \cap (X \setminus U) \neq \varnothing\}$ y llamemos

$$G = \bigcup_{j\in J} V_j, \qquad C = \bigcup_{j\in J} \overline{V}_j.$$

La finitud local implica fácilmente que C es un cerrado, y si $j \in J$, entonces V_j está contenido en un abierto del cubrimiento original, y este abierto no puede ser U, luego existe un $Q \in X \setminus U$ tal que $V_j \subset U_Q$, luego $P \notin \overline{V}_j$. En definitiva, $P \notin C$, y el abierto buscado es $V = X \setminus C$. En efecto, tenemos que

$$X \setminus U \subset G \subset C,$$

luego $V \subset X \setminus G \subset U$ y, como G es abierto, $P \in V \subset \overline{V} \subset X \setminus G \subset U$. ■

Consideremos un espacio anillado X y un $\mathcal{O}_X$-módulo $\mathcal{M}$. Para aprovechar la paracompacidad de X vamos a ver que el concepto de partición de la unidad puede trasladarse a los $\mathcal{O}_X$-módulos.

En primer lugar definimos el *soporte* de un endomorfismo $\phi : \mathcal{M} \longrightarrow \mathcal{M}$ como la clausura $\operatorname{sop}\phi$ del conjunto de los puntos $P \in X$ tales que $\phi_P \neq 0$. De este modo, si $U \subset X$ es un abierto disjunto con $\operatorname{sop}\phi$, se cumple que $\phi_P = 0$ para todo $P \in U$, luego $\phi_U = 0$.

Si $\mathcal{U} = \{U_i\}_{i\in I}$ es un cubrimiento abierto de X localmente finito, una *partición de la unidad subordinada a* $\mathcal{U}$ en $\mathcal{M}$ es una familia $\{\phi_i\}_{i\in I}$ de endomorfismos de $\mathcal{M}$ tal que, $\operatorname{sop}\phi_i \subset U_i$ y $\sum\limits_i \phi_{iP} = I_P$ (la identidad en $\mathcal{M}_P$).

Observemos que la finitud local del cubrimiento hace que todo punto $P \in X$ tenga un entorno V en el que el conjunto $\{i \in I \mid \phi_{iV} \neq 0\}$ es finito, luego, en particular, también es finito $\{i \in I \mid \phi_{iP} \neq 0\}$, por lo que la suma de endomorfismos que aparece en la definición es finita. De hecho, se cumple también que $\sum\limits_i \phi_{iV} = I_V$ (la identidad en $\mathcal{M}(V)$).

Un $\mathcal{O}_X$-módulo $\mathcal{M}$ es *paracompacto* si todo cubrimiento abierto de X localmente finito tiene una partición de la unidad subordinada.

Teorema 2.25 *Si X es un espacio topológico (paracompacto), todo C_X-módulo es paracompacto. Si X es una variedad diferencial, todo C_X^∞-módulo es paracompacto.*

Demostración: Probaremos las dos afirmaciones simultáneamente llamando $\mathcal{O}_X$ a C_X o a C_X^∞ según el caso.

Sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo y $\{U_i\}_{i\in I}$ un cubrimiento abierto de X localmente finito. Por la paracompacidad de X existe una partición de la unidad $\{f_i\}_{i\in I}$ subordinada al cubrimiento formada por funciones $f_i \in \mathcal{O}_X(X)$.

Para cada abierto $U \subset X$, definimos $\phi_{iU} : \mathcal{M}(U) \longrightarrow \mathcal{M}(U)$ mediante $\phi_{iU}(m) = f_i|_U m$. Es inmediato que los homomorfismos ϕ_{iU} conmutan con las restricciones, por lo que definen endomorfismos $\phi_i : \mathcal{M} \longrightarrow \mathcal{M}$. Se comprueba sin dificultad que $\{\phi_i\}_{i\in I}$ es una partición de la unidad de $\mathcal{M}$ tal que $\operatorname{sop}\phi_i = \operatorname{sop} f_i \subset U_i$. ■

Más adelante demostraremos que los módulos paracompactos son acíclicos, por lo que los grupos de cohomología se pueden calcular también con resoluciones paracompactas. El teorema siguiente nos garantiza la existencia de tales resoluciones:

Teorema 2.26 *Si X es un espacio anillado, para todo $\mathcal{O}_X$-módulo $\mathcal{M}$ existe un monomorfismo $\mathcal{M} \longrightarrow \mathcal{I}$, donde $\mathcal{I}$ es un $\mathcal{O}_X$-módulo paracompacto.*

Demostración: Para cada abierto $U \subset X$ definimos $\mathcal{I}(U)$ como el conjunto de todas las aplicaciones s que a cada $P \in U$ le asignan un $s(P) \in \mathcal{M}_P$, que tiene una estructura natural de $\mathcal{O}_X$-módulo. Tomamos como restricciones las restricciones usuales como aplicaciones, con lo que $\mathcal{I}$ se convierte claramente en un haz. Por otra parte, definimos $\mathcal{M}(U) \longrightarrow \mathcal{I}(U)$ como el homomorfismo que a cada $m \in \mathcal{M}(U)$ le asigna la aplicación $P \mapsto m_P$. Es claro que esto define un monomorfismo de haces. Sólo hemos de probar que $\mathcal{I}$ es paracompacto.

Fijemos un cubrimiento de X localmente finito $\{U_i\}_{i\in I}$. Por el teorema 2.24, cada punto $P \in X$ tiene un entorno abierto W tal que $P \in W \subset \overline{W} \subset U_i$, para cierto $i \in I$. Los abiertos W forman un cubrimiento de X, y podemos tomar un refinamiento localmente finito $\{W_j\}_{j\in J}$. Así, para cada $j \in J$ existe un $i_j \in I$ tal que $\overline{W}_j \subset U_{i_j}$. Para cada $i \in I$, sea $J_i = \{j \in J \mid i_j = i\}$. Si $J_i = \varnothing$ definimos $V_i = \varnothing$, y en caso contrario tomamos

$$V_i = \bigcup_{j\in J_i} W_j.$$

La finitud local del cubrimiento hace que $\overline{V}_i$ sea la unión de las clausuras de los W_j correspondientes, por lo que $\overline{V}_i \subset U_i$. Naturalmente, $\{V_i\}_{i\in I}$ es también un cubrimiento abierto localmente finito.

Para cada $P \in X$ tomemos $i_P \in I$ tal que $P \in V_{i_P}$. Sea $\chi_i : X \longrightarrow \{0,1\}$ la función dada por

$$\chi_i(P) = \begin{cases} 1 & \text{si } i_P = i, \\ 0 & \text{si } i_P \neq i. \end{cases}$$

Para cada abierto $U \subset X$, definimos el homomorfismo $\phi_{iU} : \mathcal{I}(U) \longrightarrow \mathcal{I}(U)$ dado por $\phi_{iU}(s)(P) = \chi_i(P)s(P)$. Es inmediato que estos homomorfismos son compatibles con las restricciones, luego definen homomorfismos $\phi_i : \mathcal{I} \longrightarrow \mathcal{I}$. También es obvio que $\phi_{iU} = 0$ siempre que U es disjunto con V_i, por lo que $\operatorname{sop}\phi_i \subset \overline{V}_i \subset U_i$. Así mismo es claro que $\{\phi_i\}_{i\in I}$ es una partición de la unidad. ■

El teorema siguiente sería trivial si hubiéramos demostrado ya que los módulos paracompactos son acíclicos:

Teorema 2.27 *Sea X un espacio anillado y*

$$0 \longrightarrow \mathcal{M} \xrightarrow{\alpha} \mathcal{N} \xrightarrow{\beta} \mathcal{P} \longrightarrow 0$$

una sucesión exacta de $\mathcal{O}_X$-módulos tal que $\mathcal{M}$ es paracompacto. Entonces también es exacta la sucesión

$$0 \longrightarrow \mathcal{M}(X) \xrightarrow{\alpha_X} \mathcal{N}(X) \xrightarrow{\beta_X} \mathcal{P}(X) \longrightarrow 0.$$

Demostración: Sólo hay que probar la suprayectividad de β_X. Fijado $t \in \mathcal{P}(X)$, en principio tenemos que cada punto de X tiene un entorno U en el que $t|_U$ tiene antiimagen por β_U. Por la paracompacidad de X podemos suponer que los abiertos U forman un cubrimiento localmente finito $\{U_i\}_{i\in I}$. Fijemos $s_i \in \mathcal{N}(U_i)$ tal que $\beta_{U_i}(s_i) = t|_{U_i}$.

Sea $s_{ij} = s_i - s_j \in \mathcal{N}(U_i \cap U_j)$. Observemos que, en $U_i \cap U_j \cap U_k$, se cumple la relación $s_{ij} + s_{jk} = s_{ik}$. Por otra parte, $\beta_{U_i\cap U_j}(s_{ij}) = 0$, luego (identificando a $\mathcal{M}$ con el núcleo de β a través de α), tenemos que $s_{ij} \in \mathcal{M}(U_i \cap U_j)$.

Fijemos una partición de la unidad $\{\phi_i\}_{i\in I}$ en $\mathcal{M}$ subordinada al cubrimiento $\{U_i\}_{i\in I}$ y sea $V_{ik} = U_i \setminus \operatorname{sop} \phi_k$. De este modo $U_i = V_{ik} \cup (U_i \cap U_k)$ y $\phi_{kU_i\cap U_k}(s_{ik})|_{U_i\cap U_k\cap V_{ik}} = 0$, Por consiguiente, existe $s'_{ik} \in \mathcal{M}(U_i)$ tal que $s'_{ik}|_{U_i\cap U_k} = \phi_{kU_i\cap U_k}(s_{ik})$ y $s'_{ik}|_{V_{ik}} = 0$.

Así, cada punto $P \in U_i$ tiene un entorno V que corta sólo a un número finito de abiertos U_k, luego $s'|_{ik} = 0$ para todo índice k salvo a lo sumo un número finito de ellos. Esto permite definir (en V) la suma

$$s'_i = \sum_k s'_{ik},$$

pero es claro que estas sumas para cada V son consistentes entre sí, luego se extienden a un mismo $s'_i \in \mathcal{M}(U_i)$.

Fijemos ahora un punto $P \in U_i \cap U_j$ y consideremos la diferencia

$$s'_{iP} - s'_{jP} = \sum_k (s'_{ikP} - s'_{jkP}),$$

donde la suma se puede restringir a los índices k tales que $P \in U_i \cap U_j \cap U_k$, y entonces

$$s'_{iP} - s'_{jP} = \sum_k \phi_{kP}(s_{ikP} - s_{jkP}) = \sum_k \phi_{kP}(s_{ijP}).$$

Ahora podemos considerar de nuevo que k recorre todos los índices, pues $\phi_{kP} = 0$ si $P \notin U_k$, y así podemos aplicar que $\{\phi_k\}_k$ es una partición de la unidad, con lo que concluimos que $s'_{iP} - s'_{jP} = s_{ijP}$, para todo $P \in U_i \cap U_j$, luego $s'_i - s'_j = s_{ij} = s_i - s_j$ (en $U_i \cap U_j$).

Equivalentemente, tenemos que $s_i + s'_i = s_j + s'_j$ en $U_i \cap U_j$, lo que significa que existe un $s \in \mathcal{N}(X)$ tal que $s|_{U_i} = s_i + s'_i$ para todo i, luego

$$\beta_X(s)|_{U_i} = \beta_{U_i}(s_i) + \beta_{U_i}(s'_i) = t|_{U_i} + 0,$$

luego $\beta_X(s) = t$. ■

Vamos a necesitar el siguiente hecho elemental:

Teorema 2.28 *Si X es un espacio anillado, $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos y $\mathcal{M}$ es paracompacto, entonces $\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}$ también es paracompacto.*

DEMOSTRACIÓN: Sea $\{U_i\}_{i\in I}$ un cubrimiento abierto de X y sea $\{\phi_i\}_{i\in I}$ una partición de la unidad en $\mathcal{M}$ subordinada. Es inmediato comprobar que los homomorfismos $\{\phi_i \otimes 1\}$ son una partición de la unidad para el producto tensorial con $\operatorname{sop}(\phi_i \otimes 1) \subset \operatorname{sop} \phi_i \subset U_i$. ■

A partir de aquí vamos a fijar un dominio de ideales principales D y vamos a trabajar exclusivamente con D_X-módulos, donde D_X es el haz constante asociado a D sobre el espacio topológico X. (Esto no es ninguna restricción, pues cuando $D = \mathbb{Z}$ estamos considerando todos los haces sobre X.)

Si $\mathcal{M}$ es un D_X-módulo, es fácil ver que $\mathcal{M} \otimes_{D_X} D_X \cong \mathcal{M}$.

Diremos que un D_X-módulo $\mathcal{M}$ es *libre de torsión* si todos los D-módulos $\mathcal{M}_P$, con $P \in X$ son libres de torsión.

Vamos a necesitar un resultado técnico que está demostrado en el Apéndice A (teorema A.8). Sabemos, por 2.1, que el funtor $\otimes_D M$ es exacto por la derecha, y lo que afirma A.8 es que si D es un dominio de ideales principales y M es un D-módulo libre de torsión, entonces el funtor $\otimes_D M$ es exacto. (La demostración de A.8 se basa en el teorema precedente, que a su vez es independiente de todo lo anterior.) Esto nos da el teorema siguiente:

Teorema 2.29 *Sea*

$$0 \longrightarrow \mathcal{M}' \longrightarrow \mathcal{M} \longrightarrow \mathcal{M}'' \longrightarrow 0$$

una sucesión exacta de D_X-módulos y sea $\mathcal{N}$ un D_X-módulo paracompacto. Si $\mathcal{M}''$ o $\mathcal{N}$ es libre de torsión, entonces la sucesión

$$0 \longrightarrow \mathcal{M}' \otimes_{D_X} \mathcal{N} \longrightarrow \mathcal{M} \otimes_{D_X} \mathcal{N} \longrightarrow \mathcal{M}'' \otimes_{D_X} \mathcal{N} \longrightarrow 0$$

es exacta. Si, además, $\mathcal{M}'$ o $\mathcal{N}$ es paracompacto, entonces también es exacta la sucesión

$$0 \longrightarrow (\mathcal{M}' \otimes_{D_X} \mathcal{N})(X) \longrightarrow (\mathcal{M} \otimes_{D_X} \mathcal{N})(X) \longrightarrow (\mathcal{M}'' \otimes_{D_X} \mathcal{N})(X) \longrightarrow 0.$$

DEMOSTRACIÓN: Dado $P \in X$, las observaciones previas al teorema nos dan que uno de los funtores, $\otimes_D \mathcal{M}''_P$ o $\otimes_D \mathcal{N}_P$, es exacto y, en cualquiera de los dos casos, $\operatorname{Tor}_1^D(\mathcal{M}''_P, \mathcal{N}_P) = 0$, lo que hace exacta a la sucesión

$$0 \longrightarrow (\mathcal{M}' \otimes_{D_X} \mathcal{N})_P \longrightarrow (\mathcal{M} \otimes_{D_X} \mathcal{N})_P \longrightarrow (\mathcal{M}'' \otimes_{D_X} \mathcal{N})_P \longrightarrow 0.$$

Esto prueba la primera parte del teorema. Bajo las hipótesis de la segunda parte tenemos que $\mathcal{M}' \otimes_{D_X} \mathcal{N}$ es paracompacto, por 2.28, luego el teorema 2.27 nos da la conclusión. ■

Ya tenemos todos los elementos necesarios para obtener el teorema principal de esta sección. Supongamos que

$$0 \longrightarrow D_X \xrightarrow{\eta} \mathcal{I}^0 \longrightarrow \mathcal{I}^1 \longrightarrow \mathcal{I}^2 \longrightarrow \cdots$$

es una resolución paracompacta y libre de torsión del haz constante D_X. Si $\mathcal{M}$ es un D_X-módulo arbitrario. Si la reducimos (eliminamos D_X) y aplicamos el funtor covariante $\Gamma(- \otimes_{D_X} \mathcal{M})$, obtenemos un complejo

$$0 \longrightarrow (\mathcal{I}^0 \otimes_{D_X} \mathcal{M})(X) \longrightarrow (\mathcal{I}^1 \otimes_{D_X} \mathcal{M})(X) \longrightarrow (\mathcal{I}^2 \otimes_{D_X} \mathcal{M})(X) \longrightarrow \cdots$$

Llamaremos $\bar{H}^n(X, \mathcal{M})$ a los grupos (D-módulos) de cohomología de este complejo. Cada homomorfismo $M \longrightarrow \mathcal{M}'$ induce claramente un homomorfismo entre los complejos respectivos, el cual induce a su vez homomorfismos entre los grupos de cohomología, con lo que cada

$$\bar{H}^n(X, -) : \mathrm{Mod}(D_X) \longrightarrow \mathrm{Mod}(D)$$

es un funtor covariante (que —en principio— depende de la resolución de D_X de la que hemos partido).

Vamos a probar que esta familia de funtores tiene un homomorfismo de conexión. Para ello tomamos una sucesión exacta de D_X-módulos

$$0 \longrightarrow \mathcal{M}' \longrightarrow \mathcal{M} \longrightarrow \mathcal{M}'' \longrightarrow 0.$$

Como cada $\mathcal{I}^n$ es paracompacto y libre de torsión, el teorema 2.29 nos da que la sucesión de complejos

$$0 \longrightarrow (\mathcal{I}^n)_n \otimes_{D_X} \mathcal{M}' \longrightarrow (\mathcal{I}^n)_n \otimes_{D_X} \mathcal{M} \longrightarrow (\mathcal{I}^n)_n \otimes_{D_X} \mathcal{M}'' \longrightarrow 0$$

es exacta, y su sucesión exacta de cohomología conecta los funtores $\bar{H}^n(X, -)$ aplicados a la sucesión exacta de partida. También es obvio que un homomorfismo entre dos sucesiones exactas cortas da lugar a un diagrama conmutativo entre las dos sucesiones exactas largas. En suma, tenemos un homomorfismo de conexión.

Sea $\mathcal{H}^n$ el núcleo de $\mathcal{I}^n \longrightarrow \mathcal{I}^{n+1}$. Tenemos entonces la sucesión exacta

$$0 \longrightarrow \mathcal{H}^n \longrightarrow \mathcal{I}^n \longrightarrow \mathcal{H}^{n+1} \longrightarrow 0.$$

Como $\mathcal{I}^n$ es libre de torsión, lo mismo le sucede al subhaz $\mathcal{H}^n$. El teorema 2.29 nos da entonces la exactitud de

$$0 \longrightarrow \mathcal{H}^n \otimes_{D_X} \mathcal{M} \longrightarrow \mathcal{I}^n \otimes_{D_X} \mathcal{M} \longrightarrow \mathcal{H}^{n+1} \otimes_{D_X} \mathcal{M} \longrightarrow 0,$$

y la exactitud izquierda de Γ nos da la exactitud de

$$0 \longrightarrow (\mathcal{H}^n \otimes_{D_X} \mathcal{M})(X) \longrightarrow (\mathcal{I}^n \otimes_{D_X} \mathcal{M})(X) \longrightarrow (\mathcal{H}^{n+1} \otimes_{D_X} \mathcal{M})(X).$$

Esto implica que, en el siguiente diagrama conmutativo, las flechas verticales son inyectivas,

$$\begin{tikzcd}
(\mathcal{I}^{n-1} \otimes_{D_X} \mathcal{M})(X) \arrow[r] \arrow[rd] & (\mathcal{I}^n \otimes_{D_X} \mathcal{M})(X) \arrow[r, "(d_n \otimes 1)_X"] \arrow[rd] & (\mathcal{I}^{n+1} \otimes_{D_X} \mathcal{M})(X) \\
 & (\mathcal{H}^n \otimes_{D_X} \mathcal{M})(X) \arrow[u] & (\mathcal{H}^{n+1} \otimes_{D_X} \mathcal{M})(X) \arrow[u]
\end{tikzcd}$$

luego el núcleo de $(d_n \otimes 1)_X$ es el mismo que el de la flecha oblicua, que, por la sucesión exacta precedente, es la imagen de $(\mathcal{H}^n \otimes_{D_X} \mathcal{M})(X)$.

Si $n \geq 1$ todo vale igualmente para la parte izquierda del diagrama, luego

$$\bar{H}^n(X, \mathcal{M}) = (\mathcal{H}^n \otimes_{D_X} \mathcal{M})(X)/\operatorname{Im}(d_{n-1} \otimes 1)_X.$$

Observemos ahora que si $\mathcal{M}$ es paracompacto, entonces 2.29 nos da que la sucesión exacta previa al diagrama se puede prolongar con un 0, lo que significa que las flechas oblicuas del diagrama son suprayectivas, luego

$$\bar{H}^n(X, \mathcal{M}) = 0, \qquad \text{para } n \geq 1.$$

Puesto que todo D_X-módulo puede sumergirse en un D_X-módulo paracompacto, podemos aplicar el teorema 1.50 para concluir que la sucesión de funtores $\bar{H}^n(X, -)$ es universal.

Volvamos al caso general en que $\mathcal{M}$ es arbitrario y fijémonos en el caso $n = 0$. El diagrama anterior nos da que

$$\bar{H}^0(X, \mathcal{M}) \cong (\mathcal{H}^0 \otimes_{D_X} \mathcal{M})(X).$$

Ahora bien, tenemos un isomorfismo (fijo) $D_X \xrightarrow{\eta} \mathcal{H}^0$, el cual induce un isomorfismo

$$\mathcal{M} \cong D_X \otimes_{D_X} \mathcal{M} \cong \mathcal{H}^0 \otimes_{D_X} \mathcal{M},$$

que a su vez induce un isomorfismo (obviamente funtorial)

$$(\mathcal{H}^0 \otimes_{D_X} \mathcal{M})(X) \cong \mathcal{M}(X),$$

luego el funtor $\bar{H}^0(X, -)$ es isomorfo a $\Gamma(X, -)$.

La conclusión es que los funtores $\bar{H}^n(X, -)$ son isomorfos a los funtores $H^n(X, -)$. El teorema siguiente resume lo que hemos obtenido:

Teorema 2.30 *Los grupos de cohomología de un D_X-módulo $\mathcal{M}$ pueden calcularse a partir de cualquier resolución paracompacta y libre de torsión de D_X como los grupos de cohomología del complejo que resulta de aplicarle el funtor covariante $\Gamma(X, - \otimes_{D_X} \mathcal{M})$.*

Nota Si tenemos un homomorfismo entre dos resoluciones paracompactas y libres de torsión del módulo constante D_X, es decir, un diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & D_X \arrow[r] \arrow[d, "1"] & \mathcal{I}^0 \arrow[r] \arrow[d, "\phi_0"] & \mathcal{I}^1 \arrow[r] \arrow[d, "\phi_1"] & \mathcal{I}^2 \arrow[r] \arrow[d, "\phi_2"] & \cdots \\
0 \arrow[r] & D_X \arrow[r] & \mathcal{J}^0 \arrow[r] & \mathcal{J}^1 \arrow[r] & \mathcal{J}^2 \arrow[r] & \cdots
\end{tikzcd}$$

es claro que (ϕ_i) induce transformaciones naturales entre los grupos de cohomología construidos con ambas resoluciones (compatible con los homomorfismos de conexión), pero, como ambas familias de funtores son universales, sólo hay una familia de transformaciones naturales entre ellas, y está formada por isomorfismos. ■

Casi hemos probado el teorema siguiente:

Teorema 2.31 *Si X es un espacio anillado, todos los $\mathcal{O}_X$-módulos paracompactos son acíclicos.*

En efecto, sólo falta probar que existe una resolución paracompacta y libre de torsión del haz constante $\mathbb{Z}_X$. Si existe, podemos construir los funtores $\bar{H}^n(X, -)$, de los que hemos probado, por una parte, que son isomorfos a los funtores $H^n(X, -)$ y, por otra, que se anulan sobre los $\mathbb{Z}_X$-módulos paracompactos. Esto implica que los $\mathbb{Z}_X$-módulos paracompactos son acíclicos, pero todo $\mathcal{O}_X$-módulo paracompacto lo es también como $\mathbb{Z}_X$-módulo.

El teorema 2.26 implica la existencia de resoluciones paracompactas, pero no garantiza que sean libres de torsión. La existencia de tales resoluciones la probaremos (varias veces) en las secciones siguientes, en las que mostraremos cómo las distintas cohomologías introducidas de formas diversas en topología algebraica y en geometría diferencial son, en realidad, la cohomología que hemos definido en la sección 2.2 y que hemos estudiado en esta sección. Supondremos que el lector está familiarizado con los resultados básicos sobre las cohomologías que vamos a estudiar.[1]

2.6 La cohomología singular

En esta sección supondremos que X es una variedad topológica (es decir, un espacio con una base numerable en el que todo punto tiene un entorno isomorfo a un abierto de $\mathbb{R}^n$). Consideraremos también un anillo arbitrario D (no necesariamente un dominio de ideales principales).

El *símplice canónico* [2.3] de dimensión p es el conjunto

$$\Delta_p = \{(a_1, \ldots, a_p) \in \mathbb{R}^p \mid a_i \geq 0,\ \textstyle\sum a_i \leq 1\}.$$

Un *p-símplice singular* [2.5] en un espacio topológico X es una aplicación continua $\sigma : \Delta_p \longrightarrow X$. Si X es una variedad diferencial, el p-símplice es *diferenciable* [11.1] si se extiende a una aplicación diferenciable (es decir, de clase C^∞) definida en un entorno de Δ_p.

Representaremos por $C_p(X)$ [2.6] al D-módulo libre que tiene por base al conjunto de los p-símplices singulares en X. Si X es una variedad diferencial, $C_p^\infty(X)$ será [11.1] el D-módulo libre que tiene por base a los p-símplices singulares diferenciables en X. Los elementos de $C_p(X)$ se llaman *p-cadenas*

[1]De todos modos, indicaré entre corchetes las referencias a mi libro de Topología algebraica donde se pueden encontrar todas las demostraciones junto con más detalles de los hechos que vamos a necesitar.

singulares[2] en X. Entre estos módulos puede definirse un operador frontera que da lugar a un complejo directo:

$$\cdots \longrightarrow C_2(X) \xrightarrow{\partial_2} C_1(X) \xrightarrow{\partial_1} C_0(X) \xrightarrow{\partial_0} D \longrightarrow 0.$$

No vamos a dar los detalles de cómo se define el operador frontera [2.7], pues son algo técnicos y no los vamos a necesitar. Observemos únicamente que los 0-símplices son los puntos de X y que ∂_0 asigna la imagen 1 a cada 0-símplice.

Los grupos de homología de este complejo se llaman *grupos de homología singular* [2.12] de X, y se representan[3] por $H_p(X)$. Los *grupos de homología singular diferenciable* [11.1] los representaremos por $H_p^\infty(X)$.

Conviene observar cómo afecta a estas construcciones la elección del anillo de coeficientes D. Para ello basta tener presente que al multiplicar un $\mathbb{Z}$-módulo libre por $\otimes_\mathbb{Z} D$ obtenemos el D-módulo libre del mismo rango (porque el producto tensorial conserva sumas directas y $\mathbb{Z}\otimes_\mathbb{Z} D \cong D$). Por consiguiente, se cumple que

$$C_p^D(X) = C_p^\mathbb{Z}(X)\otimes_\mathbb{Z} D.$$

Si N es un D-módulo, definimos los *grupos de cocadenas singulares* de X con coeficientes en N como los D-módulos

$$C^p(X,N) = \mathrm{Hom}_D(C_p(X),N), \qquad (\text{resp. } C^p_\infty(X,N) = \mathrm{Hom}_D(C_p^\infty(X),N)).$$

La definición dada en [5.42] de los grupos de cohomología singular no es ésta, pero es equivalente, como allí mismo se explica. Recordamos el argumento:

Es fácil comprobar en general que si M es un $\mathbb{Z}$-módulo y R y N son D-módulos, tenemos el siguiente isomorfismo de D-módulos:

$$\mathrm{Hom}_D(M\otimes_\mathbb{Z} R, N) \cong \mathrm{Hom}_\mathbb{Z}(M, \mathrm{Hom}_D(R,N)).$$

En nuestro contexto, esto implica que

$$C^p_D(X) = \mathrm{Hom}_D(C_p^D(X),N) \cong \mathrm{Hom}_D(C_p^\mathbb{Z}(X)\otimes_\mathbb{Z} D, N)$$

$$\cong \mathrm{Hom}_\mathbb{Z}(C_p^\mathbb{Z}(X), \mathrm{Hom}_D(D,N)) \cong \mathrm{Hom}_\mathbb{Z}(C_p^\mathbb{Z}(X),N).$$

En definitiva, que para definir la cohomología singular con coeficientes en un D-módulo N (en particular, en el propio D) es indistinto partir de la cohomología singular con coeficientes en D o con coeficientes en $\mathbb{Z}$, pues llegamos a los mismos módulos.

---

[2] Y los elementos de $C_p^\infty(X)$ se llaman p-cadenas singulares diferenciables. Todo cuando vamos a decir en el caso continuo tiene su análogo en el caso diferenciable, pero no volveremos a indicarlo salvo que haya alguna diferencia destacable.

[3] En [2.6] distinguimos entre la homología completa y la homología reducida según se se conserva o se elimina el módulo D en el complejo de cadenas singulares. Esto sólo modifica el resultado para $H_0(X)$.

Esto se pone de manifiesto explícitamente si observamos que, en ambos casos, las cocadenas singulares de dimensión p se corresponden biunívocamente con las aplicaciones que asignan un elemento de N a cada p-símplice singular.

Con más precisión, los funtores contravariantes $\mathrm{Mod}(\mathbb{Z}) \longrightarrow \mathrm{Mod}(D)$ dados por $\mathrm{Hom}_D(- \otimes_{\mathbb{Z}} D, N)$ y $\mathrm{Hom}_{\mathbb{Z}}(-, N)$ son isomorfos, por lo que las dos definiciones de los grupos de cohomología singular son también intercambiables a la hora de formar los *complejos de cocadenas singulares,* que son los complejos inversos que resultan de aplicar estos funtores al complejo de cadenas singulares:

$$0 \longrightarrow N \longrightarrow C^0(X, N) \xrightarrow{d_0} C^1(X, N) \xrightarrow{d_1} C^2(X, N) \longrightarrow \cdots$$

Los grupos de cohomología de este complejo se llaman *grupos de cohomología singular* de X con coeficientes en N, y los representaremos por $H^p(X, N)$.

Vamos a necesitar la versión para cohomología del teorema [2.43]. Éste afirma que si $\mathcal{U}$ es un cubrimiento abierto de X y llamamos $C_p(X; \mathcal{U})$ al submódulo de $C_p(U)$ generado por los p-símplices contenidos en algún abierto de $\mathcal{U}$, entonces estos submódulos forman un complejo con la restricción del operador frontera, y sus grupos de homología, denotados por $H_p(X; \mathcal{U})$, son isomorfos a los grupos $H_p(X)$.

La demostración consiste en construir un homomorfismo de complejos

$$\Phi_p : C_p(X) \longrightarrow C_p(X; \mathcal{U})$$

tal que si $i_p : C_p(X; \mathcal{U}) \longrightarrow C_p(X)$ es la inclusión, entonces $i \circ \Phi$ es la identidad y $\Phi \circ i$ es homotópico a la identidad.

Definimos ahora $C^p(X, N; \mathcal{U}) = \mathrm{Hom}_D(C_p(X; \mathcal{U}), N)$, que es un complejo con el operador cofrontera natural (el que resulta de aplicar al operador frontera el mismo funtor $\mathrm{Hom}_D(-, N)$), lo que a su vez nos permite definir $H^p(X, N; \mathcal{U})$ como los grupos de cohomología de este complejo.

Las inclusiones $i_p : C_p(X; \mathcal{U}) \longrightarrow C_p(X)$ se corresponden, al dualizar, con las restricciones $C^p(X, N) \longrightarrow C^p(X, N; \mathcal{U})$, y al aplicar el funtor $\mathrm{Hom}_D(-, N)$ al homomorfismo Φ y a la homotopía entre $i \circ \Phi$ y la identidad, obtenemos el dual de [2.43] al que hacíamos referencia, es decir, que las restricciones inducen isomorfismos[4]

$$H^p(X, N) \longrightarrow H^p(X, N; \mathcal{U}).$$

Consideramos ahora el prehaz $\mathcal{C}^{p-}_{X,N}$ que a cada abierto $U \subset X$ le asigna el D-módulo $\mathcal{C}^{p-}_{X,N}(U) = C^p(U, N)$ y en el que las restricciones son las restricciones usuales de homomorfismos (notemos que si $U \subset V$, entonces $C_p(U)$ es un submódulo de $C_p(V)$).

Es claro que estos prehaces cumplen la segunda condición de la definición de haz (sobre extensión de elementos consistentes), pero cuando $p \geq 1$ no tienen

[4]La prueba del teorema [2.43] vale sin cambio alguno para símplices diferenciables, luego todo cuanto diremos a continuación seguirá siendo válido igualmente para la cohomología diferenciable.

por qué cumplir la primera. (Si tenemos un cubrimiento abierto de X, puede ocurrir que ninguno de los símplices de una p-cadena de X esté contenido en ninguno de los abiertos del cubrimiento, y una cocadena que sólo tome valores no nulos sobre esta clase de símplices tendrá restricciones nulas a todos los abiertos del cubrimiento sin ser, ella misma, nula.)

Representaremos por $\mathcal{C}^p_{X,N}$ la compleción del prehaz de cocadenas singulares de dimensión p en X.

Es evidente que los operadores cofrontera d_p son consistentes con las restricciones de los prehaces de cocadenas singulares, por lo que inducen homomorfismos de prehaces, los cuales determinan un complejo de prehaces:

$$0 \longrightarrow N_X^- \longrightarrow \mathcal{C}^0_{X,N} \xrightarrow{d_0} \mathcal{C}^{1-}_{X,N} \xrightarrow{d_1} \mathcal{C}^{2-}_{X,N} \longrightarrow \cdots$$

Extendiendo estos homomorfismos a las compleciones obtenemos un complejo de haces

$$0 \longrightarrow N_X \longrightarrow \mathcal{C}^0_{X,N} \xrightarrow{d_0} \mathcal{C}^1_{X,N} \xrightarrow{d_1} \mathcal{C}^2_{X,N} \longrightarrow \cdots$$

Vamos a demostrar que se trata de una resolución paracompacta del haz constante N_X. Además será libre de torsión si N es un D-módulo libre de torsión. El caso particular $N = D = \mathbb{Z}$ terminará la prueba de que todos los D_X-módulos paracompactos son acíclicos (como $\mathbb{Z}_X$-módulos, luego también como $\mathcal{O}_X$-módulos para cualquier estructura de espacio anillado sobre X), y así, cualquier resolución paracompacta (sea libre de torsión o no) servirá para calcular los grupos de cohomología de cualquier módulo. En particular, podremos concluir que los grupos de cohomología $H^n(X, N_X)$ son los grupos de cohomología del complejo

$$0 \longrightarrow N_X \longrightarrow \mathcal{C}^0_{X,N}(X) \xrightarrow{d_0} \mathcal{C}^1_{X,N}(X) \xrightarrow{d_1} \mathcal{C}^2_{X,N}(X) \longrightarrow \cdots$$

Ahora bien, estos no son, en principio, los grupos clásicos de cohomología singular, puesto que $\mathcal{C}^p_{X,N}(X)$ no es lo mismo que $C^p(X, N)$. El teorema siguiente nos da la relación entre ambos grupos:

Teorema 2.32 *Sea $\mathcal{F}$ un prehaz que cumpla la segunda condición de la definición de haz, sea $\mathcal{F}^+$ su compleción, sea $j^+ : \mathcal{F} \longrightarrow \mathcal{F}^+$ el homomorfismo natural y sea*

$$\mathcal{F}(X)_0 = \{f \in \mathcal{F}(X) \mid f_P = 0 \text{ para todo } P \in X\}.$$

Entonces, la sucesión

$$0 \longrightarrow \mathcal{F}(X)_0 \longrightarrow \mathcal{F}(X) \xrightarrow{j^+_X} \mathcal{F}^+(X) \longrightarrow 0$$

es exacta.

Demostración: Es obvio que $\mathcal{F}(X)_0$ es el núcleo de j_X^+. Sólo hemos de probar que j_X^+ es suprayectiva. Tomemos $t \in \mathcal{F}^+(X)$. Puesto que los homomorfismos j_P^+ son isomorfismos, existe un cubrimiento abierto $\{U_i\}_{i\in I}$ de X de modo que existen elementos $s_i \in \mathcal{F}(U_i)$ con $j_{U_i}^+(s_i) = t|_{U_i}$.

La paracompacidad de X nos permite suponer que el cubrimiento es localmente finito, así como tomar un refinamiento $\{V_i\}_{i\in I}$ tal que $V_i \subset \overline{V}_i \subset U_i$. (Ver la prueba de 2.26).

Sea I_P el conjunto (finito) de índices i tales que $P \in \overline{V}_i$. Por la finitud local del cubrimiento, la unión de las clausuras de los V_i con $i \notin I_P$ es cerrada, luego podemos tomar un entorno abierto W_P de P tal que

a) $W_P \cap \overline{V}_i = \varnothing$ para todo $i \notin I_P$,

b) $W_P \subset U_i$ para todo $i \in I_P$,

c) $s_i|_{W_P} = s_j|_{W_P}$ para todo $i, j \in I_P$.

(Para la condición c, notamos que s_{iP} es necesariamente la única antiimagen de t_P por j_P^+.) Llamemos $s_P \in \mathcal{F}(W_P)$ a la restricción común indicada en c).

Veamos ahora que $s_P|_{W_P\cap W_Q} = s_Q|_{W_P\cap W_Q}$. En efecto, tomemos un punto $R \in W_P \cap W_Q$. Por a) vemos que $I_R \subset I_P \cap I_Q$. Tomemos $i \in I_R$. Por c), se cumple que $s_P = s_i|_{W_P}$ y $s_Q = s_i|_{W_Q}$, luego

$$s_P|_{W_P\cap W_Q} = s_i|_{W_P\cap W_Q} = s_Q|_{W_P\cap W_Q}.$$

Estamos suponiendo que $\mathcal{F}$ cumple la segunda condición de la definición de haz, luego existe un $s \in \mathcal{F}(X)$ tal que $s|_{W_P} = s_P$ para todo P. Entonces $j^+(s)_P = t_P$ para todo $P \in X$ y, como $\mathcal{F}^+$ es un haz, esto implica que $j^+(s) = t$.

■

Volviendo a las cocadenas singulares, tenemos una sucesión exacta

$$0 \longrightarrow C^p(X,N)_0 \longrightarrow C^p(X,N) \xrightarrow{j_X^+} \mathcal{C}^p_{X,N}(X) \longrightarrow 0,$$

que determina una sucesión exacta corta de complejos de D-módulos al variar p. Si demostramos que todos los grupos de cohomología del primer complejo son nulos, entonces la sucesión exacta larga asociada a la sucesión anterior implicará que el homomorfismo de compleción induce isomorfismos

$$\bar{j}_X^+ : H^p(X,N) \longrightarrow H^p(X,N_X)$$

entre los grupos clásicos de cohomología singular con coeficientes en N y los grupos de cohomología del D_X-módulo constante N_X.

Así pues, nos fijamos ahora en el complejo

$$0 \longrightarrow C^0(X,N)_0 \longrightarrow C^1(X,N)_0 \longrightarrow C^2(X,N)_0 \longrightarrow \cdots$$

formados por las cocadenas singulares localmente nulas. (Notemos que hemos eliminado el término correspondiente a N_X porque los grupos de cohomología se calculan con los complejos reducidos, luego son los grupos de cohomología de este complejo reducido los que tienen que ser todos nulos para obtener los isomorfismos indicados.)

Observemos en primer lugar que $C^0(X,N)_0 = 0$, porque el prehaz $\mathcal{C}^{0-}_{X,N}$ ya es un haz (aunque también se puede ver directamente sin dificultad). Esto ya prueba que el grupo de cohomología de orden 0 es nulo. Fijemos, pues, $q \geq 1$, tomemos un $f \in C^q(X,N)_0$ tal que $df = 0$ y hemos de encontrar un $g \in C^{q-1}(X,N)$ tal que $f = dg$.

Que f sea localmente nulo significa que existe un cubrimiento abierto $\mathcal{U}$ de X tal que $f|_U = 0$ para todo abierto $U \in \mathcal{U}$. Tenemos una sucesión exacta de complejos

$$0 \longrightarrow \mathcal{N} \longrightarrow \{C^p(X,N)\}_p \longrightarrow \{C^p(X,N;\mathcal{U})\}_p \longrightarrow 0,$$

donde los epimorfismos son las restricciones y los módulos $\mathcal{N}^p$ son sus núcleos. Ahora bien, sabemos que las restricciones inducen isomorfismos en los grupos de cohomología, luego la sucesión exacta larga asociada a esta sucesión de complejos prueba que el complejo $\mathcal{N}$ tiene todos sus grupos de cohomología nulos, pero $f \in \mathcal{N}^q$ cumple $df = 0$, luego existe un $g \in \mathcal{N}^{q-1} \subset C^{q-1}(X,N)$ tal que $f = dg$, que es lo que queríamos probar.

Sólo nos falta demostrar que el complejo

$$0 \longrightarrow N_X \longrightarrow \mathcal{C}^0_{X,N} \xrightarrow{d_0} \mathcal{C}^1_{X,N} \xrightarrow{d_1} \mathcal{C}^2_{X,N} \longrightarrow \cdots$$

es una resolución paracompacta y libre de torsión de N_X. Veamos en primer lugar que es una sucesión exacta, lo que equivale a probar que lo es en cada punto $P \in X$, para lo cual podemos trabajar con el complejo de prehaces

$$0 \longrightarrow N_X^- \longrightarrow \mathcal{C}^0_{X,N} \xrightarrow{d_0} \mathcal{C}^{1-}_{X,N} \xrightarrow{d_1} \mathcal{C}^{2-}_{X,N} \longrightarrow \cdots$$

ya que las localizaciones de los homomorfismos son las mismas.

Observemos que $\mathcal{C}^0_{X,N}(U) = \mathcal{C}^{0-}_{X,N}(U)$ es simplemente el conjunto de todas las aplicaciones de U en D, mientras que $N_X^-(U)$ es el conjunto de todas las aplicaciones constantes. Claramente, entonces, el primer homomorfismo es inyectivo.

Tomemos ahora un $[f] \in \mathcal{C}^0_{X,N,P}$ tal que $[df] = 0$. Podemos restringir f hasta un entorno de P arbitrariamente pequeño. Ahora usamos por primera vez la hipótesis de que X es una variedad topológica, al tomar un entorno U de P que sea arcoconexo. Para cada par de puntos $x, y \in U$ existe un arco $\sigma : \Delta_1 = [0,1] \longrightarrow U$ tal que $\sigma(0) = x$, $\sigma(1) = y$. Así, σ es un 1-símplice y, por las definiciones de los operadores frontera y cofrontera,

$$df(\sigma) = f(\partial\sigma) = f(y) - f(x) = 0.$$

Esto prueba que f es constante en U, luego $f \in N_D^-(U)$ y tenemos la exactitud en $\mathcal{C}^0_{X,N,P}$.

Fijemos ahora $p \geq 1$ y tomemos un $[f] \in \mathcal{C}^{p-}_{X,N,P}$ tal que $[df] = 0$. Usamos por segunda vez la hipótesis de que X es una variedad topológica al restringir f a un entorno U de p que sea homeomorfo a una bola abierta de $\mathbb{R}^n$, lo que en particular implica que es *homotópico a un punto* [1.26] (porque las bolas son convexas y se les puede aplicar [1.24]). Esto hace que los grupos $H^p(U, N)$ sean homeomorfos a los grupos de cohomología de un punto. En nuestro caso, $p \geq 1$, luego $H^p(U, N) = 0$. Así pues, existe un $g \in \mathcal{C}^{p-1-}_{X,N}(U)$ tal que $[f] = [dg]$. Con esto tenemos probada la exactitud del complejo, es decir, que ciertamente se trata de una resolución del haz constante N_X.

Si N es un D-módulo libre de torsión, los haces $\mathcal{C}^p_{X,N}$ también lo son. En efecto, si $[f] \in \mathcal{C}^p_{X,N,P} = \mathcal{C}^{p-}_{X,N,P}$ cumple que $[af] = 0$ para cierto $a \in D$ no nulo, entonces, restringiendo f, si es preciso, a un dominio U menor, tenemos que $af = 0$, luego, para todo $\sigma \in C_p(U, N)$, se cumple que $af(\sigma) = 0$, luego $f(\sigma) = 0$, luego $f = 0$.

Sólo nos falta probar que los haces $\mathcal{C}^p_{X,N}$ son paracompactos. Tomemos un cubrimiento abierto $\{U_i\}_{i\in I}$ de X localmente finito y consideremos las funciones $\chi_i : X \longrightarrow \{0, 1\}$ definidas como en la prueba del teorema 2.26 (lo que supone tomar previamente otro cubrimiento $\{V_i\}_{i\in I}$ tal que $V_i \subset \overline{V}_i \subset U_i$). Para cada abierto $U \subset X$, definimos $\phi^-_{iU} : C^p_{X,N}(U) \longrightarrow C^p_{X,N}(U)$ mediante

$$\phi^-_{iU}(f)(\sigma) = \chi_i(\sigma(0))f(\sigma),$$

donde $0 \in \mathbb{R}^n$ es el origen de coordenadas (un vértice del símplice Δ_p). Es obvio que estos endomorfismos conmutan con las restricciones, por lo que definen un homomorfismo de prehaces ϕ^-_i, que a su vez se extiende a un homomorfismo de haces $\phi_i : \mathcal{C}^p_{X,N} \longrightarrow \mathcal{C}^p_{X,N}$. Es evidente que $\operatorname{sop} \phi_i \subset \overline{V}_i \subset U_i$, así como que $\sum\limits_i \phi_i = I$.

El teorema siguiente resume lo que hemos obtenido:

Teorema 2.33 *Si X es una variedad topológica, D es un anillo y N es un D-módulo, entonces tenemos isomorfismos*

$$H^p(X, N_X) \cong H^p(X, N) \cong H^p_\infty(X, N)$$

entre los grupos de cohomología del haz constante N_X y los grupos de cohomología singular y cohomología singular diferenciable de X.

Observemos por último que las restricciones determinan homomorfismos de complejos

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & N_U & \longrightarrow & C^0(U,N) & \longrightarrow & C^1(U,N) & \longrightarrow & C^2(U,N) & \longrightarrow & \cdots \\
 & & \big\downarrow{\scriptstyle 1} & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\
0 & \longrightarrow & N_U & \longrightarrow & C^0_\infty(U,N) & \longrightarrow & C^1_\infty(U,N) & \longrightarrow & C^2_\infty(U,N) & \longrightarrow & \cdots
\end{array}$$

que claramente determinan un homomorfismo entre los complejos de prehaces $\{\mathcal{C}^{p-}_{X,N}\}_p$ y $\{\mathcal{C}^{p-}_{X,N,\infty}\}_p$, que a su vez se extienden a un homomorfismo entre los complejos de haces $\{\mathcal{C}^{p}_{X,N}\}_p$ y $\{\mathcal{C}^{p}_{X,N,\infty}\}_p$.

Ahora observamos que el teorema 2.30 es válido igualmente si en lugar de partir de una resolución de D_X partimos de una de N_X, sólo que la familia de funtores que obtenemos en la construcción precedente a dicho teorema ya no es la de los funtores derivados de $\Gamma(X,-)$, sino la de los funtores derivados de $\Gamma(X,-\otimes_{D_X} N_X)$. La nota posterior al teorema se aplica igualmente, y nos da que el homomorfismo que tenemos entre ambas resoluciones induce una transformación natural entre las dos construcciones de los funtores derivados, y que ésta ha de ser un isomorfismo. El isomorfismo correspondiente a D_X resulta de multiplicar el diagrama conmutativo anterior por $\otimes_{D_X} D_X$ (que es equivalente a no hacer nada), luego aplicamos $\Gamma(X,-)$, con lo que obtenemos el homomorfismo de complejos

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{C}^0_{X,N}(X) \arrow[r] \arrow[d] & \mathcal{C}^1_{X,N}(X) \arrow[r] \arrow[d] & \mathcal{C}^2_{X,N}(X) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathcal{C}^0_{X,N,\infty}(X) \arrow[r] & \mathcal{C}^1_{X,N,\infty}(X) \arrow[r] & \mathcal{C}^2_{X,N,\infty}(X) \arrow[r] & \cdots
\end{tikzcd}$$

que, según lo dicho, debe inducir isomorfismos entre los grupos de cohomología. Tenemos entonces los siguientes diagramas conmutativos:

$$\begin{tikzcd}
C^p(X,N) \arrow[r, "j_X^+"] \arrow[d, "r"'] & \mathcal{C}^p_{X,N}(X) \arrow[d] \\
C^p_\infty(X,N) \arrow[r, "j_X^+"'] & \mathcal{C}^p_{X,N,\infty}(X)
\end{tikzcd}$$

en el que las flechas horizontales y la vertical derecha inducen isomorfismos en los grupos de cohomología, luego lo mismo le sucede a la flecha vertical derecha. En resumen, hemos probado el teorema siguiente:

Teorema 2.34 *Si D es un dominio de ideales principales y N es un D-módulo libre de torsión, la restricción $C^p(X,N) \longrightarrow C^p_\infty(X,N)$ induce un isomorfismo $H^p(X,N) \longrightarrow H^p_\infty(X,N)$ entre los grupos de cohomología singular y de cohomología singular diferenciable.*

2.7 La cohomología de Alexander-Spanier

La cohomología que vamos a definir en esta sección puede considerarse como una drástica simplificación de la cohomología singular, que conserva únicamente lo esencial para que, en efecto, se trate de una cohomología, sacrificando en aras de la sencillez las ideas topológicas subyacentes en la construcción de la cohomología singular. Como una primera muestra de ello, en esta sección no necesitamos que X sea una variedad topológica, sino que sirve cualquier espacio paracompacto. De nuevo D es un anillo arbitrario y N es un D-módulo.

La idea principal es sustituir un p-símplice en X por el conjunto de sus $p+1$ vértices. Si pensamos que $\sigma = (x_0, \ldots, x_p) \in X^{p+1}$ representa un p-símplice, entonces su "cara" i-ésima es $\sigma^i = (x_0, \ldots, \hat{x}_i, \ldots, x_p)$, donde el circunflejo indica que hemos suprimido la componente i-ésima.

Definimos $A^p(X, N)$ como el conjunto de todas las aplicaciones de X^{p+1} en N, que es un D-módulo con las operaciones definidas puntualmente. Definimos el operador cofrontera $d_p : A^p(X, N) \longrightarrow A^{p+1}(X, N)$ mediante

$$(d_p f)(\sigma) = \sum_{i=0}^{p+1} (-1)^i f(\sigma^i).$$

Una comprobación sencilla muestra que $d_p \circ d_{p+1} = 0$, por lo que tenemos un complejo

$$0 \longrightarrow N \xrightarrow{\epsilon} A^0(X, N) \xrightarrow{d_0} A^1(X, N) \xrightarrow{d_1} A^2(X, N) \longrightarrow \cdots$$

donde $\epsilon(n)$ es la función constante n. (Notemos que d_0 se anula sobre las funciones constantes.)

Esto vale para todo espacio topológico X, luego en particular para todo abierto $U \subset X$, y el operador cofrontera es claramente compatible con las restricciones $A^p(U, N) \longrightarrow A^p(V, N)$ (donde $V \subset U \subset X$). Tenemos, pues, un complejo de prehaces

$$0 \longrightarrow N_X^- \longrightarrow \mathcal{A}^0_{X,N} \longrightarrow \mathcal{A}^{1-}_{X,N} \longrightarrow \mathcal{A}^{2-}_{X,N} \longrightarrow \cdots$$

Como en el caso de la cohomología singular, estos prehaces cumplen la segunda condición de haz, pero no la primera (excepto para $p = 0$, pues en este caso se cumplen ambas).

Pasando a las compleciones obtenemos un complejo de haces

$$0 \longrightarrow N_X \longrightarrow \mathcal{A}^0_{X,N} \longrightarrow \mathcal{A}^1_{X,N} \longrightarrow \mathcal{A}^2_{X,N} \longrightarrow \cdots$$

Se demuestra que los haces $\mathcal{A}^p_{X,N}$ son paracompactos, así como que son libres de torsión si N lo es. La prueba es idéntica al caso de la cohomología singular, sin más que cambiar $\sigma \in C_p(U, N)$ por $\sigma \in U^{p+1}$.

La prueba de que el complejo es exacto es mucho más simple. De hecho, todos los complejos

$$0 \longrightarrow N \longrightarrow A^0(U, N) \longrightarrow A^1(U, N) \longrightarrow A^2(U, N) \longrightarrow \cdots$$

son exactos (lo que implica inmediatamente la exactitud del complejo de prehaces, y ésta a su vez la del complejo de haces).

En efecto: La exactitud en N es inmediata, pues $A^0(U, N)$ está formado por las aplicaciones $U \longrightarrow N$ y la imagen de N la forman las funciones constantes.

La exactitud en A^0 se debe a que si $f \in A^0(U,N)$ cumple que $df = 0$, entonces, para todo par de puntos x, $y \in U$, tenemos que $0 = df(x,y) = f(y) - f(x)$, luego f es constante. Por último, para probar la exactitud en $A^p(U,N)$ (para $p \geq 1$) tomamos $f \in A^p(U,N)$ tal que $df = 0$ y fijamos un $x_0 \in U$. Entonces, para cada $\tau = (a_0,\ldots,a_p) \in U^{p+1}$, se cumple que

$$0 = df(x_0,\tau) = f(\tau) - \sum_{i=0}^{p} (-1)^i f(x_0,\tau^i).$$

Esto significa que si definimos $g \in A^{p-1}(U)$ mediante $g(\sigma) = f(x_0,\sigma)$, entonces

$$f(\tau) = \sum_{i=0}^{p} (-1)^i g(\tau^i) = dg(\tau),$$

luego $f = dg$ y tenemos la exactitud en A^p.

En definitiva, hemos vuelto a demostrar la existencia de resoluciones paracompactas y libres de torsión de los módulos constantes D_X, y ahora sabemos que los grupos de cohomología $H^p(X,N_X)$ pueden calcularse como los grupos de cohomología del complejo

$$0 \longrightarrow \mathcal{A}^0_{X,N}(X) \longrightarrow \mathcal{A}^1_{X,N}(X) \longrightarrow \mathcal{A}^2_{X,N}(X) \longrightarrow \cdots$$

Notemos que el paso a la compleción es crucial, ya que, según hemos probado, el complejo $A^p(X,N)$ es exacto (excepto en A^0, pues ahora hablamos del complejo reducido). El teorema 2.32 nos da una interpretación de este complejo que puede formularse sin hacer referencia a haces ni a compleciones:

Definición 2.35 Si X es un espacio topológico paracompacto, D es un anillo, N es un D-módulo y $A^p(X,N)$ es el conjunto de aplicaciones $X^{p+1} \longrightarrow N$, llamaremos $A^p(X,N)_0$ al submódulo de $A^p(X,N)$ formado por las funciones f para las que existe un cubrimiento abierto $\mathfrak{U}$ de X tal que $f|_{U^{p+1}} = 0$ para todo $U \in \mathfrak{U}$. El *grupo de p-cocadenas de Alexander-Spanier* con coeficientes en N es el cociente

$$A^p_*(X,N) = A^p(X,N)/A^p(X,N)_0.$$

Es claro que el operador cofrontera induce un operador en los cocientes, con lo que tenemos un complejo

$$0 \longrightarrow A^0_*(X,N) \longrightarrow A^1_*(X,N) \longrightarrow A^2_*(X,N) \longrightarrow \cdots$$

cuyos grupos de cohomología $H^p_*(X,N)$ reciben el nombre de *grupos de cohomología de Alexander-Spanier* de X con coeficientes en N.

El teorema 2.32 nos asegura que este complejo es isomorfo al complejo $\mathcal{A}^p_{X,N}(X)$, luego hemos demostrado el teorema siguiente:

Teorema 2.36 *Si X es un espacio paracompacto, D es un anillo y N es un D-módulo, entonces tenemos isomorfismos $H^p(X,N_X) \cong H^p_*(X,N)$ entre los grupos de cohomología del haz constante N_X y los grupos de cohomología de Alexander-Spanier.*

En particular, si X es una variedad topológica, tenemos isomorfismos

$$H^p_*(X,N) \cong H^p(X,N) \cong H^p_\infty(X,N)$$

entre los grupos de cohomología de Alexander-Spanier y los grupos de cohomología singular. Bajo la hipótesis de que D sea un dominio de ideales principales y N un D-módulo libre de torsión, podemos mostrarlos explícitamente. Consideremos el homomorfismo

$$\phi_{pU} : A^p(U,N) \longrightarrow C^p(U,N)$$

tal que $\phi_p(f)$ actúa sobre un p-símplice como f sobre la $(p+1)$-tupla de sus vértices. Es claro que estos homomorfismos inducen un homomorfismo ϕ_p^- prehaces, que se extiende a un homomorfismo de haces

$$\phi_p : \mathcal{A}^p_{X,N} \longrightarrow \mathcal{C}^p_{X,N}.$$

La definición del operador cofrontera de la cohomología de Alexander-Spanier se corresponde con la definición para la cohomología singular, de modo que es fácil ver que los ϕ_p determinan un homomorfismo de complejos, que a su vez induce un homomorfismo entre las resoluciones

$$\begin{tikzcd}
0 \arrow[r] & N_X \arrow[r] \arrow[d, "1"'] & \mathcal{A}^0_{X,N} \arrow[r] \arrow[d] & \mathcal{A}^1_{X,N} \arrow[r] \arrow[d] & \mathcal{A}^2_{X,N} \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & N_X \arrow[r] & \mathcal{C}^0_{X,N} \arrow[r] & \mathcal{C}^1_{X,N} \arrow[r] & \mathcal{C}^2_{X,N} \arrow[r] & \cdots
\end{tikzcd}$$

Por el mismo razonamiento con el que obtuvimos el isomorfismo explícito entre la cohomología singular y la cohomología singular diferenciable, este homomorfismo de complejos induce un isomorfismo entre las construcciones que proporciona cada resolución de los funtores derivados de $\Gamma(X, - \otimes_{D_X} N_X)$. Los isomorfismos para el módulo D_X son los inducidos por el homomorfismo de complejos

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{A}^0_{X,N}(X) \arrow[r] \arrow[d] & \mathcal{A}^1_{X,N}(X) \arrow[r] \arrow[d] & \mathcal{A}^2_{X,N}(X) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathcal{C}^0_{X,N}(X) \arrow[r] & \mathcal{C}^1_{X,N}(X) \arrow[r] & \mathcal{C}^2_{X,N}(X) \arrow[r] & \cdots
\end{tikzcd}$$

Este homomorfismo de complejos se corresponde, a través de sendos isomorfismos de complejos, con el homomorfismo formado por los homomorfismos

$$A^p_*(X,N) \longrightarrow C^p(X,N)/C^p(X,N)_0$$

inducidos por ϕ_p de forma natural. Así pues, ϕ_p induce un isomorfismo entre $H^p_*(X,N)$ y el p-ésimo grupo de cohomología del complejo de la derecha, que es isomorfo a $H^p(X,N)$. El isomorfismo $H^p_*(X,N) \longrightarrow H^p(X,N)$ resultante es el que a la clase de cohomología del cociclo determinado por $[f]$ le hace corresponder la clase de cohomología de $\phi_p(f)$. Esto es correcto porque si $[f] = [g]$, entonces f y g se diferencian en un cociclo $h \in A^p(X,N)_0$, y $\phi_p(h)$ es también un cociclo que pertenece a $C^p(X,N)_0$, pero hemos visto que todos los cociclos de este submódulo son cofronteras, luego $\phi_p(f)$ y $\phi_p(g)$ determinan la misma clase de cohomología.

Naturalmente, el mismo razonamiento es válido con la cohomología singular diferenciable.

2.8 La cohomología de De Rham

En esta sección X será una variedad diferencial y $D = \mathbb{R}$. Llamaremos $\Lambda^p(X)$ al espacio vectorial de las formas diferenciales [11.8] de grado p sobre X. Estos espacios forman un complejo con la diferencial exterior [11.10]:

$$0 \longrightarrow \mathbb{R} \longrightarrow \Lambda^0(X) \longrightarrow \Lambda^1(X) \longrightarrow \Lambda^2(X) \longrightarrow \cdots$$

(Notemos que $\Lambda^0(X) = \mathbb{C}^\infty(X)$, de modo que el primer homomorfismo es el que asigna a cada número real r la función constante igual a r.)

Los grupos de cohomología $H^p(X)$ de este complejo se llaman *grupos de cohomología de De Rham* de la variedad X. [11.11]

Es claro que los espacios $\Lambda^p(U)$, cuando U recorre los abiertos de X, forman un haz Λ^p_X, y que la diferencial exterior es compatible con las restricciones, por lo que tenemos un complejo de haces

$$0 \longrightarrow \mathbb{R}_X \longrightarrow \Lambda^0_X \longrightarrow \Lambda^1_X \longrightarrow \Lambda^2_X \longrightarrow \cdots$$

El primer homomorfismo es la compleción del homomorfismo de prehaces $\mathbb{R}^-_X \longrightarrow \Lambda^0_X$. Para cada abierto $U \subset X$, tenemos que $\mathbb{R}_X(U) \longrightarrow \Lambda^0_X(U)$ identifica a $\mathbb{R}_X(U)$ con el espacio de las funciones localmente constantes en U.

Veamos ahora que el complejo es una resolución paracompacta y libre de torsión de $\mathbb{R}_X$. Los $\mathbb{R}_X$-módulos Λ^p_X son libres de torsión porque $\mathbb{R}$ es un cuerpo, y son paracompactos porque son C^∞_X-módulos (teorema 2.25). La exactitud de la sucesión para $p \geq 1$ se comprueba exactamente igual que en el caso de la cohomología singular: es consecuencia de que todo punto $P \in X$ tiene un entorno U homotópico a un punto (es decir, contractible) y que entonces $H^p(U) = 0$ (teorema [11.14]). La exactitud en $\mathbb{R}_X$ ya la hemos comprobado (hemos visto que $\mathbb{R}_X \longrightarrow \Lambda^0_X$ es un monomorfismo) y la exactitud en Λ^0_X se debe a que una función $f \in \Lambda^0(U) = \mathbb{C}^\infty(U)$ cumple $df = 0$ si y sólo si es localmente constante en U. Así pues:

Teorema 2.37 *Si X es una variedad diferencial, entonces existen isomorfismos*

$$H^p(X, \mathbb{R}_X) \cong H^p(X)$$

entre los grupos de cohomología del haz constante $\mathbb{R}_X$ y los grupos de cohomología de De Rham.

En particular tenemos un isomorfismo

$$H^p(X) \cong H^p_\infty(X, \mathbb{R}).$$

Para exhibirlo explícitamente consideramos la aplicación lineal

$$\phi_{p,U} : \Lambda^p(U) \longrightarrow C^p_\infty(U, \mathbb{R})$$

dada por

$$\phi_p(\omega)(\sigma) = \int_\sigma \omega.$$

Es inmediato que estas aplicaciones $\phi_{p,U}$ inducen un homomorfismo de prehaces $\phi_p^- : \Lambda^p_X \longrightarrow \mathcal{C}^{p-}_{X,\mathbb{R},\infty}$, el cual se extiende a su vez a un homomorfismo de haces $\phi_p : \Lambda^p_X \longrightarrow \mathcal{C}^p_{X,\mathbb{R},\infty}$. El teorema de Stokes para símplices [11.17] afirma que los homomorfismos ϕ_p determinan un homomorfismo de complejos, de modo que tenemos un homomorfismo entre las resoluciones

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{R}_X \arrow[r] \arrow[d, "1"'] & \Lambda^0_X \arrow[r] \arrow[d] & \Lambda^1_X \arrow[r] \arrow[d] & \Lambda^2_X \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathbb{R}_X \arrow[r] & \mathcal{C}^0_{X,\mathbb{R},\infty} \arrow[r] & \mathcal{C}^1_{X,\mathbb{R},\infty} \arrow[r] & \mathcal{C}^2_{X,\mathbb{R},\infty} \arrow[r] & \cdots
\end{tikzcd}$$

Por la nota posterior al teorema 2.30, este homomorfismo entre las dos resoluciones induce un isomorfismo entre los funtores de cohomología construidos con cada una de ellas. En el caso concreto del haz $\mathbb{R}_X$, los isomorfismos correspondientes son los inducidos por el homomorfismo de complejos

$$\begin{tikzcd}
0 \arrow[r] & \Lambda^0(X) \arrow[r] \arrow[d] & \Lambda^1(X) \arrow[r] \arrow[d] & \Lambda^2(X) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathcal{C}^0_{X,\mathbb{R},\infty}(X) \arrow[r] & \mathcal{C}^1_{X,\mathbb{R},\infty}(X) \arrow[r] & \mathcal{C}^2_{X,\mathbb{R},\infty}(X) \arrow[r] & \cdots
\end{tikzcd}$$

Ahora basta considerar el diagrama conmutativo

$$\begin{tikzcd}
\Lambda^p(X) \arrow[d, "\phi_{p,X}"'] \arrow[dr] & \\
C^p_\infty(X, \mathbb{R}) \arrow[r, "j^+_X"'] & \mathcal{C}^p_{X,\mathbb{R},\infty}(X)
\end{tikzcd}$$

La flecha oblicua y la horizontal inducen isomorfismos entre los grupos de cohomología, luego la vertical también. En conclusión:

Teorema 2.38 (De Rham) *Si X es una variedad diferencial, la integración sobre símplices*

$$\int : \Lambda^p(X) \longrightarrow C^p_\infty(X, \mathbb{R})$$

induce un isomorfismo $H^p(X) \longrightarrow H^p_\infty(X, \mathbb{R})$ entre los grupos de cohomología de De Rham y los grupos de cohomología singular diferenciable de X.

Observemos que el funtor $\mathrm{Hom}_{\mathbb{R}}(-,\mathbb{R})$ es exacto, porque $\mathbb{R}$ es un $\mathbb{R}$-módulo inyectivo (esto es trivialmente cierto para cualquier cuerpo). Por consiguiente, conserva la homología de los complejos (teorema 1.37). Aplicamos este hecho al complejo

$$\cdots \longrightarrow C_2^\infty(X,\mathbb{R}) \longrightarrow C_1^\infty(X,\mathbb{R}) \longrightarrow C_0^\infty(X,\mathbb{R}) \longrightarrow 0,$$

y así concluimos que $H^p_\infty(X,\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}}(H_p^\infty(X,\mathbb{R}),\mathbb{R}) = H_p^\infty(X,\mathbb{R})^*$. Explícitamente, cada clase de cohomología $[f] \in H^p_\infty(X,\mathbb{R})$ se corresponde con la aplicación lineal $H_p^\infty(X,\mathbb{R}) \longrightarrow \mathbb{R}$ dada por $[\sigma] \mapsto f(\sigma)$. Si componemos este isomorfismo con el isomorfismo dado por el teorema de De Rham obtenemos una versión alternativa:

Teorema 2.39 (De Rham) *Si X es una variedad diferencial, tenemos una forma bilineal regular*

$$\int : H_p^\infty(X,\mathbb{R}) \times H^p(X) \longrightarrow \mathbb{R}$$

dada por $([\sigma],[\omega]) \mapsto \int_\sigma \omega$.

2.9 La estructura multiplicativa

Si X es una variedad diferencial entonces

$$H^*(X) = \bigoplus_p H^p(X), \qquad \text{y} \qquad H^*_\infty(X,\mathbb{R}) = \bigoplus_p H^p_\infty(X,\mathbb{R})$$

tienen respectivas estructuras de álgebras sobre $\mathbb{R}$ con el producto exterior ([11.11] y [Sección[5] 6.3]). Vamos a ver que el isomorfismo $H^*(X) \cong H_*(X)$ que proporciona el teorema de De Rham es un isomorfismo de álgebras.

Definimos el producto tensorial de dos complejos inversos de $\mathcal{O}_X$-módulos $\mathcal{C}$ y $\mathcal{C}'$ como el complejo dado por

$$(\mathcal{C} \otimes_{\mathcal{O}_X} \mathcal{C}')^p = \bigoplus_{i+j=p} (\mathcal{C}^i \otimes_{\mathcal{O}_X} \mathcal{C}^j),$$

con el operador cofrontera dado por

$$\bigoplus_{i+j=p} (d_i \otimes 1_j + (-1)^i 1_i \otimes d_j).$$

Se trata de la versión para haces de la estructura considerada en el teorema [6.3] (salvo que allí considerábamos complejos directos, pero esto es un mero cambio de notación). De hecho, el complejo de $\mathcal{O}_{X,P}$-módulos que resulta al localizar en un punto $P \in X$ es el considerado en [6.3], lo que prueba que realmente el producto que acabamos de definir es un complejo (es decir, que al aplicar dos veces el operador cofrontera obtenemos el homomorfismo nulo).

[5] En dicha sección trabajamos con la cohomología singular, pero todo vale igualmente para la cohomología singular diferenciable

Teorema 2.40 *El producto de dos resoluciones paracompactas y libres de torsión del haz constante $\mathbb{R}_X$ es también una resolución paracompacta y libre de torsión de $\mathbb{R}_X$.*

Demostración: Si tenemos dos resoluciones

$$0 \longrightarrow \mathbb{R}_X \longrightarrow \mathcal{C}^0 \longrightarrow \mathcal{C}^1 \longrightarrow \cdots$$

y

$$0 \longrightarrow \mathbb{R}_X \longrightarrow \mathcal{C}'^0 \longrightarrow \mathcal{C}'^1 \longrightarrow \cdots$$

entendemos que el producto de ambas resoluciones es el complejo que empieza por

$$0 \longrightarrow \mathbb{R}_X \longrightarrow \mathcal{C}^0 \otimes_{\mathbb{R}_X} \mathcal{C}'^0 \longrightarrow (\mathcal{C}^0 \otimes_{\mathbb{R}_X} \mathcal{C}'^1) \oplus (\mathcal{C}^1 \otimes_{\mathbb{R}_X} \mathcal{C}'^0) \longrightarrow \cdots$$

donde el primer homomorfismo es la composición

$$\mathbb{R}_X \longrightarrow \mathbb{R}_X \otimes_{\mathbb{R}_X} \mathbb{R}_X \longrightarrow \mathcal{C}^0 \otimes_{\mathbb{R}_X} \mathcal{C}'^0.$$

Es fácil ver que este producto es isomorfo al producto de las dos resoluciones dadas entendiendo que el término de grado 0 es $\mathbb{R}_X$. En efecto, dicho producto empezaría así:

$$0 \longrightarrow \mathbb{R}_X \otimes_{\mathbb{R}_X} \mathbb{R}_X \longrightarrow (\mathbb{R}_X \otimes_{\mathbb{R}_X} \mathcal{C}^0) \oplus (\mathcal{C}'^0 \otimes_{\mathbb{R}_X} \mathbb{R}_X) \longrightarrow \cdots$$

y basta tener en cuenta que el funtor $\mathbb{R}_X \otimes_{\mathbb{R}_X} -$ es isomorfo a la identidad.

La parte más delicada es la prueba de que el producto sigue siendo una sucesión exacta. Esto es consecuencia del teorema de Künneth [6.4] aplicado a las sucesiones de complejos locales. Puesto que ambas son sucesiones exactas, su cohomología es nula (y ambos son complejos libres porque $\mathbb{R}$ es un cuerpo y todo $\mathbb{R}$-módulo es libre). El teorema afirma entonces que la cohomología (de las localizaciones) del producto es nula, es decir, que las localizaciones del operador cofrontera del producto forman sucesiones exactas, luego el operador cofrontera forma una sucesión exacta.

Es inmediato que la suma directa de módulos paracompactos es paracompacta, y sabemos que el producto tensorial también lo es, luego los módulos de la resolución producto son paracompactos. Además son libres de torsión porque $\mathbb{R}$ es un cuerpo. ■

En lo sucesivo escribiremos $\otimes$ en lugar de $\otimes_{\mathbb{R}_X}$. Si $\mathcal{C}$ es una resolución paracompacta de $\mathbb{R}_X$, entonces $\mathcal{C} \otimes \mathcal{C}$ es otra, y podemos usarla para calcular los grupos de cohomología de cualquier $\mathbb{R}_X$-módulo. Si $\mathcal{M}$ es, concretamente, un haz de $\mathbb{R}_X$-álgebras, entonces tenemos claramente un homomorfismo de haces $\mathcal{M} \otimes \mathcal{M} \longrightarrow \mathcal{M}$, que a su vez induce un homomorfismo de haces

$$(\mathcal{C}^i \otimes \mathcal{M}) \otimes (\mathcal{C}^j \otimes \mathcal{M}) \cong \mathcal{C}^i \otimes \mathcal{C}^j \otimes \mathcal{M} \otimes \mathcal{M} \longrightarrow \mathcal{C}^i \otimes \mathcal{C}^j \otimes \mathcal{M}.$$

A su vez, podemos considerar los homomorfismos

$$(\mathcal{C}^i \otimes \mathcal{M})(X) \otimes_{\mathbb{R}} (\mathcal{C}^j \otimes \mathcal{M})(X) \xrightarrow{j_X^+} ((\mathcal{C}^i \otimes \mathcal{M}) \otimes (\mathcal{C}^j \otimes \mathcal{M}))(X)$$
$$\longrightarrow (\mathcal{C}^i \otimes \mathcal{C}^j \otimes \mathcal{M})(X),$$

que inducen un homomorfismo de complejos de $\mathbb{R}$-módulos

$$((\mathcal{C} \otimes \mathcal{M})(X)) \otimes_{\mathbb{R}} (\mathcal{C} \otimes \mathcal{M})(X)) \longrightarrow (\mathcal{C} \otimes \mathcal{C} \otimes \mathcal{M})(X).$$

Recordemos ahora que si tenemos dos complejos de A-módulos $\mathcal{A}$ y $\mathcal{B}$, podemos definir homomorfismos

$$H^i(\mathcal{A}) \otimes_A H^j(\mathcal{B}) \longrightarrow H^{i+j}(\mathcal{A} \otimes_A \mathcal{B})$$

mediante $[a] \otimes [b] \mapsto [a \otimes b]$. En efecto, la definición es correcta porque si, por ejemplo $a = da'$ es una cofrontera, entonces

$$d(a' \otimes b) = da' \otimes b - a' \otimes db = a \otimes b - a' \otimes 0 = a \otimes b,$$

luego $[a \otimes b] = 0$.

Volviendo a nuestro argumento, tenemos un homomorfismo

$$H^i((\mathcal{C} \otimes \mathcal{M})(X)) \otimes_{\mathbb{R}} H^j((\mathcal{C} \otimes \mathcal{M})(X)) \longrightarrow H^{i+j}((\mathcal{C} \otimes \mathcal{C} \otimes \mathcal{M})(X)),$$

o, en otros términos,

$$H^i(X, \mathcal{M}) \otimes_{\mathbb{R}} H^j(X, \mathcal{M}) \longrightarrow H^{i+j}(X, \mathcal{M}),$$

donde los grupos de cohomología de la izquierda están calculados con la resolución $\mathcal{C}$ y el de la derecha con la resolución $\mathcal{C} \otimes \mathcal{C}$. Si aplicamos al grupo de la derecha el único isomorfismo entre los funtores de cohomología calculados con $\mathcal{C} \otimes \mathcal{C}$ y los calculados con $\mathcal{C}$, podemos considerar que los tres grupos de cohomología están calculados con $\mathcal{C}$.

Vamos a probar que estos homomorfismos no dependen de la resolución $\mathcal{C}$ de partida, en el sentido de que si partimos de otra $\mathcal{C}'$, entonces el isomorfismo entre los grupos de cohomología calculados con una y otra resolución dan lugar a un diagrama conmutativo con el homomorfismo que acabamos de definir.

En efecto, en tal caso podemos considerar tres homomorfismos como el anterior: el construido con $\mathcal{C} \otimes \mathcal{C}$, el construido con $\mathcal{C}' \otimes \mathcal{C}'$ y el construido con $(\mathcal{C} \otimes \mathcal{C}') \otimes (\mathcal{C} \otimes \mathcal{C}')$. Basta probar que el tercero coincide con los dos primeros y, por simetría, basta probar que el primero coincide con el tercero.

Ahora bien, podemos definir un homomorfismo $\mathcal{C} \longrightarrow \mathcal{C} \otimes \mathcal{C}'$ mediante

$$\mathcal{C}^p \cong \mathcal{C}^p \otimes \mathbb{R}_X \longrightarrow \mathcal{C}^p \otimes \mathcal{C}'^0 \longrightarrow \bigoplus_{i+j=p} \mathcal{C}^i \otimes \mathcal{C}'^j = (\mathcal{C} \otimes \mathcal{C}')^p.$$

Es fácil ver que estos homomorfismos de módulos definen un homomorfismo de complejos que, de acuerdo con la nota posterior al teorema 2.30, induce un isomorfismo (el único) entre la sucesión de grupos de cohomología calculados con $\mathcal{C}$ y con $\mathcal{C}\otimes\mathcal{C}'$. Para el módulo $\mathcal{M}$, estos isomorfismos son los inducidos por el homomorfismo de complejos

$$\phi : (\mathcal{C}\otimes\mathcal{M})(X) \longrightarrow (\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{M})(X).$$

Por otra parte, el homomorfismo $\mathcal{C} \longrightarrow \mathcal{C}\otimes\mathcal{C}'$ induce claramente un homomorfismo entre las resoluciones $\mathcal{C}\otimes\mathcal{C} \longrightarrow (\mathcal{C}\otimes\mathcal{C}')\otimes(\mathcal{C}\otimes\mathcal{C}')$, que a su vez induce el único isomorfismo entre las sucesiones de grupos de cohomología calculados con cada una de ellas, y que en el caso de $\mathcal{M}$ son los isomorfismos inducidos por

$$\psi : (\mathcal{C}\otimes\mathcal{C}\otimes\mathcal{M})(X) \longrightarrow (\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{M})(X).$$

Tenemos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
(\mathcal{C}\otimes\mathcal{M})(X)\otimes_{\mathbb{R}}(\mathcal{C}\otimes\mathcal{M})(X) \arrow[r] \arrow[d, "\phi\otimes\phi"'] & (\mathcal{C}\otimes\mathcal{C}\otimes\mathcal{M})(X) \arrow[d, "\psi"] \\
(\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{M})(X)\otimes_{\mathbb{R}}(\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{M})(X) \arrow[r] & (\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{M})(X)
\end{tikzcd}$$

que a su vez induce el diagrama conmutativo

$$\begin{tikzcd}
H^i(X,\mathcal{M})\otimes_{\mathbb{R}} H^j(X,\mathcal{M}) \arrow[r] \arrow[d] & H^{i+j}(X,\mathcal{M}) \arrow[d] \\
H^i(X,\mathcal{M})\otimes_{\mathbb{R}} H^j(X,\mathcal{M}) \arrow[r] & H^{i+j}(X,\mathcal{M})
\end{tikzcd}$$

donde los grupos de la primera fila están calculados con $\mathcal{C}$ (los de la izquierda) y con $\mathcal{C}\otimes\mathcal{C}$ (el de la derecha), mientras que los de la segunda fila están calculados con $\mathcal{C}\otimes\mathcal{C}'$ y $\mathcal{C}\otimes\mathcal{C}'\otimes\mathcal{C}\otimes\mathcal{C}'$. Las flechas verticales son los únicos isomorfismos naturales. Es evidente que si añadimos en una tercera columna los grupos calculados con $\mathcal{C}$ y $\mathcal{C}\otimes\mathcal{C}'$ tenemos un cuadrado de isomorfismos, por lo que el diagrama anterior es también conmutativo cuando en la segunda columna ponemos los grupos estos últimos grupos.

Los homomorfismos que acabamos de construir inducen una estructura de $\mathbb{R}$-álgebra en

$$H^*(X,\mathcal{M}) = \bigoplus_p H^p(X,\mathcal{M}).$$

Observemos que los homomorfismos $\mathcal{C}^i(U)\otimes_{\mathbb{R}}\mathcal{C}^j(U) \longrightarrow \mathcal{C}^j(U)\otimes_{\mathbb{R}}\mathcal{C}^i(U)$ dados por $u\otimes v \mapsto (-1)^{ij} v\otimes u$, para cada abierto $U\subset X$, inducen un homomorfismo de prehaces que a su vez se extiende a un homomorfismo de haces $\mathcal{C}^i\otimes\mathcal{C}^j \longrightarrow \mathcal{C}^j\otimes\mathcal{C}^i$. Al variar i, j, estos homomorfismos inducen un homomorfismo de complejos $\epsilon : \mathcal{C}\otimes\mathcal{C} \longrightarrow \mathcal{C}\otimes\mathcal{C}$ (hay que comprobar que conmutan con el operador cofrontera del producto, pero esto no ofrece ninguna dificultad).

Podemos formar un diagrama conmutativo

$$\begin{tikzcd}
H^i(X,\mathcal{M}) \otimes_{\mathbb{R}} H^j(X,\mathcal{M}) \arrow[r] \arrow[d] & H^{i+j}(X,\mathcal{M}) \arrow[d] \\
H^j(X,\mathcal{M}) \otimes_{\mathbb{R}} H^i(X,\mathcal{M}) \arrow[r] & H^{i+j}(X,\mathcal{M})
\end{tikzcd}$$

en el que la flecha vertical izquierda es $u \otimes v \mapsto (-1)^{ij} v \otimes u$ y la flecha vertical derecha es el homomorfismo inducido por ϵ, que ha de ser la identidad. Esto significa que el álgebra $H^*(X,\mathcal{M})$ satisface la relación

$$u \cdot v = (-1)^{ij} v \cdot u, \qquad \text{para todo } u \in H^i(X,\mathcal{M}),\ v \in H^j(X,\mathcal{M}).$$

La situación es especialmente simple cuando $\mathcal{M} = \mathbb{R}_X$. Entonces la estructura de álgebra en $H^*(X,\mathbb{R}_X)$ es la inducida por los homomorfismos

$$\mathcal{C}^i(X) \otimes_{\mathbb{R}} \mathcal{C}^j(X) \longrightarrow (\mathcal{C} \otimes \mathcal{C})^{i+j}(X) \longleftarrow \mathcal{C}^{i+j}(X).$$

Si tomamos como $\mathcal{C}$ la resolución

$$0 \longrightarrow \mathbb{R}_X \longrightarrow \Lambda^0(X) \longrightarrow \Lambda^1(X) \longrightarrow \Lambda^2(X) \longrightarrow \cdots,$$

el producto exterior nos da homomorfismos

$$\Lambda^i(U) \otimes_{\mathbb{R}} \Lambda^j(U) \longrightarrow \Lambda^{i+j}(U),$$

que inducen homomorfismos de haces $\Lambda^i_X \otimes \Lambda^j_X \longrightarrow \Lambda^{i+j}_X$, que, a su vez, es fácil ver que definen un homomorfismo de complejos $\Lambda_X \otimes \Lambda_X \longrightarrow \Lambda_X$ que hace conmutativo el diagrama siguiente:

$$\begin{tikzcd}
\Lambda^i_X(X) \otimes_{\mathbb{R}} \Lambda^j_X(X) \arrow[r] \arrow[dr] & (\Lambda_X \otimes \Lambda_X)^{i+j}(X) \arrow[d] \\
& \Lambda^{i+j}_X(X)
\end{tikzcd}$$

en el que la flecha oblicua es el producto exterior. Observemos que la flecha vertical induce el único isomorfismo natural entre los grupos de cohomología de $\mathbb{R}_X$ calculados con $\Lambda_X \otimes \Lambda_X$ y los calculados con Λ_X. Este diagrama induce a su vez

$$\begin{tikzcd}
H^i(X) \otimes_{\mathbb{R}} H^j(X) \arrow[r] \arrow[dr] & H^{i+j}(X) \arrow[d] \\
& H^{i+j}(X)
\end{tikzcd}$$

donde la flecha oblicua es $[\omega] \otimes [\eta] \mapsto [\omega \wedge \eta]$ y la composición de las otras dos es $[\omega] \otimes [\eta] \mapsto [\omega] \cdot [\eta]$, donde el producto es el que hemos definido en esta sección.

En definitiva, hemos probado que $[\omega]\cdot[\eta]=[\omega\wedge\eta]$. En otras palabras, que el (único) isomorfismo natural

$$H^*(X)\cong H^*(X,\mathbb{R}_X)$$

entre el álgebra de cohomología de De Rham y el álgebra de cohomología del haz constante $\mathbb{R}_X$ (que en principio era un isomorfismo de espacios vectoriales) resulta ser un isomorfismo de álgebras.

Ahora bien, todo este razonamiento es válido palabra por palabra si sustituimos la resolución Λ_X por la resolución $\mathcal{C}_{X,\infty}$ correspondiente a la cohomología diferenciable dotada del producto exterior definido en la [sección 6.3], y la conclusión es entonces que el (único) isomorfismo natural

$$H^*_\infty(X,\mathbb{R})\cong H^*(X,\mathbb{R}_X)$$

es también un isomorfismo de álgebras. Esto implica, finalmente:

Teorema 2.41 (de Rham) *Si X es una variedad diferencial, la integración sobre símplices*

$$\int:\Lambda^*(X)\longrightarrow C^*_\infty(X,\mathbb{R})$$

induce un isomorfismo de álgebras $H^*(X)\longrightarrow H^*_\infty(X,\mathbb{R})$ entre las álgebras de cohomología de De Rham y de cohomología singular diferenciable de X.

Segunda parte

Álgebra conmutativa

Capítulo III

La geometría afín

En este capítulo mostraremos cómo se puede enfocar el estudio de un conjunto algebraico afín en términos del estudio de su anillo de funciones regulares, y veremos que las técnicas y los conceptos empleados tienen sentido sobre anillos más generales. Estos anillos de funciones regulares no son necesariamente dominios íntegros, así que empezaremos estudiando un concepto general de anillos y módulos de fracciones que no requiera esta hipótesis.

3.1 Módulos de cocientes

Sea A un anillo y M un A-módulo. Diremos que un conjunto $S \subset A$ es *multiplicativo* si $1 \in S$ y, cuando s_1, $s_2 \in S$, entonces $s_1 s_2 \in S$. Definimos $S^{-1}M$ como el conjunto cociente obtenido a partir de $S \times M$ mediante la relación de equivalencia dada por

$$(s_1, m_1) \sim (s_2, m_2) \Leftrightarrow s(s_1 m_2 - s_2 m_1) = 0 \quad \text{para cierto } s \in S.$$

A la clase de equivalencia de un par (s, m) la representaremos como $s^{-1}m$, o también m/s. Observemos que si S no contiene divisores de cero la igualdad de fracciones se reduce a la usual.

El conjunto $S^{-1}M$ adquiere estructura de A-módulo con las operaciones dadas por

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}, \qquad a\,\frac{m}{s} = \frac{am}{s}$$

Si $M = A$ podemos definir, de hecho, una estructura de anillo en $S^{-1}A$ mediante el producto

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

Más aún, podemos considerar a $S^{-1}M$ como $S^{-1}A$-módulo con el producto dado por

$$\frac{a}{s_1}\frac{m}{s_2} = \frac{am}{s_1 s_2}.$$

Es claro que la aplicación $i_S : M \longrightarrow S^{-1}M$ dada por $i_S(m) = m/1$ es un homomorfismo de A-módulos. Su núcleo es

$$\mathrm{N}(i_S) = \{m \in M \mid sm = 0 \text{ para cierto } s \in S\}.$$

En particular, $i_S : A \longrightarrow S^{-1}A$ es inyectivo si y sólo si S no contiene divisores de 0.

Los módulos de cocientes están caracterizados por esta propiedad:

Teorema 3.1 *Sea A un anillo, sea $S \subset A$ un subconjunto multiplicativo y sea $\phi : M \longrightarrow N$ un homomorfismo de A-módulos. Supongamos que, para cada elemento $s \in S$, el homomorfismo $\mu_s : N \longrightarrow N$ dado por la multiplicación por s es biyectivo. Entonces existe un único homomorfismo $\phi_S : S^{-1}M \longrightarrow N$ que hace conmutativo el diagrama siguiente:*

$$\begin{tikzcd}
S^{-1}M \arrow[r, "\phi_S"] & N \\
M \arrow[u, "i_S"] \arrow[ur, "\phi"'] &
\end{tikzcd}$$

DEMOSTRACIÓN: Dado $m \in M$ y $s \in S$, por hipótesis existe un único $n \in N$ tal que $sn = \phi(m)$. Vamos a ver que podemos definir $\phi_S(m/s) = n$. Para ello suponemos que $m/s = m'/s'$, lo que significa que existe un $s'' \in S$ tal que $s''(s'm - sm') = 0$. Aplicando ϕ vemos que $s''s'sn - s''ss'n') = 0$. Como la multiplicación por $ss's''$ es biyectiva, ha de ser $n = n'$, lo que prueba que ϕ_S está bien definida. Es fácil ver que se trata de un homomorfismo y obviamente hace el diagrama conmutativo.

La unicidad se debe a que ϕ_S ha de cumplir necesariamente la relación $s\phi_S(m/s) = \phi_S(m/1) = \phi(m)$, lo que nos lleva necesariamente a la construcción que hemos hecho. ■

Nota En el caso particular en que $\phi : A \longrightarrow B$ es un homomorfismo de anillos, la condición de que la multiplicación por s sea biyectiva equivale a que $\phi(s)$ sea una unidad en B, en cuyo caso $\phi_S : S^{-1}A \longrightarrow B$ es el homomorfismo de anillos dado por $\phi_S(a/s) = \phi(a)/\phi(s)$. ■

Ejemplos Si A es un anillo, el conjunto S formado por todos los elementos de A que no son divisores de cero es claramente multiplicativo, y al anillo $S^{-1}A$ lo llamaremos *anillo completo de cocientes* de A. Lo representaremos por $F(A)$. Si A es un dominio íntegro entonces $F(A)$ es su cuerpo de cocientes.

Si $f \in A$, el conjunto $S_f = \{f^n \mid n \geq 1\}$ es multiplicativo. Escribiremos M_f en lugar de $S_f^{-1}M$.

Si $\mathfrak{p}$ es un ideal primo de A, el conjunto $S_\mathfrak{p} = A \setminus \mathfrak{p}$ es multiplicativo. Escribiremos $M_\mathfrak{p}$ en lugar de $S_\mathfrak{p}^{-1}M$. Es inmediato comprobar que $A_\mathfrak{p}$ es un anillo local, es decir, que tiene un único ideal maximal, formado por las fracciones con numerador en $\mathfrak{p}$. ■

La idea fundamental que subyace a la definición de anillo de cocientes es que en al pasar a $S^{-1}A$ hemos convertido en unidades a todos los elementos de S. Esto tiene una interpretación geométrica en muchas ocasiones. Vamos a ver una de ellas:

Ejemplo Sea X una variedad diferencial con su estructura de espacio anillado determinada por su haz de funciones de clase C^∞ o bien un espacio métrico dotado de su haz de funciones reales continuas. En ambos casos es conocido[1] que, para cada abierto $U \subset X$ y cada punto $P \in U$, existe $s \in \mathcal{O}_X(X)$ (esto es, una función de clase C^∞ o continua, según el caso) que vale 1 en un entorno de P y vale 0 fuera de U.

Fijado un punto $P \in X$, consideremos el conjunto

$$\mathfrak{P}_P = \{f \in \mathcal{O}_X(X) \mid f(P) = 0\}.$$

Obviamente es un ideal de $\mathcal{O}_X(X)$. Más concretamente, es el núcleo del epimorfismo $\mathcal{O}_X(X) \longrightarrow \mathbb{R}$ dado por $f \mapsto f(P)$, lo que prueba que, de hecho, es un ideal maximal de $\mathcal{O}_X(X)$ (porque el cociente es un cuerpo, isomorfo a $\mathbb{R}$).

Vamos a probar que $\mathcal{O}_{X,P} \cong \mathcal{O}_X(X)_{\mathfrak{P}_P}$. Para ello observamos que el homomorfismo natural $\mathcal{O}_X(X) \longrightarrow \mathcal{O}_{X,P}$ transforma los elementos de $\mathcal{O}_X(X) \setminus \mathfrak{P}_P$ en unidades de $\mathcal{O}_{X,P}$ (una función que no se anula en P tiene inversa en un entorno de P), luego el teorema 3.1 nos da una extensión $\mathcal{O}_X(X)_{\mathfrak{P}_P} \longrightarrow \mathcal{O}_{X,P}$.

Se trata de un monomorfismo de anillos, pues si la imagen de f/s es nula, eso significa que f se anula en un entorno U de P, luego podemos tomar una función $s' \in \mathcal{O}_X(X)$ que valga 1 en un entorno de P y 0 fuera de U. Entonces $s' \in \mathcal{O}_X(X) \setminus \mathfrak{P}_P$ y $s'f = 0$, lo que implica que $f/s = 0$.

Por otra parte, un elemento de $\mathcal{O}_{X,P}$ está determinado por una función $f \in \mathcal{O}_X(U)$, para un cierto entorno U de P. Tomamos s' igual que antes y así $s'f \in \mathcal{O}_X(X)$ determina el mismo elemento dado de $\mathcal{O}_{X,P}$, que resulta ser la imagen de $s'f/1 \in \mathcal{O}_X(X)_{\mathfrak{P}_P}$.

Así pues, los anillos locales de X están determinados por el anillo $\mathcal{O}_X(X)$. ■

El teorema 3.1 implica que todo homomorfismo de A-módulos $\phi : M \longrightarrow N$ induce un homomorfismo de $S^{-1}A$-módulos $\phi_S : S^{-1}M \longrightarrow S^{-1}N$ que hace conmutativo el diagrama siguiente:

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[d, "i_S"'] & N \arrow[d, "i_S"] \\
S^{-1}M \arrow[r, "\phi_S"'] & S^{-1}N
\end{tikzcd}$$

Concretamente, ϕ_S viene dado por $\phi_S(m/s) = \phi(m)/s$.

[1]Ver los teoremas 1.12 y 9.4 de mi Topología algebraica.

Es claro entonces que podemos considerar a $S^{-1} : \mathrm{Mod}(A) \longrightarrow \mathrm{Mod}(S^{-1}A)$ como un funtor covariante. El teorema siguiente prueba que es exacto:

Teorema 3.2 *Sea A un anillo, $S \subset A$ un conjunto multiplicativo y consideremos una sucesión exacta de A-módulos $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$. Entonces también es exacta la sucesión $S^{-1}M \longrightarrow S^{-1}N \longrightarrow S^{-1}P$.*

DEMOSTRACIÓN: Si $\beta_S(n/s) = 0$, entonces existe un $s' \in S$ tal que $s'\beta(n) = \beta(s'n) = 0$, luego $s'n = \alpha(m)$, para cierto $m \in M$, luego $n/s = \alpha_S(m/ss')$. ■

La aplicación dada por $\phi \mapsto \phi_S$ define un homomorfismo de A-módulos

$$\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

Éste, a su vez, induce un homomorfismo de $S^{-1}A$-módulos

$$h : S^{-1}\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

dado por $h(\alpha/s) = \alpha_S/s$.

Teorema 3.3 *En las condiciones anteriores, si A es noetheriano y M es finitamente generado, h es un isomorfismo.*

DEMOSTRACIÓN: Pongamos que $M = \langle m_1, \ldots, m_t\rangle$. Si α/s está en el núcleo de h, entonces $\alpha(m_i)/s = 0$ para $i = 1, \ldots, t$, luego existe un $s' \in S$ tal que $s'\alpha(m_i) = 0$ para todo i. Así pues $s'\alpha = 0$, de donde $\alpha/s = 0$.

Consideremos la sucesión exacta

$$0 \longrightarrow K \longrightarrow A^t \longrightarrow M \longrightarrow 0$$

que hace corresponder la base canónica de A^t con el sistema generador de M. Como A es noetheriano, el núcleo K es finitamente generado. Tomemos un homomorfismo $\phi \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$. Sea $s \in S$ tal que $\phi(m_i/1) = n_i/s$ para todo i, con $n_i \in N$. Sea $\beta : A^t \longrightarrow N$ el homomorfismo que lleva la base canónica a los n_i. El diagrama siguiente es conmutativo:

$$\begin{tikzcd}
A^t \arrow[rr, "\beta"] \arrow[d] & & N \arrow[d] \\
M \arrow[r] & S^{-1}M \arrow[r, "s\phi"'] & S^{-1}N
\end{tikzcd}$$

Por consiguiente $i_N[\beta[K]] = 0$. Como K es finitamente generado, existe un $s' \in S$ tal que $s'\beta[K] = 0$. Por consiguiente β induce un homomorfismo $\alpha : M \longrightarrow N$ dado por $\alpha(m_i) = s'n_i$. Entonces $\phi = h(\alpha/ss')$. ■

Notemos ahora que (por la exactitud de S^{-1}, si ϕ es inyectiva, suprayectiva o biyectiva, lo mismo es cierto para ϕ_S. En particular, si M es un submódulo de N, podemos considerar a $S^{-1}M$ como submódulo de $S^{-1}N$ de forma natural.

Es fácil ver que todo submódulo de $S^{-1}M$ es de la forma $S^{-1}N$ para un cierto submódulo N de M, pero conviene precisar más la situación: Si N es un submódulo de M, definimos

$$S(N) = \{m \in M \mid sm \in N \text{ para un } s \in S\}.$$

Es inmediato comprobar que $S(N)$ es un submódulo de M que contiene a N. Además $S(S(N)) = S(N)$ y $S(N_1 \cap N_2) = S(N_1) \cap S(N_2)$.

Teorema 3.4 *Dado un A-módulo M y un conjunto multiplicativo $S \subset A$, la aplicación $N \mapsto S^{-1}N$ biyecta los submódulos N de M que cumplen $N = S(N)$ con los submódulos de $S^{-1}M$.*

Demostración: Si N' es un submódulo de $S^{-1}M$, entonces

$$N = \{m \in M \mid m/1 \in N'\}$$

es un submódulo de M tal que $N' = S^{-1}N$. En efecto, si $m/s \in U'$, entonces $m/1 \in U'$, luego $m \in N$ y $m/s \in S^{-1}N$.

Por otra parte, si $m \in S(N)$, entonces existe un $s \in S$ tal que $sm \in N$, luego $sm/1 \in N'$, luego $m/1 \in N'$, luego $m \in N$. Por consiguiente $S(N) = N$.

Tenemos así una aplicación $F(N') = N$ tal que $N' = S^{-1}(F(N))$. Recíprocamente, si un submódulo N cumple $S(N) = N$, entonces $F(S^{-1}N) = N$. En efecto, si $m \in F(S^{-1}N)$, tenemos que $m/1 \in S^{-1}N$, luego $m/1 = n/s$, con $n \in N$, $s \in S$, luego $s'(sm - n) = 0$, para cierto $s' \in S$, luego $s'sm \in N$, luego $m \in S(N) = N$. El recíproco es obvio.

Concluimos que las aplicaciones F y $N \mapsto S^{-1}N$ son mutuamente inversas, luego tenemos una biyección. ■

Ahora es evidente que si M es un A-módulo noetheriano entonces $S^{-1}M$ es un $S^{-1}A$-módulo noetheriano.

Observemos que si $S \subset A$ es un conjunto multiplicativo y $\mathfrak{p}$ es un ideal primo de A, entonces

$$S(\mathfrak{p}) = \begin{cases} \mathfrak{p} & \text{si } \mathfrak{p} \cap S = \varnothing, \\ A & \text{si } \mathfrak{p} \cap S \neq \varnothing. \end{cases}$$

Por otra parte, si $\mathfrak{P}$ es un ideal primo de $S^{-1}A$, el ideal $F(\mathfrak{P})$ construido en la demostración del teorema anterior no es sino $\mathfrak{p} = i_S^{-1}[\mathfrak{P}]$, que es un ideal primo de A. En definitiva, tenemos lo siguiente:

Teorema 3.5 *Si A es un anillo y $S \subset A$ es un conjunto multiplicativo, entonces la aplicación $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ biyecta los ideales primos de A disjuntos con S con los ideales primos de $S^{-1}A$.*

En particular, los ideales primos de $A_\mathfrak{p}$ se corresponden con los ideales primos de A contenidos en $\mathfrak{p}$.

Teorema 3.6 *Si A es un dominio de factorización única y $S \subset A$ un conjunto multiplicativo tal que $0 \notin S$, entonces $S^{-1}A$ también es un dominio de factorización única.*

Demostración: La hipótesis $0 \notin S$ implica que i_S es inyectiva, es decir, que podemos considerar a A como subanillo de $S^{-1}A$. Si π es primo en A, entonces el ideal (π) es primo. Si $(\pi) \cap S = \varnothing$, entonces $S^{-1}(\pi) = (\pi)$ es un ideal primo y π es primo en $S^{-1}A$. Si, por el contrario $(\pi) \cap S \neq \varnothing$, entonces $(\pi) = S^{-1}(\pi) = S^{-1}A$, luego π es una unidad en $S^{-1}A$. Concluimos que todo elemento de $S^{-1}A$ no nulo ni unitario se descompone en producto de primos. Esto ya implica la unicidad de la factorización. ■

Teorema 3.7 *Sea A un anillo, S un conjunto multiplicativo en A, sea M un A-módulo y N un submódulo. Entonces $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

Demostración: Es claro que la aplicación $\rho : S^{-1}(M/N) \longrightarrow S^{-1}M/S^{-1}N$ dada por

$$\rho\big((m+N)/s\big) = m/n + S^{-1}N$$

es un epimorfismo bien definido. Además es inyectivo, pues si $(m+N)/s$ tiene imagen nula, entonces $m/n \in S^{-1}N$, luego $m/s = n/s'$, para ciertos $n \in N$, $s' \in S$. Esto significa que existe $s'' \in S$ tal que $s''(s'm - sn) = 0$. Entonces

$$(m+N)/s = (s''s'm+N)/s''ss' = (s''sn+N)/s''s's = 0.$$

■

Similarmente se demuestra:

Teorema 3.8 *Sea A un anillo, I un ideal en A, S un conjunto multiplicativo y S' la imagen de S en A/I. Entonces $S'^{-1}(A/I) \cong S^{-1}A/S^{-1}I$.*

A partir de las localizaciones de un módulo respecto a ideales maximales es posible recuperar información global. Los teoremas siguientes son ejemplos elementales:

Teorema 3.9 *Sea A un anillo y M un A-módulo. Entonces $M = 0$ si y sólo si $M_{\mathfrak{m}} = 0$ para todo ideal maximal $\mathfrak{m}$ de A.*

Demostración: Si los módulos locales son nulos, entonces para cada elemento $m \in M$ y cada ideal maximal $\mathfrak{m}$ se cumple que $m = 0$ en $M_{\mathfrak{m}}$, luego existe un $s \in A \setminus M$ tal que $sm = 0$. Así pues, el ideal

$$\mathrm{An}(m) = \{a \in A \mid am = 0\}$$

no está contenido en ningún ideal maximal de A. Por lo tanto $\mathrm{An}(m) = A$, luego $1 \in \mathrm{An}(m)$ y $m = 0$. ■

Más en general:

Teorema 3.10 *Sea A un anillo, M un A-módulo y P, Q dos submódulos. Entonces $P = Q$ si y sólo si $P_{\mathfrak{m}} = Q_{\mathfrak{m}}$ para todo ideal maximal $\mathfrak{m}$ de A.*

Demostración: Aplicando 3.7 tenemos que

$$((P+Q)/Q)_{\mathfrak{m}} \cong (P_{\mathfrak{m}} + Q_{\mathfrak{m}})/Q_{\mathfrak{m}} = 0, \quad ((P+Q)/P)_{\mathfrak{m}} \cong (P_{\mathfrak{m}} + Q_{\mathfrak{m}})/P_{\mathfrak{m}} = 0.$$

Por el teorema anterior $P = Q$. ■

Teorema 3.11 *Sea A un anillo. Una sucesión $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ de homomorfismos de A-módulos es exacta si y sólo si lo son $M_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} P_{\mathfrak{m}}$ para todo ideal maximal $\mathfrak{m}$ de A.*

Demostración: Una implicación ya está probada. Sea S la imagen de α y T el núcleo de β. Es claro entonces que $S_{\mathfrak{m}}$ es la imagen de $\alpha_{\mathfrak{m}}$ y $T_{\mathfrak{m}}$ el núcleo de $\beta_{\mathfrak{m}}$. Basta aplicar el teorema anterior. ■

En particular, un homomorfismo de módulos es inyectivo o suprayectivo si y sólo si lo son todas sus localizaciones respecto a ideales maximales.

3.2 Conjuntos algebraicos afines

Si K es un cuerpo, definimos el espacio afín de dimensión n sobre K como $A^n(K) = K^n$ (aunque si no hay posibilidad de confusión escribiremos simplemente A^n).

La notación A^n en lugar de K^n pretende expresar que no consideramos ningún sistema de referencia privilegiado en K^n, sino que cualquier conjunto de $n+1$ puntos afínmente independientes determina un sistema de referencia afín respecto al cual cada punto de A^n tiene asignadas unas coordenadas en K^n.

En todo momento sobrentenderemos que k es un cuerpo arbitrario y que K es una extensión de k algebraicamente cerrada. Entonces $A^n(k) \subset A^n(K)$ y todo sistema de referencia afín de $A^n(k)$ lo es también de $A^n(K)$. Sólo admitiremos como sistemas de referencia de $A^n(K)$ los formados por puntos de $A^n(k)$. Respecto a cualquiera de ellos, $A^n(k)$ está formado por los puntos de $A^n(K)$ con coordenadas en k^n. Entenderemos que A^n significa $A^n(K)$ (y no $A^n(k)$).

Si $S \subset k[X_1, \ldots, X_n]$, definimos

$$V(S) = \{P \in A^n \mid F(P) = 0 \text{ para todo } F \in S\}.$$

Diremos que un conjunto $C \subset A^n$ es un *conjunto algebraico afín* definido sobre k si existe $S \subset k[X_1, \ldots, X_n]$ tal que $C = V(S)$. Notemos que la definición de $V(S)$ presupone un sistema de referencia, pero es inmediato que la propiedad de ser algebraico sobre k no depende de la elección de dicho sistema. Usaremos la notación C/k para indicar que C está definido sobre k.

El marco conceptual que acabamos de describir permite tratar conjuntamente varios casos de interés:

- El caso clásico de la geometría algebraica se obtiene cuando $K = k$ es un cuerpo algebraicamente cerrado. (Y el caso más clásico de todos es $K = k = \mathbb{C}$). Así estamos estudiando los subconjuntos de k^n definidos por un sistema de ecuaciones polinómicas.

- Si consideramos una extensión algebraica K/k, entonces estamos estudiando los subconjuntos de K^n definidos por ecuaciones polinómicas con coeficientes en k. Saber que los coeficientes están en un cuerpo menor puede aportar información adicional. También es el contexto adecuado para estudiar los *puntos racionales* de un conjunto algebraico C/k, es decir, los puntos del conjunto $C(k) = C \cap A^n(k)$. No obstante, aunque estemos interesados en los puntos racionales de un conjunto algebraico, hemos de ser conscientes de que $C(k)$ puede ser finito, o incluso vacío, por lo que puede no ser suficiente para determinar los conceptos geométricos que vamos a estudiar. Éste es el motivo por el que, aunque nos interesen las soluciones de un sistema de ecuaciones en un cuerpo k, trabajemos con el conjunto de sus soluciones en la clausura algebraica K de k.

- Un caso intermedio entre los dos anteriores se da cuando K y k son ambos algebraicamente cerrados. Entonces $C(k)$ es por sí mismo un conjunto algebraico completo (el que obtendríamos cambiando K por k), pero puede ser útil extenderlo con los puntos en $A^n(K)$. Un caso típico se da cuando k es la clausura algebraica de $\mathbb{Q}$ y $K = \mathbb{C}$.

Volviendo al caso general, observemos que todo conjunto algebraico (definido sobre k) puede definirse mediante un conjunto finito de polinomios. Esto se justifica en dos pasos. En primer lugar, si $C = V(S)$ es un conjunto algebraico y consideramos el ideal $I = (S)$, es evidente que $C = V(S) = V(I)$. Así pues, todo conjunto algebraico puede ser definido mediante un ideal de polinomios. En segundo, lugar, como el anillo $k[X_1, \ldots, X_n]$ es noetheriano, todos sus ideales son finitamente generados, luego $I = (S_0)$, para un cierto conjunto finito de polinomios $S_0 \subset k[X_1, \ldots, X_n]$. Por el mismo motivo que antes, tenemos que $C = V(I) = V(S_0)$.

Considerar conjuntos finitos de polinomios que definan un conjunto algebraico tiene las ventajas obvias de la finitud, pero a efectos teóricos tiene el inconveniente de la falta de unicidad: distintos conjuntos de polinomios S_1 y S_2 pueden definir el mismo conjunto algebraico $V(S_1) = V(S_2)$. Si queremos asignar de forma canónica a cada conjunto algebraico $C = V(S) \subset A^n$ (definido sobre k) un conjunto de polinomios que lo defina, hay una forma muy simple de hacerlo. Basta considerar (fijado un sistema de referencia)

$$I(C) = \{F \in k[X_1, \ldots, X_n] \mid F(P) = 0 \text{ para todo } P \in C\}.$$

Es claro que $I(C)$ es un ideal que contiene a S, lo que implica a su vez que $V(I(C)) = C$. (Si C no es un conjunto algebraico definido sobre k podemos definir igualmente $I(C)$, pero entonces $V(I(C))$ es el menor conjunto algebraico definido sobre k que contiene a C.)

Así tenemos una correspondencia que a cada conjunto algebraico C/k le asigna unívocamente un ideal, y resulta natural preguntarse si esta correspondencia es biunívoca, es decir, si cada ideal $I \subset k[X_1, \ldots, X_n]$ es de la forma $I(C)$ para un cierto conjunto algebraico C/k. La respuesta es negativa, debido a que los ideales $I(C)$ tienen necesariamente una propiedad que no la comparten todos los ideales. Vamos a definirla:

Definición 3.12 Si A es un anillo e I es un ideal de A, definimos el *radical* de I como la intersección $\operatorname{rad} I$ de todos los ideales primos de A que contienen a I. Convenimos en que $\operatorname{rad} A = A$. Obviamente $I \subset \operatorname{rad} I$. Diremos que I es un *ideal radical* si $I = \operatorname{rad} I$.

Hemos elegido como definición la propiedad más interesante a efectos teóricos del radical de un ideal, si bien en la práctica existe una caracterización mucho más operativa y que explica el nombre de "radical":

Teorema 3.13 *Si A es un anillo e I es un ideal de A, entonces*

$$\operatorname{rad} I = \{a \in A \mid a^r \in I \text{ para cierto } r \in \mathbb{N}\}.$$

DEMOSTRACIÓN: Una inclusión es inmediata. Supongamos que $a^r \notin I$ para ningún $r \in \mathbb{N}$ y veamos que $a \notin \operatorname{rad} I$. En efecto, sea Σ el conjunto de los ideales J de A tales que $I \subset J$ y $a^r \notin J$ para todo $r \in \mathbb{N}$. Tenemos que $I \in \Sigma \neq \varnothing$. Por el lema de Zorn existe un $P \in \Sigma$ maximal respecto de la inclusión. Obviamente $I \subset P \neq A$ y $a \notin P$. Basta probar que P es un ideal primo, pues entonces $a \notin \operatorname{rad} I$.

Si $x \notin P$, $y \notin P$, entonces $P + (x)$, $P + (y) \notin \Sigma$, luego existen r, $s \in \mathbb{N}$ tales que $a^r \in P + (x)$, $a^s \in P + (y)$. Por consiguiente $a^{r+s} \in P + (xy)$, luego $P + (xy) \notin \Sigma$, lo que obliga a que $xy \notin P$. ■

En otras palabras, el teorema afirma que el radical de un ideal está formado por todas las raíces de los elementos del ideal. Ahora es inmediato comprobar que $\operatorname{rad}(\operatorname{rad} I)) = \operatorname{rad} I$, así como que $\operatorname{rad} I$ es el menor ideal radical que contiene al ideal I. Otro hecho elemental es que todo ideal primo es radical.

Ahora podemos retomar nuestra discusión sobre la relación entre conjuntos algebraicos e ideales observando que si $C \subset A^n$ es un conjunto algebraico definido sobre k entonces $I(C)$ es obviamente un ideal radical, así como que si $I \subset k[X_1, \ldots, X_n]$, entonces $V(I) = V(\operatorname{rad} I)$.

En vista de estos hechos, aunque la correspondencia entre conjuntos algebraicos e ideales no sea biunívoca, todavía cabe la posibilidad de que $C \mapsto I(C)$ determine una biyección entre los subconjuntos algebraicos de A^n definidos sobre k y los ideales radicales de $k[X_1, \ldots, X_n]$. Esto equivale a afirmar que si I es un ideal radical, entonces $I = I(V(I))$, lo que nos lleva al teorema de los ceros de Hilbert:

Teorema 3.14 (Teorema de los ceros de Hilbert) *Sea K un cuerpo algebraicamente cerrado y k un subcuerpo de K. Si I es un ideal de $k[X_1, \ldots, X_n]$ tal que $V(I) = \varnothing$, entonces $I = k[X_1, \ldots, X_n]$.*

En otras palabras: si un sistema de ecuaciones polinómicas $F_i = 0$ no tiene soluciones en un cuerpo algebraicamente cerrado, ello se debe necesariamente a que es posible expresar $1 = G_1F_1 + \cdots + G_rF_r$, para ciertos polinomios G_i.

Vamos a dar una prueba del teorema de Hilbert basada en que es equivalente a este otro resultado:

Teorema 3.15 *Si L/K es una extensión de cuerpos tal que $L = K[S]$, para un cierto conjunto finito $S \subset L$, entonces la extensión L/K es algebraica.*

Demostración (de la equivalencia entre ambos teoremas): Supongamos el teorema 3.15. Si $I \neq k[X_1, \ldots, X_n]$, podemos tomar un ideal maximal M de $k[X_1, \ldots, X_n]$ que contenga a I. Llamamos $L = k[X_1, \ldots, X_n]/M$. Obviamente podemos considerar a k como subcuerpo de L y además $L = k[S]$, donde S consta de las clases de las indeterminadas X_i módulo M. Por hipótesis L/k es una extensión algebraica y, como K es algebraicamente cerrado, existe un k-monomorfismo $\phi : L \longrightarrow K$. Claramente, $\phi([X_1], \ldots, [X_n]) \in V(I) \neq \varnothing$.

Recíprocamente, si suponemos el teorema de los ceros y $L = K[a_1, \ldots, a_n]$, entonces sea M el núcleo del epimorfismo $\phi : K[X_1, \ldots, X_n] \longrightarrow L$ dado por $\phi(X_i) = a_i$. Ciertamente M es un ideal maximal de $K[X_1, \ldots, X_n]$. Si $\overline{K}$ es una clausura algebraica de K, tenemos que M tiene un cero en $A^n(\overline{K})$, digamos $(\xi_1, \ldots, \xi_n)$. La evaluación en dicho punto es un K-homomorfismo $K[X_1, \ldots, X_n] \longrightarrow \overline{K}$ cuyo núcleo es M. En total tenemos los K-isomorfismos

$$L \cong K[X_1, \ldots, X_n]/M \cong K[\xi_1, \ldots, \xi_n]$$

y, como cada ξ_i es algebraico sobre K, vemos que la extensión L/K es algebraica. ■

El teorema 3.15 es consecuencia inmediata de los dos teoremas siguientes:

Teorema 3.16 *Sean $A \subset B \subset C$ tres dominios, donde A es noetheriano y $C = A[c_1, \ldots, c_n]$. Si C es un B-módulo finitamente generado, entonces B es finitamente generado como anillo sobre A.*

Demostración: Pongamos que $C = \langle w_1, \ldots, w_m \rangle_B$. Podemos suponer que el generador contiene a $c_1, \ldots, c_n$. Digamos que

$$w_i w_j = \sum_{r=1}^{m} b_{ij}^r w_r, \qquad b_{ij}^r \in B.$$

Llamemos $B' = A[b_{ij}^r]$. Entonces $C = \langle w_1, \ldots, w_m \rangle_{B'}$, pues el miembro derecho contiene a $A[c_1, \ldots, c_n]$.

Como A es noetheriano, lo mismo le sucede a B' y C es un B'-módulo finitamente generado, luego es un B'-módulo noetheriano. En particular, B es también un B'-módulo finitamente generado (porque es un B'-submódulo de C). De aquí se sigue inmediatamente que B es finitamente generado (como anillo) sobre A. ■

Teorema 3.17 *Sea $L = K(X_1, \ldots, X_n)$ el cuerpo de las fracciones algebraicas con n indeterminadas sobre un cuerpo K. Entonces L no es finitamente generado como anillo sobre K.*

Demostración: Supongamos que $L = K[F_1, \ldots, F_m]$, donde $F_i = G_i/H_i$, con $G_i,\ H_i \in K[X_1, \ldots, X_n]$. Esto implica que cada elemento de L puede expresarse como un cociente de polinomios en cuyo denominador aparecen a lo sumo los factores primos de los polinomios H_i, que son un número finito. Por otra parte, es claro que $K[X_1, \ldots, X_n]$ contiene infinitos polinomios irreducibles. Si F es uno de ellos distinto de los que dividen a los H_i, entonces la factorización única implica que $1/F$ no admite la representación indicada anteriormente, y tenemos una contradicción. ■

La demostración del teorema 3.15 es ahora inmediata: Si L/K es trascendente, sea $\{X_1, \ldots, X_n\}$ una base de trascendencia. Aplicamos 3.16 a los anillos

$$K \subset K(X_1, \ldots, X_n) \subset L.$$

Como la extensión $L/K(X_1, \ldots, X_n)$ es algebraica y finitamente generada, concluimos que $K(X_1, \ldots, X_n)$ es finitamente generado como anillo sobre K, cuando acabamos de probar que esto es falso. ■

Con el teorema de los ceros de Hilbert ya podemos demostrar la relación fundamental:

Teorema 3.18 *Sea K un cuerpo algebraicamente cerrado y k un subcuerpo de K. Entonces, para cada ideal I de $k[X_1, \ldots, X_n]$ se cumple la relación*

$$I(V(I)) = \operatorname{rad} I.$$

Demostración: Es claro que $\operatorname{rad} I \subset I(V(I))$. Supongamos ahora que $F \in I(V(I))$, $F \neq 0$. Consideremos el anillo $k[X_1, \ldots, X_n, T]$ y en él el ideal $J = (I, FT - 1)$. Es inmediato comprobar que $V(J) = \varnothing$, luego el teorema de los ceros de Hilbert nos da que $J = k[X_1, \ldots, X_n, T]$. Así pues,

$$1 = \sum_{i=1}^{m} R_i F_i + R(FT - 1), \qquad F_i \in I,\ R_i, R \in k[X_1, \ldots, X_n, T].$$

Sea $\phi : k[X_1, \ldots, X_n, T] \longrightarrow k(X_1, \ldots, X_n)$ el homomorfismo de anillos dado por $\phi(X_i) = X_i$, $\phi(T) = 1/F$. Entonces

$$1 = \sum_{i=1}^{m} \phi(R_i) F_i,$$

y podemos expresar $\phi(R_i) = S_i/F^r$, con $S_i \in k[X_1, \ldots, X_n]$ y un cierto $r \in \mathbb{N}$. Por consiguiente $F^r \in I$ y, en definitiva, $F \in \operatorname{rad} I$. ■

En definitiva, las correspondencias $I \mapsto V(I)$, $C \mapsto I(C)$ definen biyecciones mutuamente inversas entre el conjunto de los ideales radicales de $k[X_1, \ldots, X_n]$

y el conjunto de los subconjuntos algebraicos de A^n definidos sobre k. Es inmediato que estas biyecciones invierten las inclusiones.

Veamos otra consecuencia sencilla del teorema anterior: Si $k \subset k' \subset K$ y C/k es un conjunto algebraico afín definido sobre k, también podemos considerarlo definido sobre k', con lo que podemos asociarle los ideales $I_k(C)$ e $I_{k'}(C)$. La relación entre ambos es que

$$I_{k'}(C) = \mathrm{rad}(I_k(C)k'[X_1, \ldots, X_n]). \tag{3.1}$$

En efecto, se cumple que

$$C = V(I_k(C)) = V(I_k(C)k'[X_1, \ldots, X_n]) = V(\mathrm{rad}(I_k(C)k'[X_1, \ldots, X_n])),$$

y la biyección entre conjuntos algebraicos e ideales radicales implica (3.1).

Si C/k es un conjunto algebraico, el ideal $I(C)$ determina a C de forma extrínseca, es decir, explicitando cómo C está contenido en A^n, indicando cuáles de los puntos de A^n están en C. Ahora vamos a asignar a C otro objeto algebraico que, según veremos, lo determinará intrínsecamente, sin hacer referencia a la forma en que C está sumergido en un espacio afín.

Definición 3.19 Si C/k es un conjunto algebraico, diremos que una aplicación $f : C \longrightarrow K$ es *polinómica* (definida sobre k) si existe un $F \in k[X_1, \ldots, X_n]$ tal que (respecto de un sistema de referencia prefijado), $f(P) = F(P)$ para todo $P \in C$.

Aquí se entiende que $F(P)$ representa al polinomio F evaluado en las coordenadas de P. Notemos que aunque el polinomio F depende del sistema de referencia, la noción de aplicación polinómica es independiente de esta elección.

Representaremos por $k[C]$ el conjunto de todas las aplicaciones polinómicas sobre C. Es obvio que $k[C]$ adquiere estructura de k-álgebra con las operaciones definidas puntualmente. Fijado un sistema de referencia, es inmediato el isomorfismo

$$k[C] \cong k[X_1, \ldots, X_n]/I(C). \tag{3.2}$$

Más adelante definiremos la noción de isomorfismo de conjuntos algebraicos y veremos que dos conjuntos algebraicos son isomorfos si y sólo si lo son sus álgebras de funciones polinómicas. Esto significa que las propiedades de un conjunto C/k que se conservan por isomorfismos, es decir, las propiedades que no dependen de la forma en que C está sumergido en A^n, son precisamente las propiedades que pueden expresarse en términos del álgebra $k[C]$.

Ahora vamos a ver qué puede decirse en general de las álgebras de funciones polinómicas:

Definición 3.20 Si k es un cuerpo, una *k-álgebra afín* es una k-álgebra finitamente generada sobre k (como anillo).

Obviamente, si C/k es un conjunto algebraico, entonces $k[C]$ es una k-álgebra afín, generada por las clases $x_i = [X_i]$ de las funciones coordenadas. En general, $k[C]$ puede tener divisores de cero, pero lo que no puede tener son elementos nilpotentes:

Definición 3.21 Sea A un anillo. Un elemento $a \in A$ es *nilpotente* si existe un $n \in \mathbb{N}$ tal que $a^n = 0$. Si A no tiene elementos nilpotentes diremos que es un anillo *reducido.*

Es obvio que si I es un ideal radical de un anillo A, entonces el cociente A/I es un anillo reducido. En particular, el ideal $\operatorname{rad} 0$ está formado por todos los elementos nilpotentes y se le llama *radical nilpotente* de A. Es la intersección de todos los ideales primos de A. Definimos la *reducción* de A como el anillo cociente

$$A_{\mathrm{red}} = A/\operatorname{rad} 0,$$

que ciertamente es un anillo reducido. Si I es un ideal de un anillo A, es claro que $(A/I)_{\mathrm{red}} = A/\operatorname{rad} I$.

Ejercicio: Demostrar que si I es un ideal de A y $S \subset A$ es un conjunto multiplicativo, entonces $S^{-1}\operatorname{rad} I = \operatorname{rad} S^{-1}I$. En particular, si A es reducido, también lo es $S^{-1}A$.

Si C/k es un conjunto algebraico, el álgebra $k[C]$ se obtiene como un cociente sobre un ideal radical, luego es una k-álgebra afín reducida. El teorema siguiente muestra que en general no podemos decir más:

Teorema 3.22 *Toda k-álgebra afín reducida es k-isomorfa a una k-álgebra $k[C]$, para cierto conjunto algebraico afín C/k.*

DEMOSTRACIÓN: Sea $A = k[x_1, \ldots, x_n]$ una k-álgebra afín reducida y consideremos el epimorfismo de k-álgebras $k[X_1, \ldots, X_n] \longrightarrow A$ dado por $X_i \mapsto x_i$. Como A es reducida, su núcleo I es un ideal radical. Sea $C = V(I)$, de modo que $I = I(C)$ y $A \cong k[X_1, \ldots, X_n]/I(C) = k[C]$. ■

Veamos una aplicación:

Teorema 3.23 *Sea A una k-álgebra afín e I un ideal propio de A. Entonces* $\operatorname{rad} I$ *es la intersección de los ideales maximales de A que contienen a I.*

DEMOSTRACIÓN: Los ideales maximales de A que contienen a I son los mismos que contienen a $\operatorname{rad} I$, luego podemos cambiar I por $\operatorname{rad} I$ y suponer que I es radical. Equivalentemente, hemos de probar que la intersección de los ideales maximales de A/I es nula, luego basta probar que la intersección de todos los ideales maximales de una k-álgebra afín reducida es nula. Por el teorema anterior podemos considerar una k-álgebra de la forma $k[C]$, para cierto conjunto algebraico afín C.

Si $f = [F] \in k[C]$ está contenido en todos los ideales maximales de $k[C]$, notamos que para cada punto $P \in C$ se cumple que

$$\mathfrak{m}_P = \{g \in k[C] \mid g(P) = 0\}$$

es un ideal maximal de $k[C]$. Por consiguiente $F \in I(C)$, luego $f = 0$. ■

Observemos ahora que si A y B son dos k-álgebras, entonces $A \otimes_k B$ tiene una estructura natural de k-álgebra determinada por la relación

$$(a \otimes b)(a' \otimes b') = (aa' \otimes bb').$$

La definición es correcta porque podemos definir una aplicación multilineal

$$\phi : A \times B \times A \times B \longrightarrow A \otimes_k B$$

dada por $\phi(a, b, a', b') = aa' \otimes bb'$. Esta aplicación induce a su vez un homomorfismo $\phi : A \otimes_k B \otimes_k A \otimes_k B \longrightarrow A \otimes_k B$ y el producto en $A \otimes_k B$ es su restricción a $(A \otimes_k B) \times (A \otimes_k B)$.

Teorema 3.24 *Consideremos cuerpos $k \subset k' \subset K$ y un conjunto algebraico afín C/k. Entonces*

$$k'[C] \cong (k' \otimes_k k[C])_{\mathrm{red}}.$$

DEMOSTRACIÓN: Teniendo en cuenta la relación (3.1), tenemos que

$$k'[C] = k'[X_1, \ldots, X_n]/\mathrm{rad}(I_k(C)k'[X_1, \ldots, X_n])$$

$$= (k'[X_1, \ldots, X_n]/I_k(C)k'[X_1, \ldots X_n])_{\mathrm{red}}.$$

Por otra parte, tenemos los homomorfismos naturales (de anillos)

$$k'[X_1, \ldots, X_n] \cong k' \otimes_k k[X_1, \ldots, X_n] \xrightarrow{1 \otimes p} k' \otimes_k k[C].$$

Basta observar que el núcleo de la composición de ambos es precisamente $I_k(C)k'[X_1, \ldots, X_n]$. En efecto, un elemento de $k' \otimes_k k[X_1, \ldots, X_n]$ se expresa de forma única como

$$u = \sum_i \alpha_i \otimes F_i,$$

donde α_i recorre una k-base de k' y $F_i \in k[X_1, \ldots, X_n]$. Su imagen por $1 \otimes p$ es

$$\sum_i \alpha_i \otimes p(F_i),$$

y la unicidad de esta expresión implica que $(1 \otimes p)(u) = 0$ si y sólo si $F_i \in I_k(C)$ para todo i. Así pues, el núcleo de ϕ lo forman las combinaciones lineales en k' de los elementos de $I_k(F)$, pero esto es precisamente $I_k(C)k'[X_1, \ldots, X_n]$. ■

Similarmente podemos determinar la k-álgebra afín de un producto cartesiano:

Teorema 3.25 *Sean $C \subset A^n$ y $C' \subset A^m$ dos conjuntos algebraicos afines definidos sobre k. Entonces $C \times C' \subset A^{n+m}$ es también un conjunto algebraico afín definido sobre k y $k[C \times C'] \cong (k[C] \otimes_k k[C'])_{\mathrm{red}}$.*

Demostración: Es inmediato que $C \times C'$ es un conjunto algebraico afín definido sobre k. Concretamente es $V(I(C) \cup I(C'))$, considerando ambos ideales como subconjuntos de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Claramente

$$I(C \times C') = \operatorname{rad}(I(C) \cup I(C')),$$

luego

$$k[C \times C'] = (k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(C) \cup I(C'))_{\mathrm{red}}.$$

Ahora basta tener en cuenta los homomorfismos naturales

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \cong k[X_1, \ldots, X_n] \otimes_k k[Y_1, \ldots, Y_m] \longrightarrow k[C] \otimes_k k[C'],$$

cuya composición tiene por núcleo al ideal generado por $I(C) \cup I(C')$. En efecto, una inclusión es obvia y nos da un epimorfismo

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(C) \cup I(C')) \longrightarrow k[C] \otimes_k k[C'].$$

Basta ver que se trata de una aplicación biyectiva, y ello se debe a que tiene una inversa

$$k[C] \otimes_k k[C'] \longrightarrow k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/(I(C) \cup I(C'))$$

definida naturalmente por $[F] \times [G] \mapsto [FG]$. ■

Como una primera muestra de que, en efecto, las propiedades intrínsecas de un conjunto algebraico C/k pueden expresarse en términos de $k[C]$, vamos a ver que $k[C]$ determina los subconjuntos algebraicos de C:

Si $S \subset k[C]$, podemos considerar el conjunto

$$V_C(S) = \{P \in C \mid f(P) = 0 \text{ para todo } f \in S\}.$$

Es inmediato comprobar que se trata de un subconjunto algebraico de C definido sobre k. (Es el conjunto de los ceros de los polinomios que definen a C más los que definen a las funciones de S.)

Igualmente, si D/k es un subconjunto algebraico de C/k, definimos

$$I_C(D) = \{f \in k[C] \mid f(P) = 0 \text{ para todo } P \in D\}.$$

Se trata de un ideal radical de $k[C]$ que, a través del isomorfismo (3.2), se corresponde con

$$I_C(D) \cong I(D)/I(C).$$

Ahora es fácil comprobar que los subconjuntos algebraicos de C/k (definidos sobre k) se corresponden biunívocamente con los ideales radicales de $k[C]$ a través de las correspondencias $D \mapsto I_C(D)$, $I \mapsto V_C(I)$. Para ideales arbitrarios tenemos la relación

$$I_C(V_C(I)) = \operatorname{rad} I.$$

3.3 La topología de Zariski

Observemos que si $C_1 = V(F_1, \ldots, F_r)$ y $C_2 = V(G_1, \ldots, G_s)$ son dos subconjuntos algebraicos de A^n definidos sobre k, entonces

$$C_1 \cup C_2 = V(F_iG_j \mid i = 1, \ldots, r,\ j = 1, \ldots, s)$$

es también un conjunto algebraico definido sobre k. Más en general, la unión finita de subconjuntos algebraicos de A^n definidos sobre k es de nuevo un conjunto algebraico definido sobre k. Similarmente, la intersección de una familia arbitraria (no necesariamente finita) de subconjuntos de A^n definidos sobre k es de nuevo un conjunto algebraico definido sobre k (definido por la unión de los conjuntos de polinomios que definen a los miembros de la familia).

Si añadimos a esto que $A^n = V(0)$ y $\varnothing = V(1)$ son conjuntos algebraicos definidos sobre k, vemos que podemos definir la *topología de Zariski* de A^n relativa a k como la topología que tiene por cerrados a los subconjuntos algebraicos de A^n definidos sobre k.

La *topología de Zariski* en un conjunto algebraico C/k de A^n es la restricción a C de la topología de Zariski de A^n, cuyos cerrados son los subconjuntos algebraicos de C definidos sobre k.

En lo sucesivo consideraremos a los conjuntos algebraicos (definidos sobre k) como espacios topológicos con la topología de Zariski.

Hay que tener presente que la topología de Zariski no es de Hausdorff, como veremos enseguida. En general, cuando hablemos de espacios topológicos no supondremos nunca que sean de Hausdorff.

Definición 3.26 Un espacio topológico X es *irreducible* si cuando $X = C_1 \cup C_2$ con C_1 y C_2 cerrados, necesariamente $C = C_1$ o $C = C_2$.

Llamaremos *variedades algebraicas afines* sobre k a los subconjuntos algebraicos (definidos sobre k) irreducibles respecto a la topología de Zariski relativa a k.

Teorema 3.27 *Un conjunto algebraico V/k no vacío es irreducible si y sólo si el ideal $I(V)$ es primo.*

Demostración: Si V/k es irreducible y F_1, $F_2 \in k[X_1, \ldots, X_n]$ cumplen $F_1F_2 \in I(V)$, entonces podemos tomar $H_1 = V(F_1)$, $H_2 = V(F_2)$, con lo que tenemos dos conjuntos cerrados tales que $V = (V \cap H_1) \cup (V \cap H_2)$. Por consiguiente $V = V \cap H_i$ para un i, de donde se sigue que $F_i \in I(V)$.

Recíprocamente, si $I(V)$ es primo y se cumple que $V = C_1 \cup C_2$, entonces $I(V) = I(C_1) \cap I(C_2) \supset I(C_1)I(C_2)$, luego $I(V) \supset I(C_i)$ para algún i, luego $V \subset C_i$, es decir, $V = C_i$. ■

Ejercicio: Probar que las *variedades lineales,* es decir, los subconjuntos algebraicos de A^n definidos por un sistema de ecuaciones lineales (puntos, rectas, planos, etc.) son irreducibles.

Las variedades afines definidas sobre k se corresponden biunívocamente con los ideales primos de $k[X_1, \ldots, X_n]$, de donde se sigue fácilmente que las subvariedades afines definidas sobre k de un conjunto algebraico C/k se corresponden biunívocamente con los ideales primos del álgebra $k[C]$.

Demostramos ahora algunos resultados válidos para espacios topológicos arbitrarios:

Teorema 3.28 *Sea X un espacio topológico. Las afirmaciones siguientes son equivalentes:*

a) X es irreducible.

b) Si U_1 y U_2 son abiertos no vacíos, entonces $U_1 \cap U_2 \neq \varnothing$.

c) Todo abierto no vacío es denso en X.

DEMOSTRACIÓN: La equivalencia entre a) y b) se obtiene tomando complementos, y la equivalencia entre b) y c) es trivial. ■

Como consecuencia, un subconjunto Y de un espacio topológico X es irreducible si y sólo si lo es su clausura $\overline{Y}$. En efecto, si $\overline{Y}$ es irreducible, dos abiertos no vacíos de Y son de la forma $U_1 \cap Y$, $U_2 \cap Y$, con los U_i abiertos no vacíos en $\overline{Y}$. La intersección es $U_1 \cap U_2 \cap Y$, que es no vacío, puesto que $U_1 \cap U_2 \neq \varnothing$ y Y es denso en $\overline{Y}$. El recíproco se prueba similarmente. ■

Definición 3.29 Una *componente irreducible* de un espacio topológico X es un subconjunto irreducible maximal respecto a la inclusión.

Por la observación precedente, las componentes irreducibles son cerradas.

Teorema 3.30 *Todo subconjunto irreducible de un espacio topológico está contenido en una componente irreducible. Todo espacio topológico es la unión de sus componentes irreducibles.*

DEMOSTRACIÓN: Puesto que los puntos son trivialmente irreducibles, la segunda afirmación se deduce inmediatamente de la primera. Si X es un espacio topológico y X' es un subconjunto irreducible, consideramos la familia de todos los subconjuntos irreducibles de X que contienen a X'. Basta probar que podemos aplicar el lema de Zorn, para lo cual basta a su vez demostrar que la unión de una cadena de conjuntos irreducibles es también irreducible.

En efecto, dos abiertos no vacíos de la unión M son las intersecciones con M de dos abiertos no vacíos de X, digamos U_1 y U_2. Existe un miembro de la familia, digamos M' tal que $M' \cap U_i \neq \varnothing$ para los dos índices i, con lo que $M' \cap U_1 \cap U_2 \neq \varnothing$ y también $M \cap U_1 \cap U_2 \neq \varnothing$. ■

Definición 3.31 Un espacio topológico es *noetheriano* si para toda cadena decreciente de cerrados $C_1 \supset C_2 \supset C_3 \supset \cdots$ existe un índice i tal que $C_i = C_j$ para todo $j \geq i$.

Por ejemplo, si C/k es un conjunto algebraico definido sobre k, entonces el álgebra $k[C]$ es claramente noetheriana, lo cual se traduce en que C es noetheriano, pues toda cadena decreciente de cerrados en C se corresponde con una cadena creciente de ideales en $k[C]$.

Teorema 3.32 *Un espacio topológico noetheriano tiene un número finito de componentes irreducibles, ninguna de las cuales está contenida en la unión de las demás.*

Demostración: Sea M el conjunto de los subconjuntos cerrados del espacio que no pueden expresarse como unión finita de componentes irreducibles. Vamos a demostrar que $M = \varnothing$. Si existe un $C_0 \in M$, entonces C_0 no es irreducible, luego $C_0 = C_1 \cup D_1$, donde ninguno de los dos cerrados es igual a C_0. Si ambos cerrados se descompusieran en unión finita de conjuntos irreducibles, lo mismo le sucedería a C_0, luego al menos uno de ellos, digamos C_1 no admite tal descomposición, es decir, $C_1 \in M$. Repitiendo el argumento formamos una cadena estrictamente decreciente $C_0 \supset C_1 \supset C_2 \supset \cdots$, en contradicción con el carácter noetheriano del espacio.

Así pues, todo cerrado, y en particular el propio espacio, es unión de un número finito de componentes irreducibles. Digamos que la descomposición es $X = X_1 \cup \cdots \cup X_r$ (donde podemos suponer que las componentes son distintas dos a dos). Si Y es cualquier componente irreducible de X, entonces

$$Y = Y \cap X = (Y \cap X_1) \cup \cdots \cup (Y \cap X_r),$$

de donde se sigue que $Y = Y \cap X_i$ para algún i, es decir, $Y \subset X_i$ y, por maximalidad, $Y = X_i$. Esto prueba que el número de componentes irreducibles es finito. Más aún, ninguna de ellas puede estar contenida en la unión de las restantes, pues el argumento que acabamos de emplear probaría que sería igual a una de las restantes. ■

La topología de Zariski nos permite definir la dimensión de un conjunto algebraico:

Definición 3.33 Si X es un espacio topológico, llamaremos *dimensión de Krull* de X, abreviada $\dim X \in \mathbb{N} \cup \{\infty\}$, al supremo de las longitudes n de todas las cadenas de cerrados irreducibles no vacíos

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n.$$

Convenimos en que $\dim \varnothing = -1$. La *codimensión* de un cerrado irreducible no vacío Y en X se define como el supremo $\operatorname{codim}_X Y$ de las longitudes de todas las cadenas que cumplen además $X_0 = Y$.

Como un espacio de Hausdorff irreducible (no vacío) se reduce a un punto, vemos que la dimensión de Krull de todo espacio de Hausdorff no vacío es siempre 0. Por el contrario, es fácil probar que $\dim A^n \geq n$, sin más que considerar una cadena creciente de variedades lineales. De hecho se cumple la igualdad, aunque ahora no estamos en condiciones de probarlo. Más en general, veremos que —con esta definición de dimensión— todos los conjuntos algebraicos tienen dimensión finita, los puntos tienen dimensión 0, las rectas tienen dimensión 1, etc. Para ello necesitaremos varias técnicas algebraicas que desarrollaremos en las secciones siguientes. Terminaremos esta sección con algunas observaciones sencillas sobre la dimensión de Krull:

Es evidente que si Y es un cerrado irreducible en un espacio topológico X, se cumple que

$$\dim Y + \operatorname{codim}_X Y \leq \dim X.$$

Hay que tener presente que la desigualdad puede ser estricta. (Por ejemplo, en un conjunto algebraico C que sea unión de un plano y una recta, un punto que esté sobre la recta pero no sobre el plano tiene dimensión 0 y codimensión 1, mientras que la dimensión de C es 2. Según hemos comentado, ahora no estamos en condiciones de justificar estas afirmaciones, pero más adelante serán evidentes.)

Toda cadena de cerrados irreducibles en un espacio topológico ha de estar contenida en una de sus componentes irreducibles, luego podemos concluir que la dimensión de un espacio topológico es el supremo de las dimensiones de sus componentes.

Similarmente, si $X = A_1 \cup \cdots \cup A_r$ es una descomposición de X en cerrados, cada cadena de cerrados irreducibles ha de estar contenida en uno de los conjuntos A_i, luego también tenemos que $\dim X = \max\limits_i \dim A_i$.

Por último observemos que si Y es un subconjunto cerrado de X entonces $\dim Y \leq \dim X$. Si tanto Y como X son irreducibles y $\dim X < \infty$, entonces la igualdad sólo se da si $Y = X$. En efecto, si $Y \subsetneq X$ y $\dim Y = r$, una cadena de cerrados irreducibles de Y de longitud r se completa a una cadena con un término más añadiendo X.

3.4 El espectro de un anillo

La noción de espectro de un anillo que vamos a introducir ahora es la clave que nos permitirá traducir sistemáticamente las propiedades de un conjunto algebraico C/k a propiedades de su álgebra $k[C]$ de funciones polinómicas, al mismo tiempo que nos permitirá tratar con anillos arbitrarios, que no sean necesariamente de la forma $k[C]$.

Definición 3.34 Si A es un anillo, llamaremos *espectro* de A al conjunto $\operatorname{Esp} A$ formado por todos sus ideales primos.

Si I es un ideal de A, definimos

$$V(I) = \{\mathfrak{p} \in \operatorname{Esp} A \mid \mathfrak{p} \supset I\}.$$

Llamaremos *topología de Zariski* en $\operatorname{Esp} A$ a la topología que tiene por cerrados a los conjuntos $V(I)$, cuando I recorre los ideales de A.

Esto es correcto, pues $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$ y $\bigcap\limits_{j\in J} V(I_j) = V\big(\sum\limits_{j\in J} I_j\big)$.

En lo sucesivo consideraremos siempre a $\operatorname{Esp} A$ como espacio topológico con la topología de Zariski. Los resultados siguientes muestran que $\operatorname{Esp} A$ se comporta formalmente de forma similar a un conjunto algebraico.

Si $C \subset \operatorname{Esp} A$, definimos

$$I(C) = \bigcap_{\mathfrak{p}\in C} \mathfrak{p},$$

que es un ideal radical de A.

Teorema 3.35 *Si A es un anillo y $C \subset \operatorname{Esp} A$, entonces*

$$V(I(C)) = \overline{C}.$$

DEMOSTRACIÓN: Trivialmente $C \subset V(I(C))$ y, como el miembro derecho es cerrado, también $\overline{C} \subset V(I(C))$. Recíprocamente, si $\overline{C} = V(I)$, entonces para todo $\mathfrak{p} \in C$ tenemos que $\mathfrak{p} \supset I$, luego $I \subset I(C)$, luego $V(I(C)) \subset V(I) = \overline{C}$. ■

Similarmente tenemos:

Teorema 3.36 *Si A es un anillo e I es un ideal de A, entonces*

$$I(V(I)) = \operatorname{rad} I.$$

DEMOSTRACIÓN: Claramente

$$I(V(I)) = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p} = \bigcap_{\mathfrak{p}\supset I} \mathfrak{p} = \operatorname{rad} I.$$

■

Así pues, los cerrados en $\operatorname{Esp} A$ se corresponden biunívocamente con los ideales radicales de A.

Teorema 3.37 *Sea A un anillo y $C \neq \varnothing$ un subconjunto cerrado de* $\operatorname{Esp} A$. *Entonces C es irreducible si y sólo si $I(C)$ es primo.*

DEMOSTRACIÓN: Supongamos que C es irreducible y sean f, $g \in A$ tales que $fg \in I(C)$. Para cada $\mathfrak{p} \in C$, tenemos que $f \in \mathfrak{p}$ o $g \in \mathfrak{p}$, luego

$$C = (C \cap V(f)) \cup (C \cap V(g)).$$

Por consiguiente $C \subset V(f)$ o $C \subset V(g)$, luego $f \in I(C)$ o $g \in I(C)$.

Recíprocamente, si $I(C)$ es un ideal primo y $C = C_1 \cup C_2$ es una descomposición en cerrados, entonces $I(C) = I(C_1) \cap I(C_2)$, luego $I(C_i) \subset I(C)$ para uno de los índices i. De hecho, ha de ser $I(C_i) = I(C)$, luego $C_i = C$. ■

Si C/k es un conjunto algebraico, podemos considerar $X = \operatorname{Esp} k[C]$, que es otro espacio topológico cuya relación con C es muy sutil. Los puntos de X

no se corresponden con los puntos de C, sino con los subconjuntos algebraicos de C definidos sobre k. De hecho, la relación natural entre C y X es que existe una biyección natural entre los cerrados de uno y otro, la determinada por $V_C(I) \leftrightarrow V(I)$, donde I recorre los ideales radicales de $k[C]$. Esta biyección respeta las inclusiones, uniones e intersecciones. Obviamente determina también una biyección entre los abiertos de C y los de X.

Las sutilezas aparecen a la hora de relacionar los puntos de C con los de X. Para cada punto $P \in C$ podemos definir

$$\mathfrak{p}_P = \{f \in k[C] \mid f(P) = 0\}.$$

Es claro que $\mathfrak{p}_P \in \operatorname{Esp} A$. Más precisamente, $\mathfrak{p}_P$ es el núcleo del k-homomorfismo de anillos $\psi_P : k[C] \longrightarrow K$ determinado por la evaluación en P. Si $P = (\xi_1, \ldots, \xi_n)$, tenemos el k-isomorfismo

$$k[C]/\mathfrak{p}_P \cong k[\xi_1, \ldots, \xi_n].$$

Si las coordenadas de P son algebraicas sobre k (en particular si K es la clausura algebraica de k), entonces el anillo de la derecha es un cuerpo, luego $\mathfrak{p}_P$ es un ideal maximal.

Tenemos una aplicación $\phi : C \longrightarrow \operatorname{Esp} k[C]$. Observemos que es continua: si $V(I)$ es un cerrado en $k[C]$, entonces

$$\phi^{-1}[V(I)] = \{P \in C \mid \mathfrak{p}_P \supset I\} = V_C(I)$$

es un cerrado en C.

Vamos a ver que, en general, ϕ no es inyectiva ni suprayectiva. Respecto a la inyectividad, si consideramos dos puntos $P = (\xi_1, \ldots, \xi_n)$, $Q = (\xi'_1, \ldots, \xi'_n)$ y $\mathfrak{p}_Q = \mathfrak{p}_Q$, entonces tenemos un k-isomorfismo

$$\psi : k[\xi_1, \ldots, \xi_n] \longrightarrow k[\xi'_1, \ldots, \xi'_n]$$

tal que $\psi(\xi_i) = \xi'_i$, el cual se extiende a un $\sigma \in G(K/k)$ (el grupo de k-automorfismos de K) tal que $Q = P^\sigma$. Recíprocamente, es claro que si P y Q son conjugados en este sentido entonces $\mathfrak{p}_P = \mathfrak{p}_Q$.

Así pues, la aplicación ϕ identifica los puntos conjugados de C. En particular ϕ es inyectiva sobre $C(k)$ y, si $K = k$, entonces ϕ es inyectiva.

Respecto a la suprayectividad, observemos primeramente que si $\mathfrak{m} \in \operatorname{Esp} k[C]$ es un ideal maximal, el teorema de los ceros de Hilbert implica que existe un punto $P \in C$ (de hecho, con coordenadas algebraicas sobre k) tal que $P \in V_C(\mathfrak{m})$, es decir, tal que $\mathfrak{m} \subset \mathfrak{p}_P$ y, por maximalidad, $\mathfrak{m} = \mathfrak{p}_P$.

De hecho, vemos que $\phi^{-1}(\mathfrak{m}) = V_C(\mathfrak{m})$ y, según hemos visto, está formado por una clase de conjugación respecto de $G(K/k)$ de puntos con coordenadas algebraicas sobre k.

Si $\overline{k}$ es la clausura algebraica de k, hemos demostrado que ϕ se restringe a una aplicación suprayectiva de $C(\overline{k})$ en el espacio de los ideales maximales de $k[C]$. Esta aplicación identifica las clases de conjugación respecto de $G(\overline{k}/k)$.

En particular, si k es algebraicamente cerrado, ϕ se restringe a un homeomorfismo entre $C(k)$ y el conjunto de ideales maximales de $k[C]$. (Es un homeomorfismo pues, para todo ideal I de $k[C]$, tenemos que $P \in V_C(I)$ si y sólo si $I \subset \mathfrak{p}_P$, luego $\phi[V_C(I)] = V(I) \cap \phi[C]$.)

El teorema 3.23 implica que el conjunto de los ideales maximales de $k[C]$ es denso en $\operatorname{Esp} k[C]$. En efecto, si un abierto $U = \operatorname{Esp} k[C] \setminus V(I)$ no contiene ningún ideal maximal, esto significa que I está contenido en $\operatorname{rad} 0$, luego $U = \varnothing$.

Ejemplo Por fijar ideas, consideremos $k = \mathbb{R}$, $K = \mathbb{C}$ y la circunferencia $C = V(X^2+Y^2-1)$. Entonces, cada punto real de C, como $(1,0)$, se corresponde con un ideal maximal de $\mathbb{R}[C]$, en este caso con $\mathfrak{p}_P = (x-1, y)$. Sin embargo, C contiene también puntos imaginarios, como $Q = (i, \sqrt{2})$, que se corresponde con el ideal maximal $\mathfrak{p}_Q = (x^2+1, y-\sqrt{2})$ (notemos que $\mathbb{R}[C]/\mathfrak{p}_Q \cong \mathbb{C}$), el mismo asociado a $Q' = (-i, \sqrt{2})$. Los puntos Q y Q' no se pueden distinguir con polinomios de $\mathbb{R}[X,Y]$, en el sentido de que un polinomio se anula en uno si y sólo si se anula en el otro, y por ello están representados por un único ideal maximal de $\mathbb{R}[C]$. ■

En vista de estos resultados, podría parecer que hubiera sido más razonable definir $\operatorname{Esp} A$ como el conjunto de todos los ideales maximales de A pues, al menos cuando la extensión K/k es algebraica, y C/k es un conjunto algebraico, los ideales maximales de $k[C]$ son suficientes para representar todos los puntos de C (identificando las clases de conjugación respecto al grupo de Galois, pero esto no depende de que se incluyan o no en el espectro los primos no maximales.) Sin embargo, vamos a ver que la idea de incluir en el espectro a todos los ideales primos, aunque no sea en principio muy intuitiva, es muy práctica y, de hecho, es crucial para toda la teoría que vamos a desarrollar.

Un primer ejemplo lo tenemos en que los homomorfismos de anillos definen de forma natural aplicaciones continuas entre sus espectros, lo cual no sería cierto si sólo hubiéramos incluido en ellos los ideales maximales:

Definición 3.38 Si $f : A \longrightarrow B$ es un homomorfismo de anillos, definimos $\bar{f} : \operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ mediante $\bar{f}(\mathfrak{p}) = f^{-1}[\mathfrak{p}]$.

Observemos que la antiimagen de un ideal primo es siempre un ideal primo, mientras que la antiimagen de un ideal maximal no es necesariamente maximal.

Las aplicaciones inducidas por homomorfismos son continuas, pues si I es un ideal de A, entonces

$$\bar{f}^{-1}[V(I)] = \{\mathfrak{p} \in \operatorname{Esp} B \mid f^{-1}[\mathfrak{p}] \supset I\} = \{\mathfrak{p} \in \operatorname{Esp} B \mid \mathfrak{p} \supset f[I]\} = V(f[I]B).$$

Si $f : A \longrightarrow B$ es un epimorfismo y su núcleo es I, entonces la aplicación inducida es un homeomorfismo $\bar{f} : \operatorname{Esp} B \longrightarrow V(I)$.

En efecto, es claro que los ideales primos de B se corresponden biunívocamente con los ideales primos de A que contienen a I, es decir, con los elementos de $V(I)$. Esto significa que $\bar{f}$ es biyectiva. Para probar que es cerrada observamos que si J es un ideal en B, entonces $\bar{f}[V(J)] = V(f^{-1}[J])$.

Notemos que para que $f : A \longrightarrow B$ induzca un homeomorfismo entre $\operatorname{Esp} B$ y $\operatorname{Esp} A$ es necesario y suficiente que $\operatorname{Esp} A = V(I)$, en cuyo caso

$$\operatorname{rad} 0 = \bigcap_{\mathfrak{p}} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \operatorname{rad} I.$$

Esto implica que todos los elementos de I son nilpotentes y, recíprocamente, si I está formado por elementos nilpotentes entonces $V(I) = \operatorname{Esp} A$ y los espectros son homeomorfos. En particular, para todo anillo A se cumple que $\operatorname{Esp} A$ y $\operatorname{Esp}(A_{\mathrm{red}})$ son homeomorfos.

Teorema 3.39 *Sea S un subconjunto multiplicativo de un anillo A, consideremos el homomorfismo canónico $i : A \longrightarrow S^{-1}A$ y $\Sigma = \{\mathfrak{p} \in \operatorname{Esp} A \mid \mathfrak{p} \cap S = \varnothing\}$. Entonces $\bar{\imath} : \operatorname{Esp} S^{-1}A \longrightarrow \Sigma$ es un homeomorfismo (considerando en Σ la topología inducida desde* $\operatorname{Esp} A$*).*

DEMOSTRACIÓN: En 3.4 hemos probado que $\bar{\imath}$ es biyectiva, y en general sabemos que es continua. Falta probar que es cerrada. Un cerrado en $\operatorname{Esp} S^{-1}A$ está formado por los ideales $\mathfrak{P} \in \operatorname{Esp} S^{-1}A$ tales que $I \subset \mathfrak{P}$, para un cierto ideal I de $S^{-1}A$, y su imagen en Σ la forman los ideales $\mathfrak{p} \in \operatorname{Esp} A$ tales que $i^{-1}(I) \subset \mathfrak{p}$ y $\mathfrak{p} \cap S = \varnothing$. Este conjunto es $V(i^{-1}(I)) \cap \Sigma$, que es cerrado en Σ. ■

Otra de las consecuencias de admitir a todos los ideales primos en el espectro de un anillo es que así podemos formalizar un antiguo y vago concepto de la geometría algebraica: el de "punto genérico", entendido como un punto arbitrario de un conjunto algebraico que no tenga ninguna "peculiaridad", de modo que lo que vale para él vale para "casi todos" los puntos del conjunto.

Definición 3.40 Sea X un espacio topológico y C un subconjunto cerrado. Un punto $P \in C$ es un *punto genérico* de C si es denso en C.

Observemos que para que un cerrado C pueda contener un punto genérico es necesario que C sea irreducible, pues todo punto lo es y la clausura de un conjunto irreducible es irreducible. Recíprocamente:

Teorema 3.41 *Si A es un anillo, cada cerrado irreducible no vacío $C \subset \operatorname{Esp} A$ tiene un único punto genérico, a saber, $\mathfrak{p} = I(C)$.*

DEMOSTRACIÓN: Por el teorema 3.35 vemos que

$$\overline{\mathfrak{p}} = V(I(\{\mathfrak{p}\})) = V(\mathfrak{p}) = V(I(C)) = C,$$

luego $\mathfrak{p}$ es ciertamente un punto genérico.

Si $\mathfrak{q}$ es un punto genérico arbitrario en C, entonces, de nuevo por 3.35,

$$C = \overline{\{\mathfrak{q}\}} = V(\mathfrak{q}),$$

luego $\mathfrak{q} = I(V(\mathfrak{q})) = I(C)$. ■

Veremos que, al tratar con los puntos del espectro de un anillo, el hecho de que sean o no maximales será casi siempre irrelevante, y por ello los puntos genéricos se convierten en una poderosa herramienta para estudiar cerrados irreducibles tratándolos como puntos.

Definición 3.42 Sea A un anillo y sea $I \neq A$ un ideal de A. Un *divisor primo* de I es un ideal primo $\mathfrak{p}$ de A tal que $I \subset \mathfrak{p}$. Un *divisor primo minimal* de I es un divisor primo $\mathfrak{p}$ de I tal que si $I \subset \mathfrak{q} \subset \mathfrak{p}$ para un cierto divisor primo $\mathfrak{q}$ de I, necesariamente $\mathfrak{p} = \mathfrak{q}$. Llamaremos *primos minimales* de A a los divisores primos minimales del ideal 0. Claramente A es un dominio íntegro si y sólo si su único primo minimal es el ideal 0.

Observemos que los divisores primos minimales de I son precisamente los puntos genéricos de las componentes irreducibles del cerrado (no vacío) $V(I)$ en $\operatorname{Esp} A$. En efecto, si $\mathfrak{p}$ es un divisor primo minimal de I, entonces $V(\mathfrak{p})$ es una componente irreducible de $V(I)$ y $\mathfrak{p}$ es su punto genérico. Recíprocamente, si $\mathfrak{p}$ es el punto genérico de una componente irreducible $V(\mathfrak{p})$ de $V(I)$, entonces $\mathfrak{p}$ es un divisor primo minimal de I.

El teorema 3.30 se traduce ahora en que todo ideal I de todo anillo A tiene divisores primos minimales. En particular todo anillo tiene primos minimales. Más aún, si $\operatorname{Esp} A$ es noetheriano (lo cual sucede claramente si A es noetheriano), entonces cada ideal I de A tiene sólo un número finito de divisores primos minimales y, en particular, A tiene sólo un número finito de primos minimales. Los primos minimales de un anillo están estrechamente relacionados con sus divisores de cero. Dedicamos la sección siguiente a estudiar con detalle esta relación.

3.5 Primos asociados

La relación fundamental entre los primos minimales de un anillo y sus divisores de cero viene dada por el teorema siguiente:

Teorema 3.43 *Sea A un anillo con un número finito de primos minimales $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Entonces los elementos (no nulos) de cada $\mathfrak{p}_i$ son divisores de cero, y si A es reducido entonces todo divisor de cero pertenece a algún $\mathfrak{p}_i$.*

Demostración: El punto de partida es que, evidentemente,

$$\operatorname{rad} 0 = \bigcap_{i=1}^{s} \mathfrak{p}_i.$$

Si $s = 1$ entonces $\mathfrak{p}_1$ está formado por los elementos nilpotentes de A, luego todos sus elementos (no nulos) son divisores de cero. Suponiendo $s > 1$, tomemos un $p \in \mathfrak{p}_j$ no nulo. Podemos encontrar un $q \in \bigcap_{i\neq j} \mathfrak{p}_i$, $q \notin \mathfrak{p}_j$, pues en caso contrario tendríamos que

$$\bigcap_{i\neq j} \mathfrak{p}_i \subset \mathfrak{p}_j,$$

con lo que $\mathfrak{p}_i \subset \mathfrak{p}_j$ para algún $i \neq j$, en contradicción con la minimalidad de $\mathfrak{p}_j$. Entonces $pq \in \operatorname{rad} 0$, luego $(pq)^m = 0$, para cierto $m \in \mathbb{N}$. Como $q \notin \mathfrak{p}_j$, ha de ser $q^m \neq 0$, luego podemos considerar el mínimo $t \in \mathbb{N}$ tal que $p^t q^m \neq 0$ y $p^{t+1}q^m = 0$. Esto implica que p es un divisor de cero.

Supongamos ahora que A es reducido y sea $d \in A$ un divisor de cero. Esto significa que existe un $d' \in A$ no nulo tal que $dd' = 0$. Como la intersección de los primos minimales es nula, ha de ser $d' \notin \mathfrak{p}_j$ para algún j, pero $dd' \in \mathfrak{p}_j$, luego $d \in \mathfrak{p}_j$. ■

Si el anillo A no es reducido, ya no podemos asegurar que sus divisores estén contenidos en los primos minimales. El resto de la sección está dedicado a estudiar lo que sucede en tal caso.

Definición 3.44 Sea M un módulo sobre un anillo A. Si $m \in M$, definimos el *anulador* de M como el ideal

$$\operatorname{An}(m) = \{a \in A \mid am = 0\}.$$

Similarmente, el *anulador* de M es el ideal

$$\operatorname{An}(M) = \{a \in M \mid am = 0 \text{ para todo } m \in M\}.$$

Diremos que un ideal $\mathfrak{p} \in \operatorname{Esp} A$ está *asociado* a M si existe un $m \in M$ tal que $\mathfrak{p} = \operatorname{An}(m)$. Representaremos por $\operatorname{As}(M)$ el conjunto de ideales asociados a M.

Veamos algunas propiedades sencillas:

Teorema 3.45 *Si M es un A-módulo, entonces $\operatorname{As}(M)$ es el conjunto de los ideales $\mathfrak{p} \in \operatorname{Esp} A$ tales que M tiene un submódulo isomorfo a $A/\mathfrak{p}$.*

Demostración: Si $\mathfrak{p} = \operatorname{An}(m)$, entonces $\langle m\rangle \cong A/\mathfrak{p}$. Recíprocamente, si $A/\mathfrak{p} \cong N$, para un cierto submódulo N de M, entonces $N = \langle m\rangle$, donde m es la imagen de $1 + \mathfrak{p}$ por el isomorfismo, y claramente $\mathfrak{p} = \operatorname{An}(m)$. ■

Teorema 3.46 *Si M es un A-módulo y $\mathfrak{p} \in \operatorname{Esp} A$, entonces $\operatorname{As}(A/\mathfrak{p}) = \{\mathfrak{p}\}$ y $\mathfrak{p}$ es el anulador de todo x no nulo en $A/\mathfrak{p}$.*

Demostración: La primera afirmación se deduce de la segunda. Para probar ésta observamos que si $x = a+\mathfrak{p}$, con $a \in A\setminus\mathfrak{p}$, entonces $b(a+\mathfrak{p}) = 0+\mathfrak{p}$ si y sólo si $b \in \mathfrak{p}$. ■

Teorema 3.47 *Si M es un A-módulo y N es un submódulo, entonces*

$$\mathrm{As}(N) \subset \mathrm{As}(M) \subset \mathrm{As}(N) \cup \mathrm{As}(M/N).$$

Demostración: La primera inclusión es obvia. Si $\mathfrak{p} \in \mathrm{As}(M) \setminus \mathrm{As}(N)$ y $\mathfrak{p} = \mathrm{An}(m)$, para un $m \in M$, entonces $\langle m \rangle \cong A/\mathfrak{p}$ y $\langle m \rangle \cap N = 0$, pues de lo contrario el teorema anterior nos daría que $\mathfrak{p} \in \mathrm{As}(N)$. Entonces el epimorfismo canónico $M \longrightarrow M/N$ se restringe a un isomorfismo entre $\langle m \rangle$ y un submódulo de M/N, luego $\mathfrak{p} \in \mathrm{As}(M/N)$. ■

Teorema 3.48 *Si A es un anillo noetheriano y M es un A-módulo no nulo, entonces* $\mathrm{As}(M) \neq \varnothing$.

Demostración: El conjunto de todos los ideales de A que son anuladores de elementos no nulos de M es obviamente no vacío, luego tiene un elemento maximal $\mathfrak{p}$. Vamos a probar que es un ideal primo. Pongamos que $\mathfrak{p} = \mathrm{An}(m)$ y sean $a, b \in A$ tales que $ab \in \mathfrak{p}$, $b \notin \mathfrak{p}$. Entonces $bm \neq 0$ y $\mathfrak{p} \subset \mathrm{An}(bm)$. Por la maximalidad de $\mathfrak{p}$ ha de ser $\mathfrak{p} = \mathrm{An}(bm)$. Como $abm = 0$, ha de ser $a \in \mathfrak{p}$. ■

Enseguida veremos que el teorema siguiente es una generalización de 3.43 (para anillos noetherianos):

Teorema 3.49 *Si A es un anillo noetheriano y M es un A-módulo, entonces*

$$\bigcup_{\mathfrak{p} \in \mathrm{As}(M)} \mathfrak{p}$$

es el conjunto de los divisores de cero de M (es decir, de los elementos de A anulan a algún elemento no nulo de M).

Demostración: Es obvio que los elementos de la unión son divisores de cero de M. Recíprocamente, si $am = 0$ para cierto $a \in A$ y cierto $m \in M$, $m \neq 0$, entonces $\mathrm{As}(\langle m \rangle) \neq \varnothing$ por el teorema anterior, luego existe un $\mathfrak{p} \in \mathrm{Esp}\, A$ y un $b \in A$ de modo que $\mathfrak{p} = \mathrm{An}(bm)$. Como $abm = 0$, concluimos que $a \in \mathfrak{p}$. ■

En particular, los primos de $\mathrm{As}(A)$ están formados por todos los divisores de cero de A. Teniendo en cuenta el teorema 3.43, es natural conjeturar que los primos minimales de A deben ser asociados. Esto es cierto, pero para demostrarlo necesitamos estudiar los primos asociados de un anillo de cocientes:

Teorema 3.50 *Si A es un anillo noetheriano, M es un A-módulo no nulo y $S \subset A$ es un subconjunto multiplicativo, entonces los primos asociados de $S^{-1}M$ son los de la forma $S^{-1}\mathfrak{p}$, donde $\mathfrak{p}$ es un primo asociado de M tal que $\mathfrak{p} \cap S = \varnothing$.*

Demostración: Si $\mathfrak{p}$ es un primo asociado de M disjunto con S, entonces $\mathfrak{p} = \mathrm{An}(m)$, para un cierto $m \in M$, y es fácil ver entonces que $S^{-1}\mathfrak{p} = \mathrm{An}(m/1)$. Recíprocamente, todo primo de $S^{-1}A$ es de la forma $S^{-1}\mathfrak{p}$, donde $\mathfrak{p}$ es un primo de A disjunto con S. Si $S^{-1}\mathfrak{p} = \mathrm{An}(m/s) = \mathrm{An}(m/1)$, entonces, para cada $a \in \mathfrak{p}$ existe un $s \in S$ tal que $asm = 0$. Aplicando esto a un generador finito de $\mathfrak{p}$ y multiplicando los s correspondientes, obtenemos un mismo $s \in S$ que cumple esto para todo $a \in \mathfrak{p}$. Por otra parte, si $asm = 0$ entonces $am/1 = 0$, luego $a/1 \in S^{-1}\mathfrak{p}$, luego $a \in \mathfrak{p}$. Esto prueba que $\mathfrak{p} = \mathrm{An}(sm)$, luego $\mathfrak{p}$ es un primo asociado de A. ■

Teorema 3.51 *Sea I un ideal de un anillo A y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos. Si I está contenido en la unión de los $\mathfrak{p}_i$, entonces está contenido en uno de ellos.*

Demostración: Por inducción sobre n. Para $n = 1$ es trivial. Si $n > 1$ podemos suponer que I no está contenido en la unión de $n-1$ de los ideales (o aplicaríamos la hipótesis de inducción), luego existe $f_i \in I \setminus \bigcup\limits_{j\neq i} \mathfrak{p}_j$. Como I está contenido en la unión de todos los primos, de hecho $f_i \in I \cap \mathfrak{p}_i$. Tomamos $g_j = \prod\limits_{i\neq j} f_i$ y $f = \sum\limits_j g_j$. Así $g_j \in I \cap \mathfrak{p}_i$ para $i \neq j$, pero $g_j \notin \mathfrak{p}_j$. Es claro que f está en I pero no en la unión. ■

Ahora ya podemos probar la relación entre primos minimales y asociados:

Teorema 3.52 *En un anillo noetheriano todos los primos minimales son asociados y, si el anillo es reducido, todo primo asociado es minimal.*

Demostración: Sea A un anillo noetheriano. Por el teorema anterior, un primo $\mathfrak{p}$ es asociado de A si y sólo si es asociado de $A_\mathfrak{p}$. Si $\mathfrak{p}$ es minimal, entonces $A_\mathfrak{p}$ no tiene más primo que $\mathfrak{p}$, y ha de tener algún primo asociado, luego $\mathfrak{p}$ es asociado de $A_\mathfrak{p}$ y de A.

Si A es reducido y $\mathfrak{p}$ es un primo asociado, los teoremas 3.43, 3.49 y 3.51 implican que $\mathfrak{p}$ está contenido en un primo minimal de A, pero, precisamente por ser minimal, se ha de dar la igualdad. ■

Ejercicio: Probar que en el anillo $A = k[X, Y]/(X^2, XY)$, el primo (x, y) es asociado y no minimal.

Los primos minimales de un anillo noetheriano son un número finito. Vamos a demostrar que lo mismo sucede con los primos asociados. Para ello probamos primero lo siguiente:

Teorema 3.53 *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Entonces existe una cadena de submódulos*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

de modo que $M_i/M_{i-1} \cong A/\mathfrak{p}_i$, con $\mathfrak{p}_i \in \operatorname{Esp} A$, para $i = 1, \ldots, n$.

Demostración: Podemos suponer que $M \neq 0$. El conjunto S de los submódulos no nulos de M para los que se cumple el teorema es no vacío, pues si $\mathfrak{p} \in \mathrm{As}(M)$, entonces M contiene un submódulo $N \cong A/\mathfrak{p}$. Como A es noetheriano, podemos tomar un módulo $N \in S$ maximal. Vamos a probar que $M = N$. En caso contrario M/N contiene un submódulo no nulo isomorfo a $A/\mathfrak{q}$, para cierto $\mathfrak{q} \in \operatorname{Esp} A$. Dicho submódulo será de la forma N'/N, pero entonces $N' \in S$ contradice la maximalidad de N. ■

Teorema 3.54 *Si A es un anillo noetheriano y M es un A-módulo finitamente generado, entonces* $\mathrm{As}(M)$ *es finito.*

DEMOSTRACIÓN: Consideremos una sucesión de submódulos en las condiciones del teorema anterior. Si $\mathfrak{p} \in \mathrm{As}(M)$, entonces el teorema 3.47 nos da que $\mathfrak{p} \in \mathrm{As}(M_1) = \mathrm{As}(M_1/M_0)$ o bien $\mathfrak{p} \in \mathrm{As}(M/M_1)$. En el segundo caso, o bien $\mathfrak{p} \in \mathrm{As}(M_2/M_1)$ o bien $\mathfrak{p} \in \mathrm{As}(M/M_2)$. En definitiva, llegamos a que $\mathfrak{p} \in \mathrm{As}(M_i/M_{i-1}) \cong \mathrm{As}(A/\mathfrak{p}_i)$, para cierto $i > 0$, luego por 3.46 concluimos que $\mathfrak{p} = \mathfrak{p}_i$. Así pues, hay un número finito de primos asociados a M. ■

La consecuencia siguiente resulta útil a menudo:

Teorema 3.55 *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Sea I un ideal de A que conste únicamente de divisores de cero de M. Entonces existe un $m \in M$ no nulo tal que $Im = 0$.*

DEMOSTRACIÓN: Por el teorema 3.49, el ideal I está contenido en la unión de los primos asociados a M, que son un número finito, luego por 3.51 está contenido en uno de ellos. Pongamos que $I \subset \mathrm{An}(m)$, con $m \neq 0$. Entonces $Im = 0$. ■

3.6 Extensiones enteras

En esta sección desarrollamos los preliminares necesarios para estudiar la dimensión de un conjunto algebraico y su generalización a anillos arbitrarios, de lo que nos ocuparemos en la sección siguiente.

Definición 3.56 Diremos que B/A es una *extensión de anillos* si A es un subanillo de B (con la misma unidad). Un $x \in B$ es *entero* sobre A si es raíz de un polinomio mónico con coeficientes en A. Más en general, si I es un ideal de A, diremos que x es *entero* sobre I si es raíz de un polinomio mónico cuyos coeficientes distintos del director están en I. La extensión B/A es *entera* si todo elemento de B es entero sobre A.

En lo sucesivo, cuando hablemos de los coeficientes de un polinomio mónico exceptuaremos tácitamente al coeficiente director siempre que sea necesario. Así, por ejemplo, diremos que un elemento es entero sobre un ideal I si es raíz de un polinomio mónico con coeficientes en I.

Si B/A es una extensión de anillos e I es un ideal de A, representaremos por IB al ideal generado por I en B, que está formado por las combinaciones lineales de elementos de I con coeficientes en B.

Teorema 3.57 *Sea B/A una extensión de anillos e I un ideal de A (admitimos el caso $I = A$). Para cada $x \in B$, las afirmaciones siguientes son equivalentes:*

a) x es entero sobre I.

b) $A[x]$ es un A-módulo finitamente generado y $x \in \operatorname{rad} IA[x]$.

c) Existe un subanillo B' de B tal que $A[x] \subset B'$ de modo que B' es un A-módulo finitamente generado y $x \in \operatorname{rad} IB'$.

DEMOSTRACIÓN: a) $\Rightarrow$ b) Si $F(X) \in A[X]$ es un polinomio mónico con coeficientes en I tal que $F(x) = 0$, cada elemento de $A[x]$ es de la forma $G(x)$, para cierto polinomio $G(X) \in A[X]$. Dividiendo $G(X) = F(X)C(X) + R(X)$, donde $\operatorname{grad} R(X) < \operatorname{grad} F(X)$, vemos que $G(x) = R(x)$, luego $A[x]$ está generado por las potencias de x de orden menor que $\operatorname{grad} F(X)$.

Además, si dicho grado es n, la ecuación $F(x) = 0$ implica que $x^n \in IA[x]$ (el ideal generado por I en $A[x]$), luego $x \in \operatorname{rad} IA[x]$.

b) $\Rightarrow$ c) Basta tomar $B' = A[x]$.

c) $\Rightarrow$ a) Sea $B' = \langle w_1, \ldots, w_n \rangle_A$ y $x^m \in IB'$. Entonces

$$x^m w_i = \sum_{j=1}^{n} a_{ij} w_j, \qquad \text{con } a_{ij} \in I,$$

luego

$$\sum_{j=1}^{n} (x^m \delta_{ij} - a_{ij}) w_j = 0, \qquad j = 1, \ldots, n.$$

Multiplicando por la matriz adjunta de $(x^m \delta_{ij} - a_{ij})$ obtenemos que

$$\det(x^m \delta_{ij} - a_{ij}) w_j = 0, \qquad j = 1, \ldots, n.$$

Por otra parte, 1 es combinación lineal de los w_j, de donde concluimos que $\det(x^m \delta_{ij} - a_{ij}) = 0$. Al desarrollar el determinante tenemos que x es raíz de un polinomio mónico con coeficientes en I de grado mn. ■

Como caso particular tenemos:

Teorema 3.58 *Sea B/A una extensión de anillos tal que B sea un A-módulo finitamente generado. Entonces la extensión es entera y un $x \in B$ es entero sobre un ideal I de A si y sólo si $x \in \operatorname{rad} IB$.*

Veamos algunas consecuencias de estos teoremas. Ante todo observemos que una simple inducción justifica que si adjuntamos a un anillo A un número finito de enteros obtenemos un A-módulo finitamente generado.

Teorema 3.59 *Si C/B y B/A son extensiones enteras de anillos, entonces la extensión C/A también es entera.*

DEMOSTRACIÓN: Si $x \in C$ satisface una ecuación

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0, \qquad b_i \in B,$$

es claro que $A[b_0, \ldots, b_{n-1}]$ es un A-módulo finitamente generado y b es entero sobre este anillo, luego $A[b_0, \ldots, b_{n-1}, x]$ es un A-módulo finitamente generado. El teorema 3.57 nos da entonces que x es entero sobre A. ■

Teorema 3.60 *Si B/A es una extensión de anillos, el conjunto B' de los elementos de B enteros sobre A es un anillo intermedio. Si I es un ideal de A, entonces* $\operatorname{rad} IB'$ *es el conjunto de los elementos de B enteros sobre I.*

DEMOSTRACIÓN: Si $x, y \in B'$, entonces $A[x, y]$ es un A-módulo finitamente generado, y por 3.57, $x + y$, $x - y$, $xy \in B'$.

Si $x \in B$ es entero sobre I, entonces $x \in \operatorname{rad} IA[x] \subset \operatorname{rad} IB'$. Recíprocamente, si $x \in \operatorname{rad} IB'$, entonces $x^m \in IA[x_1, \ldots, x_m]$, para ciertos $x_1, \ldots, x_n \in B'$. Como $A[x_1, \ldots, x_n]$ es un A-módulo finitamente generado, concluimos que x es entero sobre I. ■

Teorema 3.61 *Sea D un dominio íntegro con cuerpo de cocientes K y sea L un cuerpo que extienda a K. Supongamos que D es íntegramente cerrado (es decir, que todo elemento de K entero sobre D está en D). Entonces un elemento de L es entero sobre un ideal primo I de D (o bien sobre D) si y sólo si es algebraico sobre K y su polinomio mínimo tiene sus coeficientes en I (en D).*

DEMOSTRACIÓN: Una implicación es obvia. Si $x \in L$ es entero sobre I, es evidente que sus K-conjugados también son enteros sobre I. Sea B la adjunción a A de estos conjugados. El teorema 3.58 nos da que los elementos de B enteros sobre I forman un ideal, luego los coeficientes del polinomio mínimo de x son todos enteros sobre I (pues son polinomios simétricos elementales en los conjugados de x). En particular, dichos coeficientes son enteros sobre D y están en K, luego por hipótesis están en D. Ahora aplicamos nuevamente 3.58 con $B = B' = A$, para concluir que dichos coeficientes están en $\operatorname{rad} I = I$. ■

El interés de las extensiones enteras de anillos B/A se debe a que existen relaciones notables entre los ideales primos de A y los de B. Para una extensión arbitraria, podemos definir $\phi : \operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ mediante $\phi(\mathfrak{P}) = \mathfrak{P} \cap A$. Si $\mathfrak{p} = \mathfrak{P} \cap A$, diremos que $\mathfrak{P}$ está situado sobre $\mathfrak{p}$. Obviamente se trata de una aplicación continua. Si la extensión B/A es entera podemos decir mucho más, pero antes de entrar en ello conviene aislar un argumento (debido a Krull) que usaremos en otras ocasiones:

Teorema 3.62 *Sea A un anillo, I un ideal de A y sea $S \neq \varnothing$ un subconjunto de A cerrado para productos tal que $I \cap S = \varnothing$. Entonces existe un ideal primo $\mathfrak{p}$ de A tal que $I \subset \mathfrak{p}$, $\mathfrak{p} \cap S = \varnothing$ y $\mathfrak{p}$ es maximal para la inclusión respecto a los ideales de A que cumplen estas propiedades.*

DEMOSTRACIÓN: Por el lema de Zorn, existe un ideal $\mathfrak{p}$ que cumple las propiedades indicadas y que es maximal respecto de la inclusión. Sólo hay que probar que $\mathfrak{p}$ es primo. Notemos que $\mathfrak{p} \neq A$ porque $S \neq \varnothing$.

Si existen a_1, $a_2 \in A \setminus \mathfrak{p}$ tales que $a_1 a_2 \in \mathfrak{p}$, la maximalidad de $\mathfrak{p}$ implica que $(Aa_i + \mathfrak{p}) \cap S \neq \varnothing$, luego existen $a_i' \in A$, $p_i \in \mathfrak{p}$ tales que $a_i' a_i + p_i \in S$. Entonces

$$(a_1' a_1 + p_1)(a_2' a_2 + p_2) = a_1' a_2' a_1 a_2 + a_1' a_1 p_2 + a_2' a_2 p_1 + p_1 p_2 \in \mathfrak{p} \cap S = \varnothing,$$

contradicción. ■

Teorema 3.63 *Sea B/A una extensión entera de anillos. Entonces*

a) La aplicación $\phi : \operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ es cerrada y suprayectiva.

b) Si dos ideales $\mathfrak{P}_1$, $\mathfrak{P}_2 \in \operatorname{Esp} B$ cumplen $\mathfrak{P}_1 \subset \mathfrak{P}_2$, $\phi(\mathfrak{P}_1) = \phi(\mathfrak{P}_2)$, entonces $\mathfrak{P}_1 = \mathfrak{P}_2$.

c) Si $\mathfrak{P} \in \operatorname{Esp} B$, se cumple que $\mathfrak{P}$ es maximal si y sólo si $\phi(\mathfrak{P})$ es maximal.

DEMOSTRACIÓN: a) Sea $\mathfrak{p} \in \operatorname{Esp} A$. Según 3.60, todo $x \in \mathfrak{p}B$ es entero sobre $\mathfrak{p}$. Si además $x \in \mathfrak{p}B \cap A$, la ecuación de x nos da que $x^n \in \mathfrak{p}$, luego $x \in \mathfrak{p}$. Así pues, $\mathfrak{p}B \cap A = \mathfrak{p}$. Aplicamos el teorema anterior con $S = A \setminus \mathfrak{p}$, con lo que obtenemos un ideal primo $\mathfrak{P} \in \operatorname{Esp} B$ tal que $\mathfrak{p}B \subset \mathfrak{P}$, $\mathfrak{P} \cap A = \mathfrak{p}$. Así pues, $\phi(\mathfrak{P}) = \mathfrak{p}$ y ϕ es suprayectiva.

Para probar que ϕ es cerrada tomamos $C = V(J) \subset \operatorname{Esp} B$, donde J es un ideal de B. Sea $I = J \cap A$. Podemos considerar a A/I como subanillo de B/J, y es inmediato que forman una extensión entera (a partir de la propia definición). Tenemos el diagrama conmutativo

$$\begin{tikzcd}
\operatorname{Esp} B/J \arrow[r] \arrow[d, "\phi"'] & \operatorname{Esp} B \arrow[d, "\phi"] \\
\operatorname{Esp} A/I \arrow[r] & \operatorname{Esp} A
\end{tikzcd}$$

donde las flechas horizontales son las aplicaciones inducidas por los epimorfismos canónicos. Ahora bien, sabemos que las imágenes de estas aplicaciones son precisamente $V(J)$ y $V(I)$, lo que implica que $\phi[V(J)] = V(I)$.

b) Sea $\mathfrak{p} = \mathfrak{P}_1 \cap A = \mathfrak{P}_2 \cap A$. Tenemos que $B/\mathfrak{P}_1$ es un dominio íntegro y $\mathfrak{P}_2/\mathfrak{P}_1$ es un ideal. Todo $x \in \mathfrak{P}_2/\mathfrak{P}_1$ no nulo satisface una ecuación (de grado mínimo)

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \qquad a_i \in A/\mathfrak{p}.$$

Entonces $a_0 \neq 0$, o de lo contrario podríamos simplificar una x y reducir el grado de la ecuación. Vemos entonces que $a_0 \in (\mathfrak{P}_2/\mathfrak{P}_1) \cap (A/\mathfrak{p})$, es decir, que $a_0 = [t]$, con $t \in \mathfrak{P}_2 \cap A = \mathfrak{p}$, luego $a_0 = 0$, contradicción. Esto prueba que $\mathfrak{P}_2/\mathfrak{P}_1 = 0$, es decir, que $\mathfrak{P}_2 = \mathfrak{P}_1$.

c) Sea $\mathfrak{P} \in \operatorname{Esp} B$ y sea $\mathfrak{p} = \mathfrak{P} \cap A$. Si $\mathfrak{p}$ es maximal, también ha de serlo $\mathfrak{P}$ por el apartado anterior. Recíprocamente, si $\mathfrak{P}$ es maximal entonces $\operatorname{Esp} B/\mathfrak{P}$ tiene sólo un elemento y la aplicación $\phi : \operatorname{Esp} B/\mathfrak{P} \longrightarrow \operatorname{Esp} A/\mathfrak{p}$ ha de ser suprayectiva, por el apartado a), luego $\operatorname{Esp} A/\mathfrak{p}$ sólo puede tener un elemento, luego $\mathfrak{p}$ es maximal. ■

Como consecuencia inmediata:

Teorema 3.64 *Si B/A es una extensión entera de anillos y $\operatorname{Esp} B$ es noetheriano, entonces la aplicación $\phi : \operatorname{Esp} B \longrightarrow \operatorname{Esp} A$ es finita, es decir, cada ideal de $\operatorname{Esp} A$ tiene sólo un número finito de antiimágenes.*

Demostración: Si $\mathfrak{p} \in \operatorname{Esp} A$, tenemos que $\mathfrak{p}B \subset \mathfrak{P}$, para cierto $\mathfrak{P} \in \operatorname{Esp} B$ tal que $\mathfrak{P} \cap A = \mathfrak{p}$. Por lo tanto $\mathfrak{p}B \cap A = \mathfrak{p}$. El apartado b) del teorema anterior prueba que las antiimágenes de $\mathfrak{p}$ son los divisores primos minimales de $\mathfrak{p}B$, que son un número finito. ■

Con esto ya estamos en condiciones de demostrar los resultados fundamentales sobre extensiones enteras, los teoremas del ascenso y del descenso, pero los pospondremos hasta la sección siguiente, donde podremos comprender su interés.

3.7 La dimensión de Krull

Aunque hemos definido la dimensión de Krull de un espacio topológico, es poco lo que hemos podido decir sobre ella hasta ahora. Sin embargo, ahora ya estamos en condiciones de estudiar la dimensión de Krull del espectro de un anillo y, en particular, la de un conjunto algebraico. El punto de partida es el siguiente:

Definición 3.65 Llamaremos *dimensión de Krull* de un anillo A a la dimensión de su espectro: $\dim A = \dim \operatorname{Esp} A$. Equivalentemente, es el supremo de las longitudes n de las cadenas de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

Si C/k es un conjunto algebraico, sabemos que los cerrados de C se corresponden biunívocamente con los cerrados de $\operatorname{Esp} k[C]$ y claramente los cerrados irreducibles se corresponden con cerrados irreducibles (pues en ambos espacios se corresponden con los ideales primos de $k[C]$). Consecuentemente,

$$\dim C = \dim \operatorname{Esp} k[C] = \dim k[C].$$

Volviendo al caso de un anillo arbitrario A, vemos que $\dim A = 0$ significa que los ideales primos son maximales. En particular, si A es un dominio íntegro resulta que 0 es un ideal maximal, luego los dominios íntegros de dimensión 0 son los cuerpos.

Similarmente, un dominio íntegro A cumple $\dim A = 1$ si y sólo si no es un cuerpo y los ideales primos no nulos son maximales. Por ejemplo, los dominios de ideales principales tienen dimensión 1.

Si $\mathfrak{p} \in \operatorname{Esp} A$, llamaremos *altura* de $\mathfrak{p}$, y la representaremos por $\operatorname{alt} \mathfrak{p}$, al supremo de las longitudes n de las cadenas de ideales primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

con $\mathfrak{p}_n = \mathfrak{p}$. La *dimensión* de $\mathfrak{p}$ se define como $\dim \mathfrak{p} = \dim A/\mathfrak{p}$. (Por supuesto, tanto la dimensión como la altura de un primo pueden ser infinitas.) Es claro que

$$\dim \mathfrak{p} = \dim V(\mathfrak{p}), \qquad \operatorname{alt} \mathfrak{p} = \operatorname{codim}_{\operatorname{Esp} A} V(\mathfrak{p}).$$

Los teoremas siguientes son consecuencias sencillas del teorema 3.63:

Teorema 3.66 *Sea B/A una extensión entera de anillos. Si $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_n$ es una cadena de ideales primos en B y $\mathfrak{p}_i = \mathfrak{P}_i \cap A$, entonces $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ es una cadena de ideales primos en A.*

Teorema 3.67 (Teorema del ascenso) *Sea B/A una extensión entera de anillos. Para cada cadena de ideales primos $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ en A y cada primo $\mathfrak{P}_0$ de B situado sobre $\mathfrak{p}_0$ existe una cadena de ideales primos $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_n$ en B tal que $\mathfrak{P}_i \cap A = \mathfrak{p}_i$.*

DEMOSTRACIÓN: Supongamos construido $\mathfrak{P}_i$. Entonces $B/\mathfrak{P}_i$ es una extensión entera de $A/\mathfrak{p}_i$. Por el teorema 3.63 existe un primo $\mathfrak{P}_{i+1}/\mathfrak{P}_i$ en $B/\mathfrak{P}_i$ situado sobre $\mathfrak{p}_{i+1}/\mathfrak{p}_i$, de donde se sigue que $\mathfrak{P}_{i+1}$ está situado sobre $\mathfrak{p}_{i+1}$. ■

Como consecuencia inmediata:

Teorema 3.68 *Si B/A es una extensión entera de anillos, entonces se cumple que $\dim B = \dim A$ y, para cada $\mathfrak{P} \in \operatorname{Esp} B$,*

$$\operatorname{alt} \mathfrak{P} \leq \operatorname{alt}(\mathfrak{P} \cap A), \qquad \dim \mathfrak{P} = \dim(\mathfrak{P} \cap A).$$

Con hipótesis adicionales la desigualdad sobre las alturas puede convertirse en una igualdad:

Teorema 3.69 (Teorema del descenso) *Sea B/A una extensión entera de dominios íntegros y supongamos que A es íntegramente cerrado. Si $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ son ideales primos de A y $\mathfrak{P}_1$ es un ideal primo de B situado sobre $\mathfrak{p}_1$, entonces existe $\mathfrak{P}_0 \in \operatorname{Esp} B$ situado sobre $\mathfrak{p}_0$ tal que $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1$.*

DEMOSTRACIÓN: Llamemos $S_0 = A \setminus \mathfrak{p}_0$, $S_1 = B \setminus \mathfrak{P}_1$ y

$$S = S_0 S_1 = \{ab \mid a \in S_0,\ b \in N_1\}.$$

Claramente $S \subset B$ es cerrado para productos y $S_0 \cup S_1 \subset S$. Vamos a ver que $\mathfrak{p}_0 B \cap S = \varnothing$, con lo que podremos aplicar el teorema 3.62, que nos da un primo $\mathfrak{P}_0 \in \operatorname{Esp} B$ tal que $\mathfrak{p}_0 B \subset \mathfrak{P}_0$ y $\mathfrak{P}_0 \cap S = \varnothing$. En particular tenemos que $\mathfrak{P}_0 \cap S_1 = \varnothing$, lo que se traduce en que $\mathfrak{P}_0 \subset \mathfrak{P}_1$ y, como $\mathfrak{P}_0 \cap S_0 = \varnothing$, ha de ser $\mathfrak{P}_0 \cap A = \mathfrak{p}_0$.

Supongamos que existe $x \in \mathfrak{p}_0 B \cap S$. Por hipótesis x es entero sobre A y por el teorema 3.60 tenemos que, de hecho, es entero sobre $\mathfrak{p}_0$. Por el teorema 3.61 vemos que el polinomio mínimo de x sobre el cuerpo de cocientes k de A tiene sus coeficientes en $\mathfrak{p}_0$. Digamos que es

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0, \qquad a_i \in \mathfrak{p}_0.$$

Como $x \in S$, ha de ser $x = ab$, con $a \in N_0$, $b \in N_1$. El polinomio mínimo de $b = x/a$ es

$$X^n + (a_{n-1}/a)X^{n-1} + \cdots + a_0/a^n,$$

que tiene sus coeficientes en A porque b es entero sobre A. Si llamamos a_i' a estos coeficientes, tenemos que $a_i = a_i' a^{n-i} \in \mathfrak{p}_0$, pero $a \notin \mathfrak{p}_0$, luego $a_i' \in \mathfrak{p}_0$ y, por consiguiente, b es entero sobre $\mathfrak{p}_0$. Por 3.60 tenemos que $b \in \operatorname{rad} \mathfrak{p}_0 B \subset \mathfrak{P}_1$, en contradicción con que $b \in S_1$. ■

Aunque hemos enunciado el teorema del descenso para cadenas de dos primos, es obvio que vale para cadenas de longitud arbitraria, de forma análoga al teorema del ascenso. Como consecuencia inmediata tenemos:

Teorema 3.70 *Sea B/A una extensión entera de dominios íntegros y supongamos que A es íntegramente cerrado. Entonces para cada $\mathfrak{P} \in \operatorname{Esp} B$ se cumple $\operatorname{alt} \mathfrak{P} = \operatorname{alt}(\mathfrak{P} \cap A)$.*

En general un anillo noetheriano puede tener dimensión infinita, pero vamos a ver que no sucede así con las álgebras afines, en particular con los anillos $k[C]$, donde C/k es un conjunto algebraico. Empezamos por un resultado auxiliar:

Teorema 3.71 *Sea F un polinomio no constante en $k[X_1, \ldots, X_n]$. Mediante una sustitución de la forma $X_i = Y_i + X_n^{r_i}$, para ciertos $r_i \in \mathbb{N}$, $i = 1, \ldots, n-1$, el polinomio F puede transformarse en un polinomio de la forma*

$$aX_n^m + G_1 X_n^{m-1} + \cdots + G_m, \qquad a \in k^*,\ G_i \in k[Y_1, \ldots, Y_{n-1}],\ m > 0.$$

Si k es infinito podemos conseguir el mismo resultado con una sustitución de la forma $X_i = Y_i + a_i X_n$, con $a_i \in k$.

Demostración: Sea

$$F = \sum a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

Con una transformación del tipo indicado obtenemos

$$\begin{aligned} &\sum a_{i_1,\ldots,i_n} (X_n^{r_1} + Y_1)^{i_1} \cdots (X_n^{r_{n-1}} + Y_{n-1})^{i_{n-1}} X_n^{i_n} \\ &\quad = \sum a_{i_1,\ldots,i_n} (X_n^{i_1 r_1 + \cdots + i_{n-1} r_{n-1} + i_n} + \cdots), \end{aligned}$$

donde los últimos puntos suspensivos representan monomios de menor grado en X_n. Sea $k \in \mathbb{N}$ mayor que todos los índices i_j que aparecen en los coeficientes $a_{i_1,\ldots,i_n}$ no nulos.

Si elegimos $r_i = k^i$ vemos que los exponentes $i_n + i_1 k + \cdots + i_{n-1} k^{n-1}$ correspondientes a coeficientes $a_{i_1,\ldots,i_n} \neq 0$ son distintos dos a dos. Si llamamos m al mayor de estos exponentes, el polinomio tiene la forma indicada.

Si k es infinito sea $F = F_0 + F_1 + \cdots + F_m$ la descomposición de F en polinomios homogéneos. La sustitución nos lleva a

$$F_m(-a_1, \ldots, -a_{n-1}, 1) X_n^m + \cdots$$

donde de nuevo los términos omitidos tienen grado menor en X_n. Basta tomar los a_i de modo que $F_m(-a_1, \ldots, -a_{n-1}, 1) \neq 0$, lo cual es posible porque k es infinito. En efecto, hay que probar que un polinomio no nulo de $n-1$ variables no puede anularse en todo k^{n-1}. Ahora bien, expresándolo en la forma

$$G_s(X_1, \ldots, X_{n-2}) X_{n-1}^s + \cdots + G_1(X_1, \ldots, X_{n-2}) X_{n-1} + G_0(X_1, \ldots, X_{n-2})$$

y razonando por inducción obtenemos $(a_1, \ldots, a_{n-2}) \in k^{n-2}$ de manera que $G_s(a_1, \ldots, a_{n-2}) \neq 0$, con lo que el polinomio

$$G_s(a_1, \ldots, a_{n-2})X_{n-1}^s + \cdots + G_1(a_1, \ldots, a_{n-2})X_{n-1} + G_0(a_1, \ldots, a_{n-2})$$

es no nulo y la infinitud de k nos da un a_{n-1} que no lo anula. ■

Los resultados que buscamos sobre álgebras afines son consecuencias del teorema siguiente:

Teorema 3.72 (Teorema de normalización de Noether) *Sea A una k-álgebra afín e $I \neq A$ un ideal. Entonces existen números naturales $d' \leq d$ y elementos $y_1, \ldots, y_d \in A$ tales que*

a) $y_1, \ldots, y_d$ *son algebraicamente independientes sobre* k*,*

b) A *es un* $k[y_1, \ldots, y_d]$*-módulo finitamente generado,*

c) $I \cap k[y_1, \ldots, y_d] = (y_{d'+1}, \ldots, y_d)$*.*

Si k es infinito y $A = k[x_1, \ldots, x_n]$ podemos exigir que

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \qquad a_{ij} \in k, \quad i = 1, \ldots, d'.$$

Demostración: Supongamos en primer lugar que $A = k[X_1, \ldots, X_n]$ es un anillo de polinomios y que $I = (F)$ es un ideal principal (con F no constante). Definimos $y_n = F$ y elegimos $y_1, \ldots, y_{n-1}$ según el teorema anterior. (Si k es infinito podemos suponer que $y_1, \ldots, y_{n-1}$ son combinaciones lineales de las indeterminadas.) Entonces $A = k[y_1, \ldots, y_n][X_n]$ y

$$0 = F - y_n = aX_n^m + G_1X_n^{m-1} + \cdots + G_m - y_n,$$

luego X_n es raíz de un polinomio (que podemos hacer mónico) con coeficientes en $k[y_1, \ldots, y_n]$. Esto significa que X_n es entero sobre este anillo, luego A es un $k[y_1, \ldots, y_n]$-módulo finitamente generado.

Los polinomios $y_1, \ldots, y_n$ son algebraicamente independientes sobre k, pues en caso contrario el cuerpo $k(y_1, \ldots, y_n)$ tendría grado de trascendencia $< n$ sobre k, y lo mismo le sucedería a $k(y_1, \ldots, y_n, X_n) = k(X_1, \ldots, X_n)$, ya que X_n es algebraico sobre $k(y_1, \ldots, y_n)$.

Falta probar que $k[y_1, \ldots, y_n] \cap (y_n) = (y_n)$. Aquí hay que entender que (y_n) es a la izquierda el ideal generado en A, mientras que a la derecha es el ideal generado en $k[y_1, \ldots, y_n]$. Una inclusión es obvia. Si G está en la intersección, entonces $G = Hy_n$, con $H \in A$. Del hecho de que A sea un $k[y_1, \ldots, y_n]$-módulo finitamente generado se sigue que H es entero sobre $k[y_1, \ldots, y_n]$, es decir, que cumple

$$H^m + H_1H^{m-1} + \cdots + H_m = 0, \qquad H_i \in k[y_1, \ldots, y_n].$$

Multiplicando por y_n^m obtenemos la relación

$$G^m + H_1 y_n G^{m-1} + \cdots + y_n^m H_m = 0,$$

de donde resulta que y_n divide a G^m en $k[y_1, \ldots, y_n]$. Como es primo, de hecho $y_n \mid G$, como había que probar.

Sigamos suponiendo que $A = k[X_1, \ldots, X_n]$ es un anillo de polinomios pero sea ahora I un ideal arbitrario. Razonamos por inducción sobre n. Si $n = 1$ el ideal I es principal y estamos en el caso anterior. Si $I = 0$ no hay nada que demostrar. Supongamos, pues, que existe un polinomio no constante $F \in I$. Consideramos $k[y_1, \ldots, y_n]$ con $y_n = F$ como en el caso anterior. Por hipótesis de inducción, el teorema se cumple para el anillo de polinomios $k[y_1, \ldots, y_{n-1}]$ y el ideal $I \cap k[y_1, \ldots, y_{n-1}]$. Esto significa que existen $t_1, \ldots, t_{d-1} \in k[y_1, \ldots, y_{n-1}]$ algebraicamente independientes sobre k tales que $k[y_1, \ldots, y_{n-1}]$ es finitamente generado como $k[t_1, \ldots, t_{d-1}]$-módulo y además $I \cap k[y_1, \ldots, y_{n-1}] = (t_{d'+1}, \ldots, t_{d-1})$.

Obviamente $k[y_1, \ldots, y_n]$ es un $k[t_1, \ldots, t_{d-1}, y_n]$-módulo finitamente generado y por construcción A es un $k[y_1, \ldots, y_n]$-módulo finitamente generado, de donde podemos concluir que A es finitamente generado como $k[t_1, \ldots, t_{d-1}, y_n]$-módulo.

Esto implica que los elementos de A son algebraicos sobre $k(t_1, \ldots, t_{d-1}, y_n)$, y lo mismo vale para los elementos del cuerpo de cocientes $k(X_1, \ldots, X_n)$. Considerando los grados de trascendencia podemos concluir que $d = n$ y que, llamando $t_n = y_n$, los elementos $t_1, \ldots, t_n$ son algebraicamente independientes sobre k. Si k es infinito podemos suponer además que $t_1, \ldots, t_{d'}$ son combinaciones lineales de los y_i y éstos a su vez lo son de los X_i.

Todo $f \in I \cap k[t_1, \ldots, t_n]$ puede escribirse como $f = f' + ht_n$, para un cierto $f' \in I \cap k[t_1, \ldots, t_{n-1}] = (t_{d'+1}, \ldots, t_{n-1})$, $h \in k[t_1, \ldots, t_n]$. (Notemos que $t_n = y_n = F \in I$.) Por consiguiente $I \cap k[t_1, \ldots, t_n] = (t_{d'+1}, \ldots, t_n)$.

El el caso general, la k-álgebra A puede representarse en la forma

$$A = k[X_1, \ldots, X_n]/J,$$

para cierto ideal J. El caso anterior nos da una subálgebra $k[y_1, \ldots, y_n]$ de $k[X_1, \ldots, X_n]$tal que $J \cap k[y_1, \ldots, y_n] = (y_{d+1}, \ldots, y_n)$, donde los $y_1, \ldots, y_d$ son combinaciones lineales de $X_1, \ldots, X_n$ si k es infinito.

La imagen de $k[y_1, \ldots, y_n]$ en A puede identificarse con el álgebra de polinomios $k[y_1, \ldots, y_d]$. Por consiguiente, podemos ver a A como un módulo finitamente generado sobre este anillo. Ahora aplicamos de nuevo el caso anterior al ideal $I' = I \cap k[y_1, \ldots, y_d]$, lo que nos da una subálgebra $k[t_1, \ldots, t_d]$ de $k[y_1, \ldots, y_d]$ sobre la que $k[y_1, \ldots, y_d]$ es finitamente generado como módulo y tal que $I' \cap k[t_1, \ldots, t_d] = (t_{d'+1}, \ldots, t_d)$. Además si k es infinito $t_1, \ldots, t_{d'}$ son combinaciones lineales de $y_1, \ldots, y_d$, luego de los generadores $x_1, \ldots, x_n$ de A. Evidentemente $I \cap k[t_1, \ldots, t_d] = (t_{d'+1}, \ldots, t_d)$ y, como A es un $k[y_1, \ldots, y_d]$-módulo finitamente generado y $k[y_1, \ldots, y_d]$ es un $k[t_1, \ldots, t_d]$-módulo finitamente generado, concluimos que A es también un $k[t_1, \ldots, t_d]$-módulo finitamente generado. ■

Definición 3.73 Si A es una k-álgebra afín, una *normalización de Noether* de A es una subálgebra $k[y_1,\ldots,y_d]$ de A tal que $y_1,\ldots,y_d$ son algebraicamente independientes sobre k y A es un $k[y_1,\ldots,y_d]$-módulo finitamente generado.

Hemos demostrado que toda k-álgebra afín admite una normalización de Noether. De aquí se desprende que la dimensión es finita:

Teorema 3.74 *Sea A una k-álgebra afín y sea $k[y_1,\ldots,y_d]$ una normalización de Noether. Entonces* $\dim A = d$. *Si A es un dominio íntegro, toda cadena de ideales primos en A puede extenderse hasta una cadena de longitud d.*

DEMOSTRACIÓN: El hecho de que A es un $k[y_1,\ldots,y_d]$-módulo finitamente generado se traduce en que la extensión es entera y, por consiguiente, tenemos que $\dim A = \dim k[y_1,\ldots,y_d]$. Esta última álgebra es simplemente un anillo de polinomios con d indeterminadas. Obviamente

$$0 \subsetneq (y_1) \subsetneq (y_1,y_2) \cdots \subsetneq (y_1,\ldots,y_d)$$

es una cadena de ideales primos en $k[y_1,\ldots,y_d]$, luego la dimensión es $\geq d$. Consideremos ahora una cadena $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_m$ de ideales primos de A. Definiendo $\mathfrak{p}_i = \mathfrak{P}_i \cap k[y_1,\ldots,y_d]$ tenemos una cadena $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ de ideales primos de $k[y_1,\ldots,y_d]$. Vamos a probar que $m \leq d$ por inducción sobre d. Si $d = 0$ simplemente $k[y_1,\ldots,y_d] = k$ y necesariamente $m = 0$. Supongamos $d > 0$. Entonces podemos suponer que $m > 0$.

Consideramos una normalización de Noether $k[t_1,\ldots,t_d] \subset k[y_1,\ldots,y_d]$ tal que $\mathfrak{p}_1 \cap k[t_1,\ldots,t_d] = (t_{d'+1},\ldots,t_d)$. Como $\mathfrak{p}_1 \neq 0$, ha de ser $d' < d$ (aquí usamos 3.63 b). Podemos considerar a $k[t_1,\ldots,t_{d'}]$ como una normalización de Noether de $k[y_1,\ldots,y_d]/\mathfrak{p}_1$. Aquí tenemos la cadena de primos

$$0 = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_1.$$

por hipótesis de inducción $m - 1 \leq d' < d$, luego $m \leq d$. Esto prueba que $\dim A = d$.

Supongamos ahora que A es un dominio íntegro. Dada una cadena de ideales primos en A, extendámosla hasta una cadena maximal $\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_m$. Sabemos que $m \leq d$ y hemos de probar la igualdad. En primer lugar demostramos que al tomar $\mathfrak{p}_i = \mathfrak{P}_i \cap k[y_1,\ldots,y_n]$ obtenemos una cadena maximal $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ de primos en $k[y_1,\ldots,y_d]$.

Supongamos que pudiéramos insertar un primo $\mathfrak{p}_i \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_{i+1}$. Tomemos una normalización de Noether $k[t_1,\ldots,t_d] \subset k[y_1,\ldots y_d]$ tal que

$$k[t_1,\ldots,t_d] \cap \mathfrak{p}_i = (t_{d'+1},\ldots,t_d).$$

Entonces $k[t_1,\ldots,t_{d'}]$ es una normalización de Noether de $k[y_1,\ldots,y_d]/\mathfrak{p}_i$. La cadena $0 \subsetneq \mathfrak{p}/\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}/\mathfrak{p}_i \subsetneq \cdots \subsetneq \mathfrak{p}_m/\mathfrak{p}_i$ se corresponde con una cadena en $k[t_1,\ldots,t_{d'}]$, pero esta álgebra es también una normalización de Noether de $A/\mathfrak{P}_i$. Además

$$(\mathfrak{p}_{i+1}/\mathfrak{p}_i) \cap k[t_1,\ldots,t_{d'}] = (\mathfrak{P}_{i+1}/\mathfrak{P}_i) \cap k[t_1,\ldots,t_{d'}].$$

Notemos que $k[t_1,\ldots,t_{d'}]$ es íntegramente cerrado porque tiene factorización única. Podemos aplicar el teorema del descenso, que nos da un ideal $\mathfrak{P}/\mathfrak{P}_i$ en $A/\mathfrak{P}$ tal que

$$\mathfrak{P}_i/\mathfrak{P}_i \subsetneq \mathfrak{P}/\mathfrak{P}_i \subsetneq \mathfrak{P}_{i+1}/\mathfrak{P}_i.$$

(La primera inclusión es estricta porque al cortar con $k[t_1,\ldots,t_{d'}]$ obtenemos una inclusión estricta.) En definitiva, tenemos un ideal $\mathfrak{P}_i \subsetneq \mathfrak{P} \subsetneq \mathfrak{P}_{i+1}$, en contradicción con la maximalidad de la cadena inicial.

Con esto hemos demostrado que la cadena $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ es maximal. Veamos que $m = d$ por inducción sobre d. Si $d = 0$ no hay nada que probar. Si $d > 0$ tomamos una normalización de Noether $k[t_1,\ldots,t_d] \subset k[y_1,\ldots,y_d]$ tal que $\mathfrak{p}_1 \cap k[t_1,\ldots,t_d] = (t_{d'+1},\ldots,t_d)$.

El ideal $\mathfrak{p}_1$ tiene altura 1, luego la intersección también por 3.70. Esto implica que $d' = d-1$. Por otra parte, si llamamos $\mathfrak{p}_i' = \mathfrak{p}_i \cap k[t_1,\ldots,t_d]$, hemos probado que $\mathfrak{p}_1' \subsetneq \cdots \subsetneq \mathfrak{p}_m'$ es una cadena maximal en $k[t_1,\ldots,t_d]$, luego

$$0 = \mathfrak{p}_1'/\mathfrak{p}_1' \subsetneq \mathfrak{p}_2'/\mathfrak{p}_1' \subsetneq \cdots \subsetneq \mathfrak{p}_m'/\mathfrak{p}_1'$$

es una cadena maximal en $k[t_1,\ldots,t_d]/\mathfrak{p}_1 = k[t_1,\ldots,t_{d-1}]$. Por hipótesis de inducción $m-1 = d-1$, luego $m = d$. ■

De aquí deducimos además una caracterización útil de la dimensión de una k-álgebra afín:

Teorema 3.75 *Sea A una k-álgebra afín y sean $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ sus primos minimales. Sea K_i el cuerpo de cocientes de $A/\mathfrak{p}_i$. Entonces $\dim A$ es el máximo de los grados de trascendencia de las extensiones K_i/k. Si todas ellas tienen el mismo grado de trascendencia, entonces, para todo $\mathfrak{p} \in \operatorname{Esp} A$, se cumple la relación*

$$\dim A = \operatorname{alt} \mathfrak{p} + \dim \mathfrak{p}.$$

DEMOSTRACIÓN: Toda cadena maximal de ideales primos de A empieza por uno de los $\mathfrak{p}_i$. Basta probar que la longitud de una cadena maximal que empiece por $\mathfrak{p}_i$ es precisamente el grado de trascendencia de la extensión K_i/k. Ahora bien, tales cadenas se corresponden con las cadenas maximales de ideales primos de $A/\mathfrak{p}_i$. Esto significa que podemos suponer que A es un dominio íntegro.

Sea, pues, A un dominio íntegro y K su cuerpo de cocientes. Tomemos una normalización de Noether $k[y_1,\ldots,y_d] \subset A$, de modo que $\dim A = d$. Ahora bien, tenemos que K es una extensión algebraica de $k[y_1,\ldots,y_d]$, luego el grado de trascendencia de K/k es precisamente d.

Para probar la segunda parte del teorema tomamos un $\mathfrak{p} \in \operatorname{Esp} A$ y formamos una cadena maximal de ideales primos de A que contenga a $\mathfrak{p}$. Por hipótesis su longitud ha de ser la dimensión de A. Ahora bien, la longitud de la cadena hasta $\mathfrak{p}$ ha de ser la altura de $\mathfrak{p}$ o, de lo contrario, podríamos conseguir una cadena de longitud mayor. Igualmente, la longitud de la cadena desde $\mathfrak{p}$ ha de ser la $\dim \mathfrak{p}$. Esto nos da la fórmula del enunciado. ■

Otra caracterización útil de la dimensión de una k-álgebra afín es la siguiente:

Teorema 3.76 *Si A es una k-álgebra afín, su dimensión es el máximo número de elementos de A algebraicamente independientes sobre k. Si $B \subset A$ es una subálgebra, entonces* $\dim B \leq \dim A$.

DEMOSTRACIÓN: La segunda afirmación se sigue inmediatamente de la primera. Sea $d = \dim A$. La existencia de normalizaciones de Noether implica que A contiene d elementos algebraicamente independientes sobre k. Basta probar que si $z_1, \ldots, z_m \in A$ son algebraicamente independientes sobre k, entonces $m \leq d$.

Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ los primos minimales de A. Como $k[z_1, \ldots, z_m]$ no tiene elementos nilpotentes no nulos, tenemos que

$$0 = k[z_1, \ldots, z_m] \cap \bigcap_{i=1}^{s} \mathfrak{p}_i = \bigcap_{i=1}^{s} (k[z_1, \ldots, z_m] \cap \mathfrak{p}_i).$$

Ha de existir un i tal que $k[z_1, \ldots, z_m] \cap \mathfrak{p}_i = 0$, pues, en caso contrario podríamos tomar un elemento no nulo en cada ideal y su producto sería un elemento no nulo de la intersección. Podemos considerar $k[z_1, \ldots, z_m] \subset A/\mathfrak{p}_i$, con lo que m es menor o igual que el grado de trascendencia del cuerpo de cocientes K de $A/\mathfrak{p}_i$, que a su vez es menor o igual que d. ■

Ejercicio: Demostrar que la dimensión de una variedad lineal (es decir, de un conjunto algebraico definido por un sistema de ecuaciones lineales) coincide con su dimensión en el sentido usual en álgebra lineal.

Veamos otras propiedades sobre la dimensión de las k-álgebras afines que a continuación traduciremos a propiedades sobre conjuntos algebraicos:

Teorema 3.77 *Sea k'/k una extensión de cuerpos y A una k-álgebra afín. Entonces* $\dim(k' \otimes_k A) = \dim A$. *Si A es un dominio íntegro y $\mathfrak{P}$ es un primo minimal de $k' \otimes_k A$, entonces* $\dim\big((k' \otimes_k A)/\mathfrak{P}\big) = \dim A$.

DEMOSTRACIÓN: Si $k[y_1, \ldots, y_d] \subset A$ es una normalización de Noether de A, entonces $k' \otimes_k k[y_1, \ldots, y_d]$ es una subálgebra de $k' \otimes_k A$ isomorfa a $k'[y_1, \ldots, y_d]$ y es claro que se trata de una normalización de Noether de $k' \otimes_k A$. Esto prueba la igualdad de las dimensiones.

Si A es un dominio íntegro podemos considerar su cuerpo de cocientes L. Tenemos los siguientes monomorfismos de anillos:

$$\begin{tikzcd} k' \otimes_k k(y_1, \ldots, y_d) \arrow[r] & k' \otimes_k L \\ k' \otimes_k k[y_1, \ldots, y_d] \arrow[r] \arrow[u] & k' \otimes_k A \arrow[u] \end{tikzcd}$$

Observemos que si B es una base de L sobre $k(y_1, \ldots, y_d)$ entonces $1 \otimes B$ es una base de $k' \otimes_k L$ sobre $k' \otimes_k k(y_1, \ldots, y_d)$. En efecto, pongamos que $B = (b_i)$ y sea (α_j) una k-base de k'. Entonces un elemento arbitrario de $k' \otimes_k k(y_1, \ldots, y_d)$ es de la forma

$$\sum_j \alpha_j \otimes f_j, \qquad \text{con } f_j \in k(y_1, \ldots, y_d),$$

luego una combinación lineal nula de $1 \otimes B$ es de la forma

$$\sum_i \big(\sum_j \alpha_j \otimes f_{ij}\big)(1 \otimes b_i) = 0,$$

lo que equivale a

$$\sum_j \alpha_j \otimes \big(\sum_i f_{ij} b_i\big) = 0,$$

de donde se sigue que los sumatorios en i son nulos y, por consiguiente, los f_{ij} también. Esto prueba que $1 \otimes B$ es linealmente independiente. La comprobación de que es un sistema generador es inmediata.

Esto implica en primer lugar que $k' \otimes_k k(y_1, \ldots, y_d)$ es un dominio íntegro, pues si tuviera elementos no nulos f y g tales que $fg = 0$, entonces, para cualquier $b \in B$, tendríamos que o bien $1 \otimes b$, o bien $f(1 \otimes b)$ sería un elemento de torsión no nulo. A su vez esto implica que ningún elemento de $k' \otimes_k k(y_1, \ldots, y_d)$ puede ser un divisor de cero en $k' \otimes_k L$.

Ahora podemos concluir que $\mathfrak{P} \cap k' \otimes_k k[y_1, \ldots, y_d] = 0$, pues por 3.43 sabemos que cualquier elemento no nulo en la intersección tendría que ser un divisor de cero en $k' \otimes_k A$, luego también en $k' \otimes_k L$. Esto nos permite sumergir

$$k'[y_1, \ldots, y_n] \subset (k' \otimes_k A)/\mathfrak{P},$$

y es fácil ver que se trata de una normalización de Noether, luego el cociente tiene también dimensión d. ■

Teorema 3.78 *Si A y A' son dos k-álgebras afines no nulas, entonces*

$$\dim(A \otimes_k A') = \dim A + \dim A'.$$

Si A y A' son dominios íntegros y $\mathfrak{P}$ es un primo minimal de $A \otimes_k A'$, entonces

$$\dim((A \otimes_k A')/\mathfrak{P}) = \dim A + \dim A'.$$

Demostración: Si $k[y_1, \ldots, y_d] \subset A$ y $k[z_1, \ldots, z_{d'}] \subset A'$ son normalizaciones de Noether, entonces

$$k[y_1, \ldots, y_d, z_1, \ldots, z_{d'}] \cong k[y_1, \ldots, y_d] \otimes_k k[z_1, \ldots, z_{d'}] \subset A \otimes_k A'$$

es una normalización de Noether del producto, luego la dimensión es $d + d'$.

Si A y A' son dominios íntegros y llamamos L y L' a sus cuerpos de cocientes, la segunda parte del teorema se demuestra de forma análoga al teorema anterior, considerando los monomorfismos de anillos siguientes:

$$\begin{tikzcd}
k(y_1, \ldots, y_d) \otimes_k k(z_1, \ldots, z_{d'}) \arrow[r] & L \otimes_k L' \\
k[y_1, \ldots, y_d] \otimes_k k[z_1, \ldots, z_{d'}] \arrow[r] \arrow[u] & A \otimes_k A' \arrow[u]
\end{tikzcd}$$

Ahora se cumple que si B y B' son bases de L y L' sobre $k(y_1,\ldots,y_d)$ y $k(z_1,\ldots,z_{d'})$ respectivamente, entonces $B\otimes B'$ es una base de $L\otimes_k L'$ sobre $k(y_1,\ldots,y_d)\otimes_k k(z_1,\ldots,z_{d'})$. Para probar esto tomamos bases C y C' de $k(y_1,\ldots,y_d)$ y $k(z_1,\ldots,z_{d'})$ sobre k, y usamos que CB y CB' son bases de L y L' sobre k, respectivamente. Una combinación lineal arbitraria de $B\otimes B'$ es de la forma

$$\sum_{i,j,u,v}\alpha_{ijuv}(c_u\otimes c'_v)(b_i\otimes b'_j)=\sum_{i,j,u,v}\alpha_{ijuv}(c_ub_i\otimes c'_vb'_j),$$

y será nula si y sólo si todos los $\alpha_{ijuv}\in k$ son nulos. El resto de la prueba es idéntico. ■

Ahora es fácil probar los resultados siguientes sobre conjuntos algebraicos afines:

Teorema 3.79 *Sea $C\subset A^n$ un conjunto algebraico afín no vacío definido sobre un cuerpo k.*

a) Si $k\subset k'\subset K$ es un cuerpo intermedio, entonces $\dim C/k=\dim C/k'$. *Además, si C/k es irreducible, todas las componentes irreducibles de C/k' tienen la misma dimensión.*

b) $\dim C\leq n$ *y la igualdad se da sólo para $C=A^n$.*

c) Si C/k es irreducible, entonces $\dim C$ *es el grado de trascendencia de $k(C)$ (el cuerpo de cocientes de $k[C]$).*

d) Si todas las componentes irreducibles de C tienen la misma dimensión d, entonces toda cadena maximal de subvariedades $\varnothing\neq V_0\subsetneq\cdots\subsetneq V_l\subset C$ tiene longitud $l=d$.

e) Si C'/k es otro conjunto algebraico afín no vacío, entonces

$$\dim C\times C'=\dim C+\dim C'.$$

f) Si todas las componentes irreducibles de C tienen la misma dimensión d y V/k es una subvariedad de C no vacía, entonces

$$\dim C=\dim V+\operatorname{codim}_C V.$$

Demostración: a) Por el teorema 3.24 tenemos que $k'[C]\cong(k'\otimes_k k[C])_{\mathrm{red}}$, pero también hemos visto que $\operatorname{Esp}(k'\otimes_k k[C])_{\mathrm{red}}$ es homeomorfo a $\operatorname{Esp}k'\otimes_k k[C]$, luego por el teorema 3.77 vemos que

$$\dim C/k=\dim k[C]=\dim k'\otimes_k k[C]=\dim(k'\otimes_k k[C])_{\mathrm{red}}=\dim C/k'.$$

La segunda parte de a) se sigue de la segunda parte de 3.77.

b) Claramente $k[X_1,\ldots,X_n]$ es una normalización de Noether de sí mismo, de donde $\dim A^n=n$. La dimensión de C es la longitud de una cadena maximal de ideales primos en $k[C]=k[X_1,\ldots,X_n]/I(C)$, y sólo puede ser n si el primero de esos ideales es de la forma $\mathfrak{P}/I(C)$, donde $\mathfrak{P}$ es un primo minimal de $k[X_1, \ldots, X_n]$, es decir, $\mathfrak{P} = 0$.

c) y f) son consecuencias inmediatas de 3.75 y d) se sigue de 3.74. La propiedad e) se demuestra como a) pero a partir de 3.78. ■

Definición 3.80 Una *hipersuperficie* en A^n es una variedad C/k definida por una única ecuación no nula, es decir, una variedad de la forma $C = V(F)$, para cierto polinomio $F \in k[X_1, \ldots, X_n]$ no nulo.

Notemos que si descomponemos F en factores primos y eliminamos los exponentes, obtenemos un nuevo polinomio con los mismos ceros, luego toda hipersuperficie C/k está definida por un polinomio sin factores múltiples. Si F cumple esta condición, es claro que $I(C) = \operatorname{rad}(F) = (F)$.

El teorema siguiente se traduce en que un conjunto algebraico C/k es una hipersuperficie si y sólo si todas sus componentes irreducibles tienen codimensión 1 en A^n.

Teorema 3.81 *Sea A un dominio de factorización única e I un ideal radical $0 \neq I \neq A$. Entonces I es principal si y sólo si para todo divisor primo minimal $\mathfrak{p}$ de I se cumple que* $\dim A/\mathfrak{p} = \dim A - 1$.

Demostración: Si se cumple la condición sobre las dimensiones, el teorema 3.75 nos da que todo divisor primo minimal de I cumple $\operatorname{alt} \mathfrak{p} = 1$. Tomemos cualquier elemento no nulo de $\mathfrak{p}$ y descompongámoslo en factores primos. Uno de ellos, digamos π, ha de cumplir $\pi \in \mathfrak{p}$, luego $\mathfrak{p} = (\pi)$, por la condición sobre la altura. Como I es radical, es la intersección de sus divisores primos minimales, luego $I = (\pi_1) \cap \cdots \cap (\pi_r) = (\pi_1 \cdots \pi_r)$.

Si $I = (a)$, para cierto $a \in A$, el hecho de que sea radical se traduce en que a se descompone en producto de primos distintos dos a dos y dichos factores primos generan los divisores primos minimales de I. Teniendo en cuenta 3.75, sólo hay que probar que los ideales de la forma (π) con $\pi \in A$ primo tienen altura 1. Ahora bien, si $\mathfrak{p} \subset (\pi)$ es un ideal primo no nulo, como antes existe un primo $\pi' \in \mathfrak{p}$, que ha de dividir a π, luego ha de ser $(\pi') \subset \mathfrak{p} \subset (\pi) = (\pi')$. ■

Para terminar caracterizamos las álgebras afines de dimensión 0:

Teorema 3.82 *Si A es una k-álgebra afín, las afirmaciones siguientes son equivalentes:*

a) $\dim A = 0$.

b) A es un k-espacio vectorial de dimensión finita.

c) $\operatorname{Esp} A$ *es finito.*

d) A tiene un número finito de ideales maximales.

DEMOSTRACIÓN: Si $k[y_1, \ldots, y_d]$ es una normalización de Noether de A, es claro que $d = 0$ si y sólo si A es un k-espacio vectorial finitamente generado. Si $\dim A = 0$ entonces todos los ideales primos de A son minimales, luego son un número finito (porque A es noetheriano). Esto implica obviamente que A tiene un número finito de ideales maximales, y sólo falta probar que esto implica a su vez que la dimensión es 0.

La extensión $A/k[y_1, \ldots, y_d]$ es entera y el teorema 3.63 implica que el anillo de polinomios $k[y_1, \ldots, y_d]$ tiene también un número finito de ideales maximales. Ahora bien, si $d > 0$, cada ideal maximal de este anillo se corresponde con una clase de conjugación (finita) de puntos de A^d, lo cual es imposible. ■

El teorema anterior implica que un conjunto algebraico afín tiene dimensión 0 si y sólo si consta de un número finito de puntos (no necesariamente racionales).

3.8 Funciones regulares

Cada conjunto algebraico afín X/k tiene asociada su álgebra $k[X]$ de funciones polinómicas. Vamos a generalizar esto asociando una k-álgebra de funciones a cada uno de sus abiertos, con lo que dotaremos a X de estructura de espacio anillado local definido sobre k.

La idea básica es considerar las funciones definidas como cociente de dos funciones polinómicas allí donde el denominador no se anula. Para ello empezamos estudiando los conjuntos de puntos donde no se anula una función. Trataremos simultáneamente dos casos:

Si X es un conjunto algebraico afín sobre un cuerpo k y $f \in k[X]$, entonces definimos

$$D(f) = \{x \in X \mid f(x) \neq 0\}.$$

Si $X = \operatorname{Esp} A$, para un cierto anillo A y $f \in A$, entonces

$$D(f) = \{\mathfrak{p} \in X \mid f \notin \mathfrak{p}\}.$$

En cualquiera de los dos casos se comprueban sin dificultad las propiedades siguientes:

a) $D(f) = X \setminus V(f)$ es abierto en X.

b) $D(fg) = D(f) \cap D(g)$.

c) $D(f^n) = D(f)$, para todo $n \geq 1$.

d) $D(f) = \varnothing$ si y sólo si f es nilpotente.

A los abiertos de la forma $D(f)$ los llamaremos *abiertos principales* de X. Es claro que forman una base de X.

Teorema 3.83 *En las condiciones anteriores (suponiendo que A es noetheriano en el caso $X = \operatorname{Esp} A$), todo subconjunto de X es cuasicompacto, es decir, todo cubrimiento abierto admite un subcubrimiento finito.*

Demostración: Dado un cubrimiento abierto de un subconjunto A de X, podemos sustituir A por la unión de los abiertos del cubrimiento, con lo que podemos suponer que A es abierto. Es claro que también podemos suponer que los abiertos del cubrimiento son principales, digamos $\{D(g_j)\}_{j\in J}$. Entonces

$$X \setminus A = \bigcap_{j\in J} V(g_j) = V(J),$$

donde J es el ideal generado por los g_j. Como J es finitamente generado, en realidad $J = (g_{j_1}, \ldots, g_{j_n})$, para ciertos índices $j_1, \ldots, j_n$, y entonces

$$X \setminus A = \bigcap_{l=1}^{n} V(g_{j_l}),$$

luego

$$A = \bigcup_{l=1}^{n} D(g_{j_l}).$$

■

Definición 3.84 Sea C/k un conjunto algebraico afín y $U \subset C$ un abierto no vacío. Diremos que una función $r : U \longrightarrow K$ es *regular* en un punto $x \in U$ si existen $f, g \in k[C]$ tales que $x \in D(g) \subset U$ y para todo $y \in D(g)$ se cumple que $r(y) = f(y)/g(y)$. Diremos que la función r es *regular* en U si lo es en todos los puntos de U.

Es fácil ver que la regularidad en un punto x es una propiedad local, es decir, que si r es regular en x y $x \in U' \subset U$, entonces $r|_{U'}$ también es regular en x.

Representaremos por $k[U]$ al conjunto de todas las funciones regulares en U. Es inmediato comprobar que tiene estructura de k-álgebra con la suma y el producto definidos puntualmente. Convenimos en que $k[\varnothing] = 0$. Notemos que ahora $k[C]$ significa dos cosas diferentes (el álgebra de las aplicaciones polinómicas en C y el álgebra de las aplicaciones regulares en C), pero del teorema siguiente se desprende que en realidad son el mismo conjunto (teniendo en cuenta que $C = D(1)$).

Teorema 3.85 *Si C/k es un conjunto algebraico afín y $g \in k[C]$, entonces $k[D(g)] \cong k[C]_g$.*

Demostración: Recordemos que $k[C]_g$ es la localización de $k[C]$ respecto al conjunto multiplicativo $S = \{g^n \mid n \geq 1\}$. Hay que entender que, en el enunciado y en toda la demostración, $k[C]$ es el álgebra de funciones polinómicas en C, y no su álgebra de funciones regulares.

Claramente, toda función polinómica $f \in k[C]$ es regular en $D(g)$, pues se expresa como cociente $f = f/1$. Así pues, $k[C] \subset k[D(g)]$.

Como $1/g \in k[D(g)]$, vemos g es una unidad, y esto implica que la inclusión se extiende a un homomorfismo $k[C]_g \longrightarrow k[D(g)]$. Se trata de un monomorfismo, pues si $f/g^n = 0$ en $k[D(g)]$, entonces $f|_{D(g)} = 0$, luego $fg = 0$, y esto prueba que $f/g^n = 0$ en $k[C]_g$.

Por otra parte, si $r \in k[D(g)]$, por definición de aplicación regular y el teorema 3.83, tenemos que

$$D(g) = \bigcup_{i=1}^{t} D(g_i),$$

de modo que $r = f_i/g_i$ en $D(g_i)$. En $D(g_i) \cap D(g_j) = D(g_i g_j)$ tenemos la relación $f_i g_j - f_j g_i = 0$, luego $g_i g_j(f_i g_j - f_j g_i) = 0$ en todo C. Podemos cambiar f_i por $f_i g_i$ y g_i por g_i^2, con lo que la relación se reduce a $f_i g_j - f_j g_i = 0$ como funciones en C, luego $f_i g_j = f_j g_i$ como elementos de $k[C]$.

La función g se anula donde se anulan todas las g_i, lo que se traduce en que $g \in \operatorname{rad}(g_1, \ldots, g_t)$. Así pues, existe un $m \geq 0$ tal que

$$g^m = \sum_{i=1}^{t} h_i g_i,$$

para ciertas $h_i \in k[C]$. Si llamamos $f = \sum_{i=1}^{t} h_i f_i$, tenemos que

$$g^m f_j = \sum_{i=1}^{t} (h_i g_i) f_j = \sum_{i=1}^{t} (h_i f_i) g_j = f g_j,$$

luego $r = f_i/g_j = f/g^m$ en cada $D(g_j)$, luego en todo $D(g)$. Esto prueba que el homomorfismo es suprayectivo. ■

Notemos que este teorema tiene un análogo para espectros: Si $X = \operatorname{Esp} A$ y $g \in A$, entonces, por el teorema 3.39, $D(g)$ es homeomorfo a $\operatorname{Esp} A_g$.

Definición 3.86 Si C/k es un conjunto algebraico afín, para cada subconjunto abierto $U \subset C$, definimos $\mathcal{O}_C(U) = k[U]$, de modo que, con las restricciones usuales de funciones, C se convierte un espacio anillado definido sobre k.

En particular, si $P \in C$, tenemos definido el anillo $\mathcal{O}_{C,P}$ de gérmenes de funciones regulares. Enseguida determinaremos la estructura de estos anillos, pero antes observemos que los abiertos de C se corresponden biunívocamente con los abiertos de $\operatorname{Esp} k[C]$, por lo que podemos trasladar a $\operatorname{Esp} k[C]$ la estructura de espacio anillado que hemos definido en C. Sin embargo, en $\operatorname{Esp} k[C]$ hay más puntos que en C, por lo que podemos considerar anillos de gérmenes más generales.

Específicamente, si llamamos $X = \operatorname{Esp} k[C]$, cada abierto de C es de la forma $U = C \setminus V_C(I)$, para cierto ideal radical I de $k[C]$, y se corresponde con el abierto $U' = X \setminus V_X(I)$. Por otra parte, los puntos $\mathfrak{P} \in X$ se corresponden biunívocamente con los cerrados irreducibles $W = V_C(\mathfrak{P}) \subset C$, de forma que $\mathfrak{P} \in U'$ equivale a que $I \not\subset \mathfrak{P}$, y también a que $W \not\subset V_C(I)$, o a que $W \cap U \neq \varnothing$.

Por consiguiente, si llamamos $\mathcal{O}_{C,W}$ al anillo de gérmenes asociado a $\mathfrak{P}$, es claro que está formado por las clases de equivalencia de funciones racionales definidas en abiertos que cortan a W, identificadas cuando coinciden en un abierto menor que también corte a W. (Notemos que la intersección de dos abiertos que corten a W corta también a W, bien porque la intersección de dos entornos de $\mathfrak{P}$ es un entorno de $\mathfrak{P}$, bien porque los abiertos no vacíos en un conjunto irreducible son densos.)

Naturalmente, $\mathcal{O}_{C,P} = \mathcal{O}_{C,\{P\}}$.

El teorema siguiente prueba, en particular, que los conjuntos algebraicos son espacios anillados locales (y también los espacios $\operatorname{Esp} k[C]$).

Teorema 3.87 *Si C/k es un conjunto algebraico afín, W/k es un subconjunto irreducible y $\mathfrak{p}_W = I_C(W)$, entonces $\mathcal{O}_{C,W} \cong k[C]_{\mathfrak{p}_W}$.*

DEMOSTRACIÓN: Sea $\phi : k[C] \longrightarrow \mathcal{O}_{C,W}$ el homomorfismo de k-álgebras que a cada función regular le asigna el germen determinado por sus restricciones a los abiertos que cortan a W. Si $f \in k[C] \setminus \mathfrak{p}_W$, esto significa que f no es idénticamente nula en W o, equivalentemente, que $D(f) \cap W \neq \varnothing$. La función regular $1/f \in k[D(f)]$ determina un elemento de $\mathcal{O}_{C,W}$ que es el inverso de $\phi(f)$. Así pues, $\phi(f)$ es una unidad, luego ϕ se extiende a un homomorfismo $\phi : k[C]_{\mathfrak{p}_W} \longrightarrow \mathcal{O}_{C,W}$.

Si $f/g \in k[C]_{\mathfrak{p}_W}$ tiene imagen nula, eso significa que f se anula en un abierto que corta a W. Podemos tomarlo de la forma $D(h)$, con $h \in k[C] \setminus \mathfrak{p}_W$. Así, $fh = 0$, lo que prueba que $f/g = 0$. Así pues, ϕ es inyectiva.

Cada elemento de $\mathcal{O}_{C,W}$ está representado por una función r definida sobre un abierto de la forma $D(g)$, donde $g \in k[C]$ cumple que $D(g) \cap W \neq \varnothing$. Por el teorema 3.85, sabemos que r es de la forma $r = f/g^n$, para cierta $f \in k[C]$. Puesto que $g \notin \mathfrak{p}_W$, es claro que $\phi(f/g^n)$ es la clase de r en $\mathcal{O}_{C,W}$, luego ϕ es suprayectiva. ■

De esta representación se deducen las propiedades fundamentales de estos anillos locales:

Teorema 3.88 *Sea C/k un conjunto algebraico afín y W/k un subconjunto algebraico irreducible. Entonces:*

a) Los elementos de $\operatorname{Esp} \mathcal{O}_{C,W}$ se corresponden biunívocamente con las subvariedades V/k tales que $W \subset V \subset C$.

b) $\mathcal{O}_{C,W}$ es un dominio íntegro si y sólo si W está contenido en una única componente irreducible de C.

c) $\dim \mathcal{O}_{C,W} = \operatorname{codim}_C W$.

d) Los ideales radicales de $\mathcal{O}_{C,W}$ (distintos de todo $\mathcal{O}_{C,W}$) se corresponden biunívocamente con los subconjuntos algebraicos de C cuyas componentes irreducibles contienen (todas) a W.

DEMOSTRACIÓN: a) Por el teorema anterior, $\mathcal{O}_{C,W} \cong k[C]_{\mathfrak{p}_W}$, donde $\mathfrak{p}_W = I_C(W)$. Por lo tanto, los ideales primos de $\mathcal{O}_{C,W}$ se corresponden con los ideales primos de $k[C]$ contenidos en $\mathfrak{p}_W$, que a su vez se corresponden con las variedades que contienen a W.

b) Como $k[C]$ es reducido, lo mismo vale para $\mathcal{O}_{C,W}$, de donde se sigue claramente que es un dominio íntegro si y sólo si contiene un único primo minimal, lo que equivale a que $\mathfrak{p}_W$ contenga un único primo minimal de $k[C]$, luego también a que W esté contenido en una única componente de C.

c) es consecuencia inmediata de a) por las definiciones de dimensión y codimensión.

d) Los ideales citados en d) son las intersecciones de sus primos minimales, y se corresponden con las intersecciones finitas de primos de $k[C]$ contenidos en $\mathfrak{p}_W$, luego también con los conjuntos algebraicos indicados en d). ■

Capítulo IV

Anillos locales

Muchos problemas del álgebra conmutativa pueden reducirse al estudio de anillos locales, es decir, anillos con un único ideal maximal. La forma típica de llegar a esta situación es localizando un anillo dado respecto de uno de sus ideales primos. Por ejemplo, si C/k es un conjunto algebraico y $P \in C$ es un punto contenido en la componente irreducible de mayor dimensión, entonces $\dim C = \dim \mathcal{O}_{C,P}$, por lo que para estudiar la dimensión de C podemos estudiar la del anillo local $\mathcal{O}_{C,P}$.

En este capítulo empezaremos estudiando las compleciones de un anillo respecto de ciertas topologías definidas por ideales. No es una técnica que vaya a resultar esencial en lo que veremos más adelante, pero es en este contexto donde aparecen de forma natural algunos resultados que nos van a hacer falta después.

En las secciones siguientes estudiaremos más a fondo la dimensión de un anillo noetheriano local. Daremos dos caracterizaciones alternativas de la dimensión para estos anillos, de las que obtendremos diversas consecuencias, entre ellas que los anillos noetherianos locales siempre tienen dimensión finita.

4.1 Compleciones

Consideremos un grupo topológico abeliano G, es decir, un grupo abeliano G dotado de una topología de modo que tanto la suma $+ : G \times G \longrightarrow G$ como la aplicación $- : G \longrightarrow G$ son continuas. Es evidente entonces que las traslaciones son homeomorfismos, luego si $\mathcal{B}$ es una base de entornos de 0 y $g \in G$, entonces los conjuntos $\{g + U \mid U \in \mathcal{B}\}$ forman una base de entornos de g. Esto significa que la topología de G está determinada por los entornos de 0.

En principio no suponemos que los grupos tengan la propiedad de Hausdorff, pero ésta tiene una caracterización sencilla:

Teorema 4.1 *Sea G un grupo topológico abeliano y H la intersección de todos los entornos de 0. Entonces H es un subgrupo de G. Además H es la clausura de $\{0\}$ y G es un espacio de Hausdorff si y sólo si $H = 0$.*

DEMOSTRACIÓN: Si h_1, $h_2 \in H$ y U es un entorno de 0, la continuidad de la aplicación $f : G \times G \longrightarrow G$ dada por $(u, v) \mapsto u - v$ implica que existe un entorno $V_1 \times V_2$ de $(0, 0)$ en $G \times G$ tal que $V_1 \times V_2 \subset f^{-1}[U]$. Como $(h_1, h_2) \in V_1 \times V_2$, concluimos que $h_1 - h_2 \in U$, luego $h_1 - h_2 \in H$. Esto demuestra que H es un subgrupo.

Claramente $h \in H$ si y sólo si $0 \in h - U$ para todo entorno U de 0, si y sólo si 0 pertenece a todo entorno de h, si y sólo si $h \in \overline{\{0\}}$.

Obviamente, si G es un espacio de Hausdorff ha de ser $H = 0$. Si $H = 0$, basta probar que 0 puede separarse de cualquier punto $g \in G$, $g \neq 0$. En efecto, existe un entorno U de 0 tal que $g \notin U$. Por la continuidad de la suma existe un entorno V de 0 tal que $V + V \subset U$. Entonces V y $g - V$ son entornos disjuntos de 0 y g. ■

Si G es un grupo topológico abeliano y H es un subgrupo de G, consideraremos a H como grupo topológico con la topología inducida. Así mismo consideraremos en G/H la topología cociente en la que un conjunto $U \subset G/H$ es abierto si y sólo si $p^{-1}[U]$ es abierto en G, donde $p : G \longrightarrow G/H$ es la proyección natural. Observemos que con esta topología p es continua y abierta, pues si U es abierto en G entonces

$$p^{-1}[p[U]] = \bigcup_{h \in H} (h + U)$$

es abierto en G. Observemos que aunque G sea un espacio de Hausdorff el cociente G/H no tiene por qué serlo. Del teorema anterior se sigue que la condición necesaria y suficiente es que H sea cerrado en G.

Todos los grupos topológicos que vamos a considerar serán de la forma determinada por el teorema siguiente:

Teorema 4.2 *Sea G un grupo abeliano y*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots$$

una sucesión decreciente de subgrupos de G. Entonces existe una única topología con la que G se convierte en un grupo topológico y los subgrupos G_n forman una base de entornos (abiertos) de 0.

DEMOSTRACIÓN: Tomamos como base los trasladados de los subgrupos G_n. Ciertamente son base de una topología, pues si $u \in (g_1 + G_m) \cap (g_2 + G_n)$, digamos con $m \leq n$, entonces $u + G_n \subset (g_1 + G_m) \cap (g_2 + G_n)$.

Respecto a esta topología, la suma en G es continua, pues

$$(a + G_n) + (b + G_n) = a + b + G_n.$$

Igualmente, la aplicación $-$ es continua, pues $-(a + G_n) = -a + G_n$. La unicidad es evidente. ■

Nota: En lo sucesivo sobrentenderemos que todos los grupos topológicos considerados serán abelianos y tendrán una base de entornos de 0 formada por una sucesión decreciente de subgrupos $\{G_n\}_n$. A estas sucesiones las llamaremos *sistemas fundamentales de entornos de* 0.

Observemos que si G es un grupo topológico en estas condiciones y H es un subgrupo de G, entonces la topología de H está definida por el sistema fundamental $\{H \cap G_n\}_n$, y la topología de G/H está definida por $\{(G_n + H)/H\}_n$. Más aún, si G y H son grupos en estas condiciones, la topología producto en $G \times H$ está determinada por el sistema fundamental $\{G_n \times H_n\}_n$.

En general, si G es un grupo topológico y $\{G_n\}_n$ es un sistema fundamental de entornos de 0, los subgrupos G_n son necesariamente abiertos y cerrados en G, pues si $g \in G_n$ entonces $g + G_n$ es un entorno de G y $g + G_n \subset G_n$. Esto prueba que G_n es abierto, y su complementario se expresa como unión de trasladados de G_n, luego también es abierto y G_n es cerrado.

Definición 4.3 Sea G un grupo topológico. Diremos que una sucesión $\{x_n\}_n$ en G es *de Cauchy* si para todo entorno U de 0 existe un natural n_0 de modo que si m, $n \geq n_0$ entonces $x_m - x_n \in U$. Diremos que G es *completo* si y sólo si todas sus sucesiones de Cauchy son convergentes.

Es obvio que en la definición de sucesión de Cauchy podemos restringir los entornos U a los elementos de un sistema fundamental.

Diremos que dos sucesiones de Cauchy son *equivalentes* si su diferencia converge a 0 en G (es decir, está finalmente en todo entorno de 0). Es inmediato comprobar que se trata de una relación de equivalencia.

Definimos la *compleción* de G como el conjunto cociente, que adquiere estructura de grupo abeliano con la suma dada por $[\{x_n\}_n] + [\{y_n\}_n] = [\{x_n + y_n\}_n]$.

La aplicación $\phi : G \longrightarrow \hat{G}$ que a cada $g \in G$ le asocia la clase de la sucesión constante igual a g es claramente un homomorfismo de grupos. Observemos que su núcleo es la intersección de todos los entornos de 0 en G, luego sólo podemos considerar a G como subgrupo de $\hat{G}$ cuando G tiene la propiedad de Hausdorff.

Si $U \subset G$ es un entorno de 0, definimos $\hat{U} \subset \hat{G}$ como el conjunto de las clases de sucesiones que están finalmente en U. Es obvio que esta propiedad no depende del representante escogido en una clase de equivalencia dada. Además, si U es un subgrupo de G, entonces $\hat{U}$ es un subgrupo de $\hat{G}$ (de hecho, es la compleción de U como grupo). Si $\{G_n\}_n$ es un sistema fundamental de entornos de G, definimos en $\hat{G}$ la topología que tiene por sistema fundamental de entornos de 0 a la sucesión $\{\hat{G}_n\}_n$. Es inmediato comprobar que la topología de $\hat{G}$ no depende de la elección del sistema fundamental de entornos con que se define.

Más aún, si $\phi : G \longrightarrow \hat{G}$ es el homomorfismo natural y U es un entorno de 0 en G, tenemos que $\hat{U}$ es un entorno de 0 en $\hat{G}$ y $\phi^{-1}[\hat{U}] = U$. Esto prueba que ϕ es una aplicación continua. Si G tiene la propiedad de Hausdorff (con lo que ϕ es inyectiva), de hecho ϕ es un homeomorfismo en su imagen, pues al identificar a G con un subgrupo de $\hat{G}$ a través de ϕ, la relación anterior se convierte en $U = \hat{U} \cap G$.

Por otra parte $\phi[U]$ es denso en $\hat{U}$, pues si $\xi \in \hat{U}$ y $\xi + \hat{V}$ es un entorno de ξ (donde V es un entorno de 0 en G), tenemos que $\xi = [\{x_n\}_n]$, donde la sucesión $\{x_n\}_n$ es de Cauchy en G y está finalmente en U. Existe un natural m tal que si $n \geq m$ entonces $x_m - x_n \in V$ y $x_n \in U$. Esto se traduce en que

$$\phi(x_m) \in (\xi + \hat{V}) \cap \phi[U].$$

Si U es un subgrupo entonces $\hat{U} = \overline{\phi[U]}$, pues $\hat{U}$ es cerrado en $\hat{G}$ y $\phi[U]$ es denso en $\hat{U}$.

No es difícil probar que $\hat{G}$ es un grupo topológico completo, pero más adelante será inmediato, así que posponemos la prueba. Observemos de momento que $\hat{G}$ tiene la propiedad de Hausdorff, pues si $\xi \in \hat{G}$ está en todos los entornos de 0, entonces un representante de ξ es una sucesión de Cauchy que está finalmente en todos los entornos de 0 en G, luego converge a 0, luego $\xi = 0$.

Así pues, al completar G hemos identificado los puntos necesarios para que se cumpla además la propiedad de Hausdorff. En el fondo, ésta es la razón por la que G no puede sumergirse en $\hat{G}$ si no tiene la propiedad de Hausdorff.

Para terminar con las propiedades básicas de las compleciones, observemos que si $f : G \longrightarrow H$ es un homomorfismo continuo entre dos grupos topológicos, entonces f transforma sucesiones de Cauchy en sucesiones de Cauchy, por lo que induce un homomorfismo continuo $\hat{f} : \hat{G} \longrightarrow \hat{H}$ determinado por que es el único que hace conmutativo el diagrama

$$\begin{tikzcd} \hat{G} \arrow[r, "\hat{f}"] & \hat{H} \\ G \arrow[u, "\phi"] \arrow[r, "f"'] & H \arrow[u, "\phi"'] \end{tikzcd}$$

Para estudiar la estructura algebraica de las compleciones conviene observar que es posible dar una construcción alternativa de $\hat{G}$ puramente algebraica. Para ello necesitamos el concepto de límite inverso:

Definición 4.4 Un *sistema inverso* de grupos es una sucesión de grupos abelianos $\{A_n\}_n$ junto con homomorfismos $\rho_{n+1} : A_{n+1} \longrightarrow A_n$. Diremos que el sistema es *suprayectivo* si lo son todos los ρ_{n+1}. El *límite inverso* del sistema es el grupo

$$\varprojlim_n A_n = \{\xi \in \prod_n A_n \mid \rho_{n+1}(\xi_{n+1}) = \xi_n \text{ para todo natural } n\}.$$

Observemos que tenemos homomorfismos naturales $\pi_n : \varprojlim_n A_n \longrightarrow A_n$, que son epimorfismos si el sistema es suprayectivo.

Consideremos ahora un grupo topológico G con un sistema fundamental $\{G_n\}_n$ de entornos de 0. Los grupos $\{G/G_n\}_n$ forman un sistema inverso suprayectivo con las aplicaciones naturales $\rho_{n+1} : G/G_{n+1} \longrightarrow G/G_n$.

Si $\{x_n\}_n$ es una sucesión de Cauchy en G, entonces su imagen en G/G_n a través de la proyección natural es finalmente constante, digamos que es igual a $\xi_n \in G/G_n$. Es claro que $\rho_{n+1}(\xi_{n+1}) = \xi_n$, con lo que $(\xi_n) \in \varprojlim_n G/G_n$.

Es claro que dos sucesiones de Cauchy determinan el mismo elemento del límite inverso si y sólo si son equivalentes, por lo que tenemos definida una aplicación inyectiva

$$\psi : \hat{G} \longrightarrow \varprojlim_n G/G_n,$$

que claramente es un monomorfismo de grupos. De hecho es un isomorfismo, pues toda sucesión (ξ_n) en el límite inverso es la imagen de una sucesión de Cauchy $(x_n)_n$ en G. Basta elegir arbitrariamente $x_n \in \xi_n$. Entonces se cumple que $x_n - x_{n+1} \in G_{n+1}$, de donde se sigue que la sucesión es de Cauchy y su imagen es (ξ_n).

A través de ψ, el entorno fundamental $\hat{G}_m$ se corresponde con el conjunto de sucesiones (ξ_n) tales que $\xi_n = [x_n]$ con $x_n \in G_m$. Esto equivale a que $\xi_m = 0$. En otras palabras, si dotamos al límite inverso de la topología determinada por los subgrupos

$$H_n = \{\xi \in \varprojlim_n G/G_n \mid \xi_n = 0\},$$

tenemos que ψ es un homeomorfismo. En lo sucesivo identificaremos

$$\hat{G} = \varprojlim_n G/G_n, \qquad \hat{G}_n = \{\xi \in \hat{G} \mid \xi_n = 0\}.$$

Observemos que esta representación de la compleción de un grupo G depende (desde un punto de vista conjuntista) de la elección del sistema fundamental de entornos de 0, pero precisamente hemos demostrado que esta dependencia es salvo isomorfismo, es decir, que si cambiamos de sistema fundamental de entornos, los límites inversos correspondientes son topológicamente isomorfos.

El homomorfismo natural $\phi : G \longrightarrow \hat{G}$ se corresponde a través de ψ con el homomorfismo dado por $\phi(g) = (g + G_n)_n$.

Veamos cómo esta representación algebraica nos aporta mucha información sobre las compleciones. En primer lugar observemos un hecho general sobre límites inversos:

Un *homomorfismo* $\phi : \{A_n\}_n \longrightarrow \{B_n\}_n$ entre dos sistemas inversos es una sucesión de homomorfismos de grupos $\phi_n : A_n \longrightarrow B_n$ que verifiquen $\phi_{n+1} \circ \rho_{n+1} = \rho_{n+1} \circ \phi_n$ para todo natural n. Es inmediato que ϕ induce un homomorfismo $\phi : \varprojlim_n A_n \longrightarrow \varprojlim_n B_n$ de forma natural.

Teorema 4.5 *Sea* $0 \longrightarrow \{A_n\}_n \xrightarrow{\phi} \{B_n\}_n \xrightarrow{\psi} \{C_n\}_n \longrightarrow 0$ *una sucesión exacta de homomorfismos de sistemas inversos (exacta en el sentido de que* *lo es la sucesión de homomorfismos correspondiente a cada n). Entonces la sucesión*

$$0 \longrightarrow \varprojlim_n A_n \xrightarrow{\phi} \varprojlim_n B_n \xrightarrow{\psi} \varprojlim_n C_n$$

es exacta, y si el sistema $\{A_n\}_n$ es suprayectivo, también lo es la sucesión

$$0 \longrightarrow \varprojlim_n A_n \xrightarrow{\phi} \varprojlim_n B_n \xrightarrow{\psi} \varprojlim_n C_n \longrightarrow 0.$$

DEMOSTRACIÓN: Es claro que ϕ es inyectiva y que $\phi \circ \psi = 0$. Si $\psi(\beta) = 0$ entonces cada $\psi_n(\beta_n) = 0$, luego existe $\alpha_n \in A_n$ tal que $\beta_n = \phi_n(\alpha_n)$. Además

$$\phi_n(\pi_{n+1}(\alpha_{n+1})) = \pi_{n+1}(\phi_{n+1}(\alpha_{n+1})) = \pi_{n+1}(\beta_{n+1}) = \beta_n = \phi_n(\alpha_n),$$

luego $\pi_{n+1}(\alpha_{n+1}) = \alpha_n$, luego la sucesión (α_n) determina un $\alpha \in \varprojlim_n A_n$ tal que $\phi(\alpha) = \beta$.

Por último, si el primer sistema es suprayectivo, dado $\gamma \in \varprojlim_n C_n$, tomamos $\beta_0 \in B_0$ tal que $\psi_0(\beta_0) = \gamma_0$. Supongamos construidos $\beta_0, \ldots, \beta_n$ tales que $\psi_i(\beta_i) = \gamma_i$, $\pi_{i+1}(\beta_{i+1}) = \beta_i$. Entonces tomamos $\beta'_{n+1} \in B_{n+1}$ tal que $\psi_{n+1}(\beta'_{n+1}) = \gamma_{n+1}$. Se cumple que

$$\psi_n(\pi_{n+1}(\beta'_{n+1})) = \pi_{n+1}(\psi_{n+1}(\beta'_{n+1})) = \pi_{n+1}(\gamma_{n+1}) = \gamma_n = \psi_n(\beta_n).$$

Por lo tanto existe un $\alpha \in A_n$ tal que $\pi_{n+1}(\beta'_{n+1}) - \beta_n = \phi_n(\alpha)$. Sea $\alpha' \in A_{n+1}$ tal que $\alpha = \pi_{n+1}(\alpha')$. Entonces

$$\beta_n = \pi_{n+1}(\beta'_{n+1}) - \phi_n(\pi_{n+1}(\alpha')) = \pi_{n+1}(\beta'_{n+1}) - \pi_{n+1}(\phi_{n+1}(\alpha')) = \pi_{n+1}(\beta_{n+1}),$$

donde $\beta_{n+1} = \beta'_{n+1} - \phi_{n+1}(\alpha') \in B_{n+1}$ cumple además que $\psi_{n+1}(\beta_{n+1}) = \gamma_{n+1}$. De este modo hemos construido un $\beta \in \varprojlim_n B_n$ tal que $\psi(\beta) = \gamma$. ■

Como caso particular obtenemos lo siguiente:

Teorema 4.6 *Sea $0 \longrightarrow G' \longrightarrow G \xrightarrow{p} G'' \longrightarrow 0$ una sucesión exacta de grupos, sea $\{G_n\}_n$ una sucesión decreciente de subgrupos de G y consideremos en G' la sucesión $\{G_n \cap G'\}_n$ y en G'' la sucesión $\{p[G_n]\}_n$. Entonces los homomorfismos naturales*

$$0 \longrightarrow \hat{G}' \longrightarrow \hat{G} \longrightarrow \hat{G}'' \longrightarrow 0$$

forman una sucesión exacta.

DEMOSTRACIÓN: Los homomorfismos naturales son los inducidos por la sucesión exacta de homomorfismos

$$0 \longrightarrow G'/(G' \cap G_n) \longrightarrow G/G_n \longrightarrow G''/p[G_n] \longrightarrow 0,$$

que determinan una sucesión exacta por el teorema anterior. ■

Observemos que, con los sistemas fundamentales de entornos determinados por el teorema, los homomorfismos de la sucesión exacta de partida son continuos, y los homomorfismos de la sucesión exacta entre las compleciones (vistas como límites inversos) se corresponde con los homomorfismos inducidos de forma natural en términos de sucesiones de Cauchy, luego también son continuos.

Podemos aplicar este resultado a $G' = G_n$ y $G'' = G/G_n$. Observemos que la sucesión de entornos de 0 en G'' es finalmente nula, luego la proyección $\pi_n : \hat{G}'' \longrightarrow G''$ es un isomorfismo.

En definitiva obtenemos que $\hat{G}_n$ se identifica de forma natural con un subgrupo de $\hat{G}$ y además $\hat{G}/\hat{G}_n \cong G/G_n$.

Es fácil ver que la identificación es la que ya teníamos, es decir,

$$\hat{G}_n \cong \{\xi \in \hat{G} \mid \xi_n = 0\}.$$

El isomorfismo $\hat{G}/\hat{G}_n \cong G/G_n$ es simplemente el inducido por la proyección $\pi_n : \hat{G} \longrightarrow G/G_n$. Su inverso es el homomorfismo $\phi_n : G/G_n \longrightarrow \hat{G}/\hat{G}_n$ inducido por el homomorfismo natural $\phi : G \longrightarrow \hat{G}$.

Ahora observamos que los isomorfismos ϕ_n conmutan con las proyecciones que definen los sistemas inversos $\{G/G_n\}_n$ y $\{\hat{G}/\hat{G}_n\}_n$, luego determinan un isomorfismo $\hat{\phi} : \hat{G} \longrightarrow \hat{\hat{G}}$.

Explícitamente, si $\xi \in \hat{G}$ viene dado por $\xi_n = g_n + G_n$, con $g_n \in G$, tenemos que

$$\hat{\phi}(\xi)_n = \phi_n(\xi_n) = \phi(g_n) + \hat{G}_n = \xi + \hat{G}_n,$$

pues $(\xi - \phi(g_n))_n = 0$, luego $\xi - \phi(g_n) \in \hat{G}_n$.

En definitiva, vemos que $\hat{\phi}$ no es más que el homomorfismo ϕ correspondiente al grupo $\hat{G}$.

Teorema 4.7 *Si G es un grupo topológico, entonces el homomorfismo natural $\phi : G \longrightarrow \hat{G}$ es un isomorfismo si y sólo si G tiene la propiedad de Hausdorff y es completo.*

DEMOSTRACIÓN: Para probar este teorema es preferible considerar a $\hat{G}$ como el grupo de clases de equivalencia de sucesiones de Cauchy. Ya sabemos que la inyectividad de ϕ equivale a la propiedad de Hausdorff. La suprayectividad equivale a que toda sucesión de Cauchy es equivalente a una sucesión contante, lo que claramente equivale a que toda sucesión de Cauchy es convergente, es decir, a la completitud. ■

Con esto hemos demostrado que la compleción $\hat{G}$ de un grupo abeliano G es siempre un grupo topológico completo con la propiedad de Hausdorff.

Ejercicio: Probar que $f : G \longrightarrow H$ es un homomorfismo continuo entre dos grupos topológicos y H es completo, entonces existe un homomorfismo continuo $\hat{f} : \hat{G} \longrightarrow H$ tal que $i \circ \hat{f} = f$, donde $i : G \longrightarrow \hat{G}$ es el homomorfismo natural.

4.2 Topologías inducidas por ideales

En esta sección estudiaremos con detalle las compleciones obtenidas mediante un ideal de un anillo según la definición siguiente:

Definición 4.8 Sea A un anillo e I un ideal en A. Llamaremos *topología I-ádica* en A a la topología definida por la sucesión de subgrupos $\{I^n\}_n$.

Se cumple que A es un anillo topológico con la topología I-ádica, es decir, el producto $A \times A \longrightarrow A$ también es continuo. En efecto, dado un punto $(a, b) \in A \times A$ y un entorno $ab + I^n$ de su imagen, es claro que

$$(a + I^n)(b + I^n) \subset ab + I^n,$$

luego el producto es continuo en (a, b).

La compleción $\hat{A}$ tiene definida una estructura de anillo de forma natural (tanto si la consideramos en términos de sucesiones de Cauchy o en términos de límites inversos). Los conjuntos $\widehat{I^n}$ forman una sucesión decreciente de ideales de $\hat{A}$, por lo que $\hat{A}$ también es un anillo topológico.

Si M es un A-módulo, definimos la *topología I-ádica* en M como la topología determinada por los subgrupos $\{I^nM\}_n$. Se comprueba fácilmente que el producto $A \times M \longrightarrow M$ es continuo (es decir, que M es un A-módulo topológico). La compleción $\hat{M}$ tiene una estructura natural de $\hat{A}$-módulo y es fácil ver que es, de hecho, un $\hat{A}$-módulo topológico.

Si M es un A-módulo, I es un ideal de A y M' es un submódulo, entonces es claro que

$$(I^nM + N)/M' = I^n(M + M')/M'.$$

Los ideales de la izquierda definen la topología cociente en M/M', mientras que los de la derecha definen la topología I-ádica en M/M'. Vemos así que el cociente de la topología I-ádica es la topología I-ádica en el cociente. Igualmente, la identidad

$$I^n(M_1 \oplus M_2) = I^nM_1 \oplus I^nM_2$$

prueba que la topología I-ádica en una suma directa es el producto de las topologías I-ádicas. Lo que no es trivial es que la restricción de la topología I-ádica en un módulo M a un submódulo M' sea la topología I-ádica en M'. En efecto, estas topologías están determinadas, respectivamente, por los sistemas fundamentales de entornos

$$\{I^nM \cap M'\}_n \qquad \text{y} \qquad \{I^nM'\}_n,$$

que en principio no tienen por qué coincidir. Vamos a probar que, pese a ello, ambas topologías coinciden. El primer paso es la definición siguiente:

Definición 4.9 Dado un A-módulo M, una *filtración* en M es una sucesión decreciente de submódulos

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

Si I es un ideal de A, diremos que la filtración es *I-ádica* si $IM_n \subset M_{n+1}$. Una filtración I-ádica es *estable* si $IM_n = M_{n+1}$ para todo natural n suficientemente grande.

Así, $\{I^n M\}_n$ es una filtración I-ádica estable.

Teorema 4.10 *Sea M un A-módulo e I un ideal de A. Sean $\{M_n\}_n$ y $\{M'_n\}_n$ dos filtraciones I-ádicas estables. Entonces ambas filtraciones tienen diferencias acotadas, es decir, existe un natural n_0 tal que $M_{n+n_0} \subset M'_n$ y $M'_{n+n_0} \subset M_n$ para todo natural n. En particular, ambas determinan la misma topología en M (la topología I-ádica).*

DEMOSTRACIÓN: No perdemos generalidad si suponemos que $M'_n = I^n M$. El hecho de que $\{M_n\}_n$ sea I-ádica implica que $M'_n = I^n M \subset M_n$. Si cumple $IM_n = M_{n+1}$ para $n \geq n_0$, entonces $M_{n+n_0} = I^n M_{n_0} \subset I^n M = M'_n$. ■

Ahora conviene introducir un nuevo concepto:

Definición 4.11 Un *anillo graduado* es un anillo A junto con una familia de subgrupos aditivos $\{A_n\}_{n=0}^{\infty}$ tal que $A = \bigoplus\limits_n A_n$ y $A_n A_m \subset A_{n+m}$ para todos los índices n, m.

El ejemplo típico es un anillo de polinomios $A = B[X_1, \ldots, X_n]$ tomando como A_n el subgrupo de los monomios de grado n.

En general, si A es un anillo graduado tenemos que A_0 es un subanillo y todos los A_n son A_0-módulos. Los elementos de A_n se llaman elementos *homogéneos* de grado n. Además $A_+ = \bigoplus\limits_{n>0} A_n$ es un ideal de A.

Si A es un anillo graduado, un *A-módulo graduado* es un A-módulo M junto con una sucesión de subgrupos aditivos $\{M_n\}_{n=0}^{\infty}$ de modo que $M = \bigoplus\limits_n M_n$ y $A_m M_n \subset M_{m+n}$ para todos los índices m, n.

Es claro entonces que todos los M_n son A_0-módulos.

Teorema 4.12 *Un anillo graduado A es noetheriano si y sólo si A_0 es noetheriano y A es finitamente generado como A_0-álgebra.*

DEMOSTRACIÓN: Una implicación es obvia. Si A es noetheriano, entonces $A_0 \cong A/A_+$ también es noetheriano. El ideal A_+ es finitamente generado, digamos $A_+ = (x_1, \ldots, x_r)$. Podemos suponer que los generadores son homogéneos de grados $n_1, \ldots, n_r$. Sea $A' = A_0[x_1, \ldots, x_r]$. Veamos que $A_n \subset A'$ por inducción sobre n. Ciertamente se cumple para $n = 0$. Sea $y \in A_n$. Como $y \in A_+$, ha de ser $y = a_1 x_1 + \cdots + a_r x_r$, donde $a_i \in A_{n-n_i}$, con el convenio de que $A_i = 0$ si $i < 0$. (En principio los a_i no tienen por qué ser homogéneos, pero descomponiéndolos en suma de elementos homogéneos, los sumandos con grado distinto de n se han de cancelar.) Como $n_i > 0$, por hipótesis de inducción cada a_i depende polinómicamente de los x_i con coeficientes en A_0, luego lo mismo es válido para y. ■

La relación de los módulos graduados con las filtraciones es la siguiente: Si A es un anillo e I es un ideal de A, podemos formar el anillo graduado

$$A^* = \bigoplus_n I^n,$$

de modo que si M es un A-módulo y $\{M_n\}_n$ es una filtración I-ádica, entonces

$$M^* = \bigoplus_n M_n$$

es un A^*-módulo graduado. Si A es noetheriano, entonces I es finitamente generado, digamos $I = (x_1, \ldots, x_r)$, con lo que $A^* = A[x_1, \ldots, x_n]$, luego A^* también es noetheriano. Si además M es un A-módulo finitamente generado, vamos a probar que M^* es finitamente generado si y sólo si la filtración es estable.

En efecto, tenemos que M es noetheriano, luego los submódulos M_n son todos A-módulos finitamente generados. Sea M_n^* el A^*-submódulo de M^* generado por $M_0 \oplus \cdots \oplus M_n$. Explícitamente:

$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots$$

Ciertamente los módulos M_n^* son finitamente generados y forman una cadena ascendente cuya unión es todo M^*. Como A^* es noetheriano, tenemos que M^* es finitamente generado si y sólo si la cadena se estabiliza, es decir, si y sólo si $M^* = M_{n_0}^*$ para un n_0, si y sólo si $M_{n_0+m} = I^m M_{n_0}$ para todo $m \geq 0$, si y sólo si la filtración es estable. ■

Con esto podemos demostrar el resultado fundamental para el fin que estamos persiguiendo:

Teorema 4.13 *Sea A un anillo noetheriano, I un ideal de A, sea M un A-módulo finitamente generado y $\{M_n\}_n$ una filtración I-ádica estable. Si M' es un submódulo de M, entonces $\{M' \cap M_n\}_n$ es una filtración I-ádica estable de M'.*

Demostración: Tenemos que $I(M' \cap M_n) \subset IM' \cap IM_n \subset M' \cap M_{n+1}$, luego la filtración es I-ádica. Por lo tanto define un A^*-módulo graduado que es un submódulo de M^*, luego es finitamente generado (porque A^* es noetheriano). Por el teorema anterior, la filtración es estable. ■

Conviene destacar el caso correspondiente a la filtración $M_n = I^n M$:

Teorema 4.14 (Lema de Artin-Rees) *Si A es un anillo noetheriano, I un ideal de A, sea M un A-módulo finitamente generado y M' un submódulo, entonces existe un natural k tal que*

$$(I^n M) \cap M' = I^{n-k}((I^k M) \cap M'),$$

para todo $n \geq k$.

Combinando 4.13 con el teorema 4.10 obtenemos la versión más útil y clara de este resultado:

Teorema 4.15 *Sea A un anillo noetheriano, I un ideal de A, sea M un A-módulo finitamente generado y M' un submódulo de M. Entonces las filtraciones $\{I^n M'\}_n$ y $\{(I^n M) \cap M'\}_n$ tienen diferencias acotadas. En particular la topología I-ádica en M' es la restricción de la topología I-ádica en M.*

Ahora podemos aplicar el teorema 4.6 a las topologías I-ádicas:

Teorema 4.16 *Sea A un anillo noetheriano, $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de A-módulos finitamente generados e I un ideal de A. Entonces también es exacta la sucesión $0 \longrightarrow \hat{M}' \longrightarrow \hat{M} \longrightarrow \hat{M}'' \longrightarrow 0$ inducida sobre las compleciones I-ádicas.*

Recordemos que si consideramos las compleciones en términos de sucesiones de Cauchy, los homomorfismos dados por el teorema anterior son los inducidos de forma natural por los homomorfismos (continuos) de partida. Los razonamientos siguientes son mucho más simples si consideramos las compleciones en estos términos.

El homomorfismo natural $A \longrightarrow \hat{A}$ nos permite considerar a la compleción $\hat{A}$ como A-módulo, luego podemos formar el producto tensorial $\hat{A} \otimes_A M$ para cualquier A-módulo M. El homomorfismo natural $\phi : M \longrightarrow \hat{M}$ induce un homomorfismo

$$\hat{A} \otimes_A M \longrightarrow \hat{A} \otimes_A \hat{M} \longrightarrow \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M},$$

caracterizado por que $a \otimes m \mapsto a\phi(m)$.

Teorema 4.17 *Si A es un anillo, I es un ideal de A y M es un A-módulo finitamente generado, entonces el homomorfismo $\hat{A} \otimes_A M \longrightarrow \hat{M}$ es suprayectivo y si A es noetheriano entonces es un isomorfismo.*

Demostración: Es fácil definir un isomorfismo natural $\widehat{M \oplus M'} \cong \hat{M} \oplus \hat{M}'$. Si M es finitamente generado, podemos tomar un A-módulo libre $L \cong A^n$ y formar una sucesión exacta

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0.$$

Entonces $\hat{L} \cong \hat{A}^n \cong (\hat{A} \otimes_A A)^n \cong \hat{A} \otimes_A L$, y el isomorfismo es el natural. Tenemos el diagrama conmutativo

$$\begin{tikzcd}
& \hat{A} \otimes_A N \arrow[r] \arrow[d, "f"'] & \hat{A} \otimes_A L \arrow[r] \arrow[d, "g"'] & \hat{A} \otimes_A M \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & \hat{N} \arrow[r] & \hat{L} \arrow[r, "d"'] & \hat{M} \arrow[r] & 0
\end{tikzcd}$$

donde la fila superior es exacta por las propiedades del producto tensorial. Acabamos de probar que g es un isomorfismo y el teorema 4.6 nos da que la última fila sería exacta si en N consideramos la topología inducida por la topología I-ádica de L (que no podemos decir que sea la topología I-ádica sin la hipótesis de que A sea noetheriano). En cualquier caso, lo que sí podemos asegurar es que d es suprayectiva. Esto es suficiente para asegurar que h es suprayectiva. Si suponemos que A es noetheriano entonces la fila inferior es exacta. Además N es finitamente generado, luego f también es suprayectiva. Con estos datos, no es difícil obtener del diagrama que h es inyectiva. ∎

Con esto ya podemos demostrar las propiedades básicas de las compleciones I-ádicas de anillos noetherianos:

Teorema 4.18 *Sea A un anillo noetheriano e I un ideal de A. Entonces*

a) $\hat{I} = \hat{A}I \cong \hat{A} \otimes_A I$,

b) $\widehat{I^n} = \hat{I}^n$,

c) $A/I^n \cong \hat{A}/\hat{I}^n$ *y también* $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$,

d) $\hat{I}$ *está contenido en todos los ideales maximales de* $\hat{A}$.

Demostración: a) Como A es noetheriano, I es un A-módulo finitamente generado, y acabamos de probar que el homomorfismo $\hat{A} \otimes_A I \longrightarrow \hat{I}$, cuya imagen es $\hat{A}I$, es un isomorfismo.

b) El mismo razonamiento se aplica a I^n, con lo que

$$\widehat{I^n} = \hat{A}I^n = (\hat{A}I)^n = \hat{I}^n.$$

c) En la sección precedente hemos visto que $A/I^n \cong \hat{A}/\widehat{I^n}$, y aplicando b) tenemos la primera parte de c). La segunda es el caso particular que resulta de tomar $G = I^n$.

d) Si $x \in \hat{I}$, es claro que la sucesión $\{x^n\}_n$ tiende a 0 en $\hat{A}$, luego la serie que determina es convergente. Concretamente:

$$(1-x)^{-1} = 1 + x + x^2 + \cdots$$

Así pues, $1-x$ es una unidad de $\hat{A}$. Si M es un ideal maximal de $\hat{A}$, entonces $M + (1-x) = (1)$, luego $x \in M$. ∎

En particular tenemos que la compleción de la topología I-ádica de un A-módulo M es la topología $\hat{I}$-ádica en $\hat{M}$ (y también la topología I-ádica en $\hat{M}$, visto como A-módulo). Otra consecuencia sencilla es la siguiente:

Teorema 4.19 *Sea A un anillo noetheriano e I un ideal maximal de A. Entonces $\hat{A}$ es un anillo local con $\hat{I}$ como único ideal maximal.*

Demostración: Por el teorema anterior $\hat{A}/\hat{I} \cong A/I$, que es un cuerpo, luego $\hat{I}$ es un ideal maximal de $\hat{A}$. Como ha de estar contenido en todos los ideales maximales, ha de ser el único. ■

El teorema siguiente determina en qué condiciones la topología I-ádica es de Hausdorff:

Teorema 4.20 (Teorema de Krull) *Sea A un anillo noetheriano, I un ideal de A y M un A-módulo finitamente generado. El núcleo $H = \bigcap I^n M$ del homomorfismo $M \longrightarrow \hat{M}$ está formado por los elementos de M anulados por algún elemento del trasladado $1 + I$.*

Demostración: Como H es la intersección de todos los entornos de 0, su topología es trivial, es decir, no tiene más abiertos que $\varnothing$ y H. Por otra parte, hemos probado que su topología es la topología I-ádica. Como IH ha de ser abierto para esta topología, concluimos que $IH = H$. Como A es noetheriano, tenemos que H es un A-módulo finitamente generado. Pongamos que $H = \langle m_1, \ldots, m_r \rangle$. Por hipótesis

$$m_i = a_{i1} m_1 + \cdots + a_{ir} m_r,$$

para ciertos $a_{ij} \in I$. Si $B = (a_{ij})$ y $x = (m_i)$ tenemos que $x(I - B) = 0$. Multiplicando por la matriz adjunta vemos que $\det(I - B) m_i = 0$ para todo índice i, y claramente $\det(I - B) \in 1 + I$, luego todos los elementos de H anulan a un elemento de $1 + I$. Recíprocamente, si $m \in M$ cumple $(1 + a)m = 0$, con $a \in I$, entonces $m = am$ y, en general, $m = a^n m \in I^n M$ para todo natural n. ■

En particular, si A es un dominio íntegro (noetheriano) e I es un ideal de A, entonces la topología I-ádica en A es de Hausdorff. Otro caso de interés es el siguiente:

Teorema 4.21 *Sea A un anillo noetheriano e I un ideal contenido en todos los ideales maximales de A. Entonces la topología I-ádica en cualquier A-módulo finitamente generado es de Hausdorff.*

Demostración: Basta observar que todo $x \in 1 + I$ es una unidad, pues en caso contrario existiría un ideal maximal M de A tal que $x \in M$, pero $I \subset M$, luego $1 \in M$, contradicción. Así pues, los elementos de $1 + I$ no pueden anular a ningún elemento de ningún A-módulo. ■

En particular, si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, tenemos que la topología $\mathfrak{m}$-ádica en cualquier A-módulo finitamente generado es de Hausdorff.

Conviene enunciar una versión puramente algebraica del teorema anterior:

Teorema 4.22 *Sea A un anillo noetheriano e I un ideal contenido en todos los ideales maximales de A. Sea M un A-módulo finitamente generado y N un submódulo de M. Entonces*

$$\bigcap_{n=0}^{\infty} (N + I^n M) = N.$$

Demostración: Sea $M' = M/N$, que también es un A-módulo finitamente generado. Por el teorema anterior, la topología I-ádica en M' es de Hausdorff, lo cual equivale a que

$$\bigcap_{n=0}^{\infty}(I^n M') = 0.$$

De aquí se sigue inmediatamente la igualdad del enunciado. ■

En la demostración del teorema anterior se ve que, bajo sus hipótesis, todos los submódulos de M son cerrados (pues determinan cocientes de Hausdorff).

Ahora veremos la relación entre los procesos de localización y compleción. Consideremos un anillo noetheriano A y un ideal I. Entonces el conjunto $S = 1 + I$ es multiplicativo. Más aún, en el caso en que I es un ideal maximal entonces $S = S_I = A \setminus I$. Sea $\hat{A}$ la compleción de A respecto de la topología I-ádica.

Si $x \in I$, entonces la sucesión $\{x^n\}_n$ converge a 0 en $\hat{A}$, de donde se sigue la convergencia de la serie

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$$

Esto significa que el homomorfismo natural $i : A \longrightarrow \hat{A}$ transforma en unidades todos los elementos de S, luego podemos definir un homomorfismo natural $S^{-1}A \longrightarrow \hat{A}$.

Una fracción a/s está en el núcleo de este homomorfismo si y sólo si a está en el núcleo del homomorfismo $A \longrightarrow \hat{A}$. Según el teorema de Krull, esto sucede si y sólo si $as' = 0$, para cierto $s' \in S$, pero esto equivale a que $a/s = 0$.

Así pues, podemos considerar a $S^{-1}A$ como subanillo de $\hat{A}$. A través de esta identificación, el homomorfismo natural $A \longrightarrow S^{-1}A$ se identifica con el homomorfismo natural $A \longrightarrow \hat{A}$. Equivalentemente, tenemos $A \subset S^{-1}A \subset \hat{A}$.

Observemos que $I^n S^{-1}A = (S^{-1}I)^n$, luego la topología I-ádica en $S^{-1}A$ (que es la topología inducida en $S^{-1}A$ desde $\hat{A}$) es la topología $S^{-1}I$-ádica. Como la imagen de A en $\hat{A}$ es densa en $\hat{A}$, lo mismo le sucede a $S^{-1}A$, de donde podemos concluir que $\hat{A}$ es también la compleción de $S^{-1}A$ respecto de la topología $S^{-1}I$-ádica.

En particular, si $\mathfrak{m}$ es un ideal maximal de A, tenemos que la compleción $\hat{A}_{\mathfrak{m}}$ respecto de la topología $\mathfrak{m}$-ádica es también la compleción del anillo noetheriano local $A_{\mathfrak{m}}$.

Para terminar esta sección vamos a demostrar que la compleción de un anillo noetheriano respecto a una topología I-ádica es también un anillo noetheriano. Nuevamente nos apoyaremos en módulos graduados.

Definición 4.23 Sea I un ideal de un anillo A. Para cada natural $n \geq 0$ definimos $\operatorname{gr}_I^n(A) = I^n/I^{n+1}$ (entendiendo que $I^0 = A$). Consideraremos cada $\operatorname{gr}_I^n(A)$ como A/I-módulo de forma natural. Definimos el *anillo graduado* de I como

$$\operatorname{gr}_I(A) = \bigoplus_{n=0}^{\infty} \operatorname{gr}_I^n(A).$$

En principio $\mathrm{gr}_I(A)$ tiene una estructura natural de A/I-módulo, pero lo dotamos de estructura de anillo del modo siguiente:

Si $x = a + I^{m+1} \in \mathrm{gr}_I^m(A)$, $y = b + I^{n+1} \in \mathrm{gr}_I^n(A)$, definimos

$$x \cdot y = ab + I^{m+n+1} \in \mathrm{gr}_I^{m+n}(A).$$

Es inmediato que $x \cdot y$ no depende de la elección de los representantes a y b. Definimos el producto de dos elementos arbitrarios x, $y \in \mathrm{gr}_I(A)$ mediante

$$(x \cdot y)_n = \sum_{i+j=n} x_i \cdot y_j.$$

Es inmediato comprobar que $\mathrm{gr}_I(A)$ se convierte así en un anillo graduado.

Ejemplo La definición del anillo graduado de un ideal permite aplicar a anillos arbitrarios algunos conceptos y técnicas habituales en anillos de polinomios. La relación viene dada por el ejemplo siguiente: si $A = B[X_1, \ldots, X_n]$ es un anillo de polinomios y tomamos como ideal $I = (X_1, \ldots, X_n)$, entonces $A/I \cong B$ es el anillo de coeficientes y, más en general, el B-módulo $\mathrm{gr}_I^n(A)$ es isomorfo al B-submódulo de A formado por los monomios de grado n. Teniendo esto en cuenta es fácil ver que $\mathrm{gr}_I(A) \cong A$. ■

Si M es un A-módulo y $\{M_n\}_n$ es una filtración I-ádica, definimos

$$\mathrm{gr}_I(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1},$$

que se convierte en un $\mathrm{gr}_I(A)$-módulo graduado de forma obvia.

Teorema 4.24 *Sea A un anillo noetheriano e I un ideal de A. Entonces*

a) $\mathrm{gr}_I(A)$ *es noetheriano.*

b) $\mathrm{gr}_I(A)$ *y* $\mathrm{gr}_{\hat{I}}(\hat{A})$ *son isomorfos como anillos graduados.*

c) Si M es un A-módulo finitamente generado y $\{M_n\}_n$ es una filtración I-ádica estable, entonces $\mathrm{gr}_I(M)$ *es un* $\mathrm{gr}_I(A)$*-módulo finitamente generado.*

Demostración: a) Como A es noetheriano, I es finitamente generado. Pongamos que $I = (x_1, \ldots, x_r)$. Sea $\bar{x}_i$ la imagen de x_i en I/I^2. Entonces

$$\mathrm{gr}_I(A) = (A/I)[\bar{x}_1, \ldots, \bar{x}_r].$$

Como A/I es noetheriano, lo mismo le sucede a $\mathrm{gr}_I(A)$.

b) Dos anillos graduados son isomorfos si existe un isomorfismo de anillos entre ellos que transforma los elementos homogéneos de grado n de uno en los del otro. Los isomorfismos $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$ inducen obviamente un isomorfismo entre los anillos graduados correspondientes.

c) Existe un n_0 tal que $M_{n_0+r} = I^r M_{n_0}$ para todo natural r. Por lo tanto $\mathrm{gr}_I(M)$ está generado por los subgrupos $\mathrm{gr}_I^n(M) = M_n/M_{n+1}$, para $n \leq n_0$. Cada M_n es un A-módulo finitamente generado, luego M_n/M_{n+1} es un A/I-módulo finitamente generado, luego $\mathrm{gr}_I(M)$ es un $\mathrm{gr}_I(A)$-modulo finitamente generado. ■

Ahora necesitamos un resultado técnico:

Sean G y H dos grupos topológicos con sistemas fundamentales de entornos $\{G_n\}_n$ y $\{H_n\}_n$, respectivamente y sea $\phi : G \longrightarrow H$ un homomorfismo tal que $\phi[G_n] \subset H_n$ para todo n. Consideramos los grupos

$$\mathrm{gr}(G) = \bigoplus_{n=0}^{\infty} G_n/G_{n+1}, \quad \mathrm{gr}(H) = \bigoplus_{n=0}^{\infty} H_n/H_{n+1},$$

entre los cuales tenemos un homomorfismo $\mathrm{gr}(\phi) : \mathrm{gr}(G) \longrightarrow \mathrm{gr}(H)$ inducido por ϕ de forma natural. Por otra parte tenemos el homomorfismo $\hat{\phi} : \hat{G} \longrightarrow \hat{H}$ entre las compleciones. Vamos a probar que si $\mathrm{gr}(\phi)$ es inyectivo o suprayectivo, lo mismo le sucede a $\hat{\phi}$.

En efecto, tenemos el siguiente diagrama conmutativo con filas exactas:

$$\begin{tikzcd}
0 \arrow[r] & G_n/G_{n+1} \arrow[r] \arrow[d, "\mathrm{gr}^n(\phi)"] & G/G_{n+1} \arrow[r] \arrow[d, "\phi_{n+1}"'] & G/G_n \arrow[r] \arrow[d, "\phi_n"'] & 0 \\
0 \arrow[r] & H_n/H_{n+1} \arrow[r] & H/H_{n+1} \arrow[r] & H/H_n \arrow[r] & 0
\end{tikzcd}$$

Si $\mathrm{gr}(\phi)$ es inyectivo, tenemos que la flecha vertical izquierda es inyectiva. Obviamente ϕ_0 es inyectiva (pues G/G_0 y H/H_0 son triviales). Razonando por inducción, suponemos que ϕ_n es inyectiva y el diagrama nos permite probar que ϕ_{n+1} también lo es. Esto implica que $\hat{\phi}$ es inyectiva por el teorema 4.5.

Para la suprayectividad razonamos análogamente: si $h_{n+1} \in H/H_{n+1}$, tomamos $g_n \in G/G_n$ tal que $\phi_n(g_n)$ coincida con la imagen de h_{n+1}. Sea $g_{n+1} \in G/G_{n+1}$ una antiimagen en G/G_{n+1}, de modo que $\phi_{n+1}(g_{n+1})$ y h_{n+1} tienen la misma imagen. Esto implica que $\phi_{n+1}(g_{n+1}) - h_{n+1}$ es la imagen de un $h'_n \in H_n/H_{n+1}$, que a su vez tiene una antiimagen $g'_n \in G_n/G_{n+1}$. Sea g'_{n+1} su imagen en G/G_{n+1}. Entonces $\phi_{n+1}(g'_{n+1}) = \phi_{n+1}(g_{n+1}) - h_{n+1}$, luego $h_{n+1} = \phi_{n+1}(g_{n+1} - g'_{n+1})$. El teorema 4.5 implica entonces que $\hat{\phi}$ es suprayectiva. ■

Teorema 4.25 *Sea A un anillo, I un ideal de A, sea M un A-módulo y $\{M_n\}_n$ una filtración I-ádica. Supongamos que A es de Hausdorff y completo con la topología I-ádica y que M es de Hausdorff con la topología definida por la filtración. Entonces, si $\mathrm{gr}(M)$ es un $\mathrm{gr}_I(A)$-módulo finitamente generado, también M es un A-módulo finitamente generado.*

DEMOSTRACIÓN: Tomemos un generador de $\mathrm{gr}(M)$ formado por elementos homogéneos $\xi_1, \ldots, \xi_r$, de grados $k_1, \ldots, k_r$. Entonces $\xi_i = x_i + M_{k_i+1}$, con $x_i \in M_{k_i}$.

Sea L^i el módulo A con la filtración I-ádica estable dada por $L^i_n = I^{n-k_i}$ (entendiendo que $I^n = A$ si $n \leq 0$) y sea

$$L = \bigoplus_{i=1}^{r} L^i \cong A^r$$

con la filtración I-ádica estable definida por suma directa. Sea $\phi : L \longrightarrow M$ el homomorfismo de A-módulos que lleva la base canónica de L a los generadores de M. Así, los elementos de $L_n = L^1_n \oplus \cdots \oplus L^r_n$ se corresponden con elementos de M_n. Según las observaciones previas al teorema podemos formar los homomorfismos

$$\mathrm{gr}(\phi) : \mathrm{gr}(L) \longrightarrow \mathrm{gr}(M), \qquad \hat{\phi} : \hat{L} \longrightarrow \hat{M}.$$

Por construcción $\mathrm{gr}(\phi)$ es suprayectivo, luego $\hat{\phi}$ también lo es. Consideramos ahora el diagrama conmutativo siguiente:

$$\begin{tikzcd} L \arrow[r, "\phi"] \arrow[d] & M \arrow[d] \\ \hat{L} \arrow[r, "\hat{\phi}"'] & \hat{M} \end{tikzcd}$$

La topología de cada $L^i \cong A$ es la topología I-ádica, que es completa, luego L también es completo con la topología inducida por su filtración. Por el mismo motivo tiene la propiedad de Hausdorff, luego la flecha vertical izquierda es un isomorfismo. Como M tiene la propiedad de Hausdorff, la flecha vertical derecha es un monomorfismo. De aquí se sigue que ϕ es suprayectiva, luego $x_1, \ldots, x_r$ son un generador de M como A-módulo. ■

Teorema 4.26 *Bajo las hipótesis del teorema anterior, si* $\mathrm{gr}(M)$ *es un* $\mathrm{gr}_I(A)$*-módulo noetheriano, entonces M es un A-módulo noetheriano.*

DEMOSTRACIÓN: Hemos de probar que todo submódulo M' de M es finitamente generado- Sea $M'_n = M' \cap M_n$. Entonces $\{M'_n\}_n$ es una filtración I-ádica de M' y tenemos monomorfismos naturales $M'_n/M'_{n+1} \longrightarrow M_n/M_{n+1}$, que a su vez inducen un monomorfismo $\mathrm{gr}(M') \longrightarrow \mathrm{gr}(M)$. Como $\mathrm{gr}(M)$ es noetheriano, tenemos que $\mathrm{gr}(M')$ es finitamente generado, y también tiene la propiedad de Hausdorff, pues la intersección de los M'_n está contenida en la de los M_n. Por el teorema anterior M' es finitamente generado. ■

Teorema 4.27 *Si A es un anillo noetheriano e I es un ideal de A, entonces la compleción I-ádica $\hat{A}$ también es noetheriana.*

Demostración: Sabemos que $\mathrm{gr}_I(A) \cong \mathrm{gr}_{\hat{I}}(\hat{A})$. Aplicamos el teorema anterior al anillo $\hat{A}$ (de Hausdorff y completo) y al módulo $M = \hat{A}$ con la filtración $\{I^n\}_n$. Concluimos que $\hat{A}$ es un $\hat{A}$-módulo noetheriano, o sea, un anillo noetheriano. ■

Como caso particular, esto implica que si A es un anillo noetheriano, entonces el anillo de series formales de potencias $A[[X_1, \ldots, X_n]]$ también es noetheriano. Basta observar que es la compleción del anillo noetheriano $A[X_1, \ldots, X_n]$ respecto a la topología del ideal $I = (X_1, \ldots, X_n)$.

Otro resultado fundamental sobre compleciones es que si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, entonces la compleción $\hat{A}$ tiene la misma dimensión que A. Para demostrarlo veremos que la dimensión de A depende únicamente de los cocientes $A/\mathfrak{m}^n$, que ya sabemos que se conservan al pasar a la compleción. No obstante, esto no es trivial en absoluto. Los conceptos de las dos secciones siguientes son los primeros pasos para llegar a esta conclusión.

4.3 Anillos y módulos artinianos

Estudiamos aquí un concepto técnico que nos hará falta en la sección siguiente.

Definición 4.28 Un A-módulo M es *artiniano* si toda sucesión decreciente de submódulos

$$M_0 \supset M_1 \supset M_2 \supset \cdots$$

es finalmente constante. Es fácil ver que esto equivale a que toda familia no vacía de submódulos de M tiene un elemento minimal. Un anillo A es *artiniano* si lo es como A-módulo, es decir, si toda cadena decreciente de ideales es finalmente constante, o si toda familia no vacía de ideales tiene un elemento minimal.

En principio estas nociones parecen duales de las de anillos y módulos noetherianos y, en efecto, una serie de resultados básicos son válidos para ambas clases, pero en realidad la situación es muy diferente. Veremos que los anillos artinianos son los anillos noetherianos de dimensión 0, luego forman una clase muy particular de anillos, frente a la generalidad del concepto de anillo noetheriano.

Entre las propiedades básicas citadas tenemos la siguiente (que es válida igualmente para módulos noetherianos):

Teorema 4.29 *Sea $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de A-módulos. Entonces M es artiniano si y sólo si lo son M' y M''.*

Demostración: Supongamos que M es artiniano. Obviamente, una cadena descendente de submódulos de M' lo es también de M, luego si M es artiniano

M' también lo es. Similarmente, una cadena descendente de submódulos de M'' ha de ser de la forma

$$M_0/M'' \supset M_1/M'' \supset M_2/M'' \supset \cdots$$

La cadena de los "numeradores" se ha de estabilizar, luego lo mismo le sucede a la cadena dada.

Si M' y M'' son artinianos y tenemos una cadena descendente de submódulos de M, digamos

$$M_0 \supset M_1 \supset M_2 \supset \cdots$$

entonces las cadenas $\{M_n \cap M'\}_n$ y $\{(M_n + M')/M'\}_n$ se han de estabilizar para n suficientemente grande. Si

$$M_n \cap M' = M_{n+1} \cap M', \qquad (M_n + M')/M' = (M_{n+1} + M')/M',$$

entonces $M_n = M_{n+1}$, pues si $m \in M_n$ entonces $m + M' = m'' + M'$, para un $m'' \in M_{n+1}$, luego existe un $m' \in M'$ tal que $m = m' + m''$. Entonces $m' \in M' \cap M_n$, luego $m' \in M_{n+1}$, luego $m \in M_{n+1}$. Esto prueba que la cadena de partida se estabiliza. ■

Como consecuencia inmediata:

Teorema 4.30 *Si M y M' son A-módulos artinianos, también lo es $M \oplus M'$.*

Demostración: Basta considerar la sucesión exacta

$$0 \longrightarrow M \longrightarrow M \oplus M' \longrightarrow M' \longrightarrow 0.$$

■

Teorema 4.31 *Si A es un anillo artiniano y M es un A-módulo finitamente generado, entonces M es artiniano.*

Demostración: Si M tiene un generador con n elementos, por el teorema anterior A^n es artiniano, y existe un epimorfismo $A^n \longrightarrow M$, luego M también es artiniano. ■

Ahora vamos a estudiar los módulos que son a la vez artinianos y noetherianos. Conviene introducir algunos conceptos:

Definición 4.32 Diremos que un A-módulo M es *simple* si no tiene más submódulos que M y 0.

Tenemos una caracterización útil de los módulos simples:

Teorema 4.33 *Un A-módulo M no nulo es simple si y sólo si es isomorfo a un cociente $A/\mathfrak{m}$, para cierto ideal maximal $\mathfrak{m}$ de A.*

Demostración: Evidentemente un módulo de la forma $A/\mathfrak{m}$ es simple, al igual que todo módulo isomorfo a él. Por otra parte, si $M \neq 0$ es simple, tomemos $m \in M$, $m \neq 0$. Necesariamente $M = Am$, luego tenemos un epimorfismo $A \longrightarrow M$ dado por $a \mapsto am$. Su núcleo $\mathfrak{m}$ ha de ser un ideal maximal, o si no M no el cociente no sería simple. ■

Definición 4.34 Una *serie normal* en un A-módulo M es una sucesión de submódulos

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M.$$

El número l se llama *longitud* de la serie. Los cocientes M_{i+1}/M_i se llaman *factores* de la serie. Una *serie de composición* es una serie normal cuyos factores son módulos simples o, equivalentemente, una serie normal que no puede refinarse a otra de mayor longitud.

Un módulo M es *de longitud finita* si la longitud de todas sus series normales está acotada por un cierto número natural. El máximo de dichas longitudes se llama entonces *longitud* de M, y la representaremos por $l(M)$. Un anillo A es *de longitud finita* si lo es como A-módulo.

Observemos que en un módulo de longitud finita toda serie normal puede refinarse hasta una serie de composición.

Teorema 4.35 (Jordan-Hölder) *Si un módulo tiene una serie de composición entonces tiene longitud finita y todas las series de composición tienen la misma longitud.*

Demostración: Consideremos una serie de composición arbitraria:

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M.$$

Vamos a probar que cualquier otra serie normal tiene longitud menor o igual que l. Como la serie de partida es arbitraria, podremos concluir que todas las series de composición tienen la misma longitud.

Razonamos por inducción sobre l. Si $l = 0$ entonces $M = 0$ y el teorema es trivial. Si $l = 1$ entonces M es simple y tampoco hay nada que demostrar. Tomemos ahora $l > 1$ y supongamos que el teorema se cumple para módulos con una serie de composición de longitud menor que l. Sea

$$0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_r = M$$

una serie normal en M.

Si $N_{r-1} \subset M_{l-1}$ tenemos una serie de composición de M_{l-1} de longitud $l-1$ y una serie normal de longitud $r-1$, luego por hipótesis de inducción $r-1 \leq l-1$ y así $r \leq l$.

Por el contrario, si $N_{r-1} \not\subset M_{l-1}$ entonces $N_{r-1} + M_{l-1} = M$, pues M/M_{l-1} es simple. Entonces

$$M/M_{l-1} = (N_{r-1} + M_{l-1})/M_{l-1} \cong N_{r-1}/(N_{r-1} \cap M_{l-1}),$$

luego el último cociente es simple. Como M_{l-1} tiene una serie de composición de longitud $l-1$, la hipótesis de inducción nos da que en $N_{r-1} \cap M_{l-1}$ todas las series de composición tiene longitud a lo sumo $l-2$. Completando una de ellas con N_{r-1} vemos que este módulo tiene una serie de composición de longitud menor o igual que $l-1$. De nuevo por hipótesis de inducción llegamos a que $r-1 \leq l-1$. ■

Como consecuencia:

Teorema 4.36 *Un módulo tiene longitud finita si y sólo si es noetheriano y artiniano.*

DEMOSTRACIÓN: Una implicación es obvia. Si un A-módulo M es noetheriano y artiniano a la vez, podemos construir como sigue una serie de composición: Sea $M_0 = 0$, Si $M_0 \neq M$, tomamos como M_1 un submódulo minimal entre los submódulos que contienen estrictamente a M_0. Así M_1/M_0 es simple. Si $M_1 \neq M$, tomamos como M_2 un submódulo minimal entre los submódulos que contienen estrictamente a M_1, con lo que M_2/M_1 es simple. Como la serie

$$M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$$

no puede prolongarse indefinidamente, tras un número finito de pasos hemos de llegar a $M_n = M$ y así tenemos una serie de composición. ■

Teorema 4.37 *Consideremos una serie normal*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M.$$

en un módulo M. Entonces M tiene longitud finita si y sólo si la tienen todos los factores M_{i+1}/M_i, y en tal caso

$$l(M) = \sum_{i=0}^{l-1} l(M_{i+1}/M_i).$$

DEMOSTRACIÓN: Si M tiene longitud finita, podemos refinar la serie dada hasta una serie de composición, y entonces los módulos comprendidos entre cada M_i y M_{i+1} determinan una serie de composición del cociente M_{i+1}/M_i, con lo que todos ellos son de longitud finita y tenemos la relación entre las longitudes. Recíprocamente, si cada factor tiene longitud finita, tomamos una serie de composición de cada uno de ellos, con las cuales podemos extender la serie dada a una serie de composición de M. ■

De aquí se sigue en particular que la imagen por un homomorfismo de un módulo de longitud finita tiene también longitud finita. Así mismo es claro que la suma directa de un número finito de módulos de longitud finita tiene también longitud finita, y la longitud de la suma es la suma de las longitudes.

Teorema 4.38 *Un anillo $A \neq 0$ tiene longitud finita si y sólo si es noetheriano y* $\dim A = 0$.

Demostración: Si A tiene longitud finita es claramente noetheriano (si no lo fuera podríamos formar series normales de longitud arbitrariamente grande). Si $\mathfrak{p} \in \operatorname{Esp} A$, tenemos que $A/\mathfrak{p}$ tiene también longitud finita. Tomemos $a \in A/\mathfrak{p}$. Los ideales

$$(a) \supset (a^2) \supset (a^3) \supset \cdots$$

no pueden ser todos distintos, pues en tal caso darían lugar a series normales de longitud arbitrariamente grande. Así pues, $(a^n) = (a^{n+1})$ para algún n. Equivalentemente, existe un $b \in A/\mathfrak{p}$ tal que $a^n = ba^{n+1}$, de donde resulta que $a^n(1 - ab) = 0$. Como $\mathfrak{p}$ es primo, el cociente es un dominio íntegro, luego $ab = 1$, luego $A/\mathfrak{p}$ es un cuerpo y $\mathfrak{p}$ es, de hecho, maximal. Esto prueba que $\dim A = 0$.

Recíprocamente, si A es un anillo noetheriano de dimensión 0, entonces su radical nilpotente $I = \operatorname{rad} 0$ es finitamente generado, luego existe un natural n tal que $I^n = 0$. Las potencias de I forman una serie normal de A. Si demostramos que A/I tiene longitud finita, lo mismo será cierto para cada factor I^r/I^{r+1}, pues si $I^r = (a_1, \ldots, a_m)$, podemos definir un epimorfismo de A-módulos

$$\phi : (A/I)^m \longrightarrow I^r/I^{r+1}$$

mediante $\phi([x_1], \ldots, [x_m]) = [x_1a_1 + \cdots + x_ma_m]$.

El cociente A/I es también un anillo noetheriano de dimensión 0, pero además es reducido. Así pues, podemos suponer que A es reducido.

Que A tiene dimensión 0 significa que sus ideales primos son maximales, luego también son sus primos minimales, luego son un número finito, digamos $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Consideremos el homomorfismo de A-módulos

$$A \longrightarrow (A/\mathfrak{m}_1) \times \cdots \times (A/\mathfrak{m}_r)$$

dado por $a \mapsto ([a], \ldots, [a])$. Se cumple que es suprayectivo y su núcleo es

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \operatorname{rad} 0 = 0.$$

En efecto, esto es el teorema chino del resto en su versión más general. La prueba se basa en que si $i \neq j$ entonces $\mathfrak{m}_i + \mathfrak{m}_j = 1$, luego podemos expresar $1 = x_{ij} + y_{ij}$, con $x_{ij} \in \mathfrak{m}_i$, $y_{ij} \in \mathfrak{m}_j$. Así $x_{ij} \equiv 0 \ (\text{mód}\ \mathfrak{m}_i)$, $x_{ij} \equiv 1 \ (\text{mód}\ \mathfrak{m}_j)$.

Tomamos $x_j = \prod\limits_{i \neq j} x_{ij}$, de modo que

$$x_j \equiv \begin{cases} 1 \ (\text{mód}\ \mathfrak{m}_i) & \text{si } i = j, \\ 0 \ (\text{mód}\ \mathfrak{m}_i) & \text{si } i \neq j. \end{cases}$$

De este modo, si $([a_1], \ldots, [a_r]) \in (A/\mathfrak{m}_1) \times \cdots \times (A/\mathfrak{m}_r)$, una antiimagen en A viene dada por $a = a_1x_1 + \cdots + a_rx_r$. Todo lo demás es inmediato.

Tenemos así que A es isomorfo a una suma directa de r cuerpos. Estos cuerpos son A-módulos simples, de donde se sigue fácilmente que A tiene longitud r.

■

Aunque no nos va a hacer falta, vamos a probar por completitud que los anillos artinianos son noetherianos, tal y como habíamos anunciado. De este modo resulta que un anillo tiene longitud finita si y sólo si es artiniano.

Teorema 4.39 *Todo anillo artiniano es noetheriano.*

Demostración: Sea A un anillo artiniano. Entonces A tiene un número finito de ideales maximales. En efecto, si tuviera infinitos de ellos, digamos $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3, \ldots$ la sucesión de ideales

$$\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3 \supset \cdots$$

no se estabilizaría nunca, pues si $\mathfrak{m}_1 \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_{n+1}$, entonces tenemos que $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$ y, como los ideales maximales son primos, existe un $i \leq n$ tal que $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$, lo cual es absurdo.

Sea $I = \mathfrak{m}_1 \cdots \mathfrak{m}_r$ el producto de todos los ideales maximales de A. Por la propiedad de Artin existe un natural n tal que $I^n = I^{n+1}$. Vamos a probar que $I^n = 0$. En caso contrario, sea S el conjunto de todos los ideales J de A tales que $I^nJ \neq 0$. Tenemos que $I \in S$. Sea J un elemento minimal de S. Entonces existe un $x \in J$ tal que $I^n(x) \neq 0$, pero entonces $J = (x)$ por la minimalidad de J.

Ahora $(x)II^n = (x)I^{n+1} = (x)I \neq 0$ y $(x)I \subset (x)$, luego ha de ser $(x)I = (x)$. Así pues, existe un $y \in I$ tal que $xy = x$. Esto implica que $x = xy^m$ para todo m, pero $y \in I \subset \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \operatorname{rad}(0)$, luego $y^m = 0$ para cierto m, luego $x = 0$, contradicción.

Tenemos, pues, que $I^n = 0$. Consideremos ahora la cadena de ideales

$$A \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_r = I \supset I\mathfrak{m}_1 \supset \cdots \supset I\mathfrak{m}_1 \cdots \mathfrak{m}_r = I^2 \supset \cdots \supset I^n = 0.$$

Cada cociente de dos ideales consecutivos es un espacio vectorial sobre uno de los cuerpos $A/\mathfrak{m}_i$. El hecho de que A sea artiniano implica que cada uno de estos cocientes es un A-módulo artiniano, luego también es artiniano como $A/\mathfrak{m}_i$-espacio vectorial (pues los A-submódulos son los subespacios vectoriales). Es claro que un espacio vectorial es artiniano si y sólo si tiene dimensión finita, si y sólo si tiene longitud finita. Por lo tanto, los cocientes tienen longitud finita como espacios vectoriales, luego también como A-módulos, luego A tiene longitud finita por el teorema 4.37. En particular es noetheriano. ■

4.4 El polinomio de Hilbert

Si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, en esta sección vamos a definir una noción de dimensión de A que dependerá únicamente de los cocientes $A/\mathfrak{m}^n$. En particular será inmediato que A tiene la misma dimensión que su compleción $\mathfrak{m}$-ádica. Más adelante demostraremos que esta dimensión coincide con la usual.

Sea $A = \bigoplus_{n=0}^{\infty} A_n$ un anillo graduado noetheriano. Por el teorema 4.12 sabemos que A_0 es noetheriano y que A es finitamente generado sobre A_0, digamos $A = A_0[x_1, \ldots, x_r]$, donde los x_i podemos tomarlos homogéneos. Sea k_i el grado de x_i.

Sea ahora M un A-módulo graduado finitamente generado. Digamos que $M = \langle m_1, \ldots, m_s \rangle$, donde los m_i los tomamos también homogéneos. Sea l_i el grado de m_i.

Cada elemento de M_n es de la forma $\sum f_j(x) m_j$, donde $f_j(x)$ es un polinomio en $x_1, \ldots, x_r$ con coeficientes en A_0 homogéneo de grado $n - l_j$ (entendiendo que es nulo si $n < l_j$). Concluimos que M_n es un A_0-módulo finitamente generado, pues un sistema generador lo forman los elementos de la forma $f_j(x) m_j$, donde $f_j(x)$ recorre los monomios de grado $n - l_j$ con coeficiente 1.

Supongamos ahora que A_0 es artiniano, de modo que todos los módulos M_n son artinianos, y también noetherianos, luego tienen longitud finita. Definimos la *serie de Poincaré* de M como la serie de potencias formal

$$P(M, t) = \sum_{n=0}^{\infty} l(M_n) t^n \in \mathbb{Z}[[t]].$$

Teorema 4.40 *En las condiciones anteriores, existe un polinomio $f(t) \in \mathbb{Z}[t]$ tal que*

$$P(M, t) = \frac{f(t)}{\prod_{i=1}^{r} (1 - t^{k_i})}.$$

Demostración: Lo probamos por inducción sobre r. Si $r = 0$ esto significa que $A = A_0$, luego $A_n = 0$ para todo $n > 0$. Entonces M es un A_0-módulo finitamente generado, lo cual obliga a que $M_n = 0$ para n grande. Por consiguiente $P(M, t)$ es un polinomio con coeficientes enteros.

Supongamos el teorema para $r - 1$. La multiplicación por x_r es un homomorfismo de A_0-módulos $M_n \longrightarrow M_{n+k_r}$. Formemos una sucesión exacta

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_r} M_{n+k_r} \longrightarrow L_{n+k_r} \longrightarrow 0.$$

Observemos que todos los módulos tienen longitud finita. Sean

$$K = \bigoplus_{n=0}^{\infty} K_n, \qquad L = \bigoplus_{n=k_r}^{\infty} L_n$$

Entonces K es el A-submódulo de M formado por los elementos anulados por x_r y L es el A-módulo cociente de M sobre la imagen de la multiplicación por x_r. Como A es noetheriano ambos son finitamente generados. Además, ambos módulos son anulados por x_r, luego ambos son $A_0[x_1, \ldots, x_{r-1}]$-módulos, también finitamente generados (observemos que este anillo es un subanillo graduado de A).

Del teorema 4.37 se sigue en particular que $l(M/N) = l(M) - l(N)$, lo cual, aplicado a la sucesión exacta anterior, se traduce en que

$$l(K_n) - l(M_n) + l(M_{n+k_r}) - l(L_{n+k_r}) = 0.$$

Multiplicando por t^{n+k_s} y sumando respecto de n obtenemos que

$$(1 - t^{k_s})P(M,t) = P(L,t) - t^{k_s}P(K,t) + g(t), \tag{4.1}$$

donde $g(t) \in \mathbb{Z}[t]$. Aplicando la hipótesis de inducción a $P(L,t)$ y $P(K,t)$ concluimos que $P(M,t)$ tiene la forma requerida. ■

Definimos $D(M)$ como el orden del polo de $P(M,t)$ en $t = 1$. Hay un caso que es particularmente simple:

Teorema 4.41 *En las condiciones anteriores, supongamos que $k_i = 1$ para todo i y sea $D(M) = d$. Entonces existe un polinomio $g(t) \in \mathbb{Q}[t]$ de grado*[1] *$d-1$ tal que para todo n suficientemente grande se cumple $l(M_n) = g(n)$.*

Demostración: Por el teorema anterior tenemos que $l(M_n)$ es el coeficiente de t^n en la serie $f(t)(1-t)^{-r}$. Cancelando potencias de $1-t$ podemos suponer que $r = d$ y que $f(1) \neq 0$. Pongamos que

$$f(t) = \sum_{n=0}^{N} a_n t^n.$$

Trabajando en el cuerpo $\mathbb{Z}((t))$, es fácil obtener el desarrollo en serie de Taylor

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

Esto es válido para $d = 0$ si convenimos que $\binom{-1}{-1} = 1$ y $\binom{n}{-1} = 0$ para $n \geq 0$.

Por consiguiente, si $n \geq N$,

$$l(M_n) = \sum_{k=0}^{N} a_k \binom{d+n-k-1}{d-1}.$$

Cada número combinatorio es un polinomio en n de grado $d-1$ y coeficiente director $1/(d-1)!$ Por lo tanto, la expresión completa es un polinomio en n de grado $d-1$ con coeficiente director

$$\frac{\sum\limits_{k=0}^{N} a_k}{(d-1)!} = \frac{f(1)}{(d-1)!} \neq 0.$$

■

[1] Convenimos en que el grado del polinomio nulo es -1.

Ahora conviene hacer una observación sobre una variante del argumento empleado en la demostración de 4.40. En lugar de considerar la multiplicación por x_r, consideremos la multiplicación por un elemento arbitrario $x \in A_k$ que no anule a ningún elemento de M, es decir, tal que si $xm = 0$ necesariamente $x = 0$. Entonces el módulo K construido en la demostración es nulo y $L = M/xM$.

La ecuación (4.1) se convierte en

$$(1 - t^k)P(M, t) = P(L, t) + g(t),$$

de donde concluimos que $D(L) = D(M) - 1$. En resumen:

Teorema 4.42 *En las condiciones del teorema* 4.40, *si $x \in A$ es un elemento homogéneo que no anula a ningún elemento de M, se cumple que*

$$D(M/xM) = D(M) - 1.$$

Ejemplo Veamos el ejemplo más sencillo de serie de Poincaré: Consideramos un anillo artiniano A_0 y el anillo de polinomios $A = A_0[X_1, \ldots, X_r]$, considerado como A-módulo graduado. Entonces como generadores de A podemos tomar $X_1, \ldots, X_r$, todos de grado 1, y como generadores de $M = A$ como A-módulo tomamos $m = 1$. El módulo M_n es el grupo de los polinomios homogéneos de grado n, que es un A_0-módulo libre con una base formada por todos los monomios de grado n (con coeficiente 1).

El teorema 4.37 implica que la longitud de una suma directa es igual a la suma de las longitudes de los sumandos, luego la longitud de un A_0-módulo libre es igual a su rango por $l(A_0)$. En nuestro caso,[2]

$$l(M_n) = \binom{r + n - 1}{r - 1} l(A_0).$$

Por consiguiente

$$P(M, t) = \sum_{n=0}^{\infty} l(M_n)t^n = \sum_{n=0}^{\infty} \binom{r + n - 1}{r - 1} l(A_0)t^n = \frac{l(A_0)}{(1 - t)^r}.$$

En particular, $D(A_0[X_1, \ldots, X_r]) = r$. ■

Veamos cómo se relaciona todo esto con la dimensión de un anillo noetheriano local. Para ello conviene introducir un nuevo concepto:

Definición 4.43 Si A es un anillo, diremos que un ideal $\mathfrak{q} \subsetneq A$ es *primario* si los divisores de cero en $A/\mathfrak{q}$ son nilpotentes. Equivalentemente, $\mathfrak{q}$ es primario si cuando $ab \in \mathfrak{q}$ y $a \notin \mathfrak{q}$, existe un natural n tal que $b^n \in \mathfrak{q}$.

[2]El número de monomios de grado n en r indeterminadas es el número CR_r^n de combinaciones con repetición de r elementos tomados de n en n, es decir, el número de formas de escribir n números entre 1 y r con repeticiones y sin que importe el orden. Para calcularlo basta observar que tales combinaciones pueden dividirse en dos clases: las que contienen alguna r, que son CR_r^{n-1}, y las que no contienen ninguna r, que son CR_{r-1}^n. A partir de la relación $CR_r^n = CR_r^{n-1} + CR_{r-1}^n$, una simple inducción sobre $n + r$ da el valor indicado.

Es claro que los ideales primos son primarios, pero el concepto de ideal primario es más general. Observemos que si $\mathfrak{q}$ es primario y $\mathfrak{p} = \operatorname{rad}\mathfrak{q}$, entonces $\mathfrak{p}$ es un ideal primo. En efecto, si $ab \in \mathfrak{p}$, entonces existe un natural n tal que $a^n b^n \in \mathfrak{q}$. Si $a^n \notin \mathfrak{q}$, entonces existe un natural m tal que $b^{nm} \in \mathfrak{q}$. En cualquier caso, o bien $a \in \mathfrak{p}$ o bien $b \in \mathfrak{p}$.

Diremos que $\mathfrak{q}$ es $\mathfrak{p}$-*primario* si es primario y $\mathfrak{p} = \operatorname{rad}\mathfrak{q}$.

Teorema 4.44 *Sea A un anillo, $\mathfrak{m}$ un ideal maximal de A y $\mathfrak{q}$ un ideal arbitrario. Las afirmaciones siguientes son equivalentes:*

a) *$\mathfrak{q}$ es $\mathfrak{m}$-primario.*

b) $\operatorname{rad}\mathfrak{q} = \mathfrak{m}$.

c) *$\mathfrak{m}$ es el único divisor primo minimal de $\mathfrak{q}$.*

DEMOSTRACIÓN: Sólo hay que probar que c) $\Rightarrow$ a). El anillo $A/\mathfrak{p}$ tiene a $\mathfrak{m}/\mathfrak{q}$ como único ideal primo. Los elementos de $\mathfrak{m}/\mathfrak{q}$ son nilpotentes y los que no están en $\mathfrak{m}/\mathfrak{q}$ son unidades, luego ciertamente $\mathfrak{q}$ es primario y su radical es obviamente $\mathfrak{m}$. ■

En particular, si $\mathfrak{m}$ es un ideal maximal en un anillo A, sus potencias son $\mathfrak{m}$-primarias. Más en general, si un ideal $\mathfrak{q}$ cumple $\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$, entonces $\mathfrak{q}$ es $\mathfrak{m}$-primario, pues si $\mathfrak{p}$ es un ideal primo tal que $\mathfrak{q} \subset \mathfrak{p}$, entonces $\mathfrak{m}^n \subset \mathfrak{p}$ y $\mathfrak{m} = \mathfrak{p}$. Si $\mathfrak{m}$ es finitamente generado es claro que se cumple el recíproco: para cada ideal $\mathfrak{m}$-primario $\mathfrak{q}$ existe un número natural n tal que $\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$.

Teorema 4.45 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario. Sea M un A-módulo finitamente generado y $\{M_n\}_n$ una filtración $\mathfrak{q}$-ádica estable. Entonces:*

a) *Los módulos M/M_n tienen longitud finita.*

b) *Existe un polinomio $g(X) \in \mathbb{Q}[X]$ tal que para todo n suficientemente grande se cumple que $l(M/M_n) = g(n)$. Además el grado de g es menor o igual que el número de elementos de cualquier sistema generador de $\mathfrak{q}$.*

c) *El grado y el coeficiente director de $g(X)$ dependen de M y $\mathfrak{q}$, pero no de la filtración.*

DEMOSTRACIÓN: Consideremos el anillo graduado de $\mathfrak{q}$, es decir,

$$\operatorname{gr}_I(A) = \bigoplus_{n=0}^{\infty} \mathfrak{q}^n/\mathfrak{q}^{n+1},$$

así como el $\operatorname{gr}_I(A)$-módulo graduado asociado a la filtración

$$\operatorname{gr}(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}.$$

El anillo $\mathrm{gr}_I^0(A) = A/\mathfrak{q}$ es noetheriano y tiene dimensión 0, pues su único ideal primo es $\mathfrak{m}/\mathfrak{q}$. El teorema 4.38 implica que es artiniano. Por 4.24 sabemos que $\mathrm{gr}(M)$ es un $\mathrm{gr}_I(A)$-módulo finitamente generado, luego estamos en la situación discutida al principio de esta sección y, en particular, los módulos M_n/M_{n+1} tienen longitud finita. Esto implica que M/M_n también es de longitud finita y

$$l(M/M_n) = \sum_{r=1}^{n} l(M_{r-1}/M_r).$$

Sea $\mathfrak{q} = (x_1, \ldots, x_r)$. Si llamamos $\bar{x}_i = x_i + \mathfrak{q}^2 \in \mathrm{gr}_I^1(A)$, entonces es claro que $\mathrm{gr}_I(A) = (A/\mathfrak{q})[\bar{x}_1, \ldots, \bar{x}_r]$.

Teniendo en cuenta la expresión para $P(\mathrm{gr}(M), t)$ (donde hemos de considerar $k_i = 1$), tenemos que $d = D(\mathrm{gr}(M)) \leq r$. También podemos aplicar el teorema 4.41, que nos da un polinomio $f(X) \in \mathbb{Q}[X]$ de grado $\leq r-1$ tal que si n es suficientemente grande entonces

$$l(M_n/M_{n+1}) = f(n).$$

Por consiguiente $l(M/M_{n+1}) - l(M/M_n) = f(n)$. Sumando obtenemos que

$$l(M/M_n) = \sum_{k=1}^{n-1} f(k) + c,$$

donde c es una constante que corrige el hecho de que la igualdad anterior no tiene por qué cumplirse para los primeros valores de n. Ahora bien, el miembro derecho es un polinomio de grado $\leq r$ (una unidad más que el grado de f). Basta probarlo en el caso en que $f(X) = X^m$, pero entonces el polinomio buscado viene dado por las fórmulas de Bernoulli para las sumas de potencias.

Por último consideremos otra filtración estable $\{M'_n\}_n$ y consideremos el polinomio que cumple $g'(n) = l(M/M'_n)$ para n grande. Por el teorema 4.10 sabemos que existe un número natural n_0 tal que $M'_{n+n_0} \subset M_n$ y $M_{n+n_0} \subset M'_n$. Esto implica que $g'(n+n_0) \geq g(n)$ y $g(n+n_0) \geq g'(n)$.

El grado de $g(n)$ es el mismo que el de $g(n+n_0)$, y ha de ser mayor o igual que el de $g'(n)$ porque el cociente $g(n+n_0)/g'(n) \geq 1$ no tiende a 0. Igualmente obtenemos la desigualdad contraria, luego ambos polinomios tienen el mismo grado. Por consiguiente existe

$$\lim_{n\to+\infty} \frac{g(n)}{g'(n)} = \lim_{n\to+\infty} \frac{g(n+n_0)}{g'(n)} + \lim_{n\to+\infty} \frac{g(n)-g(n+n_0)}{g'(n)} \geq 1,$$

pues el último límite es 0. Invirtiendo los papeles obtenemos la desigualdad contraria, luego el límite es 1 y los coeficientes directores coinciden. ■

Definición 4.46 Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal, sea $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario y M un A-módulo finitamente generado. Llamaremos *polinomio característico* del ideal $\mathfrak{q}$ respecto al módulo M al único polinomio $\chi_{\mathfrak{q}}^M(X) \in \mathbb{Q}[X]$ tal que para todo natural n suficientemente grande se cumple

$$l(A/\mathfrak{q}^n M) = \chi_{\mathfrak{q}}^M(n).$$

Sabemos que el grado de $\chi_{\mathfrak{q}}^M(X)$ es menor o igual que el número de elementos de cualquier sistema generador de $\mathfrak{q}$.

Representaremos por $\chi_{\mathfrak{q}}(X)$ al polinomio correspondiente a $M = A$, es decir, al polinomio que cumple

$$l(A/\mathfrak{q}^n) = \chi_{\mathfrak{q}}(n),$$

para todo natural n suficientemente grande.

Teorema 4.47 *Si A es un anillo noetheriano local, $\mathfrak{m}$ su ideal maximal y $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario, entonces el grado del polinomio característico $\chi_{\mathfrak{q}}(X)$ no depende de $\mathfrak{q}$.*

Demostración: Basta probar que su grado coincide con el de $\chi_{\mathfrak{m}}(X)$. Existe un natural m tal que $\mathfrak{m}^m \subset \mathfrak{q} \subset \mathfrak{m}$. Para todo natural n tenemos entonces que $\mathfrak{m}^{mn} \subset \mathfrak{q}^n \subset \mathfrak{m}^n$, luego si n es suficientemente grande se cumple que

$$\chi_{\mathfrak{m}}(n) \leq \chi_{\mathfrak{q}}(n) \leq \chi_{\mathfrak{m}}(mn).$$

Formando cocientes y haciendo tender n a infinito vemos que los grados han de coincidir. ■

Definición 4.48 Si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, definimos $d(A)$ como el grado del polinomio $\chi_{\mathfrak{m}}(X)$.

Sabemos que es menor o igual que el número de generadores de cualquier ideal $\mathfrak{m}$-primario de A y por definición sólo depende de los módulos $A/\mathfrak{m}^n$, luego, en particular, tenemos que $d(A) = d(\hat{A})$, donde $\hat{A}$ es la compleción de A respecto a la topología $\mathfrak{m}$-ádica. En la sección siguiente demostraremos que $d(A) = \dim A$, con lo que en particular habremos demostrado que la dimensión se conserva con las compleciones.

Terminamos con una observación. El polinomio $\chi_{\mathfrak{q}}(X)$ es el construido en el teorema 4.45 para el módulo $\mathrm{gr}_{\mathfrak{q}}(A)$, y en la prueba hemos visto que su grado es una unidad mayor que el grado del polinomio dado por el teorema 4.41, cuyo grado era precisamente $D(\mathrm{gr}_{\mathfrak{q}}(A)) - 1$. En definitiva, tenemos que

$$d(A) = D(\mathrm{gr}_{\mathfrak{q}}(A)).$$

Explícitamente, $d(A)$ es el orden del polo $t = 1$ en la serie de Poincaré

$$P(\mathrm{gr}_{\mathfrak{q}}(A), t) = \sum_{n=0}^{\infty} l(\mathfrak{q}^n/\mathfrak{q}^{n+1})t^n.$$

4.5 El teorema de la dimensión

En esta sección demostraremos que si A es un anillo noetheriano local, entonces la dimensión $d(A)$ que acabamos de introducir coincide con la dimensión de Krull $\dim A$. Más aún, probaremos una tercera equivalencia de interés que pasamos a precisar ahora:

Definición 4.49 Si A es un anillo y M es un A-módulo finitamente generado, representaremos por $\mu(M)$ el menor natural m tal que M admite un sistema generador con m elementos. A los sistemas generadores con $\mu(M)$ elementos los llamaremos *sistemas generadores minimales.*

Es evidente que si a un generador minimal de un módulo le quitamos un elemento, deja de ser generador, pero un generador con esta propiedad no tiene por qué ser minimal. Por ejemplo, $\{2,3\}$ es un generador de $\mathbb{Z}$ como $\mathbb{Z}$-módulo, y no podemos eliminar ninguno de sus elementos, pero no es un generador minimal. Observemos que $\mu(M)$ generaliza a la dimensión de un módulo libre:

Teorema 4.50 *Si M es un A-módulo libre de rango finito, entonces los generadores minimales de M son sus bases, luego $\mu(M)$ es el rango de M.*

Demostración: Podemos suponer que $M = A^n$. Sea $\{b_1, \ldots, b_m\}$ un generador minimal. Entonces $m \leq n$ y tenemos un epimorfismo $f : A^n \longrightarrow A^n$ que transforma los primeros elementos de la base canónica en los b_i y anula a los restantes. Por otra parte, podemos definir $f' : A^n \longrightarrow A^n$ asignando a cada vector de la base canónica una antiimagen por f. De este modo $f' \circ f = 1$. Las matrices de f y f' respecto a la base canónica tienen por producto a la identidad, luego su determinante tiene que ser una unidad de A, luego f y f' son isomorfismos, lo que implica que $m = n$ y que el sistema generador es una base. ■

Si A es un anillo noetheriano, tenemos definido $\mu(I)$ para todos los ideales I de A. Si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, definimos

$$\delta(A) = \text{mín}\{\mu(\mathfrak{q}) \mid \mathfrak{q} \text{ es un ideal } \mathfrak{m}\text{-primario}\}.$$

En la sección anterior hemos demostrado que $d(A) \leq \delta(A)$. El teorema de la dimensión afirma que en realidad $d(A) = \delta(A) = \dim A$. El primer paso en esta dirección es recordar el omnipresente lema de Nakayama:

Teorema 4.51 (Lema de Nakayama) *Sea A un anillo e I un ideal contenido en todos los ideales maximales de A. Sea M un A-módulo arbitrario, sea $N \subset M$ un submódulo tal que M/N sea finitamente generado. Si $M = N + IM$, entonces $M = N$.*

Demostración: Sea $\overline{M} = M/N$ y consideremos un sistema generador $m_1, \ldots, m_t$ tal que t sea el mínimo posible. Supongamos que $t > 0$ (es decir, que $\overline{M} \neq 0$). Como $\overline{M} = I\overline{M}$, podemos expresar

$$m_t = \sum_{j=1}^{t} a_j m_j, \qquad a_j \in I.$$

El hecho de que a_t pertenezca a todos los ideales maximales de A implica que $1 - a_t$ es una unidad de A, pero

$$(1 - a_t)m_t = \sum_{j=1}^{t-1} a_j m_j,$$

luego $m_t \in \langle m_1, \ldots, m_{t-1} \rangle$, en contradicción con la minimalidad de t. ■

Nota Un caso particular de interés se da cuando $N = 0$, en cuyo caso la hipótesis es que $M = IM$ es finitamente generado y la conclusión es que $M = 0$. La condición $M = IM$ equivale a $M \otimes_A (A/I) = 0$, pues si se cumple esto entonces la sucesión exacta

$$I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

da lugar a la sucesión exacta

$$M \otimes_A I \longrightarrow M \longrightarrow 0,$$

que implica que $M = IM$. (El recíproco se prueba similarmente.) ■

Con esto podemos caracterizar el número de generadores minimales de un módulo sobre un anillo local:

Teorema 4.52 *Sea A un anillo local, sea $\mathfrak{m}$ su ideal maximal, sea $k = A/\mathfrak{m}$ el cuerpo de restos y sea M un A-módulo finitamente generado. Consideremos $m_1, \ldots, m_t \in M$. Las afirmaciones siguientes son equivalentes:*

a) $M = \langle m_1, \ldots, m_t \rangle$.

b) El k-espacio vectorial $M/\mathfrak{m}M$ está generado por las clases $\bar{m}_1, \ldots, \bar{m}_t$.

Por consiguiente, $\mu(M) = \dim_k(M/\mathfrak{m}M)$.

Demostración: De b) se sigue que $M = \langle m_1, \ldots, m_t \rangle + \mathfrak{m}M$ y el Lema de Nakayama implica entonces a). El recíproco es obvio. ■

Como consecuencia, en el caso de un anillo local, los generadores minimales sí coinciden con los generadores minimales respecto de la inclusión.

Necesitamos un teorema técnico que generaliza a 3.51:

Teorema 4.53 *Sea A un anillo noetheriano y sean $J \subset I$ dos ideales tales que $V(I) = V(J)$. Sea $\mu(I/J) = m$. Supongamos que $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \operatorname{Esp} A$ cumplen que $I \not\subset \mathfrak{p}_j$, para $j = 1, \ldots, s$. Entonces existen elementos $a_1, \ldots, a_m \in I$ tales que:*

a) $I = (a_1, \ldots, a_m) + J$,

b) $a_i \notin \mathfrak{p}_j$ *para todo* $j = 1, \ldots, s$, $i = 1, \ldots m$,

c) si $\mathfrak{p} \in V(a_1, \ldots, a_m)$ *y* $\mathfrak{p} \notin V(I)$, *entonces* $\operatorname{alt} \mathfrak{p} \geq m$.

Demostración: Vamos a construir inductivamente $a_1, \ldots, a_r \in I$ de modo que se cumplan las propiedades siguientes:

a) $a_i \notin \mathfrak{p}_j$ para todo i, j.

b) $\{a_1 + J, \ldots, a_r + J\}$ puede extenderse hasta un generador minimal de I/J.

c) Si $\mathfrak{p} \in V(a_1, \ldots, a_r)$ y $\mathfrak{p} \notin V(I)$, entonces $\operatorname{alt} \mathfrak{p} \geq r$.

Supongámoslos construidos para un $r < m$ (tal vez $r = 0$). Tomemos un $a \in I$ arbitrario tal que $\{a_1 + J, \ldots, a_r + J, a + J\}$ forme parte de un generador minimal de I/J. Llamemos $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ a los divisores primos minimales de $(a_1, \ldots, a_r)$ que no pertenecen a $V(I)$, y sea X el conjunto de los elementos maximales respecto a la inclusión del conjunto $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_t, \mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Descompongamos $X = X_1 \cup X_2$, donde X_1 contiene los primos tales que $a \in \mathfrak{p}$ y X_2 a los que cumplen $a \notin \mathfrak{p}$.

Como $V(I) = V(J)$, tenemos que $J \not\subset \mathfrak{p}$ para todo $\mathfrak{p} \in X$. Por 3.51 existe un $b \in J$ tal que $b \notin \mathfrak{p}$ para todo $\mathfrak{p} \in X$. Igualmente, existe

$$\lambda \in \bigcap_{\mathfrak{p} \in X_2} \mathfrak{p}, \quad \lambda \notin \bigcup_{\mathfrak{p} \in X_1} \mathfrak{p},$$

pues si la intersección estuviera contenida en un primo de X_1, también lo estaría el producto de los ideales de X_2, y tendríamos un ideal de X_2 contenido en otro de X_1.

Tomamos $a_{r+1} = a + \lambda b$. Entonces $a_{r+1} \notin \mathfrak{p}$ para todo $\mathfrak{p} \in X$, luego en particular $a_{r+1} \notin \mathfrak{p}_j$ para todo j. Como $a_{r+1} \equiv a \ (\text{mód } J)$, el conjunto $\{a_1 + J, \ldots, a_r + J, a_{r+1} + J\}$ forma parte de un sistema generador minimal de I/J.

Por último, si $\mathfrak{p} \in V(a_1, \ldots, a_{r+1}) \setminus V(I)$, entonces $\mathfrak{p}$ contiene a uno de los primos $\mathfrak{q}_i$, que cumple $\operatorname{alt} \mathfrak{q}_i \geq r$ y, por otra parte, $a_{r+1} \in \mathfrak{p} \setminus \mathfrak{q}_i$, luego $\operatorname{alt} \mathfrak{p} \geq r + 1$. ■

Ahora ya podemos relacionar la dimensión de Krull con el número de generadores minimales:

Teorema 4.54 *Sea A un anillo noetheriano y $\mathfrak{p} \in \operatorname{Esp} A$ un ideal de altura m. Entonces existen $a_1, \ldots, a_m \in \mathfrak{p}$ tales que $\mathfrak{p}$ es un divisor primo minimal de $(a_1, \ldots, a_m)$.*

DEMOSTRACIÓN: Tomamos $I = \mathfrak{p}$ y $J = \mathfrak{p}^2$. Entonces $A_\mathfrak{p}$ es un anillo local con ideal maximal $\mathfrak{m} = S_\mathfrak{p}^{-1}\mathfrak{p}$. Sea $k = A_\mathfrak{p}/\mathfrak{m}$. Por 4.52 tenemos que

$$\mu(\mathfrak{p}/\mathfrak{p}^2) \geq \mu(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = \mu(\mathfrak{m}) \geq \dim A_\mathfrak{p} = \operatorname{alt} \mathfrak{p} = m.$$

Sean $a_1, \ldots, a_m \in \mathfrak{p}$ según el teorema anterior. Entonces $\mathfrak{p}$ es un divisor primo minimal de $(a_1, \ldots, a_m)$, pues en caso contrario podríamos tomar un ideal $\mathfrak{p}' \in \operatorname{Esp} A$ tal que

$$(a_1, \ldots, a_m) \subset \mathfrak{p}' \subsetneq \mathfrak{p}.$$

El teorema anterior implica entonces que $\operatorname{alt} \mathfrak{p}' \geq m$, pero entonces sería $\operatorname{alt} \mathfrak{p} > m$, en contra de lo supuesto. ■

En particular, si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, tenemos que $\dim A = \operatorname{alt} \mathfrak{m}$. El teorema anterior nos da elementos $a_1, \ldots, a_m \in \mathfrak{m}$ tales que $\mathfrak{m}$ es un divisor primo minimal del ideal $\mathfrak{q} = (a_1, \ldots, a_m)$ (y obviamente el único), luego $\mathfrak{q}$ es $\mathfrak{m}$-primario y concluimos que

$$\delta(A) \leq \mu(\mathfrak{q}) \leq m = \dim A.$$

Sólo nos falta demostrar que $\dim A \leq d(A)$. Veamos un resultado previo:

Teorema 4.55 *Sea A un anillo noetheriano local y sea $\mathfrak{m}$ su ideal maximal. Si $x \in A$ no es un divisor de cero, entonces $d(A/(x)) \leq d(A) - 1$.*

DEMOSTRACIÓN: Sean los A-módulos $N = (x) = xA$ y $M = A/(x)$. Observemos que $A/(x)$ es también un anillo noetheriano local cuyo ideal maximal es $(\mathfrak{m} + (x))/(x) = \mathfrak{m}M$. Sea $N_n = N \cap \mathfrak{m}^n$. Por el teorema 4.13 sabemos que $\{N_n\}_n$ es una filtración $\mathfrak{m}$-ádica estable de N, luego 4.45 nos da un polinomio $g(X)$ tal que $l(N/N_n) = g(n)$ para todo n suficientemente grande.

Consideremos la sucesión exacta

$$0 \longrightarrow N/N_n \longrightarrow A/\mathfrak{m}^n \longrightarrow M/\mathfrak{m}^n M \longrightarrow 0,$$

de la que deducimos que

$$g(n) - \chi_{\mathfrak{m}}(n) + \chi_{\mathfrak{m}}^M(n) = 0,$$

siempre para n suficientemente grande. La hipótesis sobre x implica que A y N son isomorfos como A-módulos, luego la unicidad del teorema 4.45 implica que los polinomios $g(X)$ y $\chi_{\mathfrak{m}}(X)$ tienen el mismo grado y el mismo coeficiente director, luego el grado de $\chi_{\mathfrak{m}}^M(X)$ es al menos una unidad menor. Estos grados son las dimensiones consideradas en el enunciado. ■

Teorema 4.56 (Teorema de la dimensión) *Si A es un anillo noetheriano local, entonces* $\dim A = d(A) = \delta(A)$.

DEMOSTRACIÓN: Sólo nos falta demostrar la desigualdad $\dim A \leq d(A)$. La probamos por inducción sobre $d = d(A)$. Si $d = 0$ esto significa que $l(A/\mathfrak{m}^n)$ es constante para todo n suficientemente grande. En particular, un $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ tiene longitud 0, lo que significa que $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. El lema de Nakayama implica entonces que $\mathfrak{m}^n = 0$. Si $\mathfrak{p}$ es un ideal primo de A, tenemos que $\mathfrak{m}^n \subset \mathfrak{p}$, luego $\mathfrak{p} = \mathfrak{m}$. Así pues, A sólo tiene un ideal primo, lo cual implica que $\dim A = 0$.

Supongamos el teorema para dimensiones menores que d y sea

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

una cadena de ideales primos en A. Tomemos $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, sea $A' = A/\mathfrak{p}_0$ y sea $x' = x + \mathfrak{p}_0$. Así A' es un dominio íntegro y $x' \neq 0$. Por el teorema anterior tenemos que $d(A'/(x')) \leq d(A') - 1$. Por otra parte, si $\mathfrak{m}'$ es el ideal maximal de A', tenemos que $A'/\mathfrak{m}'^n$ es una imagen homomorfa de $A/\mathfrak{m}^n$, luego $l(A/\mathfrak{m}^n) \geq l(A'/\mathfrak{m}'^n)$. Para valores grandes de n estos números son polinomios en n, y el cociente es siempre mayor o igual que 1, luego el grado del primero es mayor o igual que el del segundo, es decir, $d(A) \geq d(A') > d(A'/(x))$. Por hipótesis de inducción

$$r - 1 \leq \dim A'/(x) \leq d(A'/(x)) \leq d - 1,$$

luego $r \leq d$, lo que prueba que $\dim A \leq d = d(A)$. ■

De aquí se deducen numerosas consecuencias. Por ejemplo, ahora sabemos que todo anillo noetheriano local tiene dimensión finita, lo cual no es evidente. En la sección anterior hemos visto que si $\hat{A}$ es la compleción de A respecto a la topología $\mathfrak{m}$-ádica, entonces $d(A) = d(\hat{A})$. Ahora podemos enunciar esto mismo en términos de la dimensión de Krull:

Teorema 4.57 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea $\hat{A}$ la compleción respecto a la topología $\mathfrak{m}$-ádica. Entonces $\dim A = \dim \hat{A}$.*

Ahora podemos precisar el teorema 4.55:

Teorema 4.58 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea $x \in \mathfrak{m}$ un elemento que no sea divisor de cero. Entonces $\dim A/(x) = \dim A - 1$.*

Demostración: Sea $d = \dim A/(x)$. Por el teorema 4.55 (junto con el teorema de la dimensión) sabemos que $d \leq \dim A - 1$. Por otra parte, sean $x_1, \ldots, x_d \in A$ elementos cuyas imágenes en $A/(x)$ generen un ideal $\mathfrak{m}/(x)$-primario. Entonces el ideal $(x_1, \ldots, x_d, x)$ es $\mathfrak{m}$-primario, luego concluimos que $d + 1 \geq \delta(A) = \dim A$. ■

Veamos otra consecuencia, para la cual necesitamos una definición:

Definición 4.59 Sea A un anillo noetheriano local de dimensión d y sea $\mathfrak{m}$ su ideal maximal. Un *sistema de parámetros* de A es un conjunto de elementos $x_1, \ldots, x_d \in A$ que generen un ideal $\mathfrak{m}$-primario.

La igualdad $\dim A = \delta(A)$ garantiza la existencia de sistemas de parámetros. Vamos a demostrar que satisfacen una cierta propiedad de independencia:

Teorema 4.60 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea $x_1, \ldots, x_d \in A$ un sistema de parámetros. Sea $\mathfrak{q} = (x_1, \ldots, x_d)$ el ideal $\mathfrak{m}$-primario que generan. Sea $F(X_1, \ldots, X_d) \in A[X_1, \ldots, X_d]$ un polinomio homogéneo de grado s tal que $F(x_1, \ldots, x_d) \in \mathfrak{q}^{s+1}$. Entonces todos los coeficientes de F están en $\mathfrak{m}$.*

Demostración: Consideremos el homomorfismo de anillos graduados

$$\phi : (A/\mathfrak{q})[X_1, \ldots, X_d] \longrightarrow \operatorname{gr}_{\mathfrak{q}}(A)$$

dado por $X_i \mapsto \bar{x}_i = x_i + \mathfrak{q}^2$. Si $\bar{F}$ es la imagen de F en $(A/\mathfrak{q})[X_1, \ldots, X_d]$, estamos suponiendo que $\phi(\bar{F}) = 0$.

El hecho de que $\mathfrak{q}$ sea $\mathfrak{m}$-primario significa que los únicos divisores de cero en $A/\mathfrak{q}$ son los de $\mathfrak{m}/\mathfrak{q}$. Si F tuviera algún coeficiente fuera de $\mathfrak{m}$, entonces $\bar{F}$ tendría un coeficiente que no sería un divisor de cero. Vamos a ver que esto implica que $\bar{F}$ no es un divisor de cero.

En otras palabras, vamos a ver que en un anillo de polinomios $A[X_1, \ldots, X_d]$, los divisores de cero son los polinomios cuyos coeficientes son todos divisores de cero en A. Obviamente basta demostrarlo para $A[X]$. Si $F \in A[X]$ es un divisor de cero, sea $G \in A[X]$ un polinomio no nulo de grado mínimo tal que $FG = 0$. Pongamos que

$$F = a_0 + a_1X + \cdots + a_nX^n, \qquad G = b_0 + b_1X + \cdots + b_mX^m.$$

Entonces $a_nb_m = 0$, luego $a_nG = 0$, porque anula a F y tiene grado menor que G. Veamos por inducción sobre r que $a_{n-r}G = 0$. Si se cumple hasta r, entonces $0 = FG = (a_0 + a_1X + \cdots + a_{n-r-1}X^{n-r-1})G$, luego $a_{n-(r+1)}b_m = 0$, luego $a_{n-(r+1)}G$ anula a F y tiene grado menor que G, luego $a_{n-(r+1)}G = 0$. Esto prueba que todos los a_i son divisores de cero en A.

Volviendo al argumento, el hecho de que $\bar{F}$ sea homogéneo hace que el cociente $(A/\mathfrak{q})[X_1, \ldots, X_d]/(\bar{F})$ tenga una estructura natural de anillo graduado (sólo cambia la componente de grado s). Como $\bar{F}$ está en el núcleo de ϕ, tenemos que $\mathrm{gr}_{\mathfrak{q}}(A)$ es una imagen homomorfa de este cociente, luego las longitudes de las componentes homogéneas del cociente son mayores o iguales que las correspondientes de $\mathrm{gr}_{\mathfrak{q}}(A)$. Como dependen polinómicamente del grado, el teorema 4.41 nos da que

$$D(\mathrm{gr}_{\mathfrak{q}}(A)) \leq D((A/\mathfrak{q})[X_1, \ldots, X_d]/(\bar{F})) = D(A/\mathfrak{q})[X_1, \ldots, X_d]) - 1 = d - 1,$$

donde hemos usado además el teorema 4.42 y el ejemplo que le sigue. Ahora bien, por otra parte tenemos que $D(\mathrm{gr}_{\mathfrak{q}}(A)) = d(A) = \dim A = d$, lo que nos da una contradicción. ■

Hay un caso particular en el que el teorema anterior admite una expresión mucho más simple:

Definición 4.61 Si A es un anillo local y $\mathfrak{m}$ es su ideal maximal, un *cuerpo de coeficientes* de A es un cuerpo $k \subset A$ tal que el epimorfismo natural $A \longrightarrow A/\mathfrak{m}$ se restringe a un isomorfismo sobre k.

Por ejemplo, si A es un anillo local $\mathcal{O}_{V,P}$, donde P es un punto de una variedad afín V/k, entonces las funciones constantes constituyen un cuerpo de coeficientes de A.

Teorema 4.62 *Sea A un anillo noetheriano local con un cuerpo de coeficientes k. Si $x_1, \ldots, x_d \in A$ es un sistema de parámetros de A, entonces $x_1, \ldots, x_d$ son algebraicamente independientes sobre k.*

DEMOSTRACIÓN: Sea $F \in k[X_1, \ldots, X_d]$ tal que $F(x_1, \ldots, x_d) = 0$. Si es $F \neq 0$, sea s el grado del menor monomio no nulo de F y sea F_s la parte homogénea de F grado s. Si llamamos $\mathfrak{q} = (x_1, \ldots, x_s)$, entonces $F_s(x_1, \ldots, x_d) \in \mathfrak{q}^s$, luego por el teorema anterior los coeficientes de F_s están en $\mathfrak{m}$. Como la inclusión $k \longrightarrow A/\mathfrak{m}$ es un isomorfismo, esto implica que $F_s = 0$, contradicción. ■

Veamos una última aplicación:

Teorema 4.63 *Sea A un anillo noetheriano e $I \neq A$ un ideal. Entonces*

$$\dim A[X_1, \ldots, X_n] = \dim A + n.$$

Demostración: Basta probar que $\dim A[X] = \dim A + 1$. En primer lugar demostraremos que si $\mathfrak{p} \in \operatorname{Esp} A$, entonces

$$\operatorname{alt} \mathfrak{p}A[X] = \operatorname{alt} \mathfrak{p}, \qquad \operatorname{alt}((\mathfrak{p}, X)A[X]) = \operatorname{alt} \mathfrak{p} + 1.$$

En efecto, en primer lugar observamos que $\mathfrak{p}A[X] \in \operatorname{Esp} A[X]$, pues claramente $A[X]/\mathfrak{p}A[X] \cong (A/\mathfrak{p})[X]$. También $\mathfrak{P} = (\mathfrak{p}, X)A[X] \in \operatorname{Esp} A[X]$, pues $A[X]/\mathfrak{P} \cong A/\mathfrak{p}$. Además $\mathfrak{p}A[X] \cap A = \mathfrak{p} = \mathfrak{P} \cap A$.

Podemos definir un epimorfismo $A[X]_{\mathfrak{P}} \longrightarrow A_{\mathfrak{p}}$ mediante $F/G \mapsto F(0)/G(0)$. Su núcleo es (X), luego $A[X]_{\mathfrak{P}}/(X) \cong A_{\mathfrak{p}}$. Ahora aplicamos el teorema 4.58. (Observemos que X no es un divisor de cero en $A[X]_{\mathfrak{P}}$.) Obtenemos que

$$\operatorname{alt} \mathfrak{P} = \dim A[X]_{\mathfrak{P}} = \dim(A[X]_{\mathfrak{P}}/(X)) + 1 = \dim A_{\mathfrak{p}} + 1 = \operatorname{alt} \mathfrak{p} + 1.$$

Para cada cadena de ideales primos $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_t = \mathfrak{p}$ podemos construir la cadena $\mathfrak{p}_0 A[X] \subsetneq \cdots \subsetneq \mathfrak{p}_t A[X] = \mathfrak{p}A[X]$, luego $\operatorname{alt} \mathfrak{p}A[X] \geq \operatorname{alt} \mathfrak{p}$. Además $\mathfrak{p}A[X] \subsetneq \mathfrak{P}$, luego $\operatorname{alt} \mathfrak{p}A[X] < \operatorname{alt} \mathfrak{P}$, luego $\operatorname{alt} \mathfrak{p}A[X] \leq \operatorname{alt} \mathfrak{p}$.

Con esto tenemos que si A tiene dimensión infinita lo mismo le sucede a $A[X]$. Si la dimensión es finita ha de ser $\dim A[X] \geq \dim A + 1$. Tomemos ahora un primo arbitrario $\mathfrak{P} \in \operatorname{Esp} A[X]$ y sea $\mathfrak{p} = \mathfrak{P} \cap A$.

Observemos que $A_{\mathfrak{p}}[X] \subset A[X]_{\mathfrak{P}}$ y, viendo a $S_{\mathfrak{P}} = A[X] \setminus \mathfrak{P}$ como subconjunto multiplicativo de $A_{\mathfrak{p}}[X]$, tenemos que $A_{\mathfrak{p}}[X]_{\mathfrak{P}} = A[X]_{\mathfrak{P}}$. Por 3.8:

$$A[X]_{\mathfrak{P}}/\mathfrak{p}A[X]_{\mathfrak{P}} \cong (A[X]/\mathfrak{p}A_{\mathfrak{p}}[X])_{\mathfrak{P}/\mathfrak{p}A[X]}.$$

Por otra parte $A[X]/\mathfrak{p}A[X] \cong (A/\mathfrak{p})[X]$, luego, si llamamos $\mathfrak{P}^*$ a la imagen de $\mathfrak{P}/\mathfrak{p}A[X]$ por este isomorfismo, podemos concluir que

$$A[X]_{\mathfrak{P}}/\mathfrak{p}A[X]_{\mathfrak{P}} \cong (A/\mathfrak{p})[X]_{\mathfrak{P}^*}.$$

Como el último anillo es un dominio de ideales principales, existe un $f \in \mathfrak{P}$ tal que $\mathfrak{P}A[X]_{\mathfrak{P}} = (\mathfrak{p}, f)A[X]_{\mathfrak{P}}$. Sea $d = \dim A_{\mathfrak{p}}$ y sea $a_1, \ldots, a_d \in A_{\mathfrak{p}}$ un sistema de parámetros. Esto significa que $\mathfrak{p}A_{\mathfrak{p}} = \operatorname{rad}(a_1, \ldots, a_d)$. Por consiguiente $\mathfrak{P}A_{\mathfrak{p}}[X]_{\mathfrak{P}} = \operatorname{rad}(a_1, \ldots, a_d, f)$, luego

$$\operatorname{alt} \mathfrak{P} = \dim A_{\mathfrak{p}}[X]_{\mathfrak{P}} \leq d + 1 \leq \dim A + 1.$$

Esto implica que $\dim A[X] \leq \dim A + 1$. ■

De aquí se sigue que todo anillo finitamente generado sobre un anillo noetheriano de dimensión finita tiene también dimensión finita.

Ejemplo Consideremos el anillo $A = \mathbb{Z}_p[X]$ (donde $\mathbb{Z}_p$ es la localización de $\mathbb{Z}$ respecto de un primo p) y sea $\mathfrak{m} = (pX - 1)$. Como $\mathbb{Z}_p$ es un dominio de ideales principales, $\dim \mathbb{Z}_p = 1$ y, por el teorema anterior, $\dim A = 2$. Es claro que $\mathfrak{m}$ es un ideal maximal de A, pues $A/\mathfrak{m} \cong \mathbb{Q}$. Así pues, $\dim \mathfrak{m} = 0$. Por otra parte se cumple que $\operatorname{alt} \mathfrak{m} = 1$. En efecto, si $\mathfrak{p} \subsetneq \mathfrak{m}$ es un ideal primo, un elemento $a \in \mathfrak{p}$ ha de ser de la forma $a_1(pX - 1)$, y entonces también $a_1 \in \mathfrak{p}$, luego $a = a_2(pX - 1)^2$ y, en general, obtenemos que

$$a \in \bigcap_n \mathfrak{m}^n,$$

y la intersección es nula porque el anillo A es noetheriano. Así pues, $\mathfrak{p} = 0$ y no se cumple la relación

$$\dim A = \operatorname{alt} \mathfrak{m} + \dim \mathfrak{m}.$$

Vemos así que el teorema 3.75 no es válido para anillos noetherianos arbitrarios. ■

Capítulo V

Regularidad

En este capítulo estudiaremos el álgebra subyacente en la noción de punto regular de un conjunto algebraico. Veremos que un punto P en un conjunto algebraico C es regular (en un sentido que generaliza a la regularidad en geometría diferencial) si y sólo si su anillo local $\mathcal{O}_{C,P}$ tiene una propiedad algebraica a la que llamaremos precisamente regularidad. Para introducir este concepto conviene obtener algunos resultados previos, basados en el teorema de la altura, que demostramos en la primera sección. Después introduciremos el concepto de anillo local regular y derivaremos sus propiedades básicas y algunas caracterizaciones. No obstante, las propiedades más profundas requieren técnicas del álgebra homológica, de las que nos ocuparemos en la sección cuarta. Finalmente relacionaremos la regularidad con los conjuntos algebraicos.

5.1 El teorema de la altura

En esta sección extraeremos una consecuencia sencilla del teorema de la dimensión, de la cual obtendremos a su vez muchas aplicaciones geométricas:

Teorema 5.1 (Teorema de la altura) *Sea A un anillo noetheriano e I un ideal de A. Entonces, todo divisor primo minimal $\mathfrak{p}$ de I cumple* $\operatorname{alt}\mathfrak{p} \leq \mu(I)$.

Demostración: Basta observar que $S_{\mathfrak{p}}^{-1}\mathfrak{p}$ es el ideal maximal del anillo noetheriano local $A_{\mathfrak{p}}$ y el ideal $S_{\mathfrak{p}}^{-1}I$ es $S_{\mathfrak{p}}^{-1}\mathfrak{p}$-primario, luego

$$\mu(I) \geq \mu(S_{\mathfrak{p}}^{-1}I) \geq \dim A_{\mathfrak{p}} = \operatorname{alt}\mathfrak{p}.$$

■

En particular vemos que las alturas de los ideales primos son finitas, lo cual no era evidente. Se dice que un anillo es *semilocal* si tiene un número finito de ideales maximales. Ahora es inmediato que todo anillo noetheriano semilocal tiene dimensión finita, pues la dimensión es el máximo de las alturas de los ideales maximales.

El teorema de la altura es una generalización del teorema siguiente:

Teorema 5.2 (Teorema de los ideales principales) *Sea A un anillo noetheriano y $(a) \neq 1$ un ideal principal. Entonces todo divisor primo minimal $\mathfrak{p}$ de (a) cumple $\operatorname{alt}\mathfrak{p} \leq 1$. Si a no es un divisor de cero, entonces $\operatorname{alt}\mathfrak{p} = 1$.*

DEMOSTRACIÓN: La primera parte es el teorema de la altura. La última afirmación es consecuencia de la primera, pues $(a) \subset \mathfrak{p}$ y si fuera $\operatorname{alt}\mathfrak{p} = 0$ entonces $\mathfrak{p}$ sería un primo minimal de A y sus elementos serían divisores de 0 (teorema 3.43). ■

Veamos algunas aplicaciones geométricas:

Teorema 5.3 *Sea V/k una variedad afín y $f_1, \ldots, f_m \in k[V]$ funciones tales que $C = V(f_1, \ldots, f_m) \neq \varnothing$. Entonces cada componente irreducible W de C cumple que $\dim W \geq \dim V - m$.*

DEMOSTRACIÓN: Se cumple que $W = V(\mathfrak{p})$, donde $\mathfrak{p}$ es un divisor primo minimal de $(f_1, \ldots, f_m)$. Por 3.75 y el teorema de la altura tenemos que

$$\dim W = \dim k[V]/\mathfrak{p} = \dim \mathfrak{p} = \dim k[V] - \operatorname{alt}\mathfrak{p} \geq \dim V - m.$$

■

También podemos sacar consecuencias sobre la dimensión de una intersección:

Teorema 5.4 *Sean V/k y W/k dos variedades afines en A^n no disjuntas. Entonces cada componente irreducible Z de $V \cap W$ verifica que*

$$\dim Z \geq \dim V + \dim W - n.$$

DEMOSTRACIÓN: Observemos que

$$k[V] \otimes_k k[W] \cong k[X_1, \ldots, X_n]/I(V) \otimes_k k[Y_1, \ldots, Y_n]/I(W)$$

$$\cong k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]/(I(V) + I(W)).$$

Llamemos Δ al ideal de $k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generado por los polinomios $X_i - Y_i$, y sea $\mathfrak{d}$ su imagen en $k[V] \otimes_k k[W]$. Entonces

$$k[V] \otimes_k k[W]/\mathfrak{d} \cong k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]/(I(V) + I(W) + \Delta)$$

$$\cong \big(k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]/\Delta\big) \;/\; (I(V) + I(W) + \Delta)/\Delta$$

$$\cong k[X_1, \ldots, X_n]/(I(V) + I(W)),$$

donde en el último cociente $I(W)$ se considera como ideal de $k[X_1, \ldots, X_n]$ y no de $k[Y_1, \ldots, Y_n]$. Concluimos que

$$\big(k[V] \otimes_k k[W]/\mathfrak{d}\big)_{\mathrm{red}} \cong \big(k[X_1, \ldots, X_n]/(I(V) + I(W))\big)_{\mathrm{red}} \cong k[V \cap W].$$

En el último isomorfismo usamos que $V \cap W$ es el mayor conjunto algebraico contenido en las dos variedades, luego $I(V \cap W)$ es el menor ideal radical que contiene a $I(V)$ e $I(W)$, es decir, $I(V \cap W) = \operatorname{rad}(I(V) + I(W))$.

Los primos minimales de $k[V \cap W]$ se corresponden biunívocamente con los primos minimales de $\big(k[V] \otimes_k k[W]/\mathfrak{d}\big)_{\mathrm{red}}$, que a su vez se corresponden con los primos minimales de $k[V] \otimes_k k[W]/\mathfrak{d}$, y éstos a su vez con los divisores primos minimales de $\mathfrak{d}$ en $k[V] \otimes_k k[W]$. La correspondencia conserva la dimensión.

Una componente irreducible Z de $V \cap W$ se corresponde con uno de estos primos minimales, digamos $\mathfrak{P}$, de modo que, teniendo en cuenta 3.75 (que se puede aplicar en virtud de 3.78),

$$\dim Z = \dim\big(k[V] \otimes_k k[W]/\mathfrak{P}\big) = \dim V + \dim W - \operatorname{alt} \mathfrak{P}.$$

Ahora basta observar que $\mathfrak{P}$ es un divisor primo minimal de $\mathfrak{d}$ y que $\mathfrak{d}$ está generado por n elementos, luego $\operatorname{alt} \mathfrak{P} \leq n$ por el teorema de la altura. ■

Vamos a introducir varios conceptos que nos permitirán comprender por qué es importante relacionar la altura de un ideal con su número de generadores.

Definición 5.5 Llamaremos *altura* de un ideal I en un anillo A como el ínfimo de las alturas de sus divisores primos minimales. Correspondientemente, la *codimensión* de un cerrado en un espacio topológico se define como el ínfimo de las codimensiones de sus componentes irreducibles. Así, si C/k es un conjunto algebraico afín y C' es un cerrado en C, tenemos que $\operatorname{codim}_C C' = \operatorname{alt} I_C(C')$.

El teorema de la altura implica que si A es un anillo noetheriano e $I \neq A$ es un ideal de A, entonces $\operatorname{alt} I \leq \mu(I)$.

En términos geométricos esto significa que se necesitan al menos m ecuaciones para definir un conjunto algebraico de codimensión m. Por ejemplo, es claro que para definir una variedad lineal de codimensión m en A^n se necesitan exactamente m ecuaciones. Sin embargo, en general no tiene por qué darse la igualdad. Conviene introducir las definiciones siguientes:

Definición 5.6 Sea A un anillo noetheriano e $I \neq A$ un ideal.

a) Diremos que I es una *intersección completa* si $\operatorname{alt} I = \mu(I)$.

b) Diremos que I es una *intersección completa conjuntista* si existen elementos $a_1, \ldots, a_m \in A$, donde $m = \mu(I)$, tales que $\operatorname{rad} I = \operatorname{rad}(a_1, \ldots, a_m)$.

Observemos que a) implica b). Otro hecho elemental es que b) implica que todos los divisores primos minimales $\mathfrak{p}$ de I tienen la misma altura m, pues todos ellos son también divisores primos minimales de $(a_1, \ldots, a_m)$, luego

$$m = \operatorname{alt} I \leq \operatorname{alt} \mathfrak{p} \leq \mu(a_1, \ldots, a_m) \leq m.$$

Definición 5.7 Sea C/k un subconjunto algebraico d-dimensional en A^n.

a) Diremos que C/k es una *intersección completa ideal* si $I(C)$ está generado por $n - d$ polinomios.

b) Diremos que C/k es una *intersección completa conjuntista* si C es la intersección de $n - d$ hipersuperficies definidas sobre k.

Es inmediato comprobar que un conjunto C/k cumple una de las dos propiedades de 5.7 si y sólo si el ideal $I(V)$ cumple la propiedad correspondiente de 5.6. Vemos así que la propiedad "artificial" de 5.7 b) se corresponde con la propiedad "natural" de "ser definible por $n-d$ ecuaciones" (que es el mínimo número de ecuaciones posible), mientras que la propiedad "natural" de 5.7 a) se corresponde con una propiedad algebraica de $I(V)$ de la que, de momento, no tenemos una interpretación geométrica.

Observemos, por último, que si A es un anillo noetheriano local con ideal maximal $\mathfrak{m}$, el teorema de la dimensión garantiza la existencia de ideales $\mathfrak{m}$-primarios $\mathfrak{q}$ tales que $\mu(\mathfrak{q}) = \dim A$. Todo ideal $\mathfrak{m}$-primario $\mathfrak{q}$ de A cumple que $\operatorname{alt} \mathfrak{q} = \operatorname{alt} \mathfrak{m} = \dim A$, luego la propiedad $\mu(\mathfrak{q}) = \dim A$ equivale a que $\mathfrak{q}$ sea una intersección completa.

5.2 Anillos locales regulares

Definición 5.8 Un anillo noetheriano local A es *regular* si $\dim A = \mu(\mathfrak{m})$, donde $\mathfrak{m}$ es el ideal maximal de A. Un sistema de parámetros que genere a $\mathfrak{m}$ y tenga $\dim A$ elementos se llama *sistema regular de parámetros* de A. Así, un anillo noetheriano local es regular si y sólo si tiene un sistema regular de parámetros.

Observemos que todo cuerpo es trivialmente un anillo local regular.

Si $k = A/\mathfrak{m}$, el teorema 4.52 implica que $\mu(\mathfrak{m}) = \dim_k \mathfrak{m}/\mathfrak{m}^2$, luego A es regular si y sólo si la dimensión de $\mathfrak{m}/\mathfrak{m}^2$ como k-espacio vectorial coincide con la dimensión de A.

Veremos más adelante que podemos definir la regularidad de un punto P de un conjunto algebraico afín C como la regularidad del anillo local $\mathcal{O}_{C,P}$. Veremos que para que esto suceda es necesario que P sólo pertenezca a una componente irreducible de C, y entonces $\dim \mathcal{O}_{C,P}$ es la dimensión de dicha componente. El dual del espacio vectorial $\mathfrak{m}_P/\mathfrak{m}_P^2$ puede identificarse de forma natural con la variedad tangente a C en P, por lo que la regularidad equivale a que dicha variedad tangente tenga la misma dimensión que tiene C en P.

Veamos una caracterización de la regularidad:

Teorema 5.9 *Sea A un anillo noetheriano local de dimensión d, sea $\mathfrak{m}$ su ideal maximal y sea $k = A/\mathfrak{m}$ el cuerpo de restos. Entonces A es regular si y sólo si $\operatorname{gr}_{\mathfrak{m}}(A) \cong k[X_1, \ldots, X_d]$.*

DEMOSTRACIÓN: Hay que entender que el isomorfismo del enunciado es un isomorfismo de anillos graduados. En tal caso, tenemos en particular que $\mathfrak{m}/\mathfrak{m}^2 = \operatorname{gr}^1_{\mathfrak{m}}(A)$ es isomorfo al espacio vectorial de los monomios de grado 1, luego tiene dimensión d y así A es regular.

Recíprocamente, si A es regular y $\mathfrak{m} = (x_1, \ldots, x_d)$, el teorema 4.60 implica que el epimorfismo de módulos graduados

$$\phi : k[X_1, \ldots, X_d] \longrightarrow \operatorname{gr}_{\mathfrak{m}}(A)$$

dado por $\phi(X_i) = x_i$ no tiene elementos homogéneos en su núcleo, pero un elemento está en el núcleo si y sólo si lo están sus componentes homogéneas, luego se trata de un isomorfismo. ■

En particular vemos que si A es un anillo local regular entonces $\operatorname{gr}_{\mathfrak{m}}(A)$ es un dominio íntegro. El teorema siguiente nos da que A también es un dominio íntegro.

Teorema 5.10 *Sea A un anillo e I un ideal de A tal que la topología I-ádica sea de Hausdorff. Si $\operatorname{gr}_I(A)$ es un dominio íntegro, entonces A también lo es.*

DEMOSTRACIÓN: Sean x, $y \in A$ no nulos. La hipótesis equivale a que $\bigcap\limits_n I^n = 0$, luego existen naturales r, s tales que $x \in I^r \setminus I^{r+1}$, $y \in I^s \setminus I^{s+1}$.

Sean $\bar{x} = x + I^{r+1}$, $\bar{y} = y + I^{s+1}$. Entonces $\bar{x}$, $\bar{y} \in \operatorname{gr}_I(A)$ son no nulos, luego también $\bar{x}\bar{y} = xy + I^{r+s+1}$ es no nulo, luego $xy \neq 0$. ■

Otra consecuencia inmediata del teorema 5.9 es la siguiente:

Teorema 5.11 *Si A es un anillo noetheriano local con ideal maximal $\mathfrak{m}$ y $\hat{A}$ es su compleción $\mathfrak{m}$-ádica, entonces A es regular si y sólo si lo es $\hat{A}$.*

DEMOSTRACIÓN: Hemos probado que $\hat{A}$ es también un anillo noetheriano local de la misma dimensión que A y con ideal maximal $\hat{\mathfrak{m}}$. Además sabemos que $\operatorname{gr}_{\mathfrak{m}}(A) \cong \operatorname{gr}_{\hat{\mathfrak{m}}}(\hat{A})$, luego la conclusión es evidente. ■

De los anillos locales regulares completos podemos decir más:

Teorema 5.12 *Sea A un anillo local regular completo de dimensión d que contenga un cuerpo de coeficientes k. Entonces $A \cong k[[X_1, \ldots, X_d]]$. El isomorfismo evalúa cada serie formal en un sistema regular de parámetros.*

DEMOSTRACIÓN: Sea $x_1, \ldots, x_d \in A$ un sistema regular de parámetros y consideremos el homomorfismo $k[[X_1, \ldots, X_d]] \longrightarrow A$ que evalúa cada serie en dichos parámetros. Es evidente que todas las series convergen, por lo que el homomorfismo está bien definido. Vamos a probar que es suprayectivo.

Sea $\mathfrak{m} = (x_1, \ldots, x_d)$ el ideal maximal de A. Tenemos que el epimorfismo natural $A \longrightarrow A/\mathfrak{m}$ se restringe a un isomorfismo en k. Dado $\alpha \in A$, existe un $a_0 \in k$ tal que $\alpha - a_0 \in \mathfrak{m}$. Supongamos que, en general, hemos encontrado un polinomio $F_{n-1}(X_1, \ldots, X_d) \in k[X_1, \ldots, X_d]$ de grado $\leq n-1$ de manera que $\alpha - F_{n-1}(x_1, \ldots, x_d) \in \mathfrak{m}^n$. En virtud del teorema 5.9 (teniendo en cuenta el isomorfismo concreto que se construye en la prueba), tenemos que el espacio vectorial $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ está generado sobre $A/\mathfrak{m}$ por los monomios de grado n en $x_1, \ldots, x_d$ (con coeficiente 1), luego podemos encontrar un polinomio homogéneo G_n de grado n con coeficientes en k tal que

$$\alpha - F_{n-1}(x_1, \ldots, x_d) - G_n(x_1, \ldots, x_d) \in \mathfrak{m}^{n+1}.$$

Llamando $F_n = F_{n-1} + G_n$, tenemos construida inductivamente una sucesión $\{F_n\}_n$ de polinomios F_n de grado n (cada uno de los cuales se diferencia del anterior en una forma de grado n) que determinan una serie $F \in k[[X_1, \ldots, X_d]]$ y con la propiedad de que $\lim_n F_n(x_1, \ldots, x_n) = \alpha$. Así pues, $F \mapsto \alpha$.

Teniendo en cuenta que los dos anillos tienen la misma dimensión, el epimorfismo que hemos construido tiene que ser un isomorfismo. ■

Ahora vamos a probar que los anillos locales regulares son íntegramente cerrados. Para ello necesitamos algunos preparativos.

Definición 5.13 Sea A un anillo e I un ideal de A. Si $a \in A$ cumple que $a \in I^n$ pero $a \notin I^{n+1}$, entonces $L_I(a) = a + I^{n+1} \in \mathrm{gr}_I^n(A)$ recibe el nombre de *forma directora* de a respecto de I, y el grado n de $L_I(a)$ se llama *grado* de a respecto de I. Si $a \in \bigcap_n I^n$, convenimos en que $L_I(a) = 0$.

Teorema 5.14 *Sea A un anillo, sea I un ideal de A y sean $a, b \in A$. Entonces*

$$L_I(ab) = L_I(a)L_I(b) \quad \textit{o bien} \quad L_I(a)L_I(b) = 0.$$

Demostración: Podemos suponer que $a \in I^m \setminus I^{m+1}$, $b \in I^n \setminus I^{n+1}$, pues en caso contrario tenemos que $L_I(a)L_I(b) = 0$ y se cumple el teorema.

Entonces $L_I(a)L_I(b) = ab + I^{m+n+1}$. Esta clase es $L_I(ab)$ si $ab \notin I^{m+n+1}$ y es 0 en caso contrario. ■

Teorema 5.15 *Sea A un anillo noetheriano e I un ideal contenido en todos los ideales maximales de A. Si $\mathrm{gr}_I(A)$ es íntegramente cerrado, A también lo es.*

Demostración: Por el teorema 4.21 tenemos que la topología I-ádica es de Hausdorff en A, luego

$$\bigcap_{n=0}^{\infty} I^n = 0,$$

de donde deducimos que si $a \in A$ es no nulo, también $L_I(a) \neq 0$.

Un anillo íntegramente cerrado es, por definición un dominio íntegro, luego el teorema 5.10 nos da que A también lo es. El teorema anterior implica entonces que $L_I(ab) = L_I(a)L_I(b)$ para todos los elementos $a, b \in A$.

Tomemos un elemento $x = r/s$ en el cuerpo de cocientes de A que sea entero sobre A. Hemos de probar que $x \in A$ o, equivalentemente, que $r \in (s)$. Supongamos que no es así y llegaremos a una contradicción. En particular tenemos que $r \neq 0$.

La integridad de x se traduce en que $A[x] = \langle 1, x, \ldots, x^{n-1} \rangle_A$, para cierto natural n, luego $s^{n-1}x^m \in A$ para todo natural m. Entonces $s^{m-1}r^m \in s^m A$, luego $L_{\mathfrak{m}}(s^{n-1})L_{\mathfrak{m}}(r)^m \in L_{\mathfrak{m}}(s)^m \mathrm{gr}_{\mathfrak{m}}(A)$, luego

$$\left(\frac{L_{\mathfrak{m}}(r)}{L_{\mathfrak{m}}(s)}\right)^m \in L_{\mathfrak{m}}(s^{n-1})^{-1}\mathrm{gr}_{\mathfrak{m}}(A),$$

para todo natural m. Esto implica que

$$\mathrm{gr}_{\mathfrak{m}}(A)[L_{\mathfrak{m}}(r)/L_{\mathfrak{m}}(s)] \subset L_{\mathfrak{m}}(s^{n-1})^{-1}\mathrm{gr}_{\mathfrak{m}}(A).$$

Como el anillo $\operatorname{gr}_{\mathfrak{m}}(A)$ es noetheriano (teorema 4.24), el módulo de la derecha también lo es (está generado por un elemento), luego el submódulo de la izquierda es finitamente generado, lo cual significa que $L_{\mathfrak{m}}(r)/L_{\mathfrak{m}}(s)$ es entero sobre $\operatorname{gr}_{\mathfrak{m}}(A)$. Por la hipótesis concluimos que $L_{\mathfrak{m}}(r)/L_{\mathfrak{m}}(s) \in \operatorname{gr}_{\mathfrak{m}}(A)$. Claramente ha de ser un elemento homogéneo, digamos de la forma $[t_0]$, para un cierto $t_0 \in A$. Esto se traduce en que

$$\operatorname{grad}_{\mathfrak{m}}(r - st_0) > \operatorname{grad}_{\mathfrak{m}} r.$$

Así $x_1 = (r - st_0)/s = x - t_0$ también es entero (no nulo) sobre A, luego por el mismo razonamiento existe un $t_1 \in A$ tal que $\operatorname{grad}_{\mathfrak{m}}(r - st_1) > \operatorname{grad}_{\mathfrak{m}}(r - st_0)$, etc. Por consiguiente, y teniendo en cuenta 4.22, llegamos a que

$$r \in \bigcap_{n=0}^{\infty} ((s) + \mathfrak{m}^n) = (s),$$

en contra de lo supuesto. ■

En particular:

Teorema 5.16 *Todo anillo local regular es íntegramente cerrado.*

Demostración: Si A es un anillo local regular, hemos demostrado que $\operatorname{gr}_{\mathfrak{m}}(A) \cong (A/\mathfrak{m})[X_1, \ldots, X_d]$, luego es un dominio de factorización única y, en particular, es íntegramente cerrado. Basta aplicar el teorema anterior. ■

Para anillos de dimensión 1 podemos decir más:

Teorema 5.17 *Sea A un anillo noetheriano local de dimensión 1 y sea $\mathfrak{m}$ su ideal maximal. Entonces A es regular si y sólo si $\mathfrak{m}$ es principal, si y sólo si A es un dominio de ideales principales.*

Demostración: Sea $k = A/\mathfrak{m}$. En general tenemos que $\mu(\mathfrak{m}) \geq \dim A = 1$, luego $\mathfrak{m}$ es principal si y sólo si $\mu(\mathfrak{m}) = 1 = \dim A$, si y sólo si A es regular.

Por otra parte, como $\dim A = 1$, tenemos que $\mathfrak{m}$ es el único ideal primo no nulo de A, luego todo ideal I de A distinto de 0, 1 es $\mathfrak{m}$-primario. Por lo tanto existe un natural n tal que $\mathfrak{m}^n \subset I$. Si no se da la igualdad, podemos tomar un natural r tal que $I \subset \mathfrak{m}^r$, $I \not\subset \mathfrak{m}^{r+1}$.

Si $\mathfrak{m} = (x)$, existe un $y \in I$ tal que $y = ax^r$, pero $a \notin \mathfrak{m}$, luego a es una unidad, luego $x^r \in I$, luego $\mathfrak{m}^r \subset I \subset \mathfrak{m}^r$. Concluimos que todo ideal no nulo es potencia de $\mathfrak{m}$, luego todos los ideales son principales. ■

Es fácil ver que la regularidad en dimensión 1 equivale también a que A sea un anillo de valoración discreta, es decir, el anillo de enteros de una valoración en su cuerpo de cocientes.

Otra consecuencia del teorema anterior es que si A es un dominio de factorización única, y $\pi \in A$ es primo, entonces el anillo $A_{(\pi)}$ es regular, pues sus únicos ideales no nulos son las potencias de (π), luego es noetheriano, $\dim A_{(\pi)} = \operatorname{alt}(\pi) = 1$ y el ideal maximal de $A_{(\pi)}$ está generado por π.

En particular, si A es un dominio de ideales principales y $\mathfrak{p} \in \operatorname{Esp} A$, entonces $A_{\mathfrak{p}}$ es un anillo local regular. (Para $\mathfrak{p} = 0$ tenemos el cuerpo de cocientes de A.)

En general, un cociente de un anillo local regular no tiene por qué ser regular. Para caracterizar cuándo lo es necesitamos un resultado previo:

Teorema 5.18 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sean $a_1, \ldots, a_m \in \mathfrak{m}$. Entonces:*

a) $\dim A \geq \dim A/(a_1, \ldots, a_m) \geq \dim A - m$.

b) $\dim A/(a_1, \ldots, a_m) = \dim A - m$ *si y sólo si* $\{a_1, \ldots, a_m\}$ *está contenido en un sistema de parámetros de A.*

DEMOSTRACIÓN: a) Sea $\delta = \dim A/(a_1, \ldots, a_m)$ y sean $b_1, \ldots, b_\delta \in \mathfrak{m}$ tales que sus clases módulo $(a_1, \ldots, a_m)$ formen un sistema de parámetros del cociente. Entonces $(a_1, \ldots, a_m, b_1, \ldots, b_\delta)$ es un ideal $\mathfrak{m}$-primario, pues si $\mathfrak{p}$ es un divisor primo minimal entonces $\mathfrak{p}/(a_1, \ldots, a_m)$ es un divisor primo minimal de un ideal $\mathfrak{m}/(a_1, \ldots, a_m)$-primario, luego $\mathfrak{p} = \mathfrak{m}$. Esto prueba que $m+\delta \geq \dim A$.

b) Si $m + \delta = \dim A$, entonces $\{a_1, \ldots, a_m, b_1, \ldots, b_\delta\}$ es un sistema de parámetros de A. Recíprocamente, supongamos que existe un sistema de parámetros $\{a_1, \ldots, a_m, b_1, \ldots, b_t\}$. Entonces $m+t = \dim A$ y las clases de $b_1, \ldots, b_t$ generan un ideal $\mathfrak{m}/(a_1, \ldots, a_m)$-primario. Por consiguiente

$$t \geq \dim A/(a_1, \ldots, a_m) \geq \dim A - m = t.$$

■

Teorema 5.19 *Sea A un anillo local regular e I un ideal propio de A. Entonces A/I es regular si y sólo si I admite un sistema generador que se extienda a un sistema regular de parámetros de A.*

DEMOSTRACIÓN: Supongamos que $\{a_1, \ldots, a_d\}$ es un sistema regular de parámetros de A y que $I = (a_{\delta+1}, \ldots, a_d)$. Por el teorema anterior $\dim A/I = \delta$, y el ideal maximal de A/I está generado por δ elementos, luego A/I es regular.

Recíprocamente, si A/I es regular de dimensión δ, sean $a_1, \ldots, a_\delta \in \mathfrak{m}$ elementos cuyas clases en A/I generen $\bar{\mathfrak{m}} = \mathfrak{m}/I$. Tenemos la siguiente sucesión exacta de espacios vectoriales sobre $A/\mathfrak{m}$:

$$0 \longrightarrow I/(I \cap \mathfrak{m}^2) \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 \longrightarrow 0.$$

Podemos descomponer $\mathfrak{m}/\mathfrak{m}^2$ en suma directa de dos subespacios: uno formado por las clases con un representante en I y otro el generado por las clases de $a_1, \ldots, a_\delta$. Por lo tanto, podemos encontrar $a_{\delta+1}, \ldots, a_d \in I$ de modo que las imágenes en $\mathfrak{m}/\mathfrak{m}^2$ de $a_1, \ldots, a_d$ sean una base. Por 4.52 tenemos que $\mathfrak{m} = (a_1, \ldots, a_d)$. Sea $I' = (a_{\delta+1}, \ldots, a_d) \subset I$. Sólo nos falta probar que $I = I'$.

Por la implicación ya demostrada, A/I' es un anillo local regular de dimensión δ y A/I es una imagen homomorfa de A/I'. Como A/I' es un dominio íntegro y ambos anillos tienen la misma dimensión, han de ser iguales (por ejemplo, por 4.58). Así pues, $I = I'$. ■

El teorema siguiente proporciona más ejemplos de anillos locales regulares:

Teorema 5.20 *Sea A un anillo local regular, sea $\mathfrak{m}$ su ideal maximal y sea $\mathfrak{P} \in \operatorname{Esp} A[X]$ tal que $\mathfrak{P} \cap A = \mathfrak{m}$. Entonces $A[X]_{\mathfrak{P}}$ también es un anillo local regular.*

Demostración: En la prueba del teorema 4.63 hemos visto que

$$\dim A = \operatorname{alt} \mathfrak{m} = \operatorname{alt} \mathfrak{m}A[X] \leq \operatorname{alt} \mathfrak{P} = \dim A[X]_{\mathfrak{P}}.$$

Si $\mathfrak{m}A[X] = \mathfrak{P}$, entonces $\dim A = \dim A[X]_{\mathfrak{P}}$ y $\mathfrak{P}$ está generado por $\dim A$ elementos, luego $A[X]_{\mathfrak{P}}$ es regular.

Si no se da la igualdad entonces $\dim A[X]_{\mathfrak{P}} \geq \dim A + 1$. Puesto que $A[X]/\mathfrak{m}A[X] \cong (A/\mathfrak{m})[X]$ es un dominio de ideales principales, la imagen de $\mathfrak{P}$ es ente anillo está generada por un elemento, luego $\mathfrak{P}$ está generado por $\dim A + 1$ elementos. Así pues, $\mu(\mathfrak{P}) \leq \dim A + 1 \leq \dim A[X]_{\mathfrak{P}} \leq \mu(\mathfrak{P})$, con lo que llegamos igualmente a que $A[X]_{\mathfrak{P}}$ es regular. ■

Como consecuencia:

Teorema 5.21 *Sea A un anillo tal que para todo $\mathfrak{p} \in \operatorname{Esp} A$, la localización $A_{\mathfrak{p}}$ es regular. Entonces $A[X_1, \ldots, X_n]$ tiene esta misma propiedad.*

Demostración: Obviamente basta demostrar el resultado para $n = 1$. Sea $\mathfrak{P} \in \operatorname{Esp} A[X]$ y consideremos $\mathfrak{p} = \mathfrak{P} \cap A$. Entonces

$$A[X]_{\mathfrak{P}} \cong A_{\mathfrak{p}}[X]_{\mathfrak{P}A_{\mathfrak{p}}[X]}.$$

En efecto: Observemos que todo elemento de $A_{\mathfrak{p}}[X]$ es de la forma $F(X)/s$, con $F(X) \in A[X]$, $s \in S_{\mathfrak{p}} = A \setminus \mathfrak{p}$. Los elementos de $\mathfrak{P}A_{\mathfrak{p}}[X]$ son los de esta forma con $F(X) \in \mathfrak{P}$. Esto implica que $\mathfrak{P}A_{\mathfrak{p}}[X] \cap A[X] = \mathfrak{P}$. De aquí se sigue que la aplicación $A[X]_{\mathfrak{P}} \longrightarrow A_{\mathfrak{p}}[X]_{\mathfrak{P}A_{\mathfrak{p}}[X]}$ dada por $F/G \mapsto F/G$ es un homomorfismo bien definido. Es inyectiva, pues si $F/G = 0$ en la imagen, entonces $FH/s = 0$, para cierto $H \in A[X]$, luego también $FH = 0$ y entonces $F/G = 0$ en $A[X]_{\mathfrak{P}}$. También es suprayectiva, pues todo elemento de la imagen es de la forma $(F/s)/(G/t) = (Ft)/(Gs)$, con $G \in A[X] \setminus \mathfrak{P}$, $s \in A \setminus \mathfrak{p}$, luego $Gs \notin \mathfrak{P}$.

Además $\mathfrak{P}A_{\mathfrak{p}}[X] \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, pues si $F/s = a/s'$, con $F \in \mathfrak{P}$ y $a \in A$, entonces existe $s'' \in S_{\mathfrak{p}}$ tal que $ass'' = Fs's''$, luego $ass'' \in \mathfrak{P} \cap A = \mathfrak{p}$, luego $a \in \mathfrak{p}$ y $a/s \in \mathfrak{p}A_{\mathfrak{p}}$.

Por el teorema anterior $A_{\mathfrak{p}}[X]_{\mathfrak{P}}$ es regular. ■

Según las observaciones tras el teorema 5.17, este teorema se aplica si A es un dominio de ideales principales. En particular se aplica si A es un cuerpo.

5.3 Sucesiones regulares

En esta sección introduciremos algunos conceptos que, entre otras cosas, nos darán una caracterización conveniente de los anillos locales regulares.

Definición 5.22 Sea A un anillo y M un A-módulo. Una sucesión $a_1, \ldots, a_m$ de elementos de A es *M-regular* si cumple

a) $M \neq (a_1, \ldots, a_m)M$,

b) a_{i+1} no es un divisor de cero de $M/(a_1, \ldots, a_i)M$, para $i = 0, \ldots, m-1$.

La condición b) para $i = 0$ ha de entenderse como que a_1 no es un divisor de cero de M.

Notemos que la definición de sucesión M-regular depende de la ordenación de los elementos $a_1, \ldots, a_m$.

Como primera observación, aplicando sucesivamente 4.58, vemos que una sucesión A-regular $a_1, \ldots, a_m$ en un anillo noetheriano local A cumple

$$\dim A/(a_1, \ldots, a_m) = \dim A - m,$$

luego el teorema 5.18 nos da que $a_1, \ldots, a_m$ está contenida en un sistema de parámetros de A. En particular $m \leq \dim A$ y si se da la igualdad entonces $a_1, \ldots, a_m$ es un sistema de parámetros de A.

Por otra parte, podemos hablar de sucesiones A-regulares en anillos arbitrarios. El ejemplo más simple es $X_1, \ldots, X_n$ en $A[X_1, \ldots, X_n]$.

Vamos a probar que la propiedad del teorema 5.9 caracteriza las sucesiones A-regulares en anillos noetherianos locales, con lo que en particular los sistemas regulares de parámetros serán sucesiones A-regulares. Empezamos con una implicación que no requiere que el anillo sea local:

Teorema 5.23 *Sea A un anillo, sea $a_1, \ldots, a_m$ una sucesión A-regular y sea $I = (a_1, \ldots, a_m)$. Entonces el epimorfismo*

$$\phi : (A/I)[X_1, \ldots, X_m] \longrightarrow \operatorname{gr}_I(A)$$

dado por $\phi(X_i) = a_i + I^2$ es un isomorfismo de anillos graduados.

Demostración: Vamos a trabajar en el anillo completo de cocientes de A, es decir, el anillo de las fracciones cuyos denominadores no son divisores de cero. Así a_1 es un denominador admisible. Veamos en primer lugar que el epimorfismo

$$\psi : A[Y_2, \ldots, Y_m] \longrightarrow A[a_2/a_1, \ldots, a_m/a_1]$$

dado por $\psi(Y_i) = a_i/a_1$ tiene núcleo $(a_1Y_2 - a_2, \ldots, a_1Y_m - a_m)$. (Esto ha de entenderse trivialmente si $m = 1$.)

Una inclusión es obvia. Para probar la otra suponemos primeramente $m = 2$. Dado $F(Y_2) \in A[Y_2]$, podemos dividirlo euclídeamente entre $a_1Y_2-a_2$ en el anillo $A_{a_1}[Y_2]$, y eliminando denominadores llegamos a que

$$a_1^d F(Y_2) = G(Y_2)(a_1Y_2 - a_2) + r,$$

donde $G(Y_2) \in A[Y_2]$, $d \geq 0$ y $r \in A$.

Si F está en el núcleo de ψ, entonces $r = 0$. Consideramos la ecuación módulo a_1^d. Sabemos que a_2 no es un divisor de cero en $A/(a_1)$, luego tampoco lo es en $A/(a_1^d)$. En la prueba de 4.60 hemos visto que entonces $a_1Y_2 + a_2$ no es un divisor de cero en $(A/(a_1^d))[Y_2]$, luego todos los coeficientes de G han de ser divisibles entre a_1^d, luego $F(Y_2) \in (a_1Y_2 - a_2)$.

Ahora razonamos por inducción sobre m. Sea $A' = A[a_2/a_1]$. Vamos a demostrar que $a_1, a_3, \ldots, a_m$ es una sucesión A'-regular. Para ello observamos en primer lugar que podemos definir un isomorfismo

$$f : (A/(a_1, a_2))[T] \longrightarrow A'/(a_1, a_2)A'$$

mediante $p(F(T)]) \mapsto [F(a_2/a_1)]$, donde $p : A[T] \longrightarrow (A/(a_1, a_2))[T]$ es el epimorfismo canónico. Es claro que f está bien definida y es un epimorfismo. Si $p(F)$ está en el núcleo, entonces

$$F(a_2/a_1) = a_1G_1(a_2/a_1) + a_2G_2(a_2/a_1), \qquad G_1, G_2 \in A[T].$$

Por lo tanto, $F - a_1G_1 - a_2G_2$ está en el núcleo de la aplicación ψ para el caso ya probado, es decir, $F - a_1G_1 - a_2G_2 = G(T)(a_1T - a_2)$. Por consiguiente $p(F) = 0$.

A su vez f induce un isomorfismos para $i \geq 2$:

$$\begin{aligned} (A/(a_1, \ldots, a_i))[T] &\cong \big(A/(a_1, a_2)) \,/\, ([a_1], \ldots, [a_i])\big)[T] \\ \cong (A/(a_1, a_2))[T]/([a_1], \ldots, [a_i]) &\cong (A'/(a_1, a_2)A')/([a_1], \ldots, [a_i]) \\ &\cong A'/(a_1, \ldots, a_i)A'. \end{aligned}$$

Concluimos que $(a_1, a_3 \ldots, a_m)A' \neq A'$. Del hecho de que a_1 no es un divisor de cero en A, se sigue fácilmente que tampoco lo es en A'. Para cada $i \geq 2$, si a_{i+1} fuera un divisor de cero en $A'/(a_1, a_3 \ldots, a_i)A' = A'/(a_1, \ldots, a_i)A'$, también lo sería en $(A/(a_1, \ldots, a_i))[T]$, luego en $A/(a_1, \ldots, a_i)$, lo cual es imposible.

Con esto hemos probado que $a_1, a_3, \ldots, a_m$ es A'-regular. Ahora observamos que ψ es la composición

$$A[Y_2, \ldots, Y_m] \xrightarrow{\psi_1} A[a_2/a_1][Y_3, \ldots, Y_m] \xrightarrow{\psi_2} A[a_2/a_1, \ldots, a_m/a_1].$$

Por la parte ya probada, el núcleo de ψ_1 es $(a_1Y_2 - a_2)A[Y_2, \ldots, Y_m]$ y por hipótesis de inducción el de ψ_2 es $(a_1Y_3 - a_3, \ldots, a_1Y_m - a_m)$. Por lo tanto, si F está en el núcleo de ψ, sabemos que

$$F(a_2/a_1, Y_3, \ldots, Y_m) = \sum_{i=3}^{m} G_i(a_2/a_1, Y_3, \ldots, Y_m)(a_1Y_i - a_1),$$

luego

$$F-\sum_{i=3}^{m} G_i(Y_2,\ldots,Y_m)(a_1Y_i-a_1)=G_2(Y_2,\ldots,Y_m)(a_1Y_2-a_2)$$

y F tiene la forma requerida.

Con esto ya podemos probar el teorema. Basta ver que el núcleo de ϕ no contiene polinomios homogéneos. Esto equivale a que para polinomio homogéneo F de grado d tal que $F(a_1,\ldots,a_m)\in I^{d+1}$ cumple que $F\in IA[X_1,\ldots,X_m]$.

Tenemos que $F(a_1,\ldots,a_m)=G(a_1,\ldots,a_m)$, donde G también es homogéneo de grado d pero tiene sus coeficientes en I. Basta probar que $F-G$ tiene sus coeficientes en I o, equivalentemente, podemos suponer que $F(a_1,\ldots,a_m)=0$. Ahora bien, en tal caso

$$F(1,a_2/a_1,\ldots,a_m/a_1)=(1/a_1^d)F(a_1,\ldots,a_m)=0.$$

Por consiguiente $F(1,Y_2,\ldots,Y_m)$ está en el núcleo de ψ, y tiene los mismos coeficientes que F. Como está en $(a_1Y_2-a_2,\ldots,a_1Y_m-a_m)$ y todos los generadores de este ideal tienen sus coeficientes en I, lo mismo le sucede a F.

■

Antes de probar el recíproco demostramos un resultado que se basa en los hechos que hemos obtenido en la demostración del teorema anterior y que tiene interés en sí mismo:

Teorema 5.24 *Sea A un anillo, sea $a_1,\ldots,a_m$ una sucesión A-regular y sea $I=(a_1,\ldots,a_m)$. Entonces $\operatorname{alt} I=m$, es decir, las sucesiones A-regulares generan intersecciones completas.*

DEMOSTRACIÓN: Para cada divisor primo minimal $\mathfrak{p}$ de I el teorema de la altura nos da que $\operatorname{alt}\mathfrak{p}\leq m$, luego sólo hemos de probar que $\operatorname{alt}\mathfrak{p}\geq m$. Si $m=1$ es consecuencia del teorema de los ideales principales, pues a_1 no es un divisor de cero en A.

Suponemos, pues, que $m\geq 2$ y que el teorema es cierto para $m-1$. Entonces $\mathfrak{p}A[Y_2]$ es un divisor primo minimal de $IA[Y_2]$. En efecto, es primo porque $A[Y_2]/\mathfrak{p}A[Y_2]\cong(A/\mathfrak{p})[Y_2]$, y es minimal, pues si $IA[Y_2]\subset\mathfrak{P}\subset\mathfrak{p}A[Y_2]$, entonces $I\subset\mathfrak{P}\cap A\subset\mathfrak{p}A[Y_2]\cap A=\mathfrak{p}$, luego $\mathfrak{P}\cap A=\mathfrak{p}$, luego $\mathfrak{p}A[Y_2]=\mathfrak{P}$.

En la demostración del teorema anterior hemos visto que el epimorfismo $\psi:A[Y_2]\longrightarrow A'$ dado por $\psi(Y_2)=a_2/a_1$ tiene núcleo $(a_1Y_2-a_2)\subset\mathfrak{p}A[Y_2]$.

Como $\psi[\mathfrak{p}A[Y_2]]=\mathfrak{p}A_1$, concluimos que $\mathfrak{p}A_1$ es un ideal primo de A_1. Es claro entonces que se trata de un divisor primo minimal de IA_1, pues si tenemos $IA_1\subset\mathfrak{P}\subset\mathfrak{p}A_1$, entonces $IA[Y_2]\subset\psi^{-1}[\mathfrak{P}]\subset\mathfrak{p}A[Y_2]$, luego $\psi^{-1}[\mathfrak{P}]=\mathfrak{p}A[Y_2]$ y $\mathfrak{P}=\mathfrak{p}A_1$.

En la prueba del teorema anterior también hemos visto que $a_1,a_3,\ldots,a_m$ es una sucesión A'-regular, y como $IA_1=(a_1,a_3,\ldots a_m)A_1$, la hipótesis de inducción nos da que $\operatorname{alt}\mathfrak{p}A_1\geq m-1$.

Finalmente observamos que $f = a_1 Y_2 - a_2$ está en el núcleo de ψ y no es un divisor de cero en $A[Y_2]$, porque a_1 no es un divisor de cero en A. Por el teorema de los ideales principales, $\operatorname{alt}(f) = 1$. Esto significa que si formamos una cadena de ideales primos

$$\mathfrak{P}_0 \subsetneq \cdots \subsetneq \mathfrak{P}_h = \mathfrak{p}A[Y_2]$$

de modo que $\mathfrak{P}_0$ sea un divisor primo minimal del núcleo de ψ, entonces $\mathfrak{P}_0$ contendrá un divisor primo minimal de (f), que a su vez contendrá estrictamente otro ideal primo. Por lo tanto, $m - 1 \leq h = \operatorname{alt} \mathfrak{p}A_1 < \operatorname{alt} \mathfrak{p}A[Y_2] = \operatorname{alt} \mathfrak{p}$. En definitiva, $\operatorname{alt} \mathfrak{p} \geq m$. ■

Ésta es la caracterización anunciada de las sucesiones A-regulares en anillos noetherianos locales:

Teorema 5.25 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal, sean $a_1, \ldots, a_m \in \mathfrak{m}$ y sea $I = (a_1, \ldots, a_m)$. Entonces $a_1, \ldots, a_m$ es una sucesión A-regular si y sólo si el epimorfismo*

$$\phi : (A/I)[X_1, \ldots, X_m] \longrightarrow \operatorname{gr}_I(A)$$

dado por $\phi(X_i) = a_i + I^2$ es un isomorfismo de anillos graduados.

Demostración: Una implicación es el teorema 5.23. Veamos que a_1 no es un divisor de cero. Si $ba_1 = 0$ y $b \neq 0$, por el teorema 4.21 sabemos que $L_I(b) \neq 0$. Por otra parte, $L_I(a_1) = a_1 + I^2$ no es un divisor de cero en $\operatorname{gr}_I(A)$ (pues se corresponde con X_1 a través del isomorfismo). El teorema 5.14 nos da entonces que $L_I(b)L_I(a_1) = L_I(ba_1) = 0$, lo cual es absurdo.

Sean $A_1 = A/(a_1)$ e $I_1 = I/(a_1)$. Claramente tenemos un epimorfismo natural de anillos graduados

$$\operatorname{gr}_I(A) \longrightarrow \operatorname{gr}_{I_1}(A_1).$$

Veamos que su núcleo es $(L_I(a_1))$. Una inclusión es obvia. Para probar la contraria podemos considerar un elemento homogéneo del núcleo, que será de la forma $x = L_I(b) = b + I^{n+1}$. Entonces $b + (a_1) \in I_1^{n+1}$, luego $b + (a_1) = b' + (a_1)$, donde $b' \in I^{n+1}$. Así $b - b' = ca_1$ y $x = L_I(ca_1) = L_I(c)L_I(a_1)$, por 5.14, ya que $L_I(a_1)$ no es un divisor de cero en $\operatorname{gr}_I(A)$.

Así, pues, $\operatorname{gr}_{I_1}(A_1) \cong \operatorname{gr}_I(A)/(L_I(a_1)) \cong (A/I)[X_2, \ldots, X_m]$.

Ahora el teorema es inmediato por inducción sobre m. Para $m = 1$ se reduce al hecho ya probado de que a_1 no es un divisor de cero. Supuesto cierto para $m-1$, la hipótesis de inducción nos da que $a_2, \ldots, a_m$ es una sucesión A_1-regular en A_1, lo que implica inmediatamente que $a_1, \ldots, a_m$ es A-regular. ■

En particular, el teorema 5.9 implica ahora que los sistemas regulares de parámetros son sucesiones A-regulares. Otra consecuencia es que en un anillo noetheriano local la propiedad de ser una sucesión A-regular no depende del orden de sus términos. Veamos una consecuencia más:

Teorema 5.26 *Sea A un anillo local regular de dimensión d y $\mathfrak{m} = (a_1, \ldots, a_d)$ su ideal maximal. Entonces, para cada $m \leq d$, el ideal $(a_1, \ldots, a_m)$ es primo y tiene altura m.*

DEMOSTRACIÓN: Tenemos que $a_1, \ldots, a_d$ es una sucesión A-regular, luego $a_1, \ldots, a_m$ también lo es. La altura del ideal que generan es m por el 5.24. Por último, el ideal es primo porque el cociente es regular en virtud de 5.19, luego en particular es un dominio íntegro. ■

Para el próximo resultado necesitamos un sencillo hecho previo:

Teorema 5.27 *Sea M un A-módulo y a, $b \in M$. Si a, b es una sucesión M-regular y b no es un divisor de cero de M, entonces b, a también es una sucesión M-regular.*

DEMOSTRACIÓN: Sólo hay que probar que a no es un divisor de cero de M/bM. En caso contrario existe un $m \in M \setminus bM$ tal que $am = bm'$, con $m' \in M$. Como a, b es una sucesión M-regular, ha de ser $m' \in aM$, digamos $m' = am''$, con $m'' \in M$. Entonces $m = bm''$, porque a no es un divisor de cero en M, pero entonces $m \in mM$, contradicción. ■

Teorema 5.28 *Sea A un anillo noetheriano, M un A-módulo finitamente generado e I un ideal de A tal que $IM \neq M$. Entonces toda sucesión M-regular contenida en I puede extenderse hasta una sucesión maximal (en el sentido de que no puede prolongarse a otra mayor). Además dos sucesiones M-regulares maximales en I tienen necesariamente la misma longitud.*

DEMOSTRACIÓN: Es evidente que si $a_1, \ldots, a_m$ es una sucesión M-regular se cumple que $(a_1, \ldots, a_i)M \subsetneq (a_1, \ldots, a_{i+1})M$, pues existe $m \in M \setminus (a_1, \ldots, a_i)M$ y entonces $a_{i+1}m \notin (a_1, \ldots, a_i)M$.

Así pues, si una sucesión M-regular pudiera prolongarse indefinidamente, daría lugar a una cadena estrictamente creciente de submódulos de M. Esto prueba que toda sucesión se prolonga hasta una maximal.

De entre todas las sucesiones M-regulares maximales contenidas en I, tomamos una con el menor número de elementos n. Vamos a probar el teorema por inducción sobre n. Si $n = 0$ entonces I consta únicamente de divisores de cero de M, luego no hay sucesiones M-regulares y no hay nada que probar.

Sea $a_1, \ldots, a_n$ una sucesión M-regular maximal en I de longitud mínima y sea $b_1, \ldots, b_n$ otra sucesión M-regular en I. Hemos de probar que no puede prolongarse, es decir, que todos los elementos de I son divisores de cero de $M/(b_1, \ldots, b_n)M$.

Si $n = 1$ entonces I consta únicamente de divisores de cero de M/a_1M. Por el teorema 3.55 existe un $m \in M \setminus a_1M$ tal que $Im \subset a_1M$. En particular $b_1m = a_1m'$, para un $m' \in M$. Si fuera $m' \in b_1M$, sería $b_1m = a_1b_1m''$ y, como b_1 no es un divisor de cero de M, tendríamos que $m \in a_1M$, contradicción, luego $m' \notin b_1M$. Como $a_1Im' = Ib_1m \subset a_1b_1M$, tenemos que $Im' \subset b_1M$, luego I está formado por divisores de cero de M/b_1M.

Si $n > 1$ llamamos $M_i = M/(a_1, \ldots, a_i)M$ y $M_i' = M/(b_1, \ldots, b_i)M$, para $i = 0, \ldots, n-1$. Podemos encontrar un $c \in I$ que no es un divisor de cero de ningún M_i ni de ningún M_i'. Ello se debe a que los divisores de cero de estos módulos forman una unión finita de ideales (teoremas 3.49 y 3.54), y el ideal I no está contenido en ninguno de estos ideales. Aplicamos entonces 3.51.

Tenemos que a_n es una sucesión M_{n-1}-regular maximal, luego por el caso $n = 1$, ya probado, también lo es c, luego $a_1, \ldots, a_{n-1}, c$ es M-regular maximal. Entonces a_{n-1}, c es M_{n-2}-regular maximal y por el teorema anterior c, a_{n-1} también es M_{n-2}-regular. Además es maximal, pues, claramente, la maximalidad no depende del orden. En definitiva, $a_1, \ldots, a_{n-2}, c, a_{n-1}$ es M-regular maximal.

Repitiendo el razonamiento vemos que a_{n-2}, c, a_{n-1} es M_{n-3}-regular maximal, luego a_{n-2}, c también es M_{n-3}-regular, luego c, a_{n-2} también lo es, y c, a_{n-2}, a_{n-1} es M_{n-3}-regular maximal.

Concluimos que $a_1, \ldots, a_{n-3}, c, a_{n-2}, a_{n-1}$ es M-regular maximal. En definitiva llegamos a que $c, a_1, \ldots, a_{n-1}$ es M-regular maximal en I y, análogamente, $c, b_1, \ldots, b_{n-1}$ es M-regular.

Entonces $a_1, \ldots, a_{n-1}$ y $b_1, \ldots, b_{n-1}$ son M/cM-regulares en I, y la primera es maximal. También es obvio que M/cM no puede tener sucesiones regulares maximales en I con menos de $n-1$ elementos, luego la hipótesis de inducción nos da que la segunda sucesión también es maximal, luego $c, b_1, \ldots, b_{n-1}$ también es maximal, luego $b_1, \ldots, b_{n-1}, c$ también lo es, luego c es $M/(b_1, \ldots, b_{n-1})M$-regular maximal, luego por el caso $n = 1$ también lo es b_n, luego $b_1, \ldots, b_n$ es M-regular maximal. ■

Definición 5.29 Sea A un anillo noetheriano, M un A-módulo finitamente generado e I un ideal de A tal que $IM \neq M$. La *profundidad* de M respecto de I se define como la longitud de las sucesiones M-regulares maximales en I. La representaremos por $\operatorname{pr}(I, M)$. Si el anillo A es local e I es su ideal maximal, escribiremos simplemente $\operatorname{pr}(M)$.

Es evidente que si $a_1, \ldots, a_m$ es una sucesión M-regular en I, entonces

$$\operatorname{pr}(I, M/(a_1, \ldots, a_m)M) = \operatorname{pr}(I, M) - m.$$

Si A es un anillo noetheriano local, es obvio que $\operatorname{pr}(A) \leq \dim A$. Luego necesitaremos el siguiente refinamiento de esta desigualdad:

Teorema 5.30 *Si A es un anillo noetheriano local, M es un A-módulo finitamente generado y $\mathfrak{p} \in \operatorname{As}(M)$, entonces $\operatorname{pr}(M) \leq \dim A/\mathfrak{p}$.*

Demostración: Vamos a probarlo por inducción sobre $n = \operatorname{pr}(M)$. Para $n = 0$ es trivial. Supongamos que $\operatorname{pr}(M) = n > 0$ y que la desigualdad se cumple para naturales menores. Entonces existe $a \in \mathfrak{m}$ (el ideal maximal de A) tal que $\{a\}$ es una sucesión M-regular. Por la observación previa al teorema tenemos que $\operatorname{pr}(M/aM) = n - 1$.

Basta probar que existe $\mathfrak{p}' \in \operatorname{As}(M/aM)$ tal que $\mathfrak{p} \subsetneq \mathfrak{p}'$, pues entonces

$$\operatorname{pr}(M) = \operatorname{pr}(M/aM) + 1 \leq \dim A/\mathfrak{p}' + 1 \leq \dim A/\mathfrak{p}.$$

Sea $N = \{m \in M \mid \mathfrak{p}m \subset aM\}$. Claramente es un submódulo de M que contiene a aM, así como a $N' = \{m \in M \mid \mathfrak{p}m = 0\}$.

Si fuera $N = aM$, entonces todo $n' \in N'$ sería de la forma $n' = am$, con $m \in M$, y de $\mathfrak{p}n' = 0$ pasaríamos a $\mathfrak{p}m = 0$ (pues a no es un divisor de cero de M), luego $m \in N'$ y, en definitiva, tendríamos que $N' = aN'$, y por el lema de Nakayama $N' = 0$, pero esto contradice que $\mathfrak{p}$ sea un primo asociado.

Así pues, $U = N/aM$ es un A-módulo no nulo. Tomamos $\mathfrak{p}' \in \operatorname{As}(U)$. Como $\mathfrak{p}U = 0$, se cumple que $\mathfrak{p} \subset \mathfrak{p}'$ y la inclusión es estricta porque $a \in \mathfrak{p}' \setminus \mathfrak{p}$. ■

Vamos a relacionar la profundidad de un ideal con su número de generadores minimales. Para ello necesitamos un resultado técnico:

Teorema 5.31 *Sea A un anillo y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos de A. Sea I un ideal de A y $x \in A$ tal que (I, x) no esté contenido en la unión de los $\mathfrak{p}_i$. Entonces existe un $a \in I$ tal que $x + a$ no pertenece a dicha unión.*

Demostración: Podemos suponer que ningún $\mathfrak{p}_i$ está contenido en otro $\mathfrak{p}_j$, pues en tal caso podríamos eliminar el menor. Reordenando los ideales podemos suponer que $x \in \mathfrak{p}_i$ para $i = 1, \ldots, r$, pero que $x \notin \mathfrak{p}_i$ para $i = r + 1, \ldots, n$ (sin excluir las posibilidades $r = 0$ o $r = n$). Si $r = 0$ basta tomar $a = 0$, así que podemos suponer $r > 0$.

Tenemos que $I \not\subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$, pues en otro caso (I, x) estaría contenido en dicha unión. Por lo tanto, existe un $a_0 \in I$ que no pertenece a ningún $\mathfrak{p}_i$, para $i = 1, \ldots, r$.

Por otra parte, podemos tomar un $y \in (\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n) \setminus (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r)$. En efecto, si $r = n$ basta tomar $y = 1$, y en otro caso, si no existiera tal y tendríamos que $\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$, luego el teorema 3.51 nos daría que $\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n \subset \mathfrak{p}_i$, para un $i \leq r$, y como $\mathfrak{p}_i$ es primo tendríamos también que $\mathfrak{p}_j \subset \mathfrak{p}_i$ para algún $j \leq r$, en contradicción con lo supuesto.

Ahora basta tomar $a = a_0 y$. ■

Teorema 5.32 *Sea A un anillo noetheriano, sea M un A-módulo finitamente generado e I un ideal de A tal que $IM \neq M$. Entonces $\operatorname{pr}(I, M) \leq \mu(I)$, y si se da la igualdad entonces I está generado por una sucesión M-regular.*

Demostración: Sea $I = (x_1, \ldots, x_k)$, donde podemos suponer $k > 0$. Si $\operatorname{pr}(I, M) = 0$ no hay nada que probar, luego podemos suponer que los elementos de I no son todos divisores de cero de M.

Aplicamos el teorema anterior con $x = x_1$, el ideal $(x_2, \ldots, x_k)$ (sin excluir que sea nulo si $k = 1$) y los primos asociados de M (cuya unión es el conjunto de divisores de cero de M). Concluimos que existe un $a \in (x_2, \ldots, x_k)$ tal que $u_1 = x_1 + a$ no es un divisor de cero de M. Notemos que $I = (u_1, x_2, \ldots, x_k)$.

Así, u_1 es una sucesión M-regular en I. Si $\operatorname{pr}(I, M) > 1$, entonces no es maximal, luego no todos los elementos de I son divisores de cero de M/u_1M (en particular, $k > 1$). Entonces, no todos los elementos de $(x_2, \ldots, x_k)$ son divisores de cero de M/u_1M pues, si lo fueran, un elemento arbitrario de I puede escribirse como

$$i = a_1u_1 + a_2x_2 + \cdots + a_kx_k,$$

donde $(a_2x_2 + \cdots + a_kx_k)m = 0$ para cierto $m \in M/u_1M$ no nulo, y entonces $im = 0$ también.

Ahora aplicamos el teorema anterior a $x = x_2$, el ideal $(x_3, \ldots, x_k)$ y los primos asociados de M/u_1M. Obtenemos un $a \in (x_3, \ldots, x_k)$ tal que $u_2 = x_2 + a$ no es un divisor de cero de M/u_1M. Así $I = (u_1, u_2, x_3, \ldots, x_k)$ y la sucesión u_1, u_2 es M-regular.

De este modo, si llamamos $p = \operatorname{pr}(I, M)$, llegamos a que I puede expresarse en la forma $I = (u_1, \ldots, u_p, x_{p+1}, \ldots, x_k)$, donde $u_1, \ldots, u_p$ es una sucesión M-regular. Ciertamente, concluimos que $p \leq k$ (en particular $p \leq \mu(I)$) y si $p = k$, entonces I está generado por una sucesión M-regular. ■

Observemos que si el anillo A del teorema anterior es local, entonces se cumple el recíproco: si el ideal I está generado por una sucesión M-regular, dicha sucesión es maximal en I y es un generador minimal (pues si eliminamos cualquiera de sus miembros nos queda un ideal menor). Por lo tanto se cumple la igualdad $\operatorname{pr}(I, M) = \mu(I)$. Vamos a probar que se cumple algo más fuerte: en tal caso todos los generadores minimales de I son sucesiones M-regulares. Para ello necesitamos un par de resultados previos:

Teorema 5.33 *Sea A un anillo noetheriano, sea M un A-módulo finitamente generado, sea I un ideal de A formado por divisores de cero de M y $x \in A$ un elemento contenido en todos los ideales maximales de A pero que no sea un divisor de cero de M. Entonces todos los elementos de (I, x) son divisores de cero de M/xM.*

Demostración: Basta probar que todos los elementos de I son divisores de cero de M/xM. Sea N el submódulo de M anulado por I. El teorema 3.55 nos da que $N \neq 0$. Si $N \not\subset xM$ el teorema está demostrado. Supongamos, pues que $N \subset xM$. Todo $n \in N$ puede escribirse como $n = xm$, para un $m \in M$. Tenemos que $Ixm = In = 0$, pero x no es un divisor de cero de M, luego $Im = 0$, luego $m \in N$. Así pues, $N = xN$, pero el lema de Nakayama (aplicado al ideal (x), nos da que $N = 0$, contradicción. ■

Teorema 5.34 *Sea A un anillo noetheriano, I un ideal de A, $x \in A$, $J = (I, x)$ y M un A-módulo finitamente generado. Si J está contenido en todos los ideales maximales de A, entonces* $\operatorname{pr}(J, M) \leq \operatorname{pr}(I, M) + 1$.

DEMOSTRACIÓN: Sea $\operatorname{pr}(I, M) = m$ y tomemos una sucesión M-regular $x_1, \ldots, x_m \in I$. Basta probar que la profundidad de J en $M/(x_1, \ldots, x_m)M$ es ≤ 1 o, equivalentemente, podemos suponer $m = 0$ y probar que $\operatorname{pr}(J, M) \leq 1$.

Si J está formado por divisores de cero de M entonces $\operatorname{pr}(J, M) = 0$. Supongamos que J contiene un elemento que no es divisor de cero y entonces hemos de probar que su profundidad es 1.

Aplicamos el teorema 5.31 a los primos asociados de M, con lo que obtenemos un $a \in I$ tal que $x + a$ no es un divisor de cero de M. Como $J = (I, x + a)$, podemos suponer que x no es un divisor de cero de M. Ahora basta probar que los elementos de J son divisores de cero de M/xM, pero eso es lo que afirma el teorema anterior. ■

Finalmente obtenemos el resultado que habíamos anunciado:

Teorema 5.35 *Sea A un anillo noetheriano y sea $I = (x_1, \ldots, x_n)$ un ideal contenido en todos los ideales maximales de A. Sea M un A-módulo finitamente generado no nulo. Entonces* $\operatorname{pr}(I, M) = n$ *si y sólo si los generadores de I son una sucesión M-regular.*

DEMOSTRACIÓN: Una implicación es obvia. Probamos la otra por inducción sobre n. Sea $J = (x_1, \ldots, x_{n-1})$ (admitiendo $J = 0$ si $n = 1$). Si fuera $\operatorname{pr}(J, M) < n - 1$, el teorema anterior nos daría que $\operatorname{pr}(I, M) < n$, luego ha de ser $\operatorname{pr}(J, M) = n - 1$. Por hipótesis de inducción $x_1, \ldots, x_{n-1}$ es una sucesión M-regular. (Todo esto es trivial si $n = 1$.) Hemos de probar que x_n no es un divisor de cero de M/JM, pero, si lo fuera, tendríamos que todos los elementos de I serían divisores de cero de M/JM, por lo que la sucesión regular $x_1, \ldots, x_{n-1}$ sería maximal en I, en contradicción con la hipótesis de que $\operatorname{pr}(I, M) = n$. ■

En particular si un ideal propio I de un anillo noetheriano local A cumple que $\operatorname{pr}(I, M) = \mu(I)$ (si está generado por una sucesión regular), entonces todos los generadores minimales de I son sucesiones M-regulares.

5.4 Anillos de Cohen-Macaulay

Definición 5.36 Diremos que un anillo noetheriano local A es un anillo de *Cohen-Macaulay* si cumple que $\operatorname{pr}(A) = \dim A$. Si A es un anillo noetheriano arbitrario, diremos que es de *Cohen-Macaulay* si para todo ideal maximal $\mathfrak{m}$ de A se cumple que $A_\mathfrak{m}$ es un anillo local de Cohen-Macaulay.

Según hemos visto en la sección anterior, la desigualdad $\operatorname{pr}(A) \leq \dim A$ se cumple siempre. Todo anillo local regular es de Cohen-Macaulay, pues las sucesiones regulares de parámetros son sucesiones regulares de longitud igual a la dimensión. Por consiguiente, todas las propiedades que vamos a estudiar de los anillos locales de Cohen-Macaulay se aplican a los anillos locales regulares, pero tiene interés reconocer que son válidas en este contexto más general.

En primer lugar probamos que la propiedad de Cohen-Macaulay (para anillos locales) se conserva por cocientes sobre sucesiones regulares:

Teorema 5.37 *Sea A un anillo noetheriano local y $\mathfrak{m}$ su ideal maximal. Sea $a_1, \ldots, a_m$ una sucesión A-regular contenida en $\mathfrak{m}$. Entonces A es un anillo de Cohen-Macaulay si y sólo si lo es $A/(a_1, \ldots, a_m)$.*

DEMOSTRACIÓN: Basta probar el teorema para $m = 1$, es decir, tenemos un $a \in \mathfrak{m}$ que no es un divisor de cero. Ahora bien, tras la definición de profundidad hemos observado que $\operatorname{pr}(A/(a)) = \operatorname{pr}(A) - 1$, y el teorema 4.58 nos da que $\dim A/(a) = \dim A - 1$. La conclusión es inmediata. ■

El teorema siguiente es un hecho básico sobre los anillos locales de Cohen-Macaulay:

Teorema 5.38 *Si A es un anillo local de Cohen-Macaulay y $\mathfrak{p}$ es un ideal primo de A, entonces $\mathfrak{p}$ es un primo asociado de A si y sólo si es un primo minimal, y en tal caso* $\dim A/\mathfrak{p} = \dim A$.

DEMOSTRACIÓN: Si $\mathfrak{p}$ es un primo asociado, el teorema 5.30 nos da que

$$\dim A = \operatorname{pr}(A) \leq \dim A/\mathfrak{p} \leq \dim A,$$

luego $\mathfrak{p}$ es un primo minimal y cumple la igualdad del enunciado. ■

Como primera aplicación demostramos la siguiente caracterización de las sucesiones regulares en anillos locales de Cohen-Macaulay:

Teorema 5.39 *Sea A un anillo local de Cohen-Macaulay, sea $\mathfrak{m}$ su ideal maximal y sea $a_1, \ldots, a_r$ una sucesión en $\mathfrak{m}$. Las afirmaciones siguientes son equivalentes:*

a) $a_1, \ldots, a_r$ *es una sucesión A-regular.*

b) $\operatorname{alt}(a_1, \ldots, a_r) = r$.

c) Existen $a_{r+1}, \ldots, a_n \in \mathfrak{m}$ (donde $n = \dim A$) tales que $a_1, \ldots, a_n$ es un sistema de parámetros.

DEMOSTRACIÓN: a) $\Rightarrow$ b) es el teorema 5.24 y b) $\Rightarrow$ c) está probado en las observaciones tras la definición de sucesión regular. Sólo hemos de probar que si $a_1, \ldots, a_n$ es una sucesión de parámetros en A, entonces es A-regular.

Sea $\mathfrak{p}$ un primo asociado de A. Si $a_1 \in \mathfrak{p}$, entonces, del hecho de que $\operatorname{rad}(a_1, \ldots, a_n) = \mathfrak{m}$ se sigue inmediatamente que $a_2, \ldots, a_n$ generan también un ideal $\mathfrak{m}/\mathfrak{p}$-primario en $A/\mathfrak{p}$. El teorema de la dimensión nos da que la dimensión de un anillo noetheriano local es el mínimo número de generadores de un ideal $\mathfrak{m}$-primario, luego tendríamos que $\dim A/\mathfrak{p} < n$, en contradicción con el teorema anterior.

Así pues, a_1 no pertenece a ningún primo asociado de A, es decir, no es un divisor de cero de A, forma una sucesión A-regular y $A/(a_1)$ es también un anillo de Cohen-Macaulay, en el que $a_2, \ldots, a_n$ es un sistema de parámetros. Razonando inductivamente llegamos a que la sucesión $a_1, \ldots, a_n$ es A-regular.

■

En particular, en un anillo local de Cohen-Macaulay, las sucesiones A-regulares maximales son precisamente los sistemas de parámetros. También es claro ahora que un ideal es una intersección completa si y sólo si está generado por una sucesión A-regular.

Pasamos ahora a estudiar los anillos de Cohen-Macaulay no necesariamente locales. El resultado fundamental es el siguiente:

Teorema 5.40 *Sea A un anillo de Cohen-Macaulay y sea $I = (a_1, \ldots, a_m)$ un ideal generado por una sucesión A-regular. Entonces los primos asociados de A/I son los divisores primos minimales de I y tienen todos la misma altura m.*

DEMOSTRACIÓN: El teorema 5.24 nos da que $\operatorname{alt} I = m$ (es decir, que I es una intersección completa). Tomemos un primo $\mathfrak{p}$ asociado a A/I y un ideal maximal $\mathfrak{m}$ de A que contenga a $\mathfrak{p}$. Entonces es fácil ver que la imagen de $a_1, \ldots, a_m$ en $A_\mathfrak{m}$ forma una sucesión $A_\mathfrak{m}$-regular, y que $\mathfrak{p}A_\mathfrak{m}$ es un primo asociado del módulo $A_\mathfrak{m}/(a_1, \ldots, a_m)A_\mathfrak{m} = (A/I)_\mathfrak{m}$. Equivalentemente, $\mathfrak{p}A_\mathfrak{m}/IA_\mathfrak{m}$ es un primo asociado del anillo $(A/I)_\mathfrak{m}$.

Ahora bien, por hipótesis $A_\mathfrak{m}$ es un anillo local de Cohen-Macaulay, y por 5.37 también lo es el cociente. El teorema 5.38 nos da que $\mathfrak{p}A_\mathfrak{m}$ es un primo minimal de $IA_\mathfrak{m}$, luego $\mathfrak{p}$ es un primo minimal de I. Como I es una intersección completa, concluimos que $\operatorname{alt} \mathfrak{p} = m$ (ver la observación tras 5.6).

Por otra parte, los primos minimales de I están formados por divisores de cero de A/I, luego están contenidos en primos asociados del cociente, y como éstos son minimales, concluimos que todo primo minimal es asociado. ■

De aquí deducimos diversas consecuencias:

Teorema 5.41 *Sea A un anillo de Cohen-Macaulay y sea $I \neq A$ un ideal. Entonces* $\operatorname{pr}(I, A) = \operatorname{alt}(I)$.

DEMOSTRACIÓN: Tomemos ahora una sucesión A-regular $a_1, \ldots, a_v$ maximal contenida en I. Entonces, todos los elementos de I son divisores de cero de $A/(a_1, \ldots, a_v)$, luego I está contenido en un primo asociado $\mathfrak{p}$ de este módulo. Por el teorema anterior, $\operatorname{alt} \mathfrak{p} = v$ y $\mathfrak{p}$ es un primo minimal de $(a_1, \ldots, a_v)$, luego también de I. Así pues, $\operatorname{alt} I \leq v$.

Por otra parte, si $\mathfrak{q}$ es un divisor primo minimal de I tal que $\operatorname{alt} \mathfrak{q} = \operatorname{alt} I$, como $(a_1, \ldots, a_v) \subset \mathfrak{q}$, podemos prolongar la sucesión hasta otra maximal (entre las contenidas en $\mathfrak{q}$) de longitud $v' \geq v$ y, razonando con $\mathfrak{q}$ como hemos hecho con I, obtenemos que $\mathfrak{q}$ está contenido en un primo minimal de $(a_1, \ldots, a_{v'})$; pero en este caso ha de ser el propio $\mathfrak{q}$, luego $\operatorname{alt} \mathfrak{q} = v' \geq v$. En definitiva, tenemos que $\operatorname{alt} I = v = \operatorname{pr}(I)$. ■

Teorema 5.42 *En un anillo de Cohen-Macaulay, un ideal propio I es una intersección completa si y sólo si está generado por una sucesión regular.*

DEMOSTRACIÓN: Una implicación es el teorema 5.24, y la otra el teorema anterior junto con 5.32. ■

Teorema 5.43 *Si A es un anillo de Cohen-Macaulay y $\mathfrak{p}$ es un ideal primo de A, entonces $A_{\mathfrak{p}}$ también es un anillo de Cohen-Macaulay.*

DEMOSTRACIÓN: Toda sucesión A-regular contenida en $\mathfrak{p}$ es también $A_{\mathfrak{p}}$-regular, luego $\operatorname{pr}(A_{\mathfrak{p}}) \geq \operatorname{pr}(\mathfrak{p}, A) = \operatorname{alt} \mathfrak{p} = \dim A_{\mathfrak{p}} \geq \operatorname{pr}(A_{\mathfrak{p}})$. Así pues, tenemos la igualdad. ■

Teorema 5.44 *Sea A un anillo local de Cohen-Macaulay y sea $I \neq A$ un ideal. Entonces*

$$\dim A = \dim I + \operatorname{alt}(I).$$

DEMOSTRACIÓN: Si $r = \operatorname{pr}(I) = \operatorname{alt}(I)$, podemos tomar una sucesión A-regular $a_1, \ldots, a_r \in I$. El ideal $J = (a_1, \ldots, a_r)$ tiene también altura r. Los elementos de I/J son divisores de cero de A/J, luego I está contenido en un primo asociado (minimal) de A/J, digamos $J \subset I \subset \mathfrak{p}$, donde $\operatorname{alt} \mathfrak{p} = r$ por el teorema 5.40.

El anillo A/J es también de Cohen-Macaulay, luego el teorema 5.38 nos da que $\dim A/J = \dim A/\mathfrak{p}$, luego también

$$\dim I = \dim A/I = \dim A/J = \dim A - r = \dim A - \operatorname{alt}(I).$$

■

5.5 La dimensión proyectiva

Como ya hemos comentado al principio de este capítulo, algunos resultados más profundos sobre anillos regulares necesitan técnicas más modernas, concretamente, técnicas homológicas. Empezaremos estudiando con más detalle los módulos proyectivos, sobre los que no tenemos más que la definición y el teorema 1.32. La caracterización c) de dicho teorema implica claramente que si M es un A-módulo proyectivo y $S \subset A$ es un conjunto multiplicativo, entonces $S^{-1}M$ es un $S^{-1}A$-módulo proyectivo, pues la localización es un funtor exacto y conserva sumas directas. Vamos a probar un recíproco de este hecho, para lo cual necesitamos un resultado previo. A su vez, para ello conviene dar esta definición: una sucesión exacta

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

se escinde si existe un homomorfismo $\gamma : M'' \longrightarrow M$ tal que $\gamma \circ \beta = 1$, lo cual, según hemos visto en el teorema 1.32, implica que $M \cong M' \oplus M''$, de modo que β se corresponde con la proyección canónica. (Es obvio que, de hecho, esto implica que la sucesión se escinde.)

Teorema 5.45 *Sea A un anillo noetheriano y $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ una sucesión exacta de A-módulos en la que P es finitamente generado. La sucesión se escinde si y sólo si se escinden todas las sucesiones exactas*

$$0 \longrightarrow M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}} \longrightarrow P_{\mathfrak{m}} \longrightarrow 0,$$

para todo ideal maximal $\mathfrak{m}$ de A.

Demostración: Es claro que la sucesión se escinde si y sólo si el homomorfismo natural $\mathrm{Hom}_A(P,N) \longrightarrow \mathrm{Hom}_A(P,P)$ que resulta de componer con el homomorfismo dado $N \longrightarrow P$ es un epimorfismo. Por 3.11 (ver la observación posterior), esto sucede si y sólo si todos los homomorfismos

$$\mathrm{Hom}_A(P,N)_{\mathfrak{m}} \longrightarrow \mathrm{Hom}_A(P,P)_{\mathfrak{m}}$$

son epimorfismos, pero el teorema 3.3 nos permite identificar estos homomorfismos con los homomorfismos naturales

$$\mathrm{Hom}_{A_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}}) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{m}}}(P_{\mathfrak{m}}, P_{\mathfrak{m}}).$$

A su vez, éstos son epimorfismos si y sólo si las sucesiones locales se escinden. ■

Teorema 5.46 *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Entonces M es proyectivo si y sólo si $M_{\mathfrak{m}}$ es proyectivo para todo ideal maximal $\mathfrak{m}$ de A.*

Demostración: Ya sabemos que si M es proyectivo sus localizaciones $M_{\mathfrak{m}}$ son proyectivas. Supongamos que M es localmente proyectivo. A partir de un generador finito de M podemos formar una sucesión exacta

$$0 \longrightarrow K \longrightarrow L \longrightarrow M \longrightarrow 0,$$

donde L es un A-módulo libre de rango finito. Como las localizaciones de M son proyectivas, las sucesiones exactas locales se escinden, luego la sucesión global también. Esto implica que M es un sumando directo de L, luego es proyectivo. ■

Sabemos que los módulos libres son proyectivos. En general el recíproco es falso, pero vamos a ver que sí que se cumple para módulos sobre un anillo local.

Teorema 5.47 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ su cuerpo de restos. Si M es un A-módulo finitamente generado, las afirmaciones siguientes son equivalentes:*

a) *M es libre.*

b) *M es proyectivo.*

c) $\mathrm{Tor}_n^A(M,N) = 0$ *para todo A-módulo N y todo $n \geq 1$.*

d) $\mathrm{Tor}_1^A(M,k) = 0$.

Demostración: Sólo hay que probar d) $\Rightarrow$ a). Supongamos, pues, que $\mathrm{Tor}_1^A(M,k) = 0$ y sea $\{m_1,\ldots,m_d\}$ un sistema generador minimal de M. Consideremos la sucesión exacta

$$0 \longrightarrow M' \longrightarrow A^t \longrightarrow M \longrightarrow 0$$

determinada por el epimorfismo que hace corresponder la base canónica de A^t con el generador dado de M. A partir de esta sucesión obtenemos la sucesión exacta

$$0 \longrightarrow \mathrm{Tor}_0^A(M',k) \longrightarrow \mathrm{Tor}_0^A(A^t,k) \longrightarrow \mathrm{Tor}_0^A(M,k) \longrightarrow 0.$$

Ahora bien, tenemos isomorfismos naturales

$$\mathrm{Tor}_0^A(M',k) \cong M' \otimes_A (A/\mathfrak{m}) \cong M'/\mathfrak{m}M',$$

e igualmente con A^t y M. Por consiguiente, la sucesión exacta da lugar a ésta otra:

$$0 \longrightarrow M'/\mathfrak{m}M' \longrightarrow A^t/\mathfrak{m}A^t \longrightarrow M/\mathfrak{m}M \longrightarrow 0.$$

Un análisis de los isomorfismos considerados muestra que el epimorfismo $A^t/\mathfrak{m}A^t \longrightarrow M/\mathfrak{m}M$ es el inducido por el epimorfismo $A^t \longrightarrow M$ de forma natural. El teorema 4.52 implica que las clases de $m_1, \ldots, m_t$ en $M/\mathfrak{m}M$ son una base de este k-espacio vectorial.

Por otra parte, la base canónica en A^t es un generador minimal de A^t como A-módulo, luego sus clases módulo $\mathfrak{m}A^t$ forman una base de $A^t/\mathfrak{m}A^t$. Esto prueba que el epimorfismo $A^t/\mathfrak{m}A^t \longrightarrow M/\mathfrak{m}M$ es de hecho un isomorfismo (pues es una aplicación k-lineal que transforma una base en una base). La sucesión exacta nos da entonces que $M' = \mathfrak{m}M'$, y por el lema de Nakayama ha de ser $M' = 0$. Por consiguiente $M \cong A^t$ es libre. ■

Nos ocupamos ahora de las resoluciones proyectivas. Si en una resolución proyectiva de un módulo M aparece el módulo nulo, todos los módulos siguientes pueden tomarse nulos, y entonces tenemos una resolución proyectiva finita

$$0 \longrightarrow L_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_1 \longrightarrow L_0 \longrightarrow M \longrightarrow 0.$$

Llamaremos *dimensión proyectiva* de un A-módulo M, representada por $\mathrm{dp}_A M$ a la menor longitud n de una resolución proyectiva de M, entendiendo que $\mathrm{dp}_A M = \infty$ si M no admite resoluciones proyectivas finitas.

En estos términos tenemos que M es proyectivo si y sólo si $\mathrm{dp}_A M = 0$.

Un módulo puede tener resoluciones proyectivas de longitud mayor que la prescrita por su dimensión proyectiva, pero en tal caso se pueden acortar, según se deduce del teorema siguiente:

Teorema 5.48 *Consideremos dos sucesiones exactas de A-módulos*

$$0 \longrightarrow K_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0,$$

$$0 \longrightarrow K'_n \longrightarrow L'_{n-1} \longrightarrow \cdots \longrightarrow L'_0 \longrightarrow M \longrightarrow 0,$$

donde los módulos L_i y L'_i son proyectivos. Entonces

$$K_n \oplus L'_{n-1} \oplus L_{n-2} \cdots \cong K'_n \oplus L_{n-1} \oplus L'_{n-2} \cdots$$

Por consiguiente, K_n es proyectivo si y sólo si lo es K'_n.

Demostración: Vamos a probarlo por inducción sobre n. Para $n = 1$ tenemos sucesiones

$$0 \longrightarrow K \longrightarrow L \xrightarrow{\alpha} M \longrightarrow 0, \qquad 0 \longrightarrow K' \longrightarrow L' \xrightarrow{\alpha'} M \longrightarrow 0.$$

Como L y L' son módulos proyectivos existen homomorfismos $\gamma : L \longrightarrow L'$ y $\gamma' : L' \longrightarrow L$ tales que $\gamma \circ \alpha' = \alpha$, $\gamma' \circ \alpha = \alpha'$.

Definimos $\beta, \beta' : L \otimes L' \longrightarrow L \otimes L'$ mediante $\beta(x, y) = (x, y - \gamma(x))$, $\beta'(x, y) = (x - \gamma'(y), y)$. Obviamente son automorfismos. Vamos a probar que el automorfismo $\alpha^* = \beta' \circ \beta^{-1}$ hace conmutativo el diagrama siguiente:

$$\begin{tikzcd} L \otimes L' \arrow[r, "{(\alpha,0)}"] \arrow[d, "\alpha^*"'] & M \\ L \otimes L' \arrow[ur, "{(0,\alpha')}"'] & \end{tikzcd}$$

En efecto,

$$(\alpha, \alpha')(\beta'(x, y)) = \alpha(x) - \alpha'(y) + \alpha'(y) = \alpha(x) = (\alpha, 0)(x, y),$$

$$(\alpha, \alpha')(\beta(x, y)) = \alpha(x) + \alpha'(y) - \alpha(x) = \alpha'(y) = (0, \alpha')(x, y).$$

Así pues, $\alpha^* \circ (0, \alpha') = \alpha^* \circ \beta \circ (\alpha, \alpha') = \beta' \circ (\alpha, \alpha') = (\alpha, 0)$, como había que probar. Teniendo en cuenta que $K \oplus L'$ es el núcleo de $(\alpha, 0)$ y $L \oplus K'$ el de $(0, \alpha')$, concluimos que $\alpha^*[K \oplus L'] = L \oplus K'$, lo que termina la prueba para $n = 1$.

Supuesto cierto para $n - 1$, llamemos $K_{n-1} \subset L_{n-2}$ y $K'_{n-1} \subset L'_{n-2}$ a las imágenes de los homomorfismos correspondientes de las sucesiones exactas dadas, con los que podemos formar nuevas sucesiones exactas

$$0 \longrightarrow K_{n-1} \longrightarrow L_{n-2} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0,$$

$$0 \longrightarrow K'_{n-1} \longrightarrow L'_{n-2} \longrightarrow \cdots \longrightarrow L'_0 \longrightarrow M \longrightarrow 0.$$

Por hipótesis de inducción tenemos que

$$K'_{n-1} \oplus L_{n-2} \oplus L'_{n-3} \oplus \cdots \cong K_{n-1} \oplus L'_{n-2} \oplus L_{n-3} \oplus \cdots$$

Por otra parte tenemos las sucesiones exactas

$$0 \longrightarrow K_n \longrightarrow L_{n-1} \longrightarrow K_{n-1} \longrightarrow 0,$$

$$0 \longrightarrow K'_n \longrightarrow L'_{n-1} \longrightarrow K'_{n-1} \longrightarrow 0,$$

con las que podemos formar a su vez las sucesiones exactas

$$0 \longrightarrow K_n \longrightarrow L_{n-1} \oplus L'_{n-2} \oplus L_{n-3} \oplus \cdots \longrightarrow K_{n-1} \oplus L'_{n-2} \oplus L_{n-3} \oplus \cdots \longrightarrow 0,$$

$$0 \longrightarrow K'_n \longrightarrow L'_{n-1} \oplus L_{n-2} \oplus L'_{n-3} \oplus \cdots \longrightarrow K'_{n-1} \oplus L_{n-2} \oplus L'_{n-3} \oplus \cdots \longrightarrow 0,$$

Ahora basta aplicar de nuevo el caso $n = 1$ ya probado (tomando como M los módulos isomorfos de la derecha). ■

El interés de este teorema consiste en que nos permite comparar dos resoluciones proyectivas de un mismo módulo:

Teorema 5.49 *Consideremos una sucesión exacta*

$$0 \longrightarrow K_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0,$$

donde los módulos L_i son proyectivos. Entonces

a) $\mathrm{dp}_A M \leq n$ *si y sólo si* K_n *es proyectivo.*

b) Si $\mathrm{dp}_A M \geq n$ *entonces* $\mathrm{dp}_A K_n = \mathrm{dp}_A M - n$.

Demostración: a) Si K_n es proyectivo es obvio que $\mathrm{dp}_M \leq n$. Recíprocamente, si $\mathrm{dp}_A M = m \leq n$, podemos considerar una resolución proyectiva de longitud m (que puede prolongarse con ceros hasta tener longitud n). Por el teorema anterior K_n es proyectivo.

b) Si $\mathrm{dp}_A M = \infty$, es claro que $\mathrm{dp}_A K_n = \infty$ y el teorema se cumple trivialmente. Supongamos que $\mathrm{dp}_A M = m \geq n$. Podemos construir una resolución

$$0 \longrightarrow K'_m \longrightarrow L'_{m-1} \longrightarrow \cdots \longrightarrow L'_n \longrightarrow K_n,$$

donde los módulos L'_i son proyectivos. Al enlazarla con la dada tenemos una resolución

$$0 \longrightarrow K'_m \longrightarrow L'_{m-1} \longrightarrow \cdots \longrightarrow L'_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M.$$

Por a) tenemos que K'_m es proyectivo, luego $\mathrm{dp}_A K_n \leq m - n$, pero la desigualdad no puede ser estricta o, de lo contrario, $\mathrm{dp}_A M < m$. ■

La dimensión proyectiva también puede caracterizarse localmente:

Teorema 5.50 *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Entonces*

$$\mathrm{dp}_A(M) = \sup_{\mathfrak{m}} \mathrm{dp}_{A_\mathfrak{m}} M_\mathfrak{m},$$

donde $\mathfrak{m}$ recorre los ideales maximales de A.

Toda resolución proyectiva de M se localiza a una resolución proyectiva de $M_\mathfrak{m}$, luego tenemos que $\mathrm{dp}_{A_\mathfrak{m}} M_\mathfrak{m} \leq \mathrm{dp}_A M$. Si el supremo de las dimensiones locales es infinito no hay nada que probar. Supongamos que dicho supremo es igual a d. Entonces formamos una sucesión exacta

$$0 \longrightarrow K_d \longrightarrow L_{d-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0,$$

donde los módulos L_i son libres de rango finito y K_d es finitamente generado. Al localizar respecto a un ideal maximal $\mathfrak{m}$ obtenemos una sucesión análoga con módulos proyectivos (no necesariamente libres). Por el teorema anterior los módulos $(K_d)_\mathfrak{m}$ son proyectivos, luego K_d también lo es (por el teorema 5.46). Esto implica que $\mathrm{dp}_A M \leq d$, y tenemos la igualdad. ■

El teorema siguiente generaliza las tres últimas equivalencias de 5.47:

Teorema 5.51 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal, sea $k = A/\mathfrak{m}$ su cuerpo de restos y sea M un A-módulo finitamente generado. Las afirmaciones siguientes son equivalentes:*

a) $\operatorname{dp}_A M \leq d$.

b) $\operatorname{Tor}_n^A(M, N) = 0$ *para todo A-módulo N y todo $n \geq d + 1$.*

c) $\operatorname{Tor}_{d+1}^A(M, k) = 0$.

Demostración: Si $\operatorname{dp}_A M \leq d$ podemos calcular los productos de torsión con una resolución proyectiva de M que se anule a partir del término $d+1$, lo que nos da que los correspondientes productos de torsión son nulos.

Vamos a probar c) $\Rightarrow$ a) por inducción sobre d. El caso $d = 0$ es 5.47. Supongamos que el teorema se cumple para d y que $\operatorname{Tor}_{d+1}^A(M, k) = 0$. Consideremos una sucesión exacta

$$0 \longrightarrow M' \longrightarrow L \longrightarrow M \longrightarrow 0,$$

donde L es un A-módulo libre de rango finito. A partir de ella obtenemos una sucesión exacta

$$\operatorname{Tor}_{d+1}^A(M, k) \longrightarrow \operatorname{Tor}_d^A(M', k) \longrightarrow \operatorname{Tor}_d^A(L, k)$$

El primer producto de torsión es nulo por hipótesis, y el último lo es por 5.47, ya que L es proyectivo. Concluimos que $\operatorname{Tor}_d^A(M', k) = 0$, luego por hipótesis de inducción $\operatorname{dp}_A M' \leq d$. Por el teorema 5.49 concluimos que $\operatorname{dp}_A M \leq d + 1$. ■

De aquí se sigue a su vez una versión para anillos noetherianos cualesquiera:

Teorema 5.52 *Sea A un anillo noetheriano y M un A-módulo finitamente generado. Las afirmaciones siguientes son equivalentes:*

a) $\operatorname{dp}_A M \leq d$.

b) $\operatorname{Tor}_n^A(M, N) = 0$ *para todo A-módulo N y todo $n \geq d + 1$,*

c) $\operatorname{Tor}_{d+1}^A(M, A/\mathfrak{m}) = 0$ *para todo ideal maximal $\mathfrak{m}$ de A.*

Demostración: Basta probar que c) $\Rightarrow$ a). Por el teorema 5.50 basta ver que $\operatorname{dp}_{A_\mathfrak{m}}(M_\mathfrak{m}) \leq d$. Por el teorema anterior esto equivale a su vez a que $\operatorname{Tor}_{d+1}^{A_\mathfrak{m}}(M_\mathfrak{m}, A/\mathfrak{m}) = 0$. Por consiguiente, basta ver que existe un epimorfismo de A-módulos $\operatorname{Tor}_{d+1}^A(M, A/\mathfrak{m}) \longrightarrow \operatorname{Tor}_{d+1}^{A_\mathfrak{m}}(M_\mathfrak{m}, A/\mathfrak{m})$. Para ello tomamos una resolución proyectiva de M y, al localizarla, obtenemos otra de $M_\mathfrak{m}$:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & L_1 & \longrightarrow & L_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & (L_1)_\mathfrak{m} & \longrightarrow & (L_0)_\mathfrak{m} & \longrightarrow & M_\mathfrak{m} & \longrightarrow & 0
\end{array}$$

Las flechas verticales son los epimorfismos naturales. Al multiplicar tensorialmente por $A/\mathfrak{m}$ no se pierde la suprayectividad, ni tampoco al formar los grupos de homología, luego el teorema está probado. ■

Nota Si A es un anillo noetheriano local y k es su cuerpo de restos, entonces

$$\mathrm{dp}_A k = \sup_M \mathrm{dp}_A M,$$

donde M recorre todos los A-módulos finitamente generados.

En efecto, basta probar que un miembro es menor o igual que un natural d si y sólo si lo es el otro. Ahora bien: por 5.51 tenemos que $\mathrm{dp}_A k \leq d$ si y sólo si $\mathrm{Tor}_{d+1}^A(k, M) = 0$ para todo A-módulo finitamente generado M y, cambiando el orden de los módulos, el mismo teorema implica que esto equivale a que $\mathrm{dp}_A M \leq d$ para todo A-módulo M finitamente generado. ■

Definición 5.53 Llamaremos *dimensión homológica* de un anillo A como

$$\mathrm{Dh}(A) = \sup_M \mathrm{dp}_A M,$$

donde M recorre los A-módulos finitamente generados.

Puede probarse que si suprimimos la condición de finitud sobre M obtenemos el mismo resultado, pero no necesitaremos este hecho. Uno de los resultados fundamentales que vamos a demostrar es que un anillo noetheriano local es regular si y sólo si su dimensión homológica es finita, en cuyo caso coincide con su dimensión de Krull. Esto nos permitirá, entre otras cosas, extender la noción de regularidad a anillos no locales. Empezamos con el resultado siguiente:

Teorema 5.54 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal, sea $k = A/\mathfrak{m}$ su cuerpo de restos y sea M un A-módulo no nulo finitamente generado. Sea $a \in \mathfrak{m}$ un elemento M-regular, es decir, que no sea un divisor de cero de M. Entonces $\mathrm{dp}_A(M/aM) = \mathrm{dp}_A M + 1$, donde ambos miembros pueden ser infinitos.*

Demostración: El hecho de que a sea M-regular nos da la sucesión exacta

$$0 \longrightarrow M \xrightarrow{a1_M} M \longrightarrow M/aM \longrightarrow 0,$$

donde 1_M es la identidad en M y $a1_M$ es la multiplicación por a. De ella obtenemos la sucesión exacta

$$\cdots \longrightarrow \mathrm{Tor}_n^A(M, k) \longrightarrow \mathrm{Tor}_n^A(M, k) \longrightarrow \mathrm{Tor}_n^A(M/aM, k)$$
$$\longrightarrow \mathrm{Tor}_{n-1}^A(M, k) \longrightarrow \mathrm{Tor}_{n-1}^A(M, k) \longrightarrow \cdots$$

Analicemos con más detalle el homomorfismo $\mathrm{Tor}_n^A(M, k) \longrightarrow \mathrm{Tor}_n^A(M, k)$. Se trata del homomorfismo inducido por $a1_M$ y que se construye del modo siguiente: tomamos una resolución proyectiva de M, digamos $\{L_n\}_n$, extendemos $a1_M$ a un homomorfismo de complejos, que en este caso podemos tomar $\{a1_{L_n}\}_n$, luego multiplicamos tensorialmente por la identidad en k, con lo que obtenemos $a1_{L_n} \otimes 1_k = 1_{L_n} \otimes a1_k = 0$ (pues $a \in \mathfrak{m}$). Finalmente pasamos al homomorfismo inducido sobre los grupos de homología, que resulta ser nulo.

Teniendo esto en cuenta, de la sucesión exacta anterior se extraen las sucesiones

$$0 \longrightarrow \mathrm{Tor}_n^A(M,k) \longrightarrow \mathrm{Tor}_n^A(M/aM,k) \longrightarrow \mathrm{Tor}_{n-1}^A(M,k) \longrightarrow 0.$$

Si $\mathrm{dp}_A M = \infty$ entonces tenemos que $\mathrm{Tor}_n^A(M,k) \neq 0$ para todo n, luego también $\mathrm{Tor}_n^A(M/aM,k) \neq 0$ para todo n, y así $\mathrm{dp}_A(M/aM) = \infty$.

Si, por el contrario, $\mathrm{dp}_A M = d$, entonces $\mathrm{Tor}_d^A(M,k) \neq 0$ y $\mathrm{Tor}_n^A(M,k) = 0$ para $n \geq d+1$, de donde $\mathrm{Tor}_{d+1}^A(M/aM,k) \neq 0$ y $\mathrm{Tor}_n^A(M/aM,k) \neq 0$ para todo $n \geq d+2$. Esto implica que $\mathrm{dp}_A(M/aM) = d+1$. ■

Como consecuencia inmediata:

Teorema 5.55 *Sea A un anillo local regular de dimensión d, sea $\mathfrak{m}$ su ideal maximal y $k = A/\mathfrak{m}$ su cuerpo de restos. Entonces $\mathrm{dp}_A k = d$.*

DEMOSTRACIÓN: Sea $a_1, \ldots, a_d$ un sistema fundamental de parámetros de A. Entonces $\mathfrak{m} = (a_1, \ldots, a_d)$ y se trata de una sucesión A-regular. Esto significa que a_{i+1} no es un divisor de cero de $A/(a_1, \ldots, a_i)$, luego el teorema anterior nos da que

$$\mathrm{dp}_A(A/(a_1, \ldots, a_{i+1})) = \mathrm{dp}_A(A/(a_1, \ldots, a_i)) + 1.$$

Teniendo en cuenta que $\mathrm{dp}_A A = 0$ (porque A es un A-módulo libre), tenemos la conclusión. ■

Teorema 5.56 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal, sea M un A-módulo finitamente generado y sea $a \in \mathfrak{m}$ un elemento que no sea un divisor de cero ni de A ni de M. Entonces*

$$\mathrm{dp}_A M = \mathrm{dp}_{A/(a)}(M/aM).$$

DEMOSTRACIÓN: Consideremos un generador minimal de M y a partir de él construyamos una sucesión exacta

$$0 \longrightarrow K \longrightarrow L \xrightarrow{\phi} M \longrightarrow 0,$$

donde L es un A-módulo libre de rango $\mu(M)$. Al ser libre, a no puede ser un divisor de cero de L, ni tampoco de K. Tenemos la sucesión exacta

$$0 \longrightarrow K/aK \longrightarrow L/aL \longrightarrow M/aM \longrightarrow 0.$$

La exactitud en L/aL es clara: si $\phi([x]) = 0$ es porque $\phi(x) = a\phi(y)$, para cierto $y \in L$, luego $k = x - ay \in K$, luego $[x] = [k]$ está en la imagen de K/aK. Por otra parte si $k \in K$ cumple $k = ax$, para un $x \in L$, entonces $0 = a\phi(x)$ y, como a no es un divisor de cero en M, ha de ser $\phi(x) = 0$, luego $x \in K$.

Si los dos miembros de la fórmula del enunciado son infinitos no hay nada que probar, luego podemos suponer que al menos uno de los dos es finito, en cuyo caso razonaremos por inducción sobre el mínimo de los dos. Consideramos primero el caso en que alguno de ellos es cero. Esto significa que el módulo correspondiente es proyectivo o, equivalentemente, libre.

Si M es libre entonces $M \cong A^t$, luego $M/aM \cong (A/(a))^t$ también es libre y se cumple la igualdad.

Recíprocamente, si M/aM es un $A/(a)$-módulo libre, su rango tiene que ser precisamente $\mu(M)$, pues si $[m_1], \ldots, [m_r]$ es una base de M/aM, entonces $M = \langle m_1, \ldots, m_r \rangle + aM$, y el lema de Nakayama implica que $M = \langle m_1, \ldots, m_r \rangle$. Así pues, $\mu(M) \leq \operatorname{rang} M/aM = \mu(M/aM) \leq \mu(M)$. Podemos suponer que ϕ transforma una base de L en el generador $m_1, \ldots, m_r$. Entonces es fácil ver que el epimorfismo $L/aL \longrightarrow M/aM$ es un isomorfismo, ya que transforma un sistema generador en una base. Esto implica que $K/aK = 0$, luego el lema de Nakayama nos da que $K = 0$. Así pues, $M \cong L$ es libre.

Con esto tenemos demostrado el teorema si alguno de los dos miembros de la fórmula es cero. Supongamos que el mínimo es $n > 0$ y que el teorema se cumple para $n - 1$. Al igual que hemos razonado con M, tenemos que L/aL es un $A/(a)$-módulo libre, luego el teorema 5.49 nos da que

$$\mathrm{dp}_A M = \mathrm{dp}_A(K) + 1, \qquad \mathrm{dp}_{A/(a)}(M/aM) = \mathrm{dp}_{A/(a)}(K/aK) + 1.$$

Por hipótesis de inducción los miembros derechos de estas ecuaciones son iguales, luego los izquierdos también. ■

Definición 5.57 Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea M un A-módulo finitamente generado. Una resolución libre

$$\cdots \longrightarrow L_n \xrightarrow{\alpha_{n-1}} L_{n-1} \xrightarrow{\alpha_{n-2}} \cdots \xrightarrow{\alpha_0} L_0 \xrightarrow{\epsilon} M \longrightarrow 0$$

de M es *minimal* si $\operatorname{Im}(\alpha_n) \subset \mathfrak{m}L_n$ para todo n.

Si llamamos $K_n = \operatorname{Im}\alpha_{n-1} \subset L_{n-1}$, tenemos que $L_0/K_1 \cong M$ y $K_1 \subset \mathfrak{m}L_0$. Si $\epsilon(x_1), \ldots, \epsilon(x_r)$ es un generador minimal de M, entonces

$$L_0 = \langle x_1, \ldots, x_r \rangle + \mathfrak{m}L_0,$$

y el lema de Nakayama implica que $L_0 = \langle x_1, \ldots, x_r \rangle$. Esto nos permite concluir que $\mu(L_0) = \mu(M)$. En particular K_1 es finitamente generado. El mismo razonamiento implica, en general, que $\mu(L_n) = \mu(K_n)$, para $n > 0$, luego todos los módulos son finitamente generados.

Todo A-módulo admite una resolución minimal, pues basta tomar L_0 con rango $\mu(M)$, lo que implica que $K_1 = \mathrm{N}(\epsilon) \subset \mathfrak{m}L_0$. En efecto, si $x_1, \ldots, x_r$ es una base de L_0 tal que $\epsilon(x_1), \ldots, \epsilon(x_r)$ es un generador minimal de M, un elemento de K_1 es de la forma $x = a_1x_1 + \cdots a_rx_r$ y $a_1\epsilon(x_1) + \cdots + a_r\epsilon(x_r) = 0$, luego también es nula la clase de este elemento módulo $\mathfrak{m}M$. Por 4.52 tenemos que las clases de los $\epsilon(x_i)$ módulo $\mathfrak{m}M$ son una base de $M/\mathfrak{m}M$ como $A/\mathfrak{m}$-espacio vectorial, luego concluimos que $a_1, \ldots, a_r \in \mathfrak{m}$, luego $x \in \mathfrak{m}L_0$.

Ahora tomamos L_1 con rango $\mu(K_1)$, lo que implica que $K_2 = \mathrm{N}(\alpha_1) \subset \mathfrak{m}L_1$. De este modo obtenemos la resolución minimal buscada.

Los rangos de los módulos de una resolución minimal son invariantes:

Teorema 5.58 *Si $\{L_n\}_n$ y $\{L'_n\}$ son dos resoluciones minimales de un mismo módulo M (finitamente generado sobre un anillo noetheriano local), entonces $\mu(L_n) = \mu(L'_n)$ para todo n.*

Demostración: Lo probaremos por inducción sobre m. Sabemos que $\mu(L_0) = \mu(L'_0) = \mu(M)$. Si se cumple para $i < n$, el teorema 5.48 nos da que

$$K_n \oplus L'_{n-1} \oplus L_{n-1} \oplus \cdots \cong K'_n \oplus L_{n-1} \oplus L'_{n-2} \oplus \cdots$$

Del teorema 4.52 se sigue inmediatamente que $\mu(M \oplus N) = \mu(M) + \mu(N)$, luego podemos concluir que $\mu(L_n) = \mu(K_n) = \mu(K'_n) = \mu(L'_n)$. ■

De aquí se sigue que si $\mathrm{dp}_A(M) = n$, entonces toda resolución minimal de M se anula a partir de su término $n+1$-simo. En efecto, el teorema 5.49 nos da que K_n es proyectivo, luego libre, luego

$$\cdots \longrightarrow 0 \longrightarrow K_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0$$

es también resolución minimal de M que se anula a partir de su termino $n+1$-ésimo. Por el teorema anterior lo mismo vale para cualquier otra resolución minimal.

Ahora podemos relacionar la dimensión proyectiva con la profundidad de un módulo:

Teorema 5.59 *Sea A un anillo noetheriano local y M un A-módulo finitamente generado tal que $\mathrm{dp}_A M < \infty$. Entonces*

$$\mathrm{dp}_A(M) + \mathrm{pr}\,(M) = \mathrm{pr}(A).$$

Demostración: Sea $d = \mathrm{dp}_A M$ y sea

$$0 \longrightarrow L_d \longrightarrow L_{d-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0$$

una resolución minimal de M. Llamemos $K_i \subset L_{i-1}$ a la imagen del homomorfismo correspondiente.

Probaremos el teorema por inducción sobre $p = \mathrm{pr}\,(A)$. Si $p = 0$ entonces todos los elementos del ideal maximal $\mathfrak{m}$ de A son divisores de cero, luego por 3.55 existe un $x \in A$ no nulo tal que $\mathfrak{m}x = 0$. Si fuera $d > 0$, como $L_d \subset \mathfrak{m}L_{d-1}$, tendríamos que $xL_d \subset x\mathfrak{m}L_{d-1} = 0$, luego $L_d = 0$ (ya que es libre). Como esto es imposible, concluimos que $d = 0$, luego M es libre y $\mathrm{pr}(M) = \mathrm{pr}(A) = 0$.

Supongamos que el teorema se cumple para anillos locales de profundidad menor que $p > 0$. Consideremos primeramente el caso en que $\mathrm{pr}(M) > 0$. Tenemos entonces que $\mathfrak{m}$ no puede ser el anulador de ningún elemento de A ni tampoco de un elemento de M. Esto implica que $\mathfrak{m}$ no está contenido en la unión de los primos asociados de A y los de M, pues son un número finito y si estuviera contenido en la unión estaría contenido en uno de ellos (teorema 3.51). Así pues, existe un $a \in \mathfrak{m}$ que no es ni un divisor de cero de A ni un divisor de cero de M.

Por la observación tras la definición 5.29 tenemos que $\operatorname{pr}(A/(a)) = p - 1$ y $\operatorname{pr}(M/aM) = \operatorname{pr}(M) - 1$. Además, según el teorema 5.56 se cumple que

$$\operatorname{dp}_{A/(a)}(M/aM) = \operatorname{dp}_A(M).$$

Ahora basta aplicar la hipótesis de inducción.

Nos queda finalmente el caso en que $p > 0$ y $\operatorname{pr}(M) = 0$. Ahora sólo podemos tomar un $a \in \mathfrak{m}$ que no sea un divisor de cero de A. Consideramos la sucesión exacta

$$0 \longrightarrow K_1 \longrightarrow L_0 \longrightarrow M \longrightarrow 0.$$

De ella derivamos la sucesión exacta

$$0 \longrightarrow \operatorname{An}(a) \xrightarrow{\psi} K_1/aK_1 \longrightarrow L_0/aL_0 \longrightarrow M/aM \longrightarrow 0.$$

La única parte no trivial es la definición del primer monomorfismo. Ahora bien, si $x \in \operatorname{An}(a)$, tomamos una antiimagen $x \in L$ y definimos $\psi(x) = al + aK_1$. Es fácil ver que $al \in K_1$ y que $\psi(x)$ no depende de la elección de l. La prueba de que la sucesión es exacta es la vista en la demostración de 5.56 con una mínima variación.

Como $\operatorname{pr}(M) = 0$, el teorema 3.55 nos da un $m \in M$ no nulo tal que $\mathfrak{m}m = 0$. En particular $m \in \operatorname{An}(a)$, luego todos los elementos de $\mathfrak{m}$ son divisores de cero de K_1/aK_1. Por consiguiente $\operatorname{pr}(K_1/aK_1) = 0$. Como a no es un divisor de cero de K_1 (porque L_0 es libre), llegamos a que $\operatorname{pr}(K_1) = 1$.

Por otra parte, como M tiene divisores de cero no puede ser libre, luego $\operatorname{dp}_A M > 0$ y $\operatorname{dp}_A K_1 = \operatorname{dp}_A M - 1$. Por el caso ya probado,

$$\operatorname{dp}_A K_1 + \operatorname{pr}(K_1) = \operatorname{pr}(A),$$

de donde concluimos que $\operatorname{dp}_A M = \operatorname{pr}(A)$. ■

Nos falta un último resultado técnico para obtener todos los resultados que perseguimos:

Teorema 5.60 *Sea A un anillo noetheriano local y M un A-módulo finitamente generado de dimensión proyectiva finita. Si* $\operatorname{An}(M) \neq 0$ *entonces contiene un elemento que no es un divisor de cero de A.*

Demostración: Tomemos una resolución libre finita

$$0 \longrightarrow L_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0$$

en la que todos los módulos L_i tengan rango finito. Si $\mathfrak{p} \in \operatorname{As}(M)$, entonces

$$0 \longrightarrow (L_n)_\mathfrak{p} \longrightarrow (L_{n-1})_\mathfrak{p} \longrightarrow \cdots \longrightarrow (L_0)_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow 0$$

es una resolución proyectiva de $M_{\mathfrak{p}}$ como $A_{\mathfrak{p}}$-módulo, luego $\operatorname{dp}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) < \infty$ y $\operatorname{pr}(A_{\mathfrak{p}}) = 0$, pues todos los elementos de $\mathfrak{p}$ son divisores de cero de $A_{\mathfrak{p}}$. Por el teorema anterior $\operatorname{dp}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) = 0$, es decir, $M_{\mathfrak{p}}$ es un $A_{\mathfrak{p}}$-módulo libre. Es claro que $\operatorname{rang}_{A_{\mathfrak{p}}}(L_i)_{\mathfrak{p}} = \operatorname{rang}_A L_i$, y se comprueba sin dificultad que

$$\operatorname{rang}_{A_{\mathfrak{p}}} M_{\mathfrak{p}} = \sum_{i=0}^{n} (-1)^i \operatorname{rang}_A L_i.$$

En particular $\operatorname{rang}_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ es independiente de $\mathfrak{p} \in \operatorname{As}(M)$. Supongamos que este rango es no nulo y llegaremos a una contradicción.

Sea $I = \operatorname{An}(M) \neq 0$. Tenemos que $IA_{\mathfrak{p}}M_{\mathfrak{p}} = 0$, pero, como $M_{\mathfrak{p}} \neq 0$ es libre, esto sólo puede ocurrir si $I_{\mathfrak{p}} = IA_{\mathfrak{p}} = 0$. Considerando un generador finito de I podemos encontrar un mismo $s \in A \setminus \mathfrak{p}$ tal que $sI = 0$, luego $\operatorname{An}(I) \not\subset \mathfrak{p}$ para todo $\mathfrak{p} \in \operatorname{As}(A)$. El teorema 3.49 nos da un $x \in \operatorname{An}(I)$ que no es un divisor de cero de A, pero $xI = 0$ implica entonces que $I = 0$, contradicción.

Así pues, $M_{\mathfrak{p}} = 0$ para todo $\mathfrak{p} \in \operatorname{As}(M)$. Considerando un generador finito de M encontramos un $s \in A \setminus \mathfrak{p}$ tal que $sM = 0$, luego $\operatorname{An}(M) \not\subset \mathfrak{p}$. De nuevo, el teorema 3.49 nos da que $\operatorname{An}(M)$ contiene un elemento que no es un divisor de cero de A. ■

Ahora ya podemos demostrar el teorema siguiente:

Teorema 5.61 *Sea A un anillo noetheriano local, sea $\mathfrak{m}$ su ideal maximal y sea $k = A/\mathfrak{m}$ su cuerpo de restos. Entonces A es regular si y sólo si $\operatorname{dp}_A k < \infty$.*

DEMOSTRACIÓN: Una implicación es el teorema 5.55. Supongamos que la dimensión proyectiva es finita. Sea $t = \dim_k \mathfrak{m}/\mathfrak{m}^2$. Vamos a demostrar que $\mathfrak{m}$ está generado por una sucesión A-regular de longitud t. Así el teorema 5.24 nos da que $\dim A = \operatorname{alt} \mathfrak{m} = t$, con lo que A será regular.

Si $t = 0$ entonces $\mathfrak{m} = \mathfrak{m}^2$ y el lema de Nakayama nos da que $\mathfrak{m} = 0$, por lo que A es un cuerpo y trivialmente es regular. Supongamos ahora que $t > 0$ y que el teorema está probado para valores menores de t.

Aplicamos el teorema anterior al A-módulo $M = k$, cuyo anulador es $\mathfrak{m}$, por lo que podemos concluir que $\mathfrak{m}$ contiene un elemento que no es un divisor de cero de A.

Sea $m_1, \ldots, m_t$ un generador minimal de $\mathfrak{m}$, de modo que sus clases en $\mathfrak{m}/\mathfrak{m}^2$ forman una k-base. Sea $I = (m_2, \ldots, m_t) + \mathfrak{m}^2$. Vamos a aplicar el teorema 4.53 a los ideales $I \subset \mathfrak{m}$ y a los primos maximales de $\operatorname{As}(A)$, digamos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Para ello hemos de comprobar varias cosas:

Tenemos que $V(I) = V(\mathfrak{m})$, pues si un ideal primo cumple $I \subset \mathfrak{p}$ entonces $\mathfrak{m}^2 \subset \mathfrak{p}$ y $\mathfrak{p} = \mathfrak{m}$.

Necesitamos calcular $\mu(\mathfrak{m}/I) = 1$. Observemos que no puede ser $\mathfrak{m} = I$, ya que entonces las clases de $m_2, \ldots, m_t$ generarían $\mathfrak{m}/\mathfrak{m}^2$.

Tenemos que $\mathfrak{m}$ no está contenido en la unión de los $\mathfrak{p}_i$, porque esta unión está formada por los divisores de cero de A (teorema 3.49), y ya hemos visto que $\mathfrak{m}$ contiene elementos que no son divisores de cero.

La conclusión es que existe un $a \in \mathfrak{m}$ que no es un divisor de cero de A y tal que $\mathfrak{m} = (a) + I$. Así pues, cambiando m_1 por a si es necesario, podemos suponer que m_1 no es un divisor de cero de A.

Llamemos $B = A/(m_1)$, $\mathfrak{m}' = \mathfrak{m}/(m_1)$. Así B es también un anillo noetheriano local y $\mathfrak{m}'$ es su ideal maximal. Sin embargo, la dimensión de $\mathfrak{m}'/\mathfrak{m}'^2$ es ahora $t-1$. Para aplicar la hipótesis de inducción nos falta ver que el cuerpo de restos tiene dimensión proyectiva finita como B-módulo.

En primer lugar notamos que $\mathfrak{m} = Am_1 + I$ luego

$$\mathfrak{m}/\mathfrak{m}m_1 = Am_1/\mathfrak{m}m_1 + I/\mathfrak{m}m_1.$$

Además $Am_1 \cap I = \mathfrak{m}m_1$, pues $m_1, \ldots, m_t$ son una base módulo $\mathfrak{m}$. Esto implica que la suma anterior es directa. Como m_1 no es un divisor de cero de A tenemos que $Am_1/\mathfrak{m}m_1 \cong A/\mathfrak{m}$ y

$$I/\mathfrak{m}m_1 \cong I/(Am_1 \cap I) \cong \mathfrak{m}/Am_1 = \mathfrak{m}'.$$

Así pues, $\mathfrak{m}/\mathfrak{m}m_1 \cong (A/\mathfrak{m}) \oplus \mathfrak{m}'$. Por el teorema 5.56 tenemos que

$$\mathrm{dp}_B(\mathfrak{m}/\mathfrak{m}m_1) = \mathrm{dp}_A(\mathfrak{m}).$$

La sucesión exacta $0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow A/\mathfrak{m} \longrightarrow 0$ nos da que $\mathrm{dp}_A(\mathfrak{m}) < \infty$ (por el teorema 5.49). Como $\mathfrak{m}'$ es un sumando directo de $\mathfrak{m}/\mathfrak{m}m_1$, también $\mathrm{dp}_B\mathfrak{m}' < \infty$. (Notemos que una suma directa tiene dimensión proyectiva finita si y sólo si la tienen los dos sumandos, pues sumando término a término sendas resoluciones proyectivas de los sumandos obtenemos una de la suma, y un núcleo será proyectivo si y sólo si lo son los dos núcleos de las sucesiones sumadas.)

Finalmente, la sucesión exacta $0 \longrightarrow \mathfrak{m}' \longrightarrow B \longrightarrow B/\mathfrak{m}' \longrightarrow 0$ nos permite concluir que $\mathrm{dp}_B(B/\mathfrak{m}') < \infty$, de nuevo por el teorema 5.49.

Así podemos aplicar la hipótesis de inducción y concluir que $\mathfrak{m}/(m_1)$ está generado por una sucesión B-regular de longitud $t-1$, de donde $\mathfrak{m}$ está generado por una sucesión A-regular de dimensión t. ■

Los resultados siguientes pueden enunciarse para una clase mucho más amplia de anillos regulares:

Definición 5.62 Sea A un anillo noetheriano y $\mathfrak{p} \in \operatorname{Esp} A$. Diremos que $\mathfrak{p}$ es *regular* si $A_\mathfrak{p}$ es un anillo local regular. Diremos que A es *regular* si lo son todos sus ideales maximales.

Observemos que si A es un anillo noetheriano local y $\mathfrak{m}$ es su ideal maximal, entonces $A_\mathfrak{m} \cong A$, luego A es regular en el sentido que acabamos de definir si y sólo si lo es en el que ya teníamos definido.

Por ejemplo, si A es un dominio de Dedekind tenemos que sus localizaciones $A_\mathfrak{m}$ son anillos de valoración discreta. En particular son regulares, luego todo dominio de Dedekind es un anillo regular.

La caracterización que hemos obtenido de los anillos locales regulares se extiende fácilmente a anillos arbitrarios de dimensión finita:

Teorema 5.63 *Sea A un anillo noetheriano de dimensión d. Entonces las afirmaciones siguientes son equivalentes:*

a) *A es regular.*

b) $\mathrm{Dh}(A) = d$.

c) $\mathrm{Dh}(A) < \infty$.

d) *Todo A-módulo finitamente generado tiene dimensión proyectiva finita.*

DEMOSTRACIÓN: a) $\Rightarrow$ b) Sea M un A-módulo finitamente generado. Hemos de probar que $\mathrm{dp}_A M \leq d$. Por 5.50 basta ver que $\mathrm{dp}_{A_\mathfrak{m}}(M_\mathfrak{m}) \leq d$ para todo ideal maximal $\mathfrak{m}$ de A, pues esto implica que $\mathrm{Dh}(A) \leq d$. La igualdad se sigue considerando $M = A/\mathfrak{m}$ (teorema 5.55).

Por hipótesis, $A_\mathfrak{m}$ es un anillo local regular de dimensión $\leq d$. Equivalentemente, basta probar b) bajo la hipótesis de que A es un anillo local regular (en particular un dominio íntegro).

Sea $\mathfrak{m}$ su ideal maximal. Razonamos por inducción sobre d. Si $d = 0$ entonces A es un cuerpo, M es un espacio vectorial y su dimensión proyectiva es 0.

Supongamos ahora que $d > 0$ y tomemos $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. (Recordemos que la regularidad equivale a que $\mathfrak{m}/\mathfrak{m}^2$ tiene dimensión d.) Entonces A/Ax es también un anillo local regular (por 5.19) y su dimensión es $d-1$ por 4.58. Finalmente consideramos una sucesión exacta

$$0 \longrightarrow K \longrightarrow L \longrightarrow M \longrightarrow 0,$$

donde L es un A-módulo libre finitamente generado. Por 5.56 y la hipótesis de inducción tenemos que

$$\mathrm{dp}_A K = \mathrm{dp}_{A/(x)}(K/xK) \leq d-1,$$

luego $\mathrm{dp}_A M \leq \mathrm{dp}_A K + 1 \leq d$.

Sólo falta probar que d) $\Rightarrow$ a). Si $\mathfrak{m}$ es un ideal maximal de A, tenemos que $\mathrm{dp}_A A/\mathfrak{m} < \infty$, luego $\mathrm{dp}_{A_\mathfrak{m}} A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} < \infty$ (porque localizando una resolución proyectiva de $A/\mathfrak{m}$ obtenemos una de $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$). El teorema 5.61 nos da que $A_\mathfrak{m}$ es regular, luego A también lo es. ■

El teorema siguiente es un ejemplo de resultado importante que requiere para su demostración las técnicas que hemos desarrollado aquí:

Teorema 5.64 *Un anillo noetheriano A es regular si y sólo si todos sus ideales primos son regulares.*

DEMOSTRACIÓN: Sea $\mathfrak{p} \in \operatorname{Esp} A$. Hemos de probar que el anillo local $A_\mathfrak{p}$ es regular. Sea $\mathfrak{m}$ un ideal maximal de A que contenga a $\mathfrak{p}$. Sabemos que el anillo $A_\mathfrak{m}$ es regular. Es fácil ver que $A_\mathfrak{p} \cong (A_\mathfrak{m})_{\mathfrak{p}A_\mathfrak{m}}$, luego no perdemos generalidad si suponemos que A es un anillo noetheriano local con $\mathfrak{m}$ como ideal maximal.

Claramente tenemos que $(A/\mathfrak{p})_\mathfrak{p} \cong A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, como $A_\mathfrak{p}$-módulos. Sabemos que $\mathrm{dp}_A(A/\mathfrak{p}) < \infty$ (porque $A/\mathfrak{p}$ es un A-módulo finitamente generado), y al localizar una resolución proyectiva finita de $A/\mathfrak{p}$ obtenemos una de $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Por consiguiente $\mathrm{dp}_{A_\mathfrak{p}}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}) < \infty$, lo que implica que $A_\mathfrak{p}$ es regular. ■

Ahora podemos reformular el teorema 5.21 en términos más simples:

Teorema 5.65 *Si A es un anillo regular, también lo es $A[X_1, \ldots, X_n]$.*

Ejercicio: Probar que la suma directa de dos anillos regulares es un anillo regular, luego un anillo regular puede tener divisores de cero.

Terminamos con un resultado nada trivial sobre anillos locales regulares. Hasta ahora hemos probado que son dominios íntegros e íntegramente cerrados. Ahora veremos que, de hecho, son dominios de factorización única. Necesitamos algunos resultados previos.

Teorema 5.66 *Un dominio íntegro noetheriano es un dominio de factorización única si y sólo si todo ideal primo de altura 1 es principal.*

DEMOSTRACIÓN: Sea A un dominio íntegro noetheriano en el que todo ideal primo de altura 1 sea principal. Basta probar que todo elemento irreducible $\pi \in A$ es primo. Sea $\mathfrak{p}$ un divisor primo minimal de (π). Por el teorema de los ideales principales tenemos que $\mathfrak{p}$ tiene altura 1, luego por hipótesis $\mathfrak{p} = (p)$, para cierto primo $p \in A$. Entonces $\pi = p\epsilon$, para cierto $\epsilon \in A$, que ha de ser una unidad por la irreducibilidad de π. Así pues, π es primo.

Supongamos ahora que A es un dominio de factorización única y sea $\mathfrak{p}$ un ideal primo de altura 1. En particular $\mathfrak{p} \neq 0$, luego existe un $\pi \in \mathfrak{p}$ no nulo. Descomponiendo π en factores primos podemos suponer que π es primo. Ahora bien, tenemos que $0 \subsetneq (\pi) \subset \mathfrak{p}$ y $\mathfrak{p}$ tiene altura 1, luego ha de ser $\mathfrak{p} = (\pi)$. ■

Teorema 5.67 *Sea A un dominio íntegro noetheriano y $\pi \in A$ un elemento primo. Entonces A es un dominio de factorización única si y sólo si lo es la localización A_π.*

DEMOSTRACIÓN: Supongamos que A es un dominio de factorización única. Todo elemento no nulo de A_π se expresa de forma única como $x = a\pi^n$, donde $n \in \mathbb{Z}$ y $\pi \nmid a$. Es claro que x es una unidad en A_π si y sólo si a lo es en A. Por consiguiente, si x es irreducible en A_π, tenemos que a ha de ser irreducible en A, luego ha de ser primo en A, y esto implica que x ha de ser primo en A_π. Por consiguiente A_π es un dominio de factorización única.

Supongamos ahora que A_π es un dominio de factorización única. Si $p \in A$ es irreducible y no es asociado de π, entonces p no es una unidad en A_π, pues en tal caso $pa/\pi^n = 1$, luego $pa = \pi^n$, para cierto $a \in A$ y $n \geq 0$. Tenemos que $\pi \mid pa$, luego $\pi \mid p$ o $\pi \mid a$. Si se da el primer caso entonces π es asociado a p, y en el segundo podríamos reducir la ecuación $pa'/\pi^{n-1} = 1$. Tras un número finito de pasos llegamos a que $pa = 1$ para cierto $a \in A$, lo cual es absurdo.

Más aún, si p es irreducible en A y no es asociado a π, tiene que ser irreducible en A_π, pues si $p = (u/\pi^m)(v/\pi^n)$, tenemos que $uv = p\pi^{m+n}$. Si $m+n > 0$ entonces $\pi \mid u$ o $\pi \mid v$, lo que nos permite rebajar un exponente en la descomposición de p. Tras un número finito de pasos llegamos a una descomposición $p = uv$, de la que se sigue que uno de los factores es una unidad en A, luego también en A_π.

Por consiguiente, si p es irreducible en A (no asociado a π), es primo en A_π, de donde se sigue que es primo en A, pues si $p \mid uv$ en A, entonces, por ejemplo, $u = pa/\pi^n$, con $a \in A$, $n \geq 0$, luego $\pi^n u = pa$. Entonces $\pi^n \mid a$, luego $p \mid u$ en A. Así hemos probado que todos los irreducibles de A son primos, luego A es un dominio de factorización única. ∎

Teorema 5.68 (Auslander-Buchsbaum) *Todo anillo local regular es un dominio de factorización única.*

Demostración: Sea A un anillo local regular y $\mathfrak{m}$ su ideal maximal. Razonamos por inducción sobre $d = \dim A$. Si $d = 0$ entonces A es un cuerpo y el resultado es trivial. Supongamos el teorema para anillos de dimensión menor que $d > 0$.

Podemos tomar $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$ (porque $\mathfrak{m}/\mathfrak{m}^2$ tiene dimensión d sobre $k = A/\mathfrak{m}$). Podemos extender π hasta un generador minimal de $\mathfrak{m}$ y el teorema 5.26 nos da que (π) es un ideal primo, luego π es primo. Por 5.67 basta demostrar que A_π es un dominio de factorización única. Para ello tomamos un primo $\mathfrak{p}' \in \operatorname{Esp} A_\pi$ de altura 1 y hemos de demostrar que es principal.

Si $\mathfrak{P} \in \operatorname{Esp} A_\pi$, entonces $(A_\pi)_{\mathfrak{P}} \cong A_{A\cap\mathfrak{P}}$. En efecto, el isomorfismo viene dado por $(a/\pi^m)/(b/\pi^n) \mapsto a\pi^n/b\pi^m$. Como $A \cap \mathfrak{P}$ es un ideal primo de A, tenemos que la localización es un anillo local regular. Además $A \cap \mathfrak{P} \subsetneq \mathfrak{m}$, pues en caso contrario tendríamos que $\pi \in \mathfrak{P}$, lo cual es imposible, ya que π es una unidad en A_π. Así, $\dim(A_\pi)_{\mathfrak{P}} = \operatorname{alt}(A \cap \mathfrak{P}) < \operatorname{alt}\mathfrak{m} = \dim A = d$. Por hipótesis de inducción podemos afirmar que $(A_\pi)_{\mathfrak{P}}$ es un dominio de factorización única.

El ideal $\mathfrak{p}'_{\mathfrak{P}}$ puede ser un ideal primo en $(A_\pi)_{\mathfrak{P}}$ de la misma altura que $\mathfrak{p}'$, es decir, de altura 1 (si $\mathfrak{p}' \subset \mathfrak{P}$) o bien $\mathfrak{p}'_{\mathfrak{P}} = (A_\pi)_{\mathfrak{P}}$ (en caso contrario). En el primer caso, el teorema 5.66 implica que es principal, luego lo es en cualquiera de los dos casos.

Que $\mathfrak{p}'_{\mathfrak{P}}$ sea un ideal principal de $(A_\pi)_{\mathfrak{P}}$ significa que es un $(A_\pi)_{\mathfrak{P}}$-módulo libre, luego $\operatorname{dp}_{(A_\pi)_{\mathfrak{P}}} \mathfrak{p}'_{\mathfrak{P}} = 0$. Por el teorema 5.50 concluimos que $\operatorname{dp}_{A_\pi} \mathfrak{p}' = 0$, luego $\mathfrak{p}'$ es un A_π-módulo proyectivo.

Sea $\mathfrak{p} = \mathfrak{p}' \cap A$, con lo que $\mathfrak{p}' = \mathfrak{p}A_\pi$ (ver la prueba de 3.4). La regularidad de A implica que $\operatorname{dp}_A \mathfrak{p} < \infty$, luego podemos tomar una resolución proyectiva

$$0 \longrightarrow L_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow \mathfrak{p} \longrightarrow 0,$$

donde cada L_i es libre de rango finito. Al localizar respecto de π obtenemos una sucesión exacta

$$0 \longrightarrow L'_n \longrightarrow L'_{n-1} \longrightarrow \cdots \longrightarrow L'_0 \longrightarrow \mathfrak{p}' \longrightarrow 0,$$

donde cada L_i' es un A_π-módulo libre de rango finito (pues L_i es suma directa de una cantidad finita de copias de A y la localización de una suma directa de módulos es isomorfa a la suma directa de las localizaciones.)

Descompongamos la sucesión exacta en sucesiones exactas cortas

$$0 \longrightarrow K_0' \longrightarrow L_0' \longrightarrow \mathfrak{p}' \longrightarrow 0, \quad 0 \longrightarrow K_1' \longrightarrow L_1' \longrightarrow K_0' \longrightarrow 0, \ldots$$

$$0 \longrightarrow K_{n-1}' \longrightarrow L_{n-2}' \longrightarrow K_{n-3}' \longrightarrow 0, \quad 0 \longrightarrow L_n' \longrightarrow L_{n-1}' \longrightarrow K_{n-2}' \longrightarrow 0.$$

Como $\mathfrak{p}'$ es proyectivo, también lo es K_0', e inductivamente vemos que todos los K_i' son proyectivos, luego todas las sucesiones se escinden. Así pues,

$$L_0' \cong K_0' \oplus \mathfrak{p}', \quad L_1' \cong K_1' \oplus K_0', \quad L_2' \cong K_2' \oplus K_1', \quad \ldots, \quad L_{n-1}' \cong L_n' \oplus K_{n-2}'.$$

Sumando K_1' a ambos miembros del primer isomorfismo y usando el segundo obtenemos que $K_1' \oplus L_0' \cong L_1' \oplus \mathfrak{p}'$. Ahora sumamos K_2' y usamos el tercero, con lo que $L_2' \oplus L_0' \cong K_2' \oplus L_1' \oplus \mathfrak{p}'$. Así llegamos finalmente a que la suma directa de los L_{2i}' es isomorfa a la suma de los L_{2i+1}' más $\mathfrak{p}'$. En definitiva, concluimos que $\mathfrak{p}' \oplus (A_\pi)^r \cong (A_\pi)^s$, para ciertos r, $s \geq 0$.

Si tomamos $\mathfrak{P} \in \operatorname{Esp} A_\pi$, tenemos que $\mathfrak{p}'_{\mathfrak{P}} \oplus ((A_\pi)_{\mathfrak{P}})^r \cong ((A_\pi)_{\mathfrak{P}})^s$, pero hemos visto que $\mathfrak{p}'_{\mathfrak{p}}$ es principal, luego como $(A_\pi)_{\mathfrak{p}}$-módulo tiene rango 1. Tomando rangos en el isomorfismo anterior vemos que $s = r + 1$. En definitiva, tenemos que $\mathfrak{p}' \oplus (A_\pi)^r \cong (A_\pi)^{r+1}$.

Por simplificar la notación escribiremos $B = A_\pi$ (del que sólo necesitamos saber que es un dominio íntegro) y $\mathfrak{p} = \mathfrak{p}'$ (del que sólo necesitamos saber que es un ideal de B tal que $\mathfrak{p} \oplus B^r \cong B^{r+1}$). Hemos de probar que $\mathfrak{p}$ es principal. Sea $\phi : B^{r+1} \longrightarrow \mathfrak{p} \oplus B^r$ un isomorfismo de B-módulos. Podemos considerarlo como un monomorfismo $\phi : B^{r+1} \longrightarrow B^{r+1}$. Sea M su matriz respecto a la base canónica $\{e_0, \ldots, e_r\}$, de modo que $\phi(x) = xM$ para todo $x \in B^{r+1}$.

Como ϕ es un monomorfismo, $|M| = d \in B \setminus \{0\}$. Sea $e_0' \in B^{r+1}$ la primera fila de la matriz adjunta de M, de modo que $\phi(e_0') = e_0 M = (d, 0, \ldots, 0)$.

Por otra parte, podemos tomar $e_1', \ldots, e_r' \in B^{r+1}$ tales que $\phi(e_i') = e_i$.

Sea M' la matriz que tiene por filas a $e_0', \ldots, e_r'$, que cumple

$$M'M = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Por consiguiente, $d = |M||M'| = d|M'|$, luego $|M'| = 1$. El hecho de que la matriz M' tenga determinante unitario se traduce en que $e_0', \ldots, e_r'$ es una base de B^{r+1}.

Vamos a probar que $\mathfrak{p} = (d)$. En efecto, si $b \in B$, tenemos que

$$bde_0 = b\phi(e_0') = \phi(be_0') \in \mathfrak{p} \oplus B^r,$$

luego $bd \in \mathfrak{p}$. Esto prueba que $(d) \subset \mathfrak{p}$. Recíprocamente, si $x \in \mathfrak{p}$, tenemos que $xe_0 \in \mathfrak{p} \oplus B^r$, luego existe un $y \in B^{r+1}$ tal que $\phi(y) = xe_0$. Podemos expresar

$$y = \sum_{i=0}^{r} b_i e_i'.$$

Entonces

$$xe_0 = \phi(y) = \sum_{i=0}^{r} b_i \phi(e_i) = b_0 d e_0 + \sum_{i=1}^{r} b_i e_i,$$

luego $x = b_0 d \in (d)$. ■

5.6 Variedades regulares

Finalmente vamos a mostrar la relación entre la teoría algebraica que hemos desarrollado y la noción geométrica de regularidad. Para ello vamos a definir la variedad tangente en un punto de un conjunto algebraico afín. Trabajaremos únicamente con variedades definidas sobre un cuerpo K algebraicamente cerrado.

Definición 5.69 La *diferencial* de un polinomio $F(X) \in K[X_1, \ldots, X_n]$ en un punto $P \in K^n$ es el polinomio

$$d_P F(X) = \left.\frac{\partial F}{\partial X_1}\right|_P X_1 + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_P X_n.$$

Es fácil ver que

$$F(X) = F(P) + d_P F(X - P) + F_2(X - P) + F_3(X - P) + \cdots$$

donde cada F_i es una forma de grado i. Se comprueba inmediatamente que

$$d_P(F + G) = d_P F + d_P G, \qquad d_P(FG) = F(P)\, d_P G + G(P)\, d_P F. \tag{5.1}$$

Si $C \subset A^n$ es un conjunto algebraico afín y $P \in C$. Llamaremos *variedad tangente* a C en P a la variedad lineal

$$T_P C = V(\{d_P F(X - P) \mid F \in I(V)\}).$$

Las relaciones (5.1) muestran que si $I(C) = (F_1, \ldots, F_m)$, para ciertos polinomios $F_i \in K[X_1, \ldots X_n]$, entonces

$$W = \{d_P F(X - P) \mid F \in I(V)\} = \langle d_P F_1(X - P), \ldots, d_P F_m(X - P)\rangle_K .$$

En particular

$$T_P C = V(d_P F_1(X - P), \ldots, d_P F_m(X - P)).$$

Más aún, si llamamos $r = \dim_K W$, tenemos que T_PC está generado por r ecuaciones lineales linealmente independientes. La aplicación $Q \mapsto Q - P$ biyecta T_PC con un subespacio vectorial de K^n, definido por un sistema de r ecuaciones lineales homogéneas linealmente independientes, luego su dimensión es $n - r$. Esta biyección permite definir una estructura de espacio vectorial sobre T_PC en la que P es el elemento neutro. Por otra parte, un automorfismo de $K[X_1, \ldots, X_n]$ transforma las r formas lineales que definen a T_PC en los polinomios $X_1, \ldots, X_r$, luego el ideal (W) se transforma en el ideal primo $(X_1, \ldots, X_r)$ y

$$K[T_PC] \cong K[X_1, \ldots, X_n]/(X_1, \ldots, X_r) \cong K[X_{r+1}, \ldots, X_n].$$

Esto prueba que T_PC es ciertamente una variedad (o sea, que es irreducible), que

$$I(T_PC) = (d_PF(X - P) \mid F \in I(C)) = (d_PF_1(X - P), \ldots, d_PF_m(X - P))$$

(porque el ideal (W) es primo, luego radical) y que

$$\dim T_PC = \dim_K T_P(C) = n - r.$$

Vamos a calcular esta dimensión en términos del conjunto C. Para ello consideramos a P como punto de C y también como punto de A^n. Entonces tenemos los anillos locales $\mathcal{O}_{C.P}$ y $\mathcal{O}_{A^n,P}$ con sus respectivos ideales maximales $\mathfrak{m}_P(C)$ y $\mathfrak{m}_P(A^n)$. Con ellos podemos construir una sucesión exacta

$$0 \longrightarrow \frac{I(T_PC)}{I(T_PC) \cap \mathfrak{m}_P(A^n)^2} \longrightarrow \frac{\mathfrak{m}_P(A^n)}{\mathfrak{m}_P(A^n)^2} \longrightarrow \frac{\mathfrak{m}_P(C)}{\mathfrak{m}_P(C)^2} \longrightarrow 0.$$

La primera aplicación es la inducida por la inclusión, y obviamente es inyectiva. La segunda es la inducida por el epimorfismo que a cada fracción F/G le hace corresponder la fracción de las clases correspondientes a F y G en $K[C]$. (De acuerdo con el teorema 3.87, consideramos a $\mathcal{O}_{C,P}$ como la localización de $K[C]$ respecto del ideal $I_C(P) = (x_1 - P_1, \ldots, x_n - P_n)$.) Sólo hemos de probar la exactitud en $\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$.

Observemos que $\mathfrak{m}_P(A^n)$ está formado por los cocientes F/G tales que $F(P) = 0$ y $G(P) \neq 0$. Al tomar clases módulo $\mathfrak{m}_P(A^n))^2$ resulta que $[F/G] = [F/G(P)]$, pues

$$\frac{F}{G} - \frac{F}{G(P)} = F\,\frac{G(P) - G}{GG(P)} \in \mathfrak{m}_P(A^n)^2. \tag{5.2}$$

Por lo tanto, los elementos de $\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$ son clases de polinomios. Más aún, si $F \in \mathfrak{m}_P(A^n)$, se cumple $[F] = [d_PF(X - P)]$, es decir, basta considerar combinaciones lineales de las clases $[X_i - P_i]$. En efecto

$$F - d_PF(X - P) = F_2(X - P) + F_3(X - P) + \cdots,$$

donde cada F_i es una forma de grado i, luego la diferencia está en $\mathfrak{m}_P(A^n)^2$.

De este modo, la imagen del monomorfismo está formada por elementos de la forma $[d_P F(X-P)] = [F]$ con $F \in I(C)$, luego está en el núcleo del epimorfismo.

Recíprocamente, si $[F]$ está en el núcleo del epimorfismo, ha de existir un $F'/G' \in \mathfrak{m}_P(A^n)^2$ con la misma imagen, es decir, $[F] = [F']/[G']$ en $\mathcal{O}_{C,P}$. Esto significa que existe un polinomio H tal que $H(P) \neq 0$ y $[H(FG'-F')] = 0$ en $k[C]$. Equivalentemente $H(FG'-F') \in I(C)$. En consecuencia,

$$[F] = [F - F'/G'] = [H(FG'-F')/HG'] = [T] = [d_P T(X-P)],$$

donde $T = H(FG'-F')/H(P)G'(P) \in I(C)$. Por lo tanto $[F]$ está en la imagen del monomorfismo. ■

Por otra parte, $I(T_PC)/(I(T_PC \cap \mathfrak{m}_P(A^n)^2)$ es isomorfo al k-espacio vectorial W generado por las diferenciales $d_P F(X-P)$, con $F \in I(C)$. En efecto, los elementos de $I(T_PC)$ son combinaciones lineales de dichas diferenciales y coeficientes en $k[X_1,\ldots,X_n]$, pero si un coeficiente tiene grado mayor o igual que 1 el producto está en $\mathfrak{m}_P(A^n)^2$, luego su clase en el cociente es nula. Por otra parte, si una combinación k-lineal es nula en el cociente, necesariamente es nula. Concluimos, por tanto, que la dimensión de este k-espacio vectorial es precisamente la que hemos llamado r más arriba. Así pues:

$$\begin{aligned}\dim T_PC &= n - \dim_k(I(T_PC)/(I(T_PC) \cap \mathfrak{m}_P(A^n)^2) \\ &= \dim_k \mathfrak{m}_P(C)/\mathfrak{m}_P(C)^2.\end{aligned}$$

Más precisamente, a cada $f = [F] \in K[C]$ podemos asignarle la diferencial $d_P f = [d_P F(X-P)] \in K[T_PC]$. La definición no depende de la elección del representante, pues si tenemos que $f = [F] = [F']$ entonces $F - F' \in I(C)$, luego $d_P F(X-P) - d_P F'(X-P) \in I(T_PC)$.

Más aún, es claro que $d_P f$ es una forma lineal en T_PC, pues

$$d_P f = \left.\frac{\partial F}{\partial X_1}\right|_P d_P x_1 + \cdots + \left.\frac{\partial F}{\partial X_n}\right|_P d_P x_n$$

y $d_P x_i = x_i - P_i$. Tenemos así una aplicación $d_P : k[C] \longrightarrow T_PC^*$, donde T_PC^* es el espacio dual de T_PC. Claramente se cumple:

$$d_P(f+g) = d_P f + d_P g, \qquad d_P(fg) = f(P) d_P g + g(P) d_P f.$$

Más aún, podemos extender d_P a una aplicación lineal $d_P : \mathcal{O}_P(C) \longrightarrow T_PC^*$ mediante

$$d_P(f/g) = \frac{g(P)\, d_P f - f(P)\, d_P g}{g(P)^2} \in T_PC^*.$$

No es difícil probar que esta extensión está bien definida y sigue cumpliendo las relaciones usuales para la suma y el producto. De todos modos no necesitamos este hecho, ya que vamos a restringir d_P al ideal $\mathfrak{m}_P(C)$, donde la definición se reduce a

$$d_P(f/g) = \frac{d_P f}{g(P)},$$

y en este caso las comprobaciones son mucho más sencillas. Ahora probamos:

Teorema 5.70 *Sea C/k un conjunto algebraico afín en A^n y $P \in C$. Entonces d_P induce un isomorfismo de espacios vectoriales $d_P : \mathfrak{m}_P/\mathfrak{m}_P^2 \longrightarrow T_PC^*$.*

DEMOSTRACIÓN: Observemos que los elementos de $\mathfrak{m}_P^2$ son sumas de productos fg, con f, $g \in \mathfrak{m}_P$ y entonces

$$d_P(fg) = g(P)d_Pf + f(P)d_PG = 0,$$

luego efectivamente d_P induce una aplicación k-lineal en el cociente. Como ambos espacios tienen la misma dimensión basta probar que d_P es un epimorfismo. Podemos considerar a A^n como espacio vectorial con origen en P, de modo que T_PC es un subespacio, toda forma $\phi \in T_PC^*$ se extiende a una forma lineal en A^n, que será de la forma

$$F = a_1(X_1 - P_1) + \cdots + a_n(X_n - P_n).$$

Es claro entonces que $f = [F] \in \mathfrak{m}_P(C)$ cumple que $d_Pf = \phi$. ■

Puesto que T_PV puede identificarse canónicamente con su bidual, concluimos que la codiferencial

$$d_P^* : T_PC \longrightarrow (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$$

(es decir, la aplicación dual de la diferencial) determina un isomorfismo entre T_PC y el espacio dual de $\mathfrak{m}_P/\mathfrak{m}_P^2$.

Definición 5.71 Sea C un conjunto algebraico afín. Diremos que un punto $P \in C$ es *regular* si el anillo local $\mathcal{O}_{C,P}$ es regular. Diremos que C es *regular* si todos sus puntos son regulares.

Una condición necesaria para que un punto P sea regular es que $\mathcal{O}_{C,P}$ sea un dominio íntegro, lo cual, según el teorema 3.88, equivale a que P pertenezca a una única componente irreducible de C. En tal caso, $\dim \mathcal{O}_{C,P} = \operatorname{codim}_C P$ es la dimensión de dicha componente irreducible. El punto P será regular si y sólo si

$$\dim \mathcal{O}_{C,P} = \dim_k \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim T_P(C),$$

es decir, si y sólo si la variedad tangente a C en P tiene dimensión igual a la de la componente irreducible de C a la que pertenece P.

Un conjunto algebraico afín C es regular si y sólo si todos los anillos $\mathcal{O}_{C,P}$ son regulares, es decir, si y sólo si todas las localizaciones del anillo $K[C]$ respecto a sus ideales maximales son regulares, si y sólo si $K[C]$ es un anillo regular.

Si un punto P está en una única componente irreducible V de un conjunto algebraico C, entonces la regularidad de P en C equivale a la regularidad de P en V. En términos abstractos tenemos el teorema siguiente:

Teorema 5.72 *Sea A un anillo noetheriano reducido no nulo y $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ el conjunto de sus primos minimales. Entonces los primos singulares de A son aquellos que están en una intersección $V(\mathfrak{p}_i) \cap V(\mathfrak{p}_j)$ para $i \neq j$ y los primos $\mathfrak{P}$ tales que $\mathfrak{P}/\mathfrak{p}_i$ es singular en $A/\mathfrak{p}_i$ para algún i.*

DEMOSTRACIÓN: Si $\mathfrak{P} \in V(\mathfrak{p}_i) \cap V(\mathfrak{p}_j)$, entonces $A_{\mathfrak{P}}$ contiene al menos dos primos minimales, luego no es un dominio íntegro, luego no es un anillo local regular. Por otra parte, si $\mathfrak{P}$ contiene un único primo minimal $\mathfrak{p}_i$, entonces $\mathfrak{p}_i A_{\mathfrak{P}}$ es el único primo minimal de $A_{\mathfrak{P}}$, luego está formado por los elementos idempotentes, pero como A es reducida, lo mismo le sucede a $A_{\mathfrak{P}}$, luego concluimos que $\mathfrak{p}_i A_{\mathfrak{P}} = 0$. Por consiguiente

$$A_{\mathfrak{P}} = A_{\mathfrak{P}}/\mathfrak{p}_i A_{\mathfrak{P}} \cong (A/\mathfrak{p}_i)_{\mathfrak{P}/\mathfrak{p}_i},$$

luego $\mathfrak{P}$ es singular en A si y sólo si $\mathfrak{P}/\mathfrak{p}_i$ es singular en $A/\mathfrak{p}_i$. ■

Vamos a caracterizar la regularidad de un punto en términos de matrices jacobianas, lo que nos dará la conexión entre la definición algebraica que hemos dado y la definición usual en geometría diferencial. Conviene trabajar en un contexto algo más general.

Consideremos una k-álgebra afín A, que podemos representar de la forma $A = k[X_1, \ldots, X_n]/I$, donde $I = (F_1, \ldots, F_m)$. Para cada primo $\mathfrak{p} \in \operatorname{Esp} A$, el teorema 3.8 nos da que

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong (A/\mathfrak{p})_0,$$

donde el segundo miembro no es sino el cuerpo de cocientes del dominio íntegro $A/\mathfrak{p}$. Ambos miembros son cuerpos generados sobre k por las clases de las indeterminadas. Llamemos $x_i = [X_i] \in A$ y $\xi = [x_i] \in A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. En estos términos, definimos la *matriz jacobiana* de $\mathfrak{p}$ (respecto a la representación dada de A) como la matriz

$$J(\mathfrak{p}) = \left(\left. \frac{\partial F_i}{\partial X_j} \right|_{(\xi_1, \ldots, \xi_n)} \right)_{i,j}.$$

Teorema 5.73 *Sea k un cuerpo perfecto y $A = k[X_1, \ldots, X_n]/I$ una k-álgebra afín de dimensión d sin divisores de cero. Para cada $\mathfrak{p} \in \operatorname{Esp} A$ se cumple que*

$$\operatorname{rang} J(\mathfrak{p}) = n - d - (\mu(\mathfrak{p}A_{\mathfrak{p}}) - \dim A_{\mathfrak{p}}).$$

En particular $\mathfrak{p}$ es regular si y sólo si $\operatorname{rang} J(\mathfrak{p}) = n - d$.

DEMOSTRACIÓN: Tenemos que $A/\mathfrak{p}$ es una k-álgebra afín (digamos, de dimensión t) en la que el único primo minimal es el ideal nulo. Le podemos aplicar el teorema 3.75, según el cual

$$t = \dim A/\mathfrak{p} = \operatorname{grad} \operatorname{tr}_k A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

Llamemos $L = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = k(\xi_1, \ldots, \xi_n)$. El hecho de que k sea perfecto implica que L tiene una base de trascendencia $\xi'_1, \ldots, \xi'_t$ sobre k tal que la extensión $L/k(\xi'_1, \ldots, \xi'_t)$ es separable. Más aún, podemos exigir[1] que los ξ'_i sean combinaciones k-lineales de $\xi_1, \ldots, \xi_n$. La matriz de los coeficientes que

[1] Ver el teorema 1.32 de mi Geometría Algebraica. El hecho de que los ξ'_i dependan linealmente de los ξ_i se ve en la prueba de dicho teorema y el precedente.

expresan a los ξ_i' como combinación lineal de los ξ_i ha de tener rango t, pues en caso contrario un ξ_i' sería combinación lineal de los restantes y tendríamos una base de trascendencia de L con $t-1$ elementos. Podemos completar la matriz hasta una matriz $n \times n$ de rango n, lo que nos permite extender la base de trascendencia a un sistema generador $\xi_1', \ldots, \xi_n'$ de L sobre k.

Más aún, la matriz extendida determina un automorfismo de $k[X_1, \ldots, X_n]$ que da lugar a otra representación $k[X_1, \ldots, X_n]/I'$ de A, respecto a la cual $\xi_1, \ldots, \xi_n$ pasan a ser $\xi_1', \ldots, \xi_n'$. Es inmediato comprobar que las matrices jacobianas $J(\mathfrak{p})$ y $J'(\mathfrak{p})$ se diferencian precisamente en la matriz (regular) que define el automorfismo, por lo que ambas tienen el mismo rango.

De aquí se sigue que no perdemos generalidad si suponemos que $\xi_1, \ldots, \xi_t$ son una base de trascendencia de L sobre k tal que la extensión $L/k(\xi_1, \ldots, \xi_t)$ es separable.

Sea $\mathfrak{P}$ la antiimagen de $\mathfrak{p}$ en $k[X_1, \ldots, X_n]$, de modo que

$$A/\mathfrak{p} = (k[X_1, \ldots, X_n]/I) \bigm/ (\mathfrak{P}/I) \cong k[X_1, \ldots, X_n]/\mathfrak{P}$$

y L es el cuerpo de cocientes de este anillo. Entonces

$$\mathfrak{P} \cap k[X_1, \ldots, X_t] = 0,$$

pues un polinomio no nulo en la intersección determinaría una dependencia algebraica entre $\xi_1, \ldots, \xi_t$. Por consiguiente $k(X_1, \ldots, X_t) \subset k[X_1, \ldots, X_n]_{\mathfrak{P}}$. Más aún,

$$k[X_1, \ldots, X_n]_{\mathfrak{P}} = B_{\mathfrak{P}'},$$

donde $B = k(X_1, \ldots, X_t)[X_{t+1}, \ldots, X_n]$ y $\mathfrak{P}' = \mathfrak{P}B$. Por el teorema 5.65 tenemos que B es un anillo regular, luego 5.64 nos da que $B_{\mathfrak{P}'}$ es un anillo local regular.

Además, por el teorema 3.75,

$$\begin{aligned} \dim B_{\mathfrak{P}'} &= \dim k[X_1, \ldots, X_n]_{\mathfrak{P}} = n - \dim k[X_1, \ldots, X_n]/\mathfrak{P} \\ &= n - \dim A/\mathfrak{p} = n - t. \end{aligned}$$

También tenemos que

$$A_{\mathfrak{p}} = (k[X_1, \ldots, X_n]/I)_{\mathfrak{p}} \cong k[X_1, \ldots, X_n]_{\mathfrak{P}}/I_{\mathfrak{P}} \cong B_{\mathfrak{P}'}/IB_{\mathfrak{P}'}.$$

De aquí se sigue a su vez que $L = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \cong B_{\mathfrak{P}'}/\mathfrak{P}'B_{\mathfrak{P}'}$. Entonces, el epimorfismo natural $\phi : B_{\mathfrak{P}'} \longrightarrow A_{\mathfrak{p}}$ induce una sucesión exacta de L-espacios vectoriales:

$$0 \longrightarrow N \longrightarrow \mathfrak{P}'B_{\mathfrak{P}'}/(\mathfrak{P}'B_{\mathfrak{P}'})^2 \longrightarrow \mathfrak{p}A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^2 \longrightarrow 0,$$

donde N es el ideal de $B_{\mathfrak{P}'}/(\mathfrak{P}'B_{\mathfrak{P}'})^2$ generado por las clases $[F_1], \ldots, [F_m]$.

(En efecto, si $x \in \mathfrak{P}'B_{\mathfrak{P}'}$ cumple que $\phi(x) \in (\mathfrak{p}A_{\mathfrak{p}}')^2$, entonces existe un $y \in (\mathfrak{P}'B_{\mathfrak{P}'})^2$ tal que $\phi(x) = \phi(y)$. Así, $[x] = [x-y]$ y $x-y$ está en el núcleo de ϕ, luego su clase está en la imagen de N.)

Por consiguiente, y teniendo en cuenta la regularidad de $B_{\mathfrak{P}'}$,

$$\dim_L N = n - t - \mu(\mathfrak{p}A_{\mathfrak{p}}) = n - d - (\mu(\mathfrak{p}A_{\mathfrak{p}}) - \dim A_{\mathfrak{p}}),$$

pues $d = \dim A = \dim A_{\mathfrak{p}} + \dim A/\mathfrak{p} = \dim A_{\mathfrak{p}} + t$. (Al aplicar 3.75 usamos la hipótesis de que A es un dominio íntegro.)

Así pues, basta ver que $\dim_L N = \operatorname{rang} J(\mathfrak{p})$.

El homomorfismo natural $B/\mathfrak{P}' \longrightarrow B_{\mathfrak{P}'}/\mathfrak{P}'B_{\mathfrak{P}'} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{P}} = L$ es un monomorfismo, pues si $F/1 \in \mathfrak{P}'B'_{\mathfrak{P}}$ entonces $F/1 = G/H$, donde $G \in \mathfrak{P}'$, $H \notin \mathfrak{P}'$, luego $F \in \mathfrak{P}'$. La imagen de $[X_i]$ es $[X_i] = \xi_i$, y como cada ξ_i con $i > t$ es algebraico sobre $k(\xi_1, \ldots, \xi_t)$, todo elemento de L se obtiene evaluando un elemento de B en $\xi_1, \ldots, \xi_n$. Concluimos que $B/\mathfrak{P}' \cong L$ y el isomorfismo es precisamente la evaluación en $\xi_1, \ldots, \xi_n$. En vista de esto llamaremos también ξ_i a la clase de X_i en $B/\mathfrak{P}'$.

Sea $g_i(X)$ el polinomio mínimo de ξ_{t+i} sobre $k(\xi_1, \ldots, \xi_t)[\xi_{t+1}, \ldots, \xi_{t+i-1}]$. Sea $G_i(X_1, \ldots, X_{t+i}) \in k(X_1, \ldots, X_t)[X_{t+1}, \ldots, X_{t+i}]$ el polinomio que se obtiene a partir de $g_i(X)$ eligiendo representantes para sus coeficientes en el anillo $k(X_1, \ldots, X_t)[X_{t+1}, \ldots, X_{t+i-1}]$ y cambiando X por X_{t+i}. Entonces $G(\xi_1, \ldots, \xi_{t+i}) = 0$, luego $(G_1, \ldots, G_{n-t}) \subset \mathfrak{P}'$. Ahora bien, inductivamente se ve que

$$k(X_1, \ldots, X_t)[X_{t+1}, \ldots, X_{t+i}]/(G_1, \ldots, G_i) \cong k(\xi_1, \ldots, \xi_t)[\xi_{t+1}, \ldots, \xi_{t+i}],$$

luego $B/(G_1, \ldots, G_{n-t}) \cong L$ y concluimos que $\mathfrak{P}' = (G_1, \ldots, G_{n-t})$. En particular, $\mathfrak{P}'B_{\mathfrak{P}'} = (G_1, \ldots, G_{n-t})$ y, como $B_{\mathfrak{P}'}$ es un anillo local regular de dimensión $n-t$ concluimos que $G_1, \ldots, G_{n-t}$ es un sistema regular de parámetros de $B_{\mathfrak{P}'}$ y sus clases son una L-base de $\mathfrak{P}'B_{\mathfrak{P}'}/(\mathfrak{P}'B_{\mathfrak{P}'})^2$.

Como ξ_{t+i} es separable sobre $k(\xi_1, \ldots, \xi_t)[\xi_{t+1}, \ldots, \xi_{t+i-1}]$, tenemos que

$$\left.\frac{\partial G_i}{\partial X_{t+i}}\right|_{(\xi_1, \ldots, \xi_n)} = g_i'(\xi_{t+i}) \neq 0.$$

Además G_i sólo contiene las variables $X_1, \ldots, X_{n+i}$, por lo que la matriz de las derivadas parciales anteriores tiene rango $n - t$. Por otra parte, podemos expresar

$$F_i = \sum_{j=1}^{n-t} H_{ij} G_j, \qquad H_{ij} \in B.$$

Derivando concluimos que

$$J(\mathfrak{p}) = \left(\left.\frac{\partial F_i}{\partial X_j}\right|_{(\xi_1, \ldots, \xi_n)} \right)_{i,j} = (H_{ij}(\xi_1, \ldots, \xi_n))_{i,j} \left(\left.\frac{\partial G_i}{\partial X_j}\right|_{(\xi_1, \ldots, \xi_n)} \right)_{i,j}.$$

De aquí se sigue que

$$\operatorname{rang} J(\mathfrak{p}) = \operatorname{rang}(H_{ij}(\xi_1, \ldots, \xi_n)).$$

Por otra parte, tomando clases en $\mathfrak{P}'B_{\mathfrak{P}'}/(\mathfrak{P}'B_{\mathfrak{P}'})^2$ tenemos que

$$[F_i] = \sum_{j=1}^{n-t} H_{ij}(\xi_1, \ldots, \xi_n)[G_j].$$

Las clases $[G_j]$ son una base del L-espacio vectorial $\mathfrak{P}'B_{\mathfrak{P}'}/(\mathfrak{P}'B_{\mathfrak{P}'})^2$, mientras que las clases $[F_i]$ generan el subespacio N. Por consiguiente llegamos a que $\operatorname{rang}(H_{ij}(\xi_1, \ldots, \xi_n)) = \dim_L N$, como queríamos probar. ■

Notas Observando la prueba del teorema anterior podemos enunciar variantes que nos serán útiles más adelante:

- Si suponemos que $\mathfrak{p}$ es un ideal maximal de A, entonces $A/\mathfrak{p}$ es un cuerpo y por el teorema 3.82 es una extensión finita de k, luego $t = 0$. En estas condiciones podemos suprimir la hipótesis de que A sea un dominio íntegro, pues ésta sólo se usa donde se indica explícitamente en la prueba, y sin ella obtenemos igualmente la relación

$$\operatorname{rang} J(\mathfrak{p}) = n - \mu(\mathfrak{p}A_{\mathfrak{p}}).$$

  La tesis es entonces que $\mathfrak{p}$ es regular si y sólo si $\operatorname{rang} J(\mathfrak{p}) = n - \dim A_{\mathfrak{p}}$.

- En las condiciones del caso anterior también podemos sustituir la hipótesis de que k sea perfecto por la hipótesis de que el cuerpo $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ sea una extensión separable de k.

- Por último, si suprimimos incluso la hipótesis de separabilidad, podemos concluir igualmente que

$$\operatorname{rang} J(\mathfrak{p}) \leq n - \mu(\mathfrak{p}A_{\mathfrak{p}}) \leq n - \dim A_{\mathfrak{p}}.$$

  En efecto, lo único que perdemos es que la matriz $(\partial G_i/\partial X_j)$ ya no tiene por qué tener rango n, con lo que sólo obtenemos la desigualdad

$$\operatorname{rang} J(\mathfrak{p}) \leq \operatorname{rang}(H_{ij}(\xi_1, \ldots, \xi_n)) = \dim_L N.$$

  Así podemos concluir que si $\operatorname{rang} J(\mathfrak{p}) = n - \dim A_{\mathfrak{p}}$ entonces $\mathfrak{p}$ es regular, pero el recíproco no es necesariamente cierto.

En términos de variedades, hemos probado que si $C \subset A^n$ es una variedad algebraica afín de dimensión d y $P \in C$, tenemos que P es regular en C si y sólo si el anillo $\mathcal{O}_{C,P}$ es regular. Este anillo puede verse como $k[C]_{\mathfrak{p}}$, donde $\mathfrak{p} = (x_1 - P_1, \ldots, x_n - P_n)$. Pongamos que $I(C) = (F_1, \ldots, F_m)$. El teorema anterior nos da que P es regular en C si y sólo si la matriz

$$J(\mathfrak{p}) = \left(\left. \frac{\partial F_i}{\partial X_j} \right|_P \right)_{i,j}$$

tiene rango $n-d$. (De hecho, es fácil ver directamente que el rango de esta matriz es precisamente la codimensión en A^n de $T_P(C)$.) Esta caracterización permite probar, por ejemplo, que todo punto regular en una variedad compleja tiene un entorno conformemente equivalente a un abierto de $\mathbb{C}^d$. En particular, las variedades regulares complejas son variedades analíticas.

Aunque para las observaciones precedentes no es necesario realmente el teorema anterior, sino sólo un caso particular trivial, lo hemos probado en general para obtener el siguiente teorema de existencia de puntos regulares:

Teorema 5.74 *Sea A un álgebra reducida afín no nula sobre un cuerpo perfecto k. Entonces el conjunto de los primos regulares de A es un abierto no vacío en* $\operatorname{Esp} A$ *y contiene al menos un ideal maximal. Más aún, un primo $\mathfrak{p}$ es regular si y sólo si está contenido en un ideal maximal regular.*

Demostración: Si $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ son los primos minimales de A, entonces $V(\mathfrak{p}_i)$ es homeomorfo a $\operatorname{Esp} A/\mathfrak{p}_i$. Si probamos que el conjunto de puntos singulares de $\operatorname{Esp} A/\mathfrak{p}_i$ es cerrado, entonces el teorema 5.72 nos da que el conjunto de puntos singulares de $\operatorname{Esp} A$ es la unión de los cerrados $V(\mathfrak{p}_i)\cap V(\mathfrak{p}_j)$ y de los cerrados formados por los puntos de cada $V(\mathfrak{p}_i)$ que se corresponden con puntos singulares de $A/\mathfrak{p}_i$. En conclusión, tendremos que el conjunto de puntos singulares de $\operatorname{Esp} A$ es cerrado. Equivalentemente, podemos suponer que A es un dominio íntegro de dimensión d. Esto nos pone en las hipótesis de 5.73.

Podemos representar $A=k[X_1,\ldots,X_n]/(F_1,\ldots,F_m)$. Llamemos x_i a la imagen de X_i en A y sea $J(A)$ el ideal de A generado por los menores de orden $n-d$ de la matriz

$$\left(\left.\frac{\partial F_i}{\partial X_j}\right|_{(x_1,\ldots,x_n)}\right)_{i,j}.$$

Vamos a demostrar que un $\mathfrak{p}\in\operatorname{Esp} A$ es singular si y sólo si $J(A)\subset\mathfrak{p}$. En efecto, la inclusión equivale a que todos los menores de orden $n-d$ de la matriz

$$J(\mathfrak{p})=\left(\left.\frac{\partial F_i}{\partial X_j}\right|_{(\xi_1,\ldots,\xi_n)}\right)_{i,j}$$

se anulen en $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. (Si dichos menores se anulan, entonces los menores que generan $J(A)$ están en $A\cap\mathfrak{p}A_{\mathfrak{p}}=\mathfrak{p}$.)

El teorema 5.73 nos da en general que $\operatorname{rang} J(\mathfrak{p})\leq n-d$, luego los menores de orden $n-d$ son todos nulos si y sólo si $\operatorname{rang} J(\mathfrak{p})<n-d$, lo que equivale a que $\mathfrak{p}$ es singular.

Esto prueba que el conjunto de puntos singulares de A es $V(J(A))$, luego es un cerrado, y el conjunto de puntos regulares es abierto. Más aún, es un abierto no vacío, ya que el ideal 0 es regular, pues la localización A_0 es un cuerpo. De aquí se sigue fácilmente que A tiene primos regulares aunque no sea un dominio íntegro.

En el caso general, si $\mathfrak{p}$ es un primo regular de A, podemos encontrar un $f\in A$ tal que el abierto principal $D(f)$ esté contenido en el conjunto de primos regulares de A y $\mathfrak{p} \in D(f)$. Entonces $f \notin \mathfrak{p}$. Por el teorema 3.23 existe un ideal maximal $\mathfrak{m}$ de A tal que $\mathfrak{p} \subset \mathfrak{m}$ y $f \notin \mathfrak{m}$, es decir, $\mathfrak{m} \in D(f)$, luego $\mathfrak{m}$ es regular.

Recíprocamente, si $\mathfrak{p}$ está contenido en un ideal maximal regular $\mathfrak{m}$, entonces $A_\mathfrak{p} \cong (A_\mathfrak{m})_{\mathfrak{p}A_\mathfrak{m}}$. Tenemos que $A_\mathfrak{m}$ es regular y entonces $A_\mathfrak{p}$ también lo es por el teorema 5.64. ■

En particular, si C es un conjunto algebraico afín, tenemos que C es homeomorfo al espacio de los ideales maximales de $K[C]$ y los puntos regulares de C se corresponden con los ideales maximales regulares. Por el teorema anterior podemos concluir que el conjunto de los puntos regulares de C es abierto en C.

Si V es un subconjunto irreducible, se suele decir que V es regular en C si el anillo local $\mathcal{O}_{C,V}$ es regular o, equivalentemente, si el ideal primo $I_C(V)$ es regular en $K[C]$. Según el teorema anterior esto equivale a que V contenga a un punto regular de C (y no a que V sea regular como conjunto algebraico, es decir, no a que todos sus puntos sean regulares en V).

Para terminar vamos a analizar con algo más de detalle la geometría de los puntos regulares. Consideremos un conjunto algebraico afín $C \subset A^n$ y $P \in C$ un punto regular. No perdemos generalidad si hacemos un cambio de coordenadas y suponemos que $P = (0, \ldots, 0)$. Entonces

$$\mathcal{O}_{C,P} = K[C]_{(x_1,\ldots,x_n)} = A/I(C)A,$$

donde $A = K[X_1, \ldots, X_n]_{(X_1,\ldots,X_n)} = \mathcal{O}_P(A^n)$. Tenemos que A es un anillo local regular y si $F/G \in \mathfrak{m}_P(A^n)$, entonces su clase en $\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$ es la misma que la de $F/G(P)$ (ver (5.2)). Puesto que un sistema regular de parámetros de $\mathcal{O}_{A^n,P}$ es un generador de $\mathfrak{m}_P(A^n)$ que induce una base en $\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$, vemos que, multiplicando por una constante, todo sistema fundamental de parámetros de $\mathcal{O}_{A^n,P}$ puede transformarse en otro de la forma $F_1, \ldots, F_n$ con $F_i \in K[X_1, \ldots, X_n]$.

El hecho de que P sea regular en P significa que el ideal $I(C)A$ tiene cociente regular, luego el teorema 5.19 nos da que existe un sistema fundamental de parámetros $F_1, \ldots, F_n$ de A (que, según la observación precedente podemos tomar en $K[X_1, \ldots, X_n]$) tal que $I(C)A = (F_{d+1}, \ldots, F_n)$.

En este punto conviene notar que si tuviéramos que $I(C) = (F_{d+1}, \ldots, F_n)$ para ciertos $F_i \in K[X_1, \ldots, X_n]$, entonces 5.19 nos permite completar este generador (de forma distinta para cada P) a un sistema $F_1, \ldots, F_n$ en las condiciones anteriores.

Llamemos $H_i = V(F_i)$, que es una hipersuperficie que pasa por P y cuya variedad tangente $T_P(H_i)$ está definida por la parte lineal de F_i. Las partes lineales de los F_i determinan una base de $\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$, luego son linealmente independientes sobre K (en particular no nulas). Esto significa que las hipersuperficies H_i son todas regulares en P y los hiperplanos $T_P(H_i)$ son linealmente independientes en P (en el sentido de que sus vectores directores lo son).

Observemos ahora que las funciones $F_{d+1},\ldots,F_n$ definen localmente a C alrededor de P, es decir, existe un abierto U en A^n tal que $P\in U$ y

$$C\cap U = H_{d+1}\cap\cdots\cap H_n\cap U.$$

En efecto, como $I(C)A=(F_{d+1},\ldots,F_n)$ deducimos que los F_i son combinaciones lineales de un generador de $I(C)$ con coeficientes en A y, recíprocamente, que los elementos de un generador de $I(C)$ son combinaciones lineales de los F_i. Tomamos como U el abierto en A^n formado por los puntos donde no se anulan los denominadores de los coeficientes de las combinaciones lineales indicadas. De este modo $P\in U$ y, para cada punto $X\in U$, tenemos que $F_{d+1},\ldots,F_n$ se anulan en X si y sólo si lo hace un generador de $I(C)$, o sea, si y sólo si $X\in C$.

Notemos que si C es irreducible ha de ser $C\subset H_{d+1}\cap\cdots\cap H_n$ (porque las funciones F_i se han de ser idénticamente nulas en C), pero no podemos asegurar la igualdad porque la intersección no tiene por qué ser irreducible. La igualdad caracteriza precisamente a las intersecciones completas ideales:

Teorema 5.75 *Sea $C\subset A^n$ un conjunto algebraico afín regular de dimensión d. Entonces C es una intersección completa ideal si y sólo si existen $n-d$ hipersuperficies $H_{d+1},\ldots,H_n$ en A^n tales que*

a) $C=H_{d+1}\cap\cdots\cap H_n$,

b) Para todo $P\in C$ las hipersuperficies H_i son regulares en P,

c) Para todo $P\in C$, los hiperplanos $T_P(H_i)$ son linealmente independientes.

DEMOSTRACIÓN: Que C sea una intersección completa quiere decir que $I(C)=(F_{d+1},\ldots,F_n)$, y en la discusión anterior hemos visto que entonces podemos tomar las mismas hipersuperficies $H_{d+1},\ldots,H_n$ para todo P. Esto prueba una implicación.

Recíprocamente, si existen hipersuperficies en las condiciones indicadas, serán de la forma $H_i=V(F_i)$, para ciertos polinomios $F_i\in K[X_1,\ldots,X_n]$. Por lo tanto, $I(C)=\operatorname{rad}(F_{d+1},\ldots,F_n)$. Hemos de ver que $I(C)=(F_{d+1},\ldots,F_n)$. Llamamos I al ideal de la derecha.

Para cada $P\in C$, la hipótesis nos da que las diferenciales d_PF_i son linealmente independientes sobre K. Podemos tomar polinomios $F_1,\ldots,F_d$ (por ejemplo de grado 1) de manera que $F_i(P)=0$ y las diferenciales d_PF_i, para $i=1,\ldots,n$, sean linealmente independientes sobre K, lo que equivale a que las clases $[F_i]\in\mathfrak{m}_P(A^n)/\mathfrak{m}_P(A^n)^2$ sean una base de este espacio y a su vez esto equivale a que $\mathfrak{m}_P(A^n)=(F_1,\ldots,F_n)\mathcal{O}_{A^n,P}$. Por el teorema 5.26 concluimos que el ideal $I\mathcal{O}_{A^n,P}$ es primo. Ahora bien, por otra parte tenemos que

$$I(C)\mathcal{O}_{A^n,P}=\operatorname{rad}(I\mathcal{O}_{A^n,P}),$$

luego llegamos a que $I(C)\mathcal{O}_{A^n,P}=I\mathcal{O}_{A^n,P}$ para todo $P\in C$. Equivalentemente, hemos probado que si $I(C)\subset\mathfrak{m}\subset K[X_1,\ldots,X_n]$ y $\mathfrak{m}$ es un ideal maximal, entonces $I(C)_{\mathfrak{m}}=I_{\mathfrak{m}}$.

Observemos que los ideales maximales que contienen a $I(C)$ son los mismos que los que contienen a I, puesto que $I(C) = \operatorname{rad} I$. Claramente tenemos que $(I(C)/I)_{\mathfrak{m}} = 0$ para todo ideal maximal $\mathfrak{m}$ de $K[X_1, \ldots, X_n]/I$, luego 3.9 nos da que $I(C) = I$. ■

Apéndice A

Módulos planos

En este apéndice combinaremos las técnicas que hemos visto de álgebra homológica y álgebra conmutativa para obtener algunos resultados sobre una clase de módulos de gran importancia en geometría algebraica:

Sabemos que si A es un anillo y M es un A-módulo, entonces el funtor $\otimes_A M$ es exacto por la derecha. El módulo M se llama *plano* cuando el funtor es exacto, lo cual equivale claramente a que, para todo monomorfismo de A-módulos $N \longrightarrow R$, el homomorfismo $N \otimes_A M \longrightarrow R \otimes_A M$ es también inyectivo.

Si B es una A-álgebra, diremos que es *plana* si lo es como A-módulo. Un homomorfismo de álgebras $A \longrightarrow B$ es *plano* si B es plano como A-álgebra.

Las propiedades siguientes son consecuencias elementales de las propiedades del producto tensorial:

Teorema A.1 *Sea A un anillo:*

a) Todo A-módulo libre es plano.

b) El producto tensorial de dos módulos planos es plano.

c) Sea B una A-álgebra y M un A-módulo plano. Entonces $M \otimes_A B$ es un B-módulo plano.

d) Si B es una A-álgebra plana, entonces todo B-módulo plano es también un A-módulo plano.

Teorema A.2 *Si A es un anillo y $S \subset A$ es un conjunto multiplicativo, entonces el homomorfismo $A \longrightarrow S^{-1}A$ es plano.*

DEMOSTRACIÓN: Si $M \longrightarrow N$ es un monomorfismo de A-módulos entonces $S^{-1}A \otimes_A M \longrightarrow S^{-1}A \otimes_A N$ es, salvo isomorfismos, el homomorfismo canónico $S^{-1}M \longrightarrow S^{-1}N$, que es inyectivo por 3.2. ■

Los módulos planos tienen la siguiente caracterización homológica inmediata:

Teorema A.3 *Si A es un anillo y M es un A-módulo, las afirmaciones siguientes son equivalentes:*

a) *M es un A-módulo plano.*

b) $\operatorname{Tor}_n^A(N, M) = 0$ *para todo A-módulo N y todo $n \geq 1$.*

c) $\operatorname{Tor}_1^A(N, M) = 0$ *para todo A-módulo N.*

Uniendo esto al teorema 5.47, obtenemos la caracterización siguiente para el caso de módulos sobre un anillo local:

Teorema A.4 *Sea M un módulo finitamente generado sobre un anillo local A. Entonces M es plano sobre A si y sólo si es libre.*

Ahora probamos que el carácter plano de un módulo depende únicamente de sus localizaciones:

Teorema A.5 *Sea $A \longrightarrow B$ un homomorfismo de anillos y M un B-módulo. Las afirmaciones siguientes son equivalentes:*

a) *M es un A-módulo plano.*

b) *Si $\mathfrak{q}$ es un ideal primo de B y $\mathfrak{p}$ es su antiimagen en A, entonces $M_\mathfrak{q}$ es un $A_\mathfrak{p}$-módulo plano.*

c) *Si $\mathfrak{q}$ es un ideal maximal de B y $\mathfrak{p}$ es su antiimagen en A, entonces $M_\mathfrak{q}$ es un $A_\mathfrak{p}$-módulo plano.*

Demostración: a) $\Rightarrow$ b) Sea $N \longrightarrow R$ un monomorfismo de $A_\mathfrak{p}$-módulos. Entonces $N \otimes_A M \longrightarrow R \otimes_A M$ es un monomorfismo de B-módulos. Multiplicando por $\otimes_B B_\mathfrak{q}$ obtenemos un monomorfismo $N \otimes_A M_\mathfrak{q} \longrightarrow R \otimes_A M_\mathfrak{q}$, pero es fácil ver que, salvo isomorfismos, este monomorfismo se corresponde con el monomorfismo $N \otimes_{A_\mathfrak{q}} M_\mathfrak{q} \longrightarrow R \otimes_{A_\mathfrak{p}} M_\mathfrak{q}$, luego $M_\mathfrak{q}$ es plano.

b) $\Rightarrow$ c) es trivial.

c) $\Rightarrow$ a) Sea $N \longrightarrow R$ un monomorfismo de A-módulos y consideremos la sucesión exacta de B-módulos

$$0 \longrightarrow L \longrightarrow N \otimes_A M \longrightarrow R \otimes_A M,$$

donde L es el núcleo del homomorfismo de la derecha. Para cada ideal maximal $\mathfrak{q}$ de B, al multiplicar por $\otimes_B B_\mathfrak{q}$ obtenemos una sucesión exacta

$$0 \longrightarrow L_\mathfrak{q} \longrightarrow N \otimes_A M_\mathfrak{q} \longrightarrow R \otimes_A M_\mathfrak{q}.$$

Es fácil ver que, salvo isomorfismos, se corresponde con

$$0 \longrightarrow L_\mathfrak{q} \longrightarrow N_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{q} \longrightarrow R_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{q}.$$

Ahora bien, el homomorfismo de la derecha es inyectivo por hipótesis, luego $L_{\mathfrak{q}} = 0$. El teorema 3.9 nos da que $L = 0$. ■

El lector debería observar las particularizaciones del teorema anterior a los casos $M = B$ y $A = B$.

Los epimorfismos no son planos salvo en un caso muy particular:

Teorema A.6 *Si A es un anillo e I un ideal finitamente generado, son equivalentes:*

a) A/I es un A-módulo plano.

b) $I^2 = I$.

c) $I = (e)$, donde $e \in A$ cumple $e^2 = e$.

DEMOSTRACIÓN: Si A/I es plano, la inclusión $I \longrightarrow A$ induce un monomorfismo de anillos $I \otimes_A (A/I) \longrightarrow A \otimes_A (A/I) \cong A/I$ cuya imagen es $I(A/I) = 0$, luego $I \otimes_A (A/I) = 0$. De la sucesión exacta $I \longrightarrow A \longrightarrow A/I \longrightarrow 0$ obtenemos la sucesión exacta $I \otimes_A I \longrightarrow I \longrightarrow 0$, de la que se sigue que $I^2 = I$.

Si $I^2 = I$, elijamos un sistema generador $I = (a_1, \ldots, a_m)$. Entonces

$$a_i = \sum_{j=1}^{m} r_{ij} a_j, \qquad \text{para ciertos } r_{ij} \in I.$$

Matricialmente, $(a_j)(I_m - (r_{ij})) = 0$, donde I_m es la matriz identidad. Multiplicando por la matriz adjunta traspuesta resulta que $\det(I_m - (r_{ij}))a_j = 0$ para $j = 1, \ldots, m$. El determinante es de la forma $1 - e$, con $e \in I$. Como e es combinación lineal de los a_j resulta que $(1 - e)e = 0$, luego $e^2 = e$ y $a_j = a_j e$, luego $I = (e)$.

Si I es de esta forma, llamamos $I' = (1 - e)$, de modo que $A = I \oplus I'$ y $A/I \cong I'$. Si $M \longrightarrow N$ es un monomorfismo de A-módulos, entonces tenemos que $M \cong M \otimes_A A \cong (M \otimes_A I) \oplus (M \otimes_A I')$, e igualmente $N \cong (N \otimes_A I) \oplus (N \otimes_A I')$, de donde se sigue que $M \otimes_A I' \longrightarrow N \otimes_A I'$ es inyectiva (pues se corresponde con la restricción de $M \longrightarrow N$), y lo mismo vale para $M \otimes_A (A/I) \longrightarrow N \otimes_A (A/I)$. ■

Veamos ahora un criterio útil para comprobar el carácter plano de un módulo:

Teorema A.7 *Un A-módulo M es plano si y sólo si para todo ideal I de A el homomorfismo $I \otimes_A M \longrightarrow IM$ es un isomorfismo.*

DEMOSTRACIÓN: Si M es plano, la inclusión $I \longrightarrow A$ induce el monomorfismo $I \otimes_A M \longrightarrow A$, cuya imagen es IM.

Veamos ahora que la condición es necesaria. Sea $N' \longrightarrow N$ un monomorfismo de módulos. Supongamos en primer lugar que N es libre de rango n y vamos a probar que $N' \otimes_A M \longrightarrow N \otimes_A M$ es inyectiva por inducción sobre n. Si

$n = 1$ entonces $N \cong A$ y N' se corresponde con un ideal de A. La conclusión es inmediata.

Si $n \geq 2$ descomponemos $N = N_1 \oplus N_2$, donde los dos sumandos son libres de rango $< n$. Sea $N_1' = N' \cap N_1$, y sea N_2' la imagen de N' en $N_2 = N/N_1$. Tenemos el diagrama conmutativo siguiente

$$\begin{tikzcd} N_1' \arrow[r] \arrow[d] & N' \arrow[r] \arrow[d] & N_2' \arrow[r] \arrow[d] & 0 \\ N_1 \arrow[r] & N \arrow[r] & N_2 \arrow[r] & 0 \end{tikzcd}$$

donde las filas son exactas y las columnas inyectivas. De aquí obtenemos el diagrama conmutativo

$$\begin{tikzcd} N_1' \otimes_A M \arrow[r] \arrow[d, "\beta"'] & N' \otimes_A M \arrow[r] \arrow[d] & N_2' \otimes_A M \arrow[r] \arrow[d, "\gamma"] & 0 \\ N_1 \otimes_A M \arrow[r, "\alpha"'] & N \otimes_A M \arrow[r] & N_2 \otimes_A M \arrow[r] & 0 \end{tikzcd}$$

en el que las filas son también exactas. Además α es inyectivo porque N_1 es un sumando directo de N y β, γ son inyectivos por hipótesis de inducción. Esto implica la inyectividad de la flecha central.

Supongamos ahora que N es libre de rango infinito. Un elemento $x \in N' \otimes M$ se expresa como suma de tensores $n \otimes m$, con $n \in N'$. Cada n es combinación de un número finito de elementos de una base de N, luego podemos encontrar un submódulo $N_0 \subset N$ libre de rango finito tal que x está en la imagen del homomorfismo $(N' \cap N_0) \otimes_A M \longrightarrow N' \otimes_A M$.

Por la parte ya probada sabemos que $(N' \cap N_0) \otimes_A M \longrightarrow N_0 \otimes_A M$ es inyectiva, luego también lo es $(N' \cap N_0) \otimes_A M \longrightarrow N \otimes_A M$, pues N_0 es un sumando directo de N. El diagrama conmutativo

$$\begin{tikzcd} (N' \cap N_0) \otimes_A M \arrow[r] \arrow[d] & N \otimes_A M \\ N' \otimes_A M \arrow[ru] & \end{tikzcd}$$

nos da que si x está en el núcleo de $N' \otimes_A M \longrightarrow N \otimes_A M$ entonces $x = 0$, luego este homomorfismo es inyectivo.

Sea N un A-módulo arbitrario y consideremos un epimorfismo $p : L \longrightarrow N$, donde L es un A-módulo libre. Sea $L' = p^{-1}[N']$. Tenemos el siguiente diagrama conmutativo con filas exactas:

$$\begin{tikzcd} \mathrm{N}(p) \arrow[r] \arrow[d] & L' \arrow[r] \arrow[d] & N' \arrow[r] \arrow[d] & 0 \\ \mathrm{N}(p) \arrow[r] & L \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

De él obtenemos a su vez el diagrama

$$\begin{tikzcd}
\mathrm{N}(p) \otimes_A M \arrow[r] \arrow[d] & L' \otimes_A M \arrow[r] \arrow[d] & N' \otimes_A M \arrow[r] \arrow[d] & 0 \\
\mathrm{N}(p) \otimes_A M \arrow[r] & L \otimes_A M \arrow[r] & N \otimes_A M \arrow[r] & 0
\end{tikzcd}$$

Las filas son también exactas y las dos primeras flechas verticales son monomorfismos (la primera es la identidad y la segunda por la parte ya probada). De aquí se sigue que la tercera también es un monomorfismo. ■

Como aplicación obtenemos los resultados siguientes:

Teorema A.8 *Si A es un dominio de ideales principales, un A-módulo M es plano si y sólo si es libre de torsión.*

Demostración: Por el teorema anterior, M es plano si y sólo si para todo $a \in A$ el homomorfismo $f_a : (a) \otimes_A M \longrightarrow aM$ es biyectivo. Sean $t_a : A \longrightarrow (a)$ y $u_a : M \longrightarrow aM$ la multiplicación por a. Entonces t_a es un isomorfismo para todo $a \neq 0$ y tenemos el diagrama conmutativo

$$\begin{tikzcd}
M = A \otimes_A M \arrow[r, "u_a"] \arrow[d, "t_a \otimes 1"'] & aM \\
(a) \otimes_A M \arrow[ur, "f_a"'] &
\end{tikzcd}$$

Vemos que f_a es un isomorfismo si y sólo si lo es u_a, y los u_a son isomorfismos si y sólo si M es libre de torsión. ■

Teorema A.9 *Si A es un anillo noetheriano y $\hat{A}$ es su compleción respecto a la topología inducida por un ideal I, entonces $\hat{A}$ es plano sobre A.*

Demostración: Según el teorema A.7, basta considerar un ideal J de A y hemos de probar que el homomorfismo $J \otimes_A \hat{A} \longrightarrow J\hat{A}$ es un isomorfismo o, lo que es lo mismo, que el homomorfismo natural $\phi : J \otimes_A \hat{A} \longrightarrow \hat{A}$ es inyectivo.

Por el teorema 4.16, el monomorfismo $J \longrightarrow A$ da lugar a un monomorfismo $\hat{J} \longrightarrow \hat{A}$ que, a través del isomorfismo natural $J \otimes_A \hat{A} \cong \hat{J}$ dado por el teorema 4.17, se convierte en ϕ. ■

Veamos otra aplicación elemental de las técnicas homológicas. En lo sucesivo convenimos en que Tor^A significa Tor_1^A.

Teorema A.10 *Sea $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de A-módulos y supongamos que M'' es plano. Entonces M es plano si y sólo si lo es M'.*

Demostración: Supongamos que M y M'' son planos y sea $N \longrightarrow P$ un monomorfismo de A-módulos. Entonces tenemos el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' \otimes_A N & \longrightarrow & M \otimes_A N & \longrightarrow & M'' \otimes_A N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' \otimes_A P & \longrightarrow & M \otimes_A P & \longrightarrow & M'' \otimes_A P & \longrightarrow & 0 \end{array}$$

Notemos que la exactitud por la izquierda se debe a que $\operatorname{Tor}^A(M'', N) = 0$ porque M'' es plano, e igualmente con P. Es fácil ver que la primera flecha vertical es inyectiva, teniendo en cuenta que la siguiente lo es.

Si son planos M' y M'' es mucho más simple: para todo A-módulo N tenemos la sucesión exacta

$$0 = \operatorname{Tor}^A(M', N) \longrightarrow \operatorname{Tor}^A(M, N) \longrightarrow \operatorname{Tor}^A(M'', N) = 0,$$

luego $\operatorname{Tor}^A(N, M) = 0$, y A.3 implica que M es plano. ■

Vamos a plantear unas propiedades en principio más débiles que A.3, pero veremos que —bajo ciertas hipótesis— equivalen a que el módulo M sea plano.

Teorema A.11 *Sea A un anillo, I un ideal de A y M un A-módulo. Las afirmaciones siguientes son equivalentes:*

a) $\operatorname{Tor}^A(N, M) = 0$ *para todo A/I-módulo N.*

b) M/IM es un A/I-módulo plano y $I \otimes_A M \cong IM$ con el homomorfismo natural.

c) M/IM es un A/I-módulo plano y $\operatorname{Tor}^A(A/I, M) = 0$.

Demostración: a) $\Rightarrow$ b) Sea $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ una sucesión exacta de A/I-módulos. De ella obtenemos una sucesión exacta

$$0 = \operatorname{Tor}^A(N'', M) \longrightarrow N' \otimes_A M \longrightarrow N \otimes_A M.$$

Es fácil ver que $N \otimes_A M \cong N \otimes_{A/I} (M/IM)$ como A/I-módulos, e igualmente $N' \otimes_A M \cong N' \otimes_{A/I} (M/IM)$, con lo que la sucesión anterior prueba que M/IM es plano sobre A/I.

Ahora consideramos la sucesión exacta $0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$, de la que obtenemos la sucesión exacta

$$0 \longrightarrow \operatorname{Tor}^A(A/I, M) \longrightarrow I \otimes_A M \longrightarrow M.$$

Concluimos que $I \otimes_A M \cong IM$.

b) $\Rightarrow$ c) Recíprocamente, como

$$0 = \operatorname{Tor}^A(A, M) \longrightarrow \operatorname{Tor}^A(A/I, M) \longrightarrow I \otimes_A M \longrightarrow M$$

es exacta, ha de ser $\mathrm{Tor}^A(A/I, M) = 0$. (Aquí usamos que A es un A-módulo libre.)

c) $\Rightarrow$ a) Sea N un A/I-módulo y sea $0 \longrightarrow R \longrightarrow L \longrightarrow N \longrightarrow 0$ una sucesión exacta de A/I-módulos, donde L es libre sobre A/I.

Es fácil probar que $\mathrm{Tor}^A(\bigoplus_i N_i, M) \cong \bigoplus_i \mathrm{Tor}^A(N_i, M)$ (tomando como resolución proyectiva de la suma directa una suma directa de resoluciones proyectivas). Esto nos da que $\mathrm{Tor}^A(L, M) = 0$. Por lo tanto tenemos la sucesión exacta

$$0 = \mathrm{Tor}^A(L, M) \longrightarrow \mathrm{Tor}^A(N, M) \longrightarrow R \otimes_A M \longrightarrow L \otimes_A M.$$

El último homomorfismo se corresponde, salvo isomorfismo, con

$$R \otimes_{A/I} (M/IM) \longrightarrow L \otimes_{A/I} (M/IM),$$

que es inyectivo porque M/IM es plano. Así pues, $\mathrm{Tor}^A(N, M) = 0$. ■

Es evidente que las tres propiedades del teorema anterior se cumplen cuando M es un A-módulo plano. Por otra parte, si I es un ideal maximal entonces la primera parte de b) y c) se cumple trivialmente, pues A/I es un cuerpo y todos los A/I-módulos son libres. Observemos también que, en virtud del teorema A.7, la segunda parte de b) implica que M es plano sobre A si se cumple para todo ideal I.

Vamos a buscar condiciones suficientes sobre I y M para que las propiedades del teorema anterior impliquen que M es plano sobre A. Empezaremos extrayendo algunas consecuencias de dichas propiedades:

- *El homomorfismo natural*

$$\gamma_n : I^n/I^{n+1} \otimes_{A/I} (M/IM) \longrightarrow I^n M/I^{n+1} M$$

es un isomorfismo.

Demostración: Consideramos la sucesión exacta

$$0 \longrightarrow I^{n+1} \longrightarrow I^n \longrightarrow I^n/I^{n+1} \longrightarrow 0,$$

que da lugar al diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & I^{n+1} \otimes_A M \arrow[r] \arrow[d, "\alpha_{n+1}"] & I^n \otimes_A M \arrow[r] \arrow[d, "\alpha_n"] & (I^n/I^{n+1}) \otimes_A M \arrow[r] \arrow[d, "\gamma_n"] & 0 \\
0 \arrow[r] & I^{n+1}M \arrow[r] & I^n M \arrow[r] & I^n M/I^{n+1}M \arrow[r] & 0
\end{tikzcd}$$

La fila superior es exacta por a), pues $\mathrm{Tor}^A(I^n/I^{n+1}, M) = 0$, y la fila inferior es claramente exacta. Los homomorfismos α_i son todos suprayectivos. Además α_1 es inyectivo por b), luego inductivamente concluimos que todos los α_i son inyectivos, de donde a su vez se sigue que todos los γ_n son isomorfismos. ■

- $\mathrm{Tor}^A(N, M) = 0$ *para todo* A/I^n*-módulo* N *(*$n \geq 1$*).*

DEMOSTRACIÓN: Razonamos por inducción sobre n. Para $n = 1$ es la propiedad a). Ahora observamos que si N es un A/I^n-módulo, entonces IN y N/IN son A/I^{n-1}-módulos, luego por hipótesis de inducción

$$\mathrm{Tor}_1^A(IN, M) = 0, \quad \mathrm{Tor}_1^A(N/IN, M) = 0.$$

Consideramos la sucesión exacta $0 \longrightarrow IN \longrightarrow N \longrightarrow N/IN \longrightarrow 0$, de la que obtenemos

$$0 = \mathrm{Tor}_1^A(IN, M) \longrightarrow \mathrm{Tor}_1^A(N, M) \longrightarrow \mathrm{Tor}_1^A(N/IN, M) = 0,$$

luego $\mathrm{Tor}_1^A(N, M) = 0$. ■

- $M_n = M/I^{n+1}M$ *es plano sobre* $A_n = A/I^{n+1}$ *(para* $n \geq 0$*).*

DEMOSTRACIÓN: Si $n = 0$ es la primera parte de b). Supongamos $n \geq 1$. Tenemos el diagrama conmutativo con filas exactas:

$$\begin{tikzcd}
 & (I^{i+1}/I^{n+1}) \otimes_A M \arrow[r] \arrow[d, "\alpha_{i+1}"] & (I^i/I^{n+1}) \otimes_A M \arrow[r] \arrow[d, "\alpha_i"] & (I^i/I^{i+1}) \otimes_A M \arrow[r] \arrow[d, "\gamma_i"] & 0 \\
0 \arrow[r] & I^{i+1}M/I^{n+1}M \arrow[r] & I^iM/I^{n+1}M \arrow[r] & I^iM/I^{i+1}M \arrow[r] & 0
\end{tikzcd}$$

Hemos visto que los homomorfismos γ_i son isomorfismos. Por otra parte, $\alpha_{n+1} = 0$ es un isomorfismo. Razonando por inducción (decreciente) concluimos que todos los α_i son isomorfismos. En particular

$$\alpha_1 : (I/I^{n+1}) \otimes_A M = IA_n \otimes_{A_n} M_n \longrightarrow IM_n$$

es un isomorfismo. Esto significa que se cumple la propiedad b) para A_n, IA_n y M_n, luego también se cumple a), es decir, $\mathrm{Tor}^{A_n}(N, M_n) = 0$ para todo A_n-módulo N. Esto significa que M_n es plano sobre A_n. ■

Ahora es claro que una condición suficiente para que las propiedades a), b) y c) equivalgan a que M es plano sobre A es que el ideal I sea nilpotente, pues entonces $M_n = M$ y $A_n = A$ para n suficientemente grande. No obstante, no es ésta la condición que nos interesa. La forma más general de la condición que buscamos es la siguiente:

Teorema A.12 *Sea* A *un anillo noetheriano sea* I *un ideal de* A*, sea* M *un* A*-módulo y supongamos que, para todo ideal* J *de* A*, la topología* I*-ádica en el* A*-módulo* $J \otimes_A M$ *tiene la propiedad de Hausdorff. Entonces* M *es plano sobre* A *si y sólo si se cumplen las propiedades del teorema* A.11.

Demostración: Por el teorema A.7 basta probar que si J es un ideal de A, el homomorfismo natural $j : J \otimes_A M \longrightarrow M$ es inyectivo. Por hipótesis $J \otimes_A M$ es de Hausdorff para la topología I-ádica, lo que significa que

$$\bigcap_n I^n(J \otimes_A M) = 0.$$

Así pues, basta probar que $\mathrm{N}(j) \subset I^n(J \otimes_A M)$ para todo n. Aplicamos el lema de Artin-Rees a $M = A$, $M' = J$, que nos da un natural $r \geq n$ tal que $J \cap I^k = I^{k-r}(I^r \cap J)$, para todo $k \geq r$. Tomando k de modo que $k - r \geq n$ concluimos que $J \cap I^k \subset I^n J$. Consideramos los homomorfismos naturales

$$J \otimes_A M \xrightarrow{f} (J/(I^k \cap J)) \otimes_A M \xrightarrow{g} (J/I^n J) \otimes_A M = (J \otimes_A M)/I^n(J \otimes_A M).$$

Como M_{k-1} es plano sobre A_{k-1}, el homomorfismo

$$(J/(I^k \cap J)) \otimes_A M = (J/(I^k \cap J)) \otimes_{A_{k-1}} M_{k-1} \longrightarrow M_{k-1}$$

es inyectivo, y tenemos el diagrama conmutativo

$$\begin{tikzcd} J \otimes_A M \arrow[r, "f"] \arrow[d, "j"'] & (J/(I^k \cap J)) \otimes_A M \arrow[d] \\ M \arrow[r] & M_{k-1} \end{tikzcd}$$

Esto implica que $\mathrm{N}(j) \subset \mathrm{N}(f) \subset \mathrm{N}(f \circ g) = I^n(J \otimes_A M)$ ■

Un caso particular en que se cumple la condición que hemos impuesto es el siguiente:

Teorema A.13 *Sea A un anillo noetheriano, sea I un ideal de A, sea B una A-álgebra noetheriana tal que IB esté contenido en todos los ideales maximales de B. Sea M un B-módulo finitamente generado. Entonces, M es plano sobre A si y sólo si se cumplen las afirmaciones a), b), c) del teorema* A.11.

Demostración: Basta ver que se cumple la condición del teorema anterior. Ahora bien, si J es un ideal de A, la topología I-ádica en $J \otimes_A M$ como A-módulo es la misma que la topología IB-ádica como B-módulo. Además $J \otimes_A M$ es un B-módulo finitamente generado, luego el teorema 4.21 nos da que $J \otimes_A M$ es un espacio de Hausdorff con la topología I-ádica. ■

El resultado se simplifica aún más para anillos locales:

Teorema A.14 *Sea $A \longrightarrow B$ un homomorfismo de anillos locales noetherianos y sea M un B-módulo finitamente generado. Sea $\mathfrak{m}_A$ el ideal maximal de A y sea $k = A/\mathfrak{m}_A$. Las afirmaciones siguientes son equivalentes:*

a) $\mathrm{Tor}^A(N, M) = 0$ *para todo k-espacio vectorial N.*

b) $\mathfrak{m}_A \otimes_A M \cong \mathfrak{m}_A M$ *con el homomorfismo natural.*

c) $\mathrm{Tor}^A(k, M) = 0$.

d) M *es un* A*-módulo plano.*

Si comparamos con los teoremas 5.47 y A.4, la principal diferencia es que en el teorema anterior no estamos suponiendo que el módulo M sea finitamente generado sobre A.

Como primera aplicación demostramos el siguiente resultado, técnico, pero útil en algunas ocasiones.

Teorema A.15 *Sea* $A \longrightarrow B$ *un homomorfismo plano entre dos anillos noetherianos locales y sea* $b \in B$ *tal que su imagen en* $B/\mathfrak{m}_A B$ *no sea un divisor de cero. Entonces* b *no es un divisor de cero en* B *y* B/bB *es plano sobre* A.

Demostración: Supongamos que $x \in B$ cumple $bx = 0$ y vamos a ver que $x = 0$. Para ello basta probar que $x \in \mathfrak{m}_A^n B$ para todo n, pues $\mathfrak{m}_A B \subset \mathfrak{m}_B$ y el teorema 4.21 (aplicado a B) nos da que la topología definida por $\mathfrak{m}_A B$ es de Hausdorff.

Como b no es un divisor de 0 en $B/\mathfrak{m}_A B$, necesariamente $x \in \mathfrak{m}_A B$, es decir, se cumple el resultado para $n = 1$. Supuesto que $x \in \mathfrak{m}_A^n B$, sea $a_1, \ldots, a_r$ un generador minimal de $\mathfrak{m}_A^n$. Por el teorema 4.52, sabemos que estos elementos inducen k-una base de $\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1}$, donde $k = A/\mathfrak{m}_A$.

Podemos expresar $x = \sum_i a_i x_i$, con $x_i \in B$. Entonces $bx = \sum_i a_i(bx_i) = 0$ en $\mathfrak{m}_A^n B$. Por el teorema A.7 sabemos que $\mathfrak{m}_A^n B \cong \mathfrak{m}_A^n \otimes_A B$, luego se cumple que $\sum_i a_i \otimes bx_i = 0$ en $\mathfrak{m}_A^n \otimes_A B$.

Consideremos la sucesión exacta $0 \longrightarrow R \longrightarrow A^r \longrightarrow \mathfrak{m}_A^n \longrightarrow 0$ determinada por el generador minimal que hemos tomado. Como B es plano, de ella obtenemos otra sucesión exacta

$$0 \longrightarrow R \otimes_A B \longrightarrow A^r \otimes_A B \longrightarrow \mathfrak{m}_A^n \otimes_A B \longrightarrow 0.$$

Si llamamos $e_1, \ldots, e_r$ a la base canónica de A^r, tenemos que $\sum_i e_i \otimes bx_i$ tiene imagen nula, luego existe un $\sum_j r_j \otimes x'_j \in R \otimes_A B$ tal que

$$\sum_j r_j \otimes x'_j = \sum_i e_i \otimes bx_i.$$

Si $r_j = (c_{ij})$, entonces

$$\sum_i e_i \otimes \sum_j c_{ij} x'_j = \sum_i e_i \otimes bx_i,$$

luego $bx_i = \sum_j c_{ij} x'_j$. Por otra parte, el hecho de que $r_j \in R$ implica que $\sum_i c_{ij} a_i = 0$ y tomando clases módulo $\mathfrak{m}_A^{n+1}$ concluimos que $c_{ij} \in \mathfrak{m}_A$, por la k-independencia lineal de los a_i. Esto prueba que $x \in \mathfrak{m}_A^{n+1} B$ y, en definitiva, que $x = 0$.

Como b no es un divisor de cero de B, tenemos una sucesión exacta

$$0 \longrightarrow B \longrightarrow B \longrightarrow B/bB \longrightarrow 0,$$

donde el monomorfismo es la multiplicación por b. De aquí obtenemos la sucesión exacta

$$0 = \operatorname{Tor}^A(B,k) \longrightarrow \operatorname{Tor}^A(B/bB,k) \longrightarrow B\otimes_A k \longrightarrow B\otimes_A k.$$

Ahora observamos que $B\otimes_A k \cong B/\mathfrak{m}_A B$, así como que el último homomorfismo de la sucesión se corresponde con la multiplicación por b en el cociente, que es inyectiva por hipótesis. Con esto llegamos a que $\operatorname{Tor}^A(B/bB,k) = 0$, lo que implica que B/bB es plano, por el teorema anterior. ■

Veamos ahora una versión para anillos no necesariamente locales:

Teorema A.16 *Sea $A \longrightarrow B$ un homomorfismo plano y sea $b \in B$ tal que, para todo ideal maximal $\mathfrak{m}$ de A, su imagen en $B/\mathfrak{m}B$ no sea un divisor de cero. Entonces B/bB es plano sobre A.*

Demostración: Sea $\mathfrak{q}/(bB)$ un ideal primo en B/bB y sea $\mathfrak{p}$ su antiimagen en A. Por el teorema A.5 basta probar que $(B/bB)_{\mathfrak{q}/(bB)} \cong B_{\mathfrak{q}}/bB_{\mathfrak{q}}$ es plano sobre $A_{\mathfrak{p}}$. Por el teorema anterior basta ver que b no es un divisor de cero en $B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} \cong (B/\mathfrak{p}B)_{\mathfrak{q}} \cong (B/\mathfrak{p}B)\otimes_B B_{\mathfrak{q}}$. Como $B_{\mathfrak{q}}$ es plano sobre B, para ello basta con que b no sea un divisor de cero en $B/\mathfrak{p}$ (pues si la multiplicación por b es inyectiva en $B/\mathfrak{p}B$ lo seguirá siendo al multiplicar por $B_{\mathfrak{q}}$). Si $\mathfrak{m}$ es un ideal maximal de A que contenga a $\mathfrak{p}$, basta con que b no sea un divisor de cero en $B/\mathfrak{m}B$, que es precisamente la hipótesis del teorema. ■

Ejemplo Se comprueba sin dificultad que el teorema anterior es aplicable si $B = A[X_1,\ldots,X_n]$ y b es un polinomio mónico. ■

Terminamos el apéndice con la siguiente aplicación del teorema A.13:

Teorema A.17 *Sea A un anillo noetheriano, sea B una A-álgebra finitamente generada y sea M un B-módulo finitamente generado. Entonces el conjunto*

$$U = \{\mathfrak{p} \in \operatorname{Esp} B \mid M_{\mathfrak{p}} \text{ es plano sobre } A\}$$

es abierto (tal vez vacío).

Necesitamos algunos resultados previos. En primer lugar recordamos una propiedad elemental de los módulos libres:

Teorema A.18 *Si A es un anillo, M es un A-módulo, $L \subset M$ es un submódulo libre y M/L también es libre, entonces M es libre.*

Demostración: Sea $B \subset M$ tal que $\{[b] \mid b \in B\}$ sea una base de M/L y sea $L' = \langle B\rangle \subset M$. Entonces la aplicación $[b] \mapsto b$ se extiende a un homomorfismo $M/L \longrightarrow L'$ que claramente es un isomorfismo. En particular L' es libre, y es fácil ver que $M = L \oplus L'$, luego también es libre. ■

Teorema A.19 *Sea A un dominio íntegro noetheriano, sea B una A-álgebra finitamente generada y M un B-módulo finitamente generado. Entonces existe un $f \in A$, $f \neq 0$ tal que M_f es un A_f-módulo libre.*

DEMOSTRACIÓN: Podemos suponer que $M \neq 0$. En tal caso existe una sucesión de B-submódulos

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M$$

tal que $M_i/M_{i-1} \cong B/\mathfrak{p}_i$, para ciertos $\mathfrak{p}_i \in \operatorname{Esp} B$. En efecto, por el teorema 3.48 existe un $\mathfrak{p}_1 \in \operatorname{As}(M)$, que será de la forma $\mathfrak{p}_1 = \operatorname{An}(m_1)$, y entonces definimos $M_1 = \langle m_1 \rangle$. Luego obtenemos $\mathfrak{p}_2$ razonando con M/M_1, y hemos de llegar a que $M = M_l$ para un cierto l porque M es un B-módulo noetheriano.

De aquí deducimos que basta probar el teorema cuando B es un dominio íntegro y $M = B$, pues si lo tenemos probado en estas condiciones entonces hay un $f_1 \in A$ no nulo tal que $(M_1)_{f_1}$ es un A_{f_1}-módulo libre, igualmente hay un $f_2 \in A$ no nulo tal que $(M_2/M_1)_{f_2}$ es un A_{f_2}-módulo libre, pero entonces $f = f_1 f_2 \in A$ es no nulo y tanto $(M_1)_f$ como $(M_2/M_1)_f \cong (M_2)_f/(M_1)_f$ son A_f-módulos libres. Por el teorema anterior $(M_2)_f$ es un A_f-módulo libre. Continuando de este modo llegamos a un $f \in A$ no nulo tal que M_f es libre.

Si el homomorfismo $A \longrightarrow B$ tiene núcleo no nulo, basta tomar f en dicho núcleo para que sea $B_f = 0$ y el teorema se cumpla trivialmente. Así pues, podemos suponer que A es un subanillo de B. Llamemos k al cuerpo de cocientes de A y sea Bk la subálgebra del cuerpo de cocientes de B generada por B y k. Conviene observar que $Bk \cong B \otimes_A k$. En efecto, si llamamos K al cuerpo de cocientes de B, como k es plano sobre A (porque es una localización de A), la inclusión $B \longrightarrow K$ da lugar a un monomorfismo $B \otimes_A k \longrightarrow K \otimes_A k \cong K$ cuya imagen es Bk.

Tenemos que Bk es una k-álgebra finitamente generada, por lo que tiene dimensión finita $n = \operatorname{gr.tr.}_k Bk$. Demostraremos el teorema por inducción sobre n. Por el teorema de normalización de Noether existen $y_1, \ldots, y_n \in Bk$ algebraicamente independientes sobre k tales que Bk es un módulo finitamente generado sobre $k[y_1, \ldots, y_n]$. Cada generador es entero sobre $k[y_1, \ldots, y_n]$, luego también sobre $A_g[y_1, \ldots, y_n]$, para cierto $g \in A$, $g \neq 0$. En definitiva, todo Bk y, en particular, B_g es entero sobre $A_g[y_1, \ldots, y_n]$. Eligiendo g adecuadamente podemos exigir también que $y_i \in B_g$ para todo i.

No perdemos generalidad si cambiamos A y B por A_g y B_g, lo que significa que podemos suponer que B es un módulo finitamente generado sobre el anillo de polinomios $C = A[y_1, \ldots, y_n]$.

Sea $b_1, \ldots, b_m \in B$ un conjunto C-linealmente independiente maximal. Podemos tomarlo porque su cardinal es como máximo la dimensión del cuerpo de cocientes de B sobre el cuerpo de cocientes de C, que es finita. Entonces tenemos una sucesión exacta

$$0 \longrightarrow C^m \longrightarrow B \longrightarrow B' \longrightarrow 0,$$

donde B' es un C-módulo finitamente generado y de torsión. Esto implica que su anulador I es no nulo, y podemos ver a B' como módulo sobre C/I.

Vamos a ver que la hipótesis de inducción nos da que el teorema se cumple para la A-álgebra C/I y el módulo B'. Esto significa que existe un $f \in A$, $f \neq 0$ tal que B'_f es A_f-libre, lo cual, unido a que $C_f^m = A_f[y_1, \ldots, y_m]^m$ también es A_f-libre, implica (por el teorema anterior) que B_f es A_f-libre, como teníamos que probar.

Para probar el teorema en el caso de C/I y B', la misma reducción que hemos empleado al principio de la demostración nos remite al caso de las álgebras $C/\mathfrak{p}$, donde $\mathfrak{p}/I$ es un ideal primo de C/I.

Esto nos lleva al caso trivial en que el núcleo de $A \longrightarrow C/\mathfrak{p}$ es no nulo (por ejemplo, éste es el caso si $n = 0$, pues entonces $C = A$), o bien, si A es un subanillo de $C/\mathfrak{p}$. usando que $Ck \cong C \otimes_A k$ y que $(C/\mathfrak{p})k = (C/\mathfrak{p}) \otimes_A k$ es fácil ver que $(C/\mathfrak{p})k \cong Ck/\mathfrak{p}k$, donde $\mathfrak{p}k$ es un ideal primo de Ck. Obviamente, $\dim (C/\mathfrak{p})k < \dim Ck = n$, luego podemos aplicar la hipótesis de inducción. ■

Veamos a continuación una caracterización técnica de los abiertos de un espectro:

Teorema A.20 *Si B es un anillo noetheriano y $U \subset \operatorname{Esp} B$, entonces U es abierto si y sólo si cumple las dos propiedades siguientes:*

a) Si $\mathfrak{p} \in U$, $\mathfrak{q} \in \operatorname{Esp} B$ y $\mathfrak{q} \subset \mathfrak{p}$, entonces $\mathfrak{q} \in U$.

b) Si $\mathfrak{p} \in U$, entonces U contiene un abierto no vacío del cerrado $V(\mathfrak{p})$.

DEMOSTRACIÓN: Veamos que si se cumplen estas condiciones entonces U es abierto (es la única implicación que vamos a usar). Llamemos $F = \operatorname{Esp} B \setminus U$. Hemos de probar que F es cerrado. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ los puntos cuasigenéricos de la clausura $\overline{F}$.

Si $\mathfrak{p}_i \in U$, entonces, por la propiedad b) existe un abierto no vacío $V \subset V(\mathfrak{p}_i)$ contenido en U, pero $V(\mathfrak{p}_i) \subset \overline{F}$, luego tendría que ser $V \cap F \neq \varnothing$, lo cual es absurdo.

Concluimos que $\mathfrak{p}_i \in F$ para todo i, con lo que la propiedad a) implica que $V(\mathfrak{p}_i) \subset F$. (Si $\mathfrak{q} \in V(\mathfrak{p}_i)$, no puede ser que $\mathfrak{q} \in U$, pues entonces $\mathfrak{p}_i \in U$.) Por consiguiente, $\overline{F} \subset F$ y F es cerrado. ■

Finalmente, demostramos el resultado que habíamos anunciado:

DEMOSTRACIÓN (de A.17): Probaremos que U es abierto comprobando que cumple las dos condiciones del teorema anterior.

Supongamos que $\mathfrak{p} \in U$ y que $\mathfrak{q} \subset \mathfrak{p}$. Entonces $M_\mathfrak{q} \cong M_\mathfrak{p} \otimes_B B_\mathfrak{q}$, luego para cualquier A-módulo N se cumple que $N \otimes_A M_\mathfrak{q} \cong (N \otimes_A M_\mathfrak{p}) \otimes_B B_\mathfrak{q}$. Así, una sucesión exacta de A-módulos sigue siendo exacta al multiplicarla por $\otimes_A M_\mathfrak{q}$, pues $M_\mathfrak{p}$ es plano sobre A y $B_\mathfrak{q}$ es plano sobre B. Concluimos que $M_\mathfrak{q}$ es plano sobre A y que se cumple la propiedad a) del teorema anterior.

Para probar b) tomamos de nuevo $\mathfrak{p} \in U$ y llamamos $\mathfrak{q} = \mathfrak{p} \cap A$ (más precisamente, $\mathfrak{q}$ es la antiimagen de $\mathfrak{p}$ por el homomorfismo $A \longrightarrow B$). Sea $\overline{A} = A/\mathfrak{q}$. Vamos a dar condiciones sobre un $\mathfrak{P} \in V(\mathfrak{p})$ para que esté en U.

Tenemos que $\mathfrak{p} \subset \mathfrak{P}$, luego $\mathfrak{q}B_{\mathfrak{P}}$ está contenido en $\mathfrak{P}B_{\mathfrak{P}}$, que es el único ideal maximal de $B_{\mathfrak{P}}$. Esto nos sitúa en las hipótesis del teorema A.13 para el anillo A, el ideal $I = \mathfrak{q}$, el álgebra $B_{\mathfrak{P}}$ y el módulo $M_{\mathfrak{P}}$. Por lo tanto, $M_{\mathfrak{P}}$ es plano sobre A si y sólo si $M_{\mathfrak{P}}/\mathfrak{q}M_{\mathfrak{P}}$ es plano sobre $\overline{A}$ y $\operatorname{Tor}^A(M_{\mathfrak{P}}, \overline{A}) = 0$.

Aplicamos el teorema A.19 al anillo $\overline{A}$, el álgebra $B/\mathfrak{q}B$ y el módulo $M/\mathfrak{q}M$: Existe un $f \in \overline{A}$, $f \neq 0$, tal que $(M/\mathfrak{q}M)_f$ es libre sobre $\overline{A}_f$.

Sea $f = [f']$, donde $f' \in A \setminus \mathfrak{q}$. Entonces $V = V(\mathfrak{p}) \cap D(f')$ es un entorno de $\mathfrak{p}$ en $V(\mathfrak{p})$. Vamos a probar que si $\mathfrak{P} \in V$ entonces $M_{\mathfrak{P}}/\mathfrak{q}M_{\mathfrak{P}}$ es plano sobre $\overline{A}$. En efecto, tenemos que $(M/\mathfrak{q}M)_f$ es libre sobre $\overline{A}_f$, luego es plano sobre $\overline{A}_f$ y también sobre $\overline{A}$. Como $f' \notin \mathfrak{P}$, tenemos que $S_f \subset S_{\mathfrak{P}}$, luego

$$M_{\mathfrak{P}}/\mathfrak{q}M_{\mathfrak{P}} \cong (M/\mathfrak{q}M)_{\mathfrak{P}} \cong (M/\mathfrak{q}M)_{f\,\mathfrak{P}} \cong (M_{\mathfrak{q}}M)_f \otimes_B B_{\mathfrak{P}}.$$

De este modo, si tenemos una sucesión exacta de $\overline{A}$-módulos, multiplicarla por $\otimes_{\overline{A}}(M_{\mathfrak{P}}/\mathfrak{q}M_{\mathfrak{P}})$ equivale a multiplicarla primero por $\otimes_{\overline{A}}(M/\mathfrak{q}M)_f$ y luego por $\otimes_B B_{\mathfrak{P}}$, y ambos productos conservan la exactitud.

Por otra parte, se cumple que

$$0 = \operatorname{Tor}^A(M_{\mathfrak{p}}, \overline{A}) = \operatorname{Tor}^A(M, \overline{A}) \otimes_B B_{\mathfrak{p}}.$$

En efecto, por la simetría de Tor podemos hacer los cálculos con una resolución proyectiva del A-módulo $\overline{A}$, digamos

$$\cdots \longrightarrow L_2 \longrightarrow L_1 \longrightarrow L_0 \longrightarrow \overline{A}.$$

Entonces, $\operatorname{Tor}^A(M, \overline{A})$ es el grupo de homología de

$$L_2 \otimes_A M \longrightarrow L_1 \otimes_A M \longrightarrow L_0 \otimes_A M,$$

mientras que $\operatorname{Tor}^A(M_{\mathfrak{p}}, \overline{A})$ es el grupo de homología de

$$L_2 \otimes_A M \otimes_B B_{\mathfrak{p}} \longrightarrow L_1 \otimes_A M \otimes_B B_{\mathfrak{p}} \longrightarrow L_0 \otimes_A M \otimes_B B_{\mathfrak{p}}.$$

En particular vemos que podemos considerar en $\operatorname{Tor}^A(M, \overline{A})$ una estructura de B-módulo y basta aplicar el teorema 1.37 al funtor exacto $\otimes_B B_{\mathfrak{p}}$. Observemos además que, al ser A noetheriano y $\overline{A}$ un A-módulo finitamente generado (un generador es la unidad), podemos exigir que los módulos L_i sean libres y finitamente generados. Entonces los módulos $L_i \otimes_A M$ son B-módulos finitamente generados y así $\operatorname{Tor}^A(M, \overline{A})$ es un B-módulo finitamente generado. Entonces $\operatorname{Tor}^A(M, \overline{A})_{\mathfrak{p}} = 0$ implica que existe un $g \in B \setminus \mathfrak{p}$ tal que $\operatorname{Tor}^A(M, \overline{A})_g = 0$, lo que a su vez implica que $\operatorname{Tor}^A(M, \overline{A})_{\mathfrak{P}} = 0$ para todo $\mathfrak{P} \in D(g)$.

Así llegamos a que $V \cap D(g)$ es un entorno de $\mathfrak{p}$ en $V(\mathfrak{p})$ contenido en U, lo que prueba que U es abierto. ■

Apéndice B

Imágenes directas e inversas de módulos

Terminaremos con algunas propiedades de las imágenes directas e inversas de módulos por homomorfismos de espacios anillados que no nos han hecho falta para desarrollar la teoría de funtores derivados ni en sus aplicaciones, pero que complementan la teoría general sobre los espacios anillados. Muchas de estas propiedades requieren que los homomorfismos considerados sean inmersiones cerradas, en el sentido de la definición siguiente:

Definición B.1 Un homomorfismo de espacios anillados locales $f : X \longrightarrow Y$ es una *inmersión cerrada* si f_0 es un homeomorfismo entre X y un cerrado de Y y para todo $P \in X$ la aplicación $f_P^\# : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ es un epimorfismo.

Empezamos ocupándonos de las imágenes directas, que hemos definido en 1.10 para haces arbitrarios sobre espacios topológicos y aplicaciones continuas. En el caso en que $f : X \longrightarrow Y$ es un homomorfismo de espacios anillados y $\mathcal{M}$ es un $\mathcal{O}_X$-módulo, para cada abierto U de Y, el grupo $(f_*\mathcal{M})(U) = \mathcal{M}(f^{-1}[U])$ tiene una estructura de $\mathcal{O}_X(f^{-1}[U])$-módulo, pero a través del homomorfismo de anillos $f_U^\# : \mathcal{O}_Y(U) \longrightarrow \mathcal{O}_X(f^{-1}[U])$ se convierte de forma natural en un $\mathcal{O}_Y(U)$-módulo. Es inmediato que estas estructuras de módulo son compatibles con las restricciones, por lo que la imagen directa $f_*\mathcal{M}$ es un $\mathcal{O}_Y$-módulo.

Observemos también que si $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ es un homomorfismo de $\mathcal{O}_X$-módulos, podemos definir $f_*(\phi) : f_*\mathcal{M} \longrightarrow f_*\mathcal{N}$ mediante $f_*(\phi)_U = \phi_{f^{-1}[U]}$, lo que convierte a $f_* : \mathrm{Mod}(X) \longrightarrow \mathrm{Mod}(Y)$ en un funtor covariante.

Si $\mathcal{M}$ y $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, para cada abierto U de Y tenemos isomorfismos naturales

$$(f_*\mathcal{M})(U) \otimes_{\mathcal{O}_Y(U)} (f_*\mathcal{N})(U) = \mathcal{M}(f^{-1}[U]) \otimes_{\mathcal{O}_Y(U)} \mathcal{N}(f^{-1}[U])$$

$$\cong \mathcal{M}(f^{-1}[U]) \otimes_{\mathcal{O}_X(f^{-1}[U])} \mathcal{N}(f^{-1}[U]) = (\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^-(f^{-1}[U])$$

que, compuestos con

$$(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})^-(f^{-1}[U]) \longrightarrow (\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})(f^{-1}[U]) = f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})(U),$$

inducen un homomorfismo

$$((f_*\mathcal{M}) \otimes_{\mathcal{O}_Y} (f_*\mathcal{N}))^- \longrightarrow f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}),$$

el cual a su vez induce un homomorfismo natural

$$(f_*\mathcal{M}) \otimes_{\mathcal{O}_Y} (f_*\mathcal{N}) \longrightarrow f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N}).$$

En general este homomorfismo no es inyectivo ni suprayectivo, pero, cuando f es una inmersión cerrada, es un isomorfismo:

Teorema B.2 *Si $f : X \longrightarrow Y$ es una inmersión cerrada de espacios anillados y $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, entonces $(f_*\mathcal{M}) \otimes_{\mathcal{O}_Y} (f_*\mathcal{N}) \cong f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})$.*

Demostración: Para cada punto $P \in X$ tenemos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
((f_*\mathcal{M}) \otimes_{\mathcal{O}_Y} (f_*\mathcal{N}))_{f(P)} \arrow[r] \arrow[d] & f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})_{f(P)} \arrow[d] \\
f_*(\mathcal{M})_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} f_*(\mathcal{N})_{f(P)} \arrow[r] & \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{N}_P
\end{tikzcd}$$

donde las flechas verticales son isomorfismos y la flecha horizontal inferior es la composición de los isomorfismos

$$f_*(\mathcal{M})_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} f_*(\mathcal{N})_{f(P)} \cong \mathcal{M}_P \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{N}_P \cong \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{N}_P.$$

(El último isomorfismo se debe a que $\mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ es un epimorfismo.)

Así pues, la flecha horizontal superior del diagrama es también un isomorfismo. Si $Q \in Y$ es un punto que no está en la imagen de X, entonces

$$((f_*\mathcal{M}) \otimes_{\mathcal{O}_Y} (f_*\mathcal{N}))_Q \cong f_*(\mathcal{M})_Q \otimes_{\mathcal{O}_{Y,Q}} f_*(\mathcal{N})_Q \cong 0 \cong f_*(\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{N})_Q,$$

luego todos los homomorfismos locales del homomorfismo definido en la discusión previa al teorema son isomorfismos, por lo que éste es también un isomorfismo. ■

Por otra parte, si U es un abierto en Y, la aplicación $\phi \mapsto f_*(\phi)$ define un homomorfismo

$$\mathrm{Hom}_{\mathcal{O}_{f^{-1}[U]}}(\mathcal{M}|_{f^{-1}[U]}, \mathcal{N}|_{f^{-1}[U]}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_U}(f_*(\mathcal{M})|_U, f_*(\mathcal{N})|_U),$$

y estos homomorfismos determinan a su vez un homomorfismo natural

$$f_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N}) \longrightarrow \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_*\mathcal{M}, f_*\mathcal{N}).$$

Teorema B.3 *Si $f :\longrightarrow Y$ es una inmersión cerrada de espacios anillados y $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_X$-módulos, entonces*

$$f_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{M},\mathcal{N}) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_*\mathcal{M}, f_*\mathcal{N}).$$

Hay que probar (en principio para un abierto U de Y, pero basta verlo para $U = Y$), que

$$f_* : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{M},\mathcal{N}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_Y}(f_*\mathcal{M}, f_*\mathcal{N}),$$

es un isomorfismo. Ello se debe a que los abiertos $f^{-1}[U]$, donde U recorre los abiertos de Y, forman una base de X, por lo que un homomorfismo $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ está determinado por su restricción a estos abiertos, y dicha restricción es esencialmente $f_*\phi$. Así mismo, cada homomorfismo $f_*\mathcal{M} \longrightarrow f_*\mathcal{N}$ determina un homomorfismo $\mathcal{M} \longrightarrow \mathcal{N}$ definido únicamente sobre los abiertos básicos $f^{-1}[U]$, y es claro que se extiende a un homomorfismo definido sobre todos los abiertos de X. ■

Vamos a estudiar ahora las imágenes inversas, cuya definición es más sofisticada, pero su comportamiento es mejor.

Si $f : X \longrightarrow Y$ es un homomorfismo de espacios anillados y $\mathcal{N}$ es un $\mathcal{O}_Y$-módulo, el haz $f^{-1}[\mathcal{N}]$ definido en 1.10 no posee una estructura natural de $\mathcal{O}_X$-módulo, pero sí de $f^{-1}[\mathcal{O}_Y]$-módulo.

Más detalladamente, cada $f^{-1}[\mathcal{N}]^-(U)$ es un $f^{-1}[\mathcal{O}_Y]^-(U)$-módulo con el producto $[(V,s)] \cdot [(V',n)] = [(V \cap V', s|_{V\cap V'} n|_{V\cap V'}]$ y de la construcción de la compleción de un prehaz se sigue fácilmente que cada $f^{-1}[\mathcal{N}](U)$ tiene una estructura natural de $f^{-1}[\mathcal{O}_Y](U)$-módulo.

Por otra parte, podemos definir homomorfismos $f^{-1}[\mathcal{O}_Y]^-(U) \longrightarrow \mathcal{O}_X(U)$ mediante $[(V,s)] \mapsto f_V^{\#}(s)|_U$, que determinan un homomorfismo de prehaces $f^{-1}[\mathcal{O}_Y]^- \longrightarrow \mathcal{O}_X$, el cual a su vez induce un homomorfismo de haces $f^{-1}[\mathcal{O}_Y] \longrightarrow \mathcal{O}_X$, caracterizado por que, para cada $P \in X$, el homomorfismo local $f^{-1}[\mathcal{O}_Y]_P \longrightarrow \mathcal{O}_{X,P}$ se corresponde con $f_P^{\#} : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ a través del isomorfismo natural $f^{-1}[\mathcal{O}_Y]_P \cong \mathcal{O}_{Y,f(P)}$.

Este homomorfismo convierte a $\mathcal{O}_X$ en un $f^{-1}[\mathcal{O}_Y]$-módulo. Volviendo al $\mathcal{O}_Y$-módulo $\mathcal{N}$, ahora podemos considerar el producto tensorial

$$f^*\mathcal{N} = f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X,$$

que es un $\mathcal{O}_X$-módulo al que llamaremos *imagen inversa* de $\mathcal{N}$ por f. Por ejemplo, es obvio que $f^*\mathcal{O}_Y = \mathcal{O}_X$.

Observemos que si $P \in X$ tenemos un isomorfismo natural

$$f^*(\mathcal{N})_P \cong \mathcal{N}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P}.$$

Es fácil ver que cada homomorfismo de $\mathcal{O}_Y$-módulos $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ induce de forma natural un homomorfismo de $\mathcal{O}_X$-módulos $f^*\phi : f^*(\mathcal{M}) \longrightarrow f^*(\mathcal{N})$ tal que para cada $P \in X$ el homomorfismo $(f^*\phi)_P$ se corresponde con $\phi_{f(P)} \otimes 1$. De este modo $f^* : \mathrm{Mod}(Y) \longrightarrow \mathrm{Mod}(X)$ resulta ser un funtor covariante. (Se define primero un homomorfismo $f^{-1}[\phi] : f^{-1}[\mathcal{M}] \longrightarrow f^{-1}[\mathcal{N}]$.)

Teorema B.4 *Si $f : X \longrightarrow Y$ es un homomorfismo de haces y $\mathcal{M}$, $\mathcal{N}$ son dos $\mathcal{O}_Y$-módulos, entonces existen isomorfismos naturales*

$$f^*(\mathcal{M} \oplus \mathcal{N}) \cong (f^*\mathcal{M}) \oplus (f^*\mathcal{N}), \quad f^*(\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}) \cong (f^*\mathcal{M}) \otimes_{\mathcal{O}_X} (f^*\mathcal{N}).$$

Demostración: Veamos el caso del producto tensorial, pues el de la suma directa es más sencillo. Si W es un abierto en X, entonces, según la definición de compleción de un prehaz, un elemento de $f^{-1}[\mathcal{M}](W)$ está determinado por un conjunto de pares (U, t_U), donde los abiertos $U \subset W$ forman un cubrimiento de W y $t_U \in f^{-1}[\mathcal{M}]^-(U)$, de modo que, si U_1 y U_2 son dos de estos abiertos, $t_{U_1,P} = t_{U_2,P}$ para todo $P \in U_1 \cap U_2$. A su vez, $t_U = [(V, s)]$, donde V es un abierto en Y tal que $f[U] \subset V$ y $s \in \mathcal{M}(V)$. Igualmente, cada elemento de $f^{-1}[\mathcal{N}](W)$ está determinado por pares $(U', t'_{U'})$, donde $t'_{U'} = [(V', s')]$.

En estas condiciones, los abiertos $U'' = U \cap U'$ forman un tercer cubrimiento de W tal que $f[U \cap U'] \subset V \cap V' = V''$ y podemos considerar el producto tensorial

$$s'' = s|_{V''} \otimes s'|_{V''} \in \mathcal{M}(V'') \otimes_{\mathcal{O}_Y(V'')} \mathcal{N}(V'') = (\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N})^-(V'').$$

Así $t''_{V''} = [V'', \hat{s}''] \in f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}]^-(U'')$, donde el circunflejo denota el homomorfismo $(\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N})^- \longrightarrow \mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}$.

Una comprobación rutinaria muestra que los pares $(U'', t''_{V''})$ determinan un elemento de $f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}]^-(W)$ que no depende de los conjuntos de pares elegidos como representantes de los elementos de partida. Desde éste pasamos a su vez a un elemento de la compleción $f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}](W)$. Más aún, esta asignación induce un homomorfismo de $f^{-1}[\mathcal{O}_Y]$-módulos

$$f^{-1}[\mathcal{M}](W) \otimes_{f^{-1}[\mathcal{O}_Y](W)} f^{-1}[\mathcal{N}](W) \longrightarrow f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}](W).$$

Se comprueba así mismo que estos homomorfismos inducen un homomorfismo

$$(f^{-1}[\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} f^{-1}[\mathcal{N}])^- \longrightarrow f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}],$$

que a su vez se extiende a un homomorfismo

$$f^{-1}[\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} f^{-1}[\mathcal{N}] \longrightarrow f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}].$$

Además, para cada $P \in X$, el homomorfismo local asociado a P se corresponde a través de los isomorfismos canónicos con el isomorfismo

$$f^{-1}[\mathcal{M}]_P \otimes_{f^{-1}[\mathcal{O}_Y]_P} f^{-1}[\mathcal{N}]_P \longrightarrow \mathcal{M}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{N}_{f(P)}$$

inducido por los isomorfismos naturales $f^{-1}[\mathcal{M}]_P \cong \mathcal{M}_{f(P)}$, $f^{-1}[\mathcal{N}]_P \cong \mathcal{N}_{f(P)}$, $f^{-1}[\mathcal{O}_Y]_P \cong \mathcal{O}_{Y,f(P)}$. Esto prueba que el homomorfismo que hemos construido es un isomorfismo. Al multiplicar por $\otimes_{f^{-1}[\mathcal{O}_Y]}\mathcal{O}_X$ obtenemos un isomorfismo

$$f^{-1}[\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X \longrightarrow f^{-1}[\mathcal{M} \otimes_{\mathcal{O}_Y} \mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X.$$

Es fácil ver que el módulo de la izquierda es isomorfo de forma natural a

$$(f^{-1}[\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X) \otimes_{\mathcal{O}_X} (f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X),$$

lo que nos da el segundo isomorfismo del enunciado. ■

Veamos ahora las relaciones entre las imágenes directas e inversas. Consideremos un homomorfismo de espacios anillados $f : X \longrightarrow Y$ y sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo. Podemos definir un homomorfismo canónico $f^*f_*\mathcal{M} \longrightarrow \mathcal{M}$. En efecto, si U es un abierto en X, definimos

$$\phi_U^- : f^{-1}[f_*\mathcal{M}]^-(U) \longrightarrow \mathcal{M}(U)$$

mediante $\phi_U([V, s]) = s|_U$. Estos homomorfismos definen un homomorfismo de prehaces $\phi^- : f^{-1}[f_*\mathcal{M}]^- \longrightarrow \mathcal{M}$, que a su vez se extiende a un homomorfismo de haces $\phi : f^{-1}[f_*\mathcal{M}] \longrightarrow \mathcal{M}$, que a su vez define un homomorfismo

$$\bar{\phi}^- : (f^{-1}[f_*\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X)^- \longrightarrow \mathcal{M}$$

mediante $\bar{\phi}_U^-(s \otimes t) = \phi_U(s)t$, que a su vez define un homomorfismo

$$\bar{\phi} : f^*f_*\mathcal{M} = f^{-1}[f_*\mathcal{M}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X \longrightarrow \mathcal{M}.$$

Si $P \in X$, el homomorfismo $\bar{\phi}_P$ resulta ser la composición

$$(f^*f_*\mathcal{M})_P \cong (f_*\mathcal{M})_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P} \longrightarrow \mathcal{M}_P \otimes_{\mathcal{O}_{X,P}} \mathcal{O}_{X,P} \cong \mathcal{M}_P.$$

En particular, si f es una inmersión, el homomorfismo $(f_*\mathcal{M})_{f(P)} \longrightarrow \mathcal{M}_P$ es un isomorfismo, por lo que $\bar{\phi}_P$ también lo es. Así pues, hemos probado el teorema siguiente:

Teorema B.5 *Sea $f : X \longrightarrow Y$ una inmersión entre espacios anillados y sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo. Entonces $f^*f_*\mathcal{M} \cong \mathcal{M}$.*

Consideremos ahora un $\mathcal{O}_Y$-módulo $\mathcal{N}$ y vamos a definir un homomorfismo natural

$$\psi : \mathcal{N} \longrightarrow f_*f^*\mathcal{N}.$$

Para ello tomamos un abierto $U \subset Y$ y definimos el homomorfismo

$$\bar{\psi}_U : \mathcal{N}(U) \longrightarrow f^{-1}[\mathcal{N}](f^{-1}[U])$$

mediante $\bar{\psi}_U(n) = \widetilde{[U, n]}$, donde el circunflejo denota el homomorfismo

$$f^{-1}[\mathcal{N}]^- \longrightarrow f^{-1}[\mathcal{N}].$$

A su vez, $\bar{\psi}_U$ define un homomorfismo

$$(\bar{\psi} \otimes 1)_U : \mathcal{N}(U) \longrightarrow (f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X)^-(f^{-1}[U]) \longrightarrow (f^*\mathcal{N})(f^{-1}[U])$$

(donde el segundo homomorfismo es la compleción del producto tensorial), y estos homomorfismos definen el homomorfismo buscado $\psi : \mathcal{N} \longrightarrow f_*f^*\mathcal{N}$.

Observemos que si f es una inmersión cerrada y $P \in X$, entonces

$$f_*(f^*(\mathcal{N}))_{f(P)} \cong f^*(\mathcal{N})_P \cong \mathcal{N}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P}.$$

Es fácil ver que la localización de ψ a cada punto $f(P)$ se corresponde con el homomorfismo natural

$$\psi_{f(P)} : \mathcal{N}_{f(P)} \longrightarrow \mathcal{N}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P}.$$

Por otra parte, si $Q \in Y \setminus f[X]$, entonces $f_*(f^*(\mathcal{N}))_Q = 0$, por lo que $\psi_Q = 0$.

Estos hechos muestran que en general ψ no es inyectivo ni suprayectivo, pero se cumple lo siguiente:

Teorema B.6 *Sea $f : X \longrightarrow Y$ una inmersión cerrada de espacios anillados y sea $\mathcal{I} = \mathrm{N}(f^\#)$, que es un haz de ideales de $\mathcal{O}_Y$. Sea $\mathcal{N}$ un $\mathcal{O}_Y$-módulo.*

a) Si $\mathcal{N}_Q = 0$ para todo punto $Q \in Y \setminus f[X]$, entonces el homomorfismo natural $f_*(f^*(\mathcal{N})) \longrightarrow \mathcal{N}$ es suprayectivo.

b) Si además $\mathcal{I}\mathcal{N} = 0$, entonces[1] *$f_*(f^*(\mathcal{N})) \cong \mathcal{N}$.*

Demostración: Puesto que el homomorfismo $\mathcal{O}_{X,P} \longrightarrow \mathcal{O}_{Y,f(P)}$ es suprayectivo, es obvio que $\psi_{f(P)}$ es suprayectivo, y si $Q \in Y \setminus f[P]$, la hipótesis de a) hace que $\psi_Q = 0$ también lo sea. Por lo tanto ψ es suprayectivo.

Bajo la hipótesis de b) podemos construir un homomorfismo natural

$$\mathcal{N}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P} \longrightarrow \mathcal{N}_{f(P)},$$

pues $\mathcal{O}_{X,P} = \mathcal{O}_{Y,f(P)}/\mathcal{I}_{f(P)}$ y tenemos que $\mathcal{I}_{f(P)}\mathcal{N}_{f(P)} = 0$, luego $\mathcal{N}_{f(P)}$ tiene una estructura natural de $\mathcal{O}_{X,P}$-módulo. Este homomorfismo es el inverso de $\psi_{f(P)}$, luego $\psi_{f(P)}$ es un isomorfismo. Para puntos $Q \in Y \setminus f[P]$ tenemos que $\psi_Q = 0$ es un también isomorfismo. ■

Podemos pensar en este teorema como una condición suficiente para que un $\mathcal{O}_Y$-módulo $\mathcal{N}$ esté inducido por un $\mathcal{O}_X$-módulo, concretamente, por $f^*\mathcal{N}$.

Veamos ahora la relación fundamental entre los funtores f^* y f_*:

Teorema B.7 *Sea $f : X \longrightarrow Y$ un homomorfismo de espacios anillados, sea $\mathcal{M}$ un $\mathcal{O}_X$-módulo y $\mathcal{N}$ un $\mathcal{O}_Y$-módulo. Entonces existe un isomorfismo natural (de grupos)*

$$\mathrm{Hom}_{\mathcal{O}_X}(f^*\mathcal{N}, \mathcal{M}) \cong \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{N}, f_*\mathcal{M}).$$

Demostración: De la propia definición de compleción se sigue que

$$\mathrm{Hom}_{\mathcal{O}_X}(f^*\mathcal{N}, \mathcal{M}) \cong \mathrm{Hom}_{\mathcal{O}_X}((f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X)^-, \mathcal{M}).$$

Un homomorfismo $\phi : (f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X)^- \longrightarrow \mathcal{M}$ está determinado por una familia de homomorfismos de $\mathcal{O}_X(U)$-módulos

$$\phi_U : f^{-1}[\mathcal{N}](U) \otimes_{f^{-1}[\mathcal{O}_Y](U)} \mathcal{O}_X(U) \longrightarrow \mathcal{M}(U)$$

[1]El haz $\mathcal{I}\mathcal{N}$ se define como la compleción del prehaz dado por $(\mathcal{I}\mathcal{N})^-(U) = \mathcal{I}(U)\mathcal{N}(U)$. Es inmediato que $(\mathcal{I}\mathcal{N})_Q = \mathcal{I}_Q\mathcal{N}_Q$ para todo $Q \in Y$.

compatibles con las restricciones. Componiendo con el homomorfismo

$$f^{-1}[\mathcal{N}](U) \longrightarrow f^{-1}[\mathcal{N}](U) \otimes_{f^{-1}[\mathcal{O}_Y](U)} \mathcal{O}_X(U)$$

dado por $s \mapsto s \otimes 1$, obtenemos un homomorfismo de $f^{-1}[\mathcal{O}_Y](U)$-módulos

$$\phi'_U : f^{-1}[\mathcal{N}](U) \longrightarrow \mathcal{M}(U).$$

Estos homomorfismos también son compatibles con las restricciones, luego determinan un homomorfismo de haces $\phi' : f^{-1}[\mathcal{N}] \longrightarrow \mathcal{M}$. La asignación $\phi \mapsto \phi'$ define un homomorfismo

$$\mathrm{Hom}_{\mathcal{O}_X}((f^{-1}[\mathcal{N}] \otimes_{f^{-1}[\mathcal{O}_Y]} \mathcal{O}_X)^-, \mathcal{M}) \longrightarrow \mathrm{Hom}_{f^{-1}[\mathcal{O}_Y]}(f^{-1}[\mathcal{N}], \mathcal{M}),$$

y es inmediato comprobar que se trata de un isomorfismo de grupos. Teniendo en cuenta la construcción de la compleción de un prehaz, es fácil ver que

$$\mathrm{Hom}_{f^{-1}[\mathcal{O}_Y]}(f^{-1}[\mathcal{N}], \mathcal{M}) \cong \mathrm{Hom}_{f^{-1}[\mathcal{O}_Y]^-}(f^{-1}[\mathcal{N}]^-, \mathcal{M}).$$

Para completar la prueba basta ver que

$$\mathrm{Hom}_{f^{-1}[\mathcal{O}_Y]^-}(f^{-1}[\mathcal{N}], \mathcal{M}) \cong \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{N}, f_*\mathcal{M}).$$

Un homomorfismo $\phi : f^{-1}[\mathcal{N}]^- \longrightarrow \mathcal{M}$ está determinado por una familia de homomorfismos $\phi_U : f^{-1}[\mathcal{N}]^-(U) \longrightarrow \mathcal{M}(U)$ de $f^{-1}[\mathcal{O}_Y]^-(U)$-módulos compatibles con las restricciones. Para cada abierto V tal que $f[U] \subset V \subset Y$, tenemos que ϕ_U define homomorfismos $\psi_{V,U} : \mathcal{N}(V) \longrightarrow \mathcal{M}(U)$ de $\mathcal{O}_Y(U)$-módulos mediante la composición con el homomorfismo natural $\mathcal{N}(V) \longrightarrow f^{-1}[\mathcal{N}]^-(U)$ dado por $s \mapsto [(V, s)]$. Llamando $\psi_V = \psi_{V,f^{-1}[V]} : \mathcal{N}(V) \longrightarrow \mathcal{M}(f^{-1}[V])$, tenemos que $\psi_{V,U} = \psi_V \circ \rho_V^{f^{-1}[V]}$, así como que los homomorsimos ψ_V son compatibles con las restricciones, por lo que determinan un homomorfismo $\psi : \mathcal{N} \longrightarrow f_*\mathcal{M}$.

La asignación $\phi \mapsto \psi$ es un homomorfismo

$$\mathrm{Hom}_{f^{-1}[\mathcal{O}_Y]^-}(f^*\mathcal{N}^-, \mathcal{M}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{N}, f_*\mathcal{M}).$$

Es inmediato que ψ determina a ϕ (es decir, que el homomorfismo es inyectivo) y que todo ψ determina un ϕ (por lo que el homomorfismo es suprayectivo).

■

Nota El isomorfismo dado por el teorema anterior es natural en el sentido de que es un isomorfismo de funtores, tanto si consideramos ambos miembros como funtores covariantes en $\mathcal{M}$ como si los consideramos como funtores contravariantes en $\mathcal{N}$. Esta relación entre los funtores f^* y f_* es la misma que el teorema 2.13 demuestra para los funtores $\otimes_{\mathcal{O}_X}\mathcal{N}$ y $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{N}, -)$, y se expresa diciendo que son dos pares de *funtores adjuntos.* Más concretamente, f^* es *adjunto por la izquierda* a f_* y f_* es *adjunto por la derecha* a f^*. Hay una serie de resultados de interés sobre funtores adjuntos en los que no vamos a entrar aquí.

Por ejemplo, puede probarse que un funtor determina a su adjunto —cuando existe— salvo isomorfismo, y que los funtores adjuntos por la izquierda (resp. por la derecha) son exactos por la derecha (resp. por la izquierda). ■

La exactitud de f_* y f^* es fácil de probar directamente: si $f : X \longrightarrow Y$ es un homomorfismo de espacios anillados y

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0$$

es una sucesión exacta de $\mathcal{O}_Y$-módulos, entonces, para cada $P \in X$, la sucesión

$$(f^*\mathcal{M})_P \longrightarrow (f^*\mathcal{N})_P \longrightarrow (f^*\mathcal{P})_P \longrightarrow 0$$

es isomorfa a

$$\mathcal{M}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P} \longrightarrow \mathcal{N}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P} \longrightarrow \mathcal{P}_{f(P)} \otimes_{\mathcal{O}_{Y,f(P)}} \mathcal{O}_{X,P} \longrightarrow 0,$$

que es exacta por la exactitud derecha del producto tensorial, lo que prueba la exactitud de

$$f^*\mathcal{M} \longrightarrow f^*\mathcal{N} \longrightarrow f^*\mathcal{P} \longrightarrow 0.$$

Por otra parte, si ahora

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{N} \longrightarrow \mathcal{P} \longrightarrow 0$$

es una sucesión exacta de $\mathcal{O}_X$-módulos, para cada abierto $U \subset Y$, la sucesión

$$0 \longrightarrow \mathcal{M}(f^{-1}[U]) \longrightarrow \mathcal{N}(f^{-1}[U]) \longrightarrow \mathcal{P}(f^{-1}[U])$$

es exacta, de donde se sigue fácilmente la exactitud de las sucesiones

$$0 \longrightarrow (f_*\mathcal{M})_P \longrightarrow (f_*\mathcal{N})_P \longrightarrow (f_*\mathcal{P})_P,$$

para todo $P \in Y$, luego también la de

$$0 \longrightarrow f_*\mathcal{M} \longrightarrow f_*\mathcal{N} \longrightarrow f_*\mathcal{P}.$$

Observemos que, en el caso en que f es una inmersión cerrada y $P = f(Q)$, la sucesión

$$0 \longrightarrow (f_*\mathcal{M})_P \longrightarrow (f_*\mathcal{N})_P \longrightarrow (f_*\mathcal{P})_P \longrightarrow 0$$

se corresponde, salvo isomorfismo, con

$$0 \longrightarrow \mathcal{M}_Q \longrightarrow \mathcal{N}_Q \longrightarrow \mathcal{P}_Q \longrightarrow 0,$$

que es exacta, mientras que si $P \notin f[X]$, entonces es la sucesión nula (luego también es exacta). Esto prueba que si f es una inmersión cerrada entonces el funtor f_* es exacto.

Bibliografía

[1] Atiyah, M.F, Macdonald, I.G. *Introduction to Commutative Algebra.* Addison-Wesley, Massachussetts, 1969.

[2] Hartshorne, R. *Algebraic Geometry.* Springer, New York, 1977.

[3] Hilton, P. J., Stammbach, U. *A Course in Homological Algebra.* Springer, New York, 1971.

[4] Kaplansky, I *Commutative Rings.* Polygonal publishing house, Washington, 1974

[5] Kunz, E. *Introducction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston, 1991.

[6] Liu, Q. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, 2002.

[7] Matsumura, H. *Commutative Algebra.* Benjamin, New York, 1970.

[8] Miyanishi, M. *Algebraic Geometry.* American Mathematical Society, 1994.

[9] Rotman, J.J. *Notes on Homological Algebra.* Van Nostrand, New York, 1970.

[10] Shafarevich, I. R. *Basic Algebraic Geometry 1–2.* Springer, New York, 1994.

[11] Warner, F.K. *Foundations of Differentiable Manifolds and Lie Groups,* Scott, Foresman and Co., Londres 1971.

Índice de Materias